

**A
Project Report On**

“Design and development of smart contract system for blockchain based applications”

In fulfillment for the award of the degree of

MASTER OF TECHNOLOGY

Submitted To



RAJIV GANDHI PROUDYOGIKI VISHWA VIDYALAYA

Submitted By

Shivang Kumar Kushwaha

M.TECH. IV Semester

BATCH : 2021-24



**GYAN GANGA INSTITUTE OF TECHNOLOGY & SCIENCES,
JABALPUR (M.P.)**

GYAN GANGA COLLEGE OF TECHNOLOGY, JABALPUR (M.P.)



FORWARD

I hereby forward the project entitled **“DESIGN AND DEVELOPMENT OF SMART CONTRACT SYSTEM FOR BLOCKCHAIN BASED APPLICATIONS”** Submitted by **Shivang Kushwaha** student of M.TECH. IV Semester, in fulfillment of the requirement forward of degree of Master of Technology of **RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA**.

GYAN GANGA COLLEGE OF TECHNOLOGY, JABALPUR (M.P.)



DECLARATION

I hereby declare that the project entitled “**DESIGN AND DEVELOPMENT OF SMART CONTRACT SYSTEM FOR BLOCKCHAIN BASED APPLICATIONS**” Which is being submitted in partial fulfillment of the requirement for the award of the degree of M.TECH RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, is an authentic record and all the information furnished by me are true to my knowledge and information and facts furnished by me are based on my own findings and as per the information collected through primary / secondary research.

The matter reported in this project is neither being used elsewhere nor has been submitted earlier for the award of degree of Master of Technology.

Submitted By
Shivang Kushwaha
M.TECH. IV Semester

Abstract

The work presented in this paper describes the design and implementation of smart contracts for blockchain applications. The main purpose is to explore the current state and application of blockchain technology and show how the main points of this technology can change the "business as usual". This project examines blockchain technology as a whole and explores its potential for developing business applications. Blockchain-based smart contract is suitable for different applications and demonstrates the creation and implementation of simple management using the Ethereum blockchain. Ethereum advances second-generation blockchain technology by providing a global open computing/environmental platform that enables the exchange of cryptocurrency (Ether) and the intelligent creation of self-generated contracts

Smart contracts provide a framework for ownership of digital assets and various equity applications in the blockchain space. Because Ethereum and smart contracts are open, distributed, and immutable, they are vulnerable to vulnerabilities caused by simple mistakes from developers.

We design and implement smart contracts for blockchain medical management applications to support the medical ecosystem and power to increase energy efficiency by creating smart contracts for energy saving certification. We also identify key concepts, advances, and outcomes in clinical and radiological research.

In this article, blockchain technology is used in areas such as health and energy. Health applications are the main focus of this research and electrical power studies show further involvement of this research. It is hoped that the work presented in this article can provide sufficient motivation for the development of ethical applications (Apps) using blockchain-based smart contracts.

Acknowledgements

We would like to thank our professors and supervisors, in particular Ms. Yasha Dubey, for their supervision and support during this thesis. Secondly, we want to thank our interview partners who provided us with their expertise and made this research possible.

Finally, we would like to thank especially our families and friends for their manifold support during the time of the thesis and the Master's program.

Acronyms & Abbreviations

DAPP	Decentralized Application
DFS	Distributed File System
POW	Proof-Of-Work
POS	Proof-Of-Stake
DPOS	Delegated Proof-of-Stake
PBFT	Practical Byzantine Fault Tolerance
EVM	Ethereum Virtual Machine
TX	Transaction
EHRS	Electronic Healthcare Records
NTPF	National Treatment Purchase Fund
HSE	Health Service Executive
OP	Outpatient
IP	Inpatient
IPDC	Inpatient Day Cases
DNS	Domain Name System
ID	Identifier
API	Application Programming Interface
ICTs	Information and Communication Technologies
IOTs	Internet of Things
EV	Electric Vehicle
ESCOs	Energy Service Companies
P2P	Peer to Peer
EPC	Energy Performance Contracting
ACEEE	American Council for Energy Efficient Economy
GoO	Guarantee of Origin
MWh	Mega-Watt hour
EEOS	Energy Efficiency Obligation Schemes
WCS	White Certificate Scheme
DSOs	Distribution System Operators

M&V	Measurement & Verification
NA	National Authority
GWh	Gigawatt hours
JS	Java Script
GETH	Go-Ethereum
SUT	System Under Test
RAM	Random Access Memory
IP	Internet Protocol
ETH-NETSTATS	Ethereum Network Status
EMMC	Embedded Multimedia Card
LPDDR	Low-Power Double Data Rate
SDRAM	Synchronous Dynamic Random Access Memory
mA	Milliampere
mV	Millivolts
SoC	System-on-Chip
VM	Virtual Machine
ECC	Elliptic-curve cryptography
RPC	Remote Procedure Calls
NIST	National Institute of Standards and Technology
ABI	Application Binary Interface
LLL	Low Level Language
IPFS	InterPlanetary File System
ENS	Ethereum Name Service
OOP	Object-oriented Programming
BTC	Bitcoin
ICOs	Initial Coin Offering
ETH	Ether
IoMT	Internet of Medical Things
XRP	Ripple
BCH	Bitcoin Cash
LTC	Litecoin
XLM	Stellar

Table of contents

Abstract	i
Acknowledgements	ii
Acronyms and Abbreviations.....	iii
Table of contents.....	v
List of tables.....	vi
1 Introduction	1
1.1 Research objectives.	4
1.2 Thesis motivation and contributions.....	5
1.3 Thesis organization.....	6
2 Background.....	8
2.1 Blockchain and cryptocurrencies.....	8
2.2 First generation of a blockchain technology: The Bitcoin.....	10
2.3 Consensus algorithm and hashing	10
2.4 Blockchain characteristics and technology types	13
2.5 Blockchain based smart contracts	14
2.6 Ethereum blockchain	16
2.7 Public key cryptography	17
2.8 Ethereum virtual machine	19
2.9 Ethereum based smart contracts.	19
2.10 Solidity	22
2.11 Smart contracts programming on Ethereum platform	24
2.12 Metamask.....	24
2.13 Etherscan.....	25
2.14 Blockchain based smart contract applications	26
2.15 Conclusion.	26
3 Literature review: Blockchain healthcare applications.....	28
3.1 Traditional healthcare system vs Blockchain based healthcare infrastructure ..	28

3.2	Existing blockchain based healthcare solutions and applications	30
3.3	Discussion and motivation for a blockchain powered healthcare infrastructure	36
3.4	Blockchain based applications for energy Efficiency	37
3.5	Conclusion.	39
4	Blockchain framework for healthcare management applications.....	40
4.1	System design and implementation framework Ethereum.....	41
4.2	Medical Blockchain smart contracts.....	43
4.3	System design and development	46
4.3.1	The process flow of a smart contract for medical prescriptions.....	48
4.3.2	Laboratory test results... ..	49
4.3.3	Communication between patients and service Providers	50
4.3.4	Healthcare reimbursement.....	52
4.3.5	Ethereum Blockchain smart contracts for clinical trials	53
4.3.6	Surgical procedure via smart contracts	55
4.4	Cost estimation.....	57
4.5	Validation of workflows HSE datasets.....	58
4.5.1	HSE Dataset.....	58
4.5.2	Cost estimation using real datasets.....	60
4.6	Discussion.	69
4.7	Conclusion.	70
5	Implementation of Ethereum Smart Contracts	71
5.1	Medical smart contracts.....	71
5.2	Clinical trials	74
5.3	Lab test results	76
5.4	Patient consultant communication.....	77
5.5	Health Insurance.....	79
5.6	Surgery	81
5.7	Conclusion.	84
6	Blockchain Smart Contract System for Energy Efficiency Applications.....	85
6.1	Smart Contract implementation for Energy Saving Certificates.....	87
6.2	Blockchain applications in the previous energy efficiency schemes	92

6.2.1	The Case Study 1: The Italian White Certificate Scheme	93
6.2.2	The Case Study 2: The UK Energy Company Obligation Scheme.....	96
6.3	Benefits of utilizing blockchain technology in the energy efficiency market...	97
6.3.1	Encryption of the energy savings.....	97
6.3.2	Exchange of the energy savings.....	98
6.3.3	Valuation of energy savings	98
6.3.4	Increasing transparency.....	98
6.3.5	Lowering the transaction cost.....	99
6.3.6	Increasing reliability	99
6.3.7	Increasing customer trust and security	99
6.3.8	Increasing the market success.....	99
6.4	Conclusions.....	100
7	Conclusions and future directions.....	102
7.1	Smart contracts for Healthcare Management to facilitate Medical Eco-system	102
7.2	Blockchain based smart contract system for energy efficiency	104
7.3	Reflection and Impact Assesment.....	105
7.4	Future Work.....	105
	References.....	107

1 Introduction

Over the past few years, interest in Bitcoin and distributed ledger technology has increased. Bitcoin is actually a cryptocurrency based on blockchain technology. Cryptocurrencies are the most common and widely used application of blockchain technology, although different uses have been proposed recently. In this article, we will examine modern blockchain-based applications, focusing on metadata, smart contracts and different rules. To explain how the blockchain technology proposed in this article works and its applications, it is important to understand the basic concepts of distributed information.

Blockchain is the technology behind the virtual cryptocurrency Bitcoin. Blockchain is a distributed ledger of all permissions, executions and transmissions of participants. Network participants generally verify all transactions. This contains information about all transactions occurring on the network. Blockchain is an immutable collection of records, called blocks, that are linked and secured using cryptographic hashes.

Digital virtual currency maintains a record containing the exact name of the currency exchange [1]. In this way, when the customer chooses to pay, a transaction containing the necessary information such as the amount sent and the recipient is created and shared. Finally, the transaction is put into a new block to be added to the blockchain. Blockchain was first proposed by a man named Satoshi Nakamoto in 2008. He published a white paper about "Bitcoin: Peer-to-Peer Electronic Cash System"[2]. Blockchain technology records digital accounts distributed over the internet, making them resistant to destruction. Land resources, cars, etc. All digital assets can be recorded as a blockchain transaction.

In the simplest terms, blockchain can be defined as a data system that stores records of transactions while maintaining security, privacy and distribution principles. It can be thought of as information stored in a block structure that is not controlled by a central authority. It is a list of products that are safe and publicly available on the web.

When information is stored in a decentralized ledger, it is difficult to manipulate or replace it. It is a digital ledger containing all real-time checks on the network. It helps digital wallets measure their balances, ensuring that they belong entirely to the partner when verifying transaction data. Cryptographic technology enhances the authenticity and history of blockchain. Crypto wallets contain a secret piece of information called a cryptographic key or pattern, which is used to sign transactions and provides evidence that it comes from the original owner of the account. This cryptographic signature also prevents anyone from altering the digital transaction once it is published. All transactions are distributed throughout the system, and verification through a process called mining usually begins immediately upon receipt. The mining process can be described as a consensus process used to identify significant changes in the blockchain network. It encodes decisions on the blockchain, preserving net neutrality and allowing multiple processors to determine the network structure. To receive confirmation, transactions must be packaged in a block that follows a very complex cryptographic rule that the system can verify. These rules prohibit changing layers because doing so would rot all previous blocks in the chain. The mining process also creates a competitive lottery that prevents anyone from adding new blocks to the network. Therefore, no one can control the content on the blockchain network or modify various parts of the blockchain to recover their own expenses.

The table below provides a brief introduction to blockchain technology, the Ethereum blockchain, and smart contracts to help understand this section and the rest of the article. Blockchain can be used for many applications, including Internet communications, utilities, supply chain management, Internet of Things (IoT), finance and business.

Blockchain technology and cryptocurrency have attracted the attention of the business world and academia. We can define it as a fully public and peer-to-peer digital platform that uses cryptography to hold applications, transfer digital currency and digital assets, and store information security. Bitcoin is one of the most popular and widely used decentralized cryptocurrencies. Moreover, the Ethereum platform has also attracted a lot of attention for its smart contracts and the execution of smart contracts (that is, services that work very well with its services and support). These applications can be completely new ideas or adaptations of existing concepts. It effectively eliminates intermediaries and all costs associated with the collaboration of third-party services.

manner, with its native help and support. Such apps can be either completely new ideas or distributed reworks of existing concepts. It effectively cut off the intermediaries and all the associated costs with third - party service participation.

Ethereum has taken digital technology behind Bitcoin and expanded its operations. It is a complete network with its own web browser, programming language and trading platform. Most importantly, it helps users build equity applications on the Ethereum blockchain. For example, the only benefit of people "sharing" and "liking" the content of their favorite celebrities on the social media platform Facebook is created by advertisements placed on their profiles, and the advertisement is sent directly to Facebook. Both artists and audiences will benefit from collaboration and communication in the Ethereum version of such a social network. Ethereum has a better infrastructure and usage than Bitcoin. Ethereum is a complete advantage over Bitcoin alternatives as it seems to have more uses than Bitcoin and therefore serves many purposes. Since blockchain technology is still in its infancy, Ethereum and Bitcoin are constantly being updated. However, Ethereum is now the clear winner due to its unique features, as the Ethereum blockchain uses smart contracts that add an additional layer of permission control and security to the platform. It is a more established platform than Bitcoin. Conducting business on the Ethereum platform is cheaper than other blockchain platforms. Additionally, Ethereum's trading process is very fast.

According to the current cryptocurrency market, the second most popular and widely used blockchain platform as of November 2017 is Ethereum, which is also the focus of this research article. According to Ethereum founder Vitalik Buterin, Ethereum is a blockchain platform that can understand the world's texts. and acts as a peer-to-peer decentralized cryptocurrency (Ether) trading network[3]. The idea of a Turing-complete blockchain was first implemented by Ethereum. A device or computer language that can use sufficient resources to compute the computation is said to be Turing complete. The Turing-complete development environment of blockchain-based platforms provides incentives for the deployment of various business applications in various domains.

These decision-making applications, called smart contracts on the Ethereum platform and other blockchain networks, drive Turing's success.

As we said before, this is the main point that distinguishes Ethereum not only from Bitcoin but also from other blockchain-based platforms, because it has its own features and it is here for the first time. However, Nick Szabo first introduced the concept of smart contracts in 1997, where he described a humble vending machine using a real-life bible/ancient example [27]. Smart contract can be defined as one of the execution rules of EVM. This is essentially a "computer" where everyone provides computing power together. All network nodes that provide electricity pay for these services in Ether. These are called smart contracts because they are executed when a goal is achieved. For example, consider using the Ethereum blockchain platform to build a resource equity application. Some people will create smart contracts that collect cash for Ethereum and give it to others. The smart contract will be coded to indicate that when the required amount is collected, the entire amount will be transferred to the recipient, or if the requirement is not reached within one month, the entire money will be returned to the beneficiary. expert. This will use Ethereum instead of USD. All of this will be done according to the rules of the smart contract contained in the programming code, which will complete the transaction without the need for a trusted party to hold the money and sign the contract. Smart contracts can be used to create many business applications. Coders can create smart contracts that provide functionality to other smart contracts, similar to using different software. These smart contracts will be used to store information on the Ethereum blockchain for applications. It needs to send a sufficient amount of ether as a transaction fee to complete the smart contract. This will effectively cover the cost of collaboration between Ethereum nodes and distributed computing devices. Ethereum is considered a new and highly experimental platform, not only because of its emergence (July 2015) but also because of its ability to use Turing-complete algorithms written on peer-to-peer platforms such as blockchain. Build decentralized applications.

1.1 Research objectives

This research project investigates the feasibility of blockchain-based smart contracts. The main goal of this research project is to design and develop smart contracts for blockchain-based decentralized applications. The main objectives of this paper can be summarized as follows:

- Adopting the blockchain technology for enhancing the security and auditability of EHRs in current Healthcare systems
- Designing of healthcare smart contracts to facilitate different stakeholders involved in the system and how much computational resources do they consume
- Deployment of a blockchain-supported medical healthcare system which comply with the regulations and estimating the economic costs related to implementation of blockchain based smart contracts
- Trading mechanisms for energy-saving certificates designed to achieve energy efficiency as blockchain applications, and analysing the computing resources they are consuming
- Blockchain-supported local energy market which comply with legislation and can help the local governments to achieve energy efficiency, and analysing the economic cost associated with the real-world implementation
- Building a chain code implementations for the blockchain based smart contracts
- Implementation of the proposed reward system
- Implementing the business logic and processes needed for the blockchain network to remain operational
- Creating a self-contained distributed applications

These research goals were achieved through the creation and development of blockchain-based smart contracts for the implementation of distributed systems. These were transferred to the blockchain testnet. Simulate from the standard model and tolerance of the control system and product design. The calculation results are then analyzed to show the significance of the performance. Moreover, these research studies form the basis for the research work of this article.

1.2 Thesis Motivation and Contributions

This article focuses on how blockchain technology can be used to improve the security and auditability of these systems in health management, based on existing smart systems in the field of drinking water and electricity.

This article will enable the implementation of blockchain-based smart contracts using the Ethereum blockchain platform described in the research objective section. The delivery process will include smart contracts in healthcare to improve the security and reliability of the existing healthcare system and replace the energy saving certificate to achieve energy efficiency through the implementation of new management policies. Smart contracts act as a representation of intelligence that connects all stakeholders in the system. It encodes metadata to allow only authorized users to access secure information, thus providing access to information across the entire network. Metadata contains information about the ownership, authorization, and integrity of the requested data. The smart contract-based framework demonstrates how decentralized management and the blockchain design concept can create a secure, interconnected system. These smart contracts are used to support authentication and access rights, as well as content management networks of multiple storage and service providers, while providing information documentation, analysis, and information sharing to all stakeholders. Operating costs are integrated into the system using smart contracts.

1.3 Thesis organisation

The chapters of this thesis are as follows in chronological order:

Summary - Summary of the most important points discussed and presented in the thesis

1 Introduction - Chapter 1 introduction Be clear about the research objectives and the background that will be covered in the thesis will be examined throughout. To achieve the desired results. Outlines the purpose, motivation, resources and details of future collaboration.

2 History - Explain the theory and history of blockchain technology. Different systems of cryptocurrencies are explained. An introduction to the Ethereum blockchain is available here, explaining the use of smart contracts and the definition of participants, including Metamask extensions and Etherscan content.

3 Literature Review - Chapter 3 provides detailed information about blockchain-based decentralized applications in healthcare and electronics. He also shares that the theory also applies to blockchain and electronic medical records. This includes a description of traditional healthcare systems and blockchain-driven healthcare ecosystems. Blockchain-based decentralized applications in healthcare and energy use are discussed here.

4 Smart Contracts for Healthcare Management - Describe the process and details of the implementation process for the design and development of the healthcare management system used in distribution equipment.

Section 4 explains the process and application of medical blockchain. This includes a description of the components that make up Ethereum blockchain-based healthcare smart contracts and the different healthcare systems presented in this section.

5 Ethereum Smart Contract Implementation – Chapter 5 details the structure and functionality of an Ethereum smart contract with a flowchart.

6 Blockchain Smart Contract System for Electricity - In this section, we present the blockchain-based smart electricity service solution, the results obtained, and explain how to properly set up and use the network.

7 Conclusion - Discussion of the findings and conclusions drawn from the results obtained.

2 Background

In this section, cryptographic algorithms, hashing algorithms, and consensus algorithms are briefly introduced and discussed. This section provides a detailed description of the first blockchain Bitcoin and other cryptocurrencies. Contains a detailed overview of blockchain technology, Ethereum, and smart contracts, and some examples of smart contract writing. The difference between the product and the model included in the contract is clearly explained.

2.1 Blockchain and cryptocurrencies

Blockchain is defined as a decentralized ledger technology managed by different nodes of a peer-to-peer network [4]. The system operates without central data management or central administrators. Data is often distributed across multiple nodes, and replication and encryption can protect the integrity of the data. The blockchain concept was announced in a white paper written by Satoshi Nakamoto on October 31, 2008. He proposed the concept of Bitcoin trading over the Internet, where online payments can be sent directly from one to another without going through a bank. The main idea of Satoshi is to create a reliable ledger [5] that solves the problem of double spending by using financial tools that integrate and calculate the chronology of digital marketing. When we say blockchain, it refers to a blockchain where each block in the chain stores information about all transactions occurring at any given time [6]. Therefore, when part of the chain enters the system, each block plays an important role in connecting to the block header and subsequent blocks. The main function of each block is to collect, analyze and distribute the transactions of other blocks. This means that no single block in the system can be isolated or significantly changed because all subsequent blocks will change [7].

Thus, the system is a decentralized information system that works according to a predetermined protocol that contains information on all past transactions, but also determines the working capacity and functionality of the entire system and the direction of business

success and proof. 8]. This network is also often called decentralized registry because information is stored on each node authorized to operate on each channel.

Groups of transactions in a blockchain network are placed in a chain linked to hash values from previous records [9]. Therefore, the basic security features of blockchain networks are managed as immutable features [10]. The further (and later) a blockchain goes, the more securely immutable the information it contains. When the attacker tries to change some keys, the local data will not be valid immediately because the hash value in the next block header will change completely according to the cryptographic hash function. [11th]. Figure 2.1 shows the longest proof of the work chain and the information contained in each block.

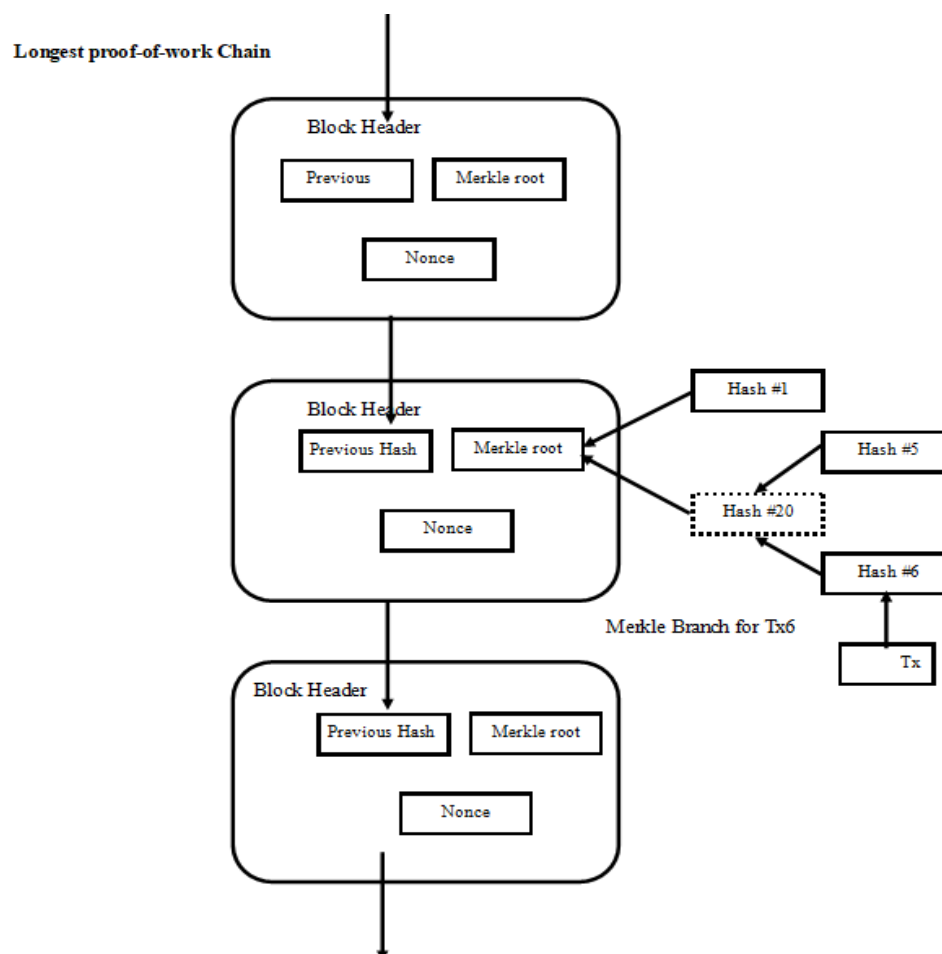


Figure. 2.1 Schematic of a blockchain Proof-of-work.

2.2 First generation of a blockchain technology: The Bitcoin

Bitcoin, the first and perhaps most well-known cryptocurrency, has attracted a great deal of attention, and the amount of research on Bitcoin (BTC) continues to grow. The biggest advantage of Bitcoin [12] is that it enables transactions without the need for central control, even if there are unknown parties to the system. Blockchain has many blocks related to proof, durability and timestamps. A miner's job is to add new blocks to the network, a process called mining, which refers to the process by creating new blocks. Essentially, the process starts with solving a mathematical challenge [13], and whenever a new block is created and added to the existing chain of blocks, a special mechanism will be used to solve the mathematical challenge that must be completed with the work. Miners take part in the network and the whole process is called proof of work and continues in the form of a chain. In Figure 2.2 we present a block diagram that can help us understand the basics of blockchain. The information contained in each block has been verified so that the entire process can be understood.

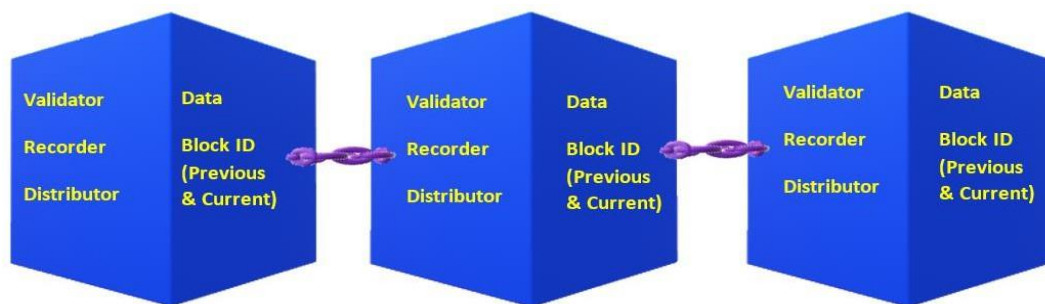


Figure. 2.2 Basic concept of blockchain.

2.3 Consensus algorithm and hashing

It is important to solve the consensus algorithm of new Bitcoin blocks. There are many consensus algorithms, such as: Proof of Stake; But Bitcoin is based on proof of work. . This solution is called mining; This is a real hassle and fails in attempting to create the wrong blocks in the network, but it is a simple and secure process to verify blocks in the network. The mining process in the blockchain is shown in Figure 2.3.

The goal is to create the most secure hash value generated for the next block. A consensus

algorithm is a method for organizing users or systems in a decentralized environment. It must ensure that all participants in the system can rely on one of the proofs even if the system peers fail. In short, the system must be fault tolerant. An organization keeps the power of the system in a central location. In many cases, they can make significant changes of their own accord, without needing approval from system administrators. But in a decentralized system this problem is completely different. Let's say someone needs to interact with a decentralized system - how do they view the data being linked? Perhaps the most sensitive time to make room for Blockchain is to gain a competitive advantage in a world where people do not trust each other. In cryptocurrencies, participants' balances are recorded in a blockchain ledger. Basically everyone (or more specifically, every network node) keeps an equal copy of the list. Otherwise, it is easy for contradictory content to emerge that undermines the entire goals of the cryptocurrency network.

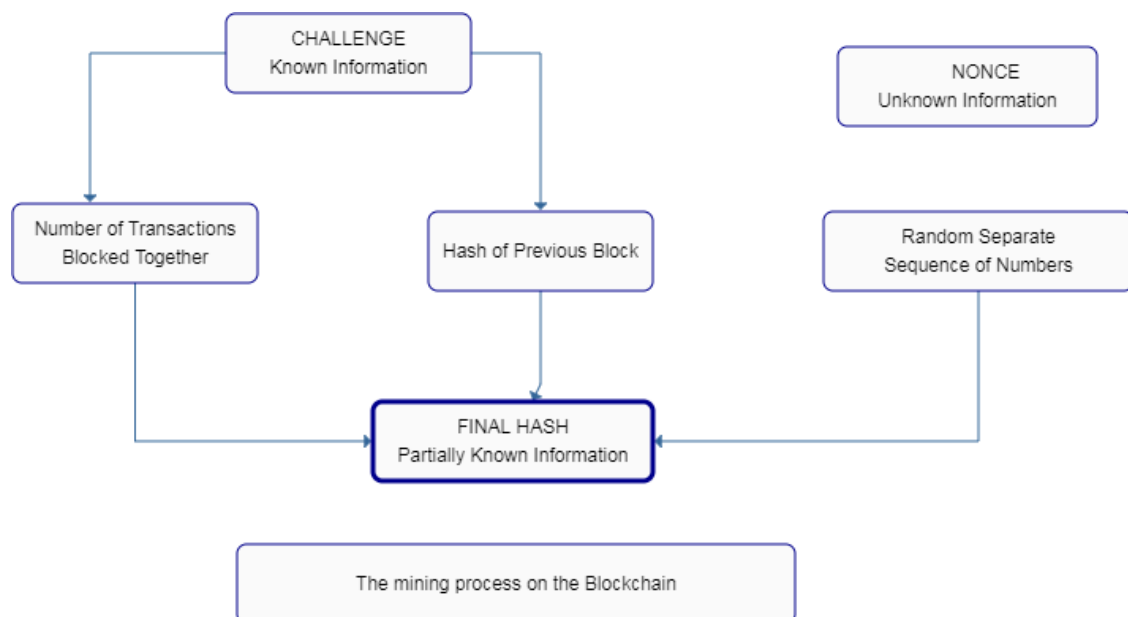


Figure. 2.3 Mining process in a blockchain.

Public-key cryptography determines that participants would not be able to use each other's coin. But also there requires to be a central source of authority on which network members depend, in order to be able to decide whether the funds are being allocated yet. Bitcoin's founder Satoshi Nakamoto has suggested a Proof of Work method for organizing

stakeholders. When we say blockchain is resilient, we means that it is really hard to attack on this system because hacker should have control over 51% of Blockchain to completely hack the system. Proof of Work (PoW) is the real base of consensus algorithms in blockchain. It was first introduced through Bitcoin. In Proof of Work, participating nodes termed as validator nodes (miners) encrypt (generate hash) the data they wish to add when a particular solution is generated.

A hash is apparently a random string of numbers and symbols that would be generated whenever you execute a hash function. And, if you pass through same data again, you'll still finish up with the same results being generated. And change just one item, and the hash will be entirely opposite. There is another very popular consensus algorithm called as proof of stack on which ethereum Blockchain has based [14]. In reality, Proof of stake [15] algorithm works better with 51% attack, it would detects the anomaly in the distributed network and held the value of coins. Exchanging the digital assets is one of the widely used concept and very common application of a Blockchain now a days. Around 2,957 cryptocurrencies [16] are traded with a combined market capitalization of \$221bn (as of Oct 8th 2019). Therefore, the top 10 cryptocurrencies [17] [18] [19]account for about 85% of the overall market cap [20] [21] [22]. The mostly used crypto-currencies are Ethereum, Bitcoin and Litecoin [23] .

There are other features besides the exchange of digital assets and one of the most popular among these is smart contracts. Smart contracts can be described as computer programs that function like the legal contract system and make it easier to check, execute and negotiate legal contracts. They run as blockchain transactions and communicate as a rule defined by the blockchain network participants with crypto-currencies. After the predefined rules / conditions are met, these contracts run autonomously. As we know that these smart contracts operate on Blockchain, they operate as planned without any alteration of the rules laid down before their execution and no third party can interfere with the Ethereum smart contracts network.

Furthermore, implementations of blockchain technology have started to emerge for items other than currencies. It has great potential to handle contracts like digital rights management because of its ability to resist against security attacks and minimise the third part cost as the system works without any central authority.

2.4 Blockchain characteristics and technology types

Basically, there are three major types of blockchain widely discussed as public, private and consortium Blockchain [24]. These types of technology vary in terms of usability, permission management and operating characteristics, such that each type of blockchain can be used in various applications. The most important features of these Blockchain types have been compared and discussed in Table 2.1.

Table 2.1. A summary of the blockchain types and characteristics.

	Public Blockchain	Private Blockchain	Consortium Blockchain
Database	Every participant can access database and store the copy of a transaction and change them.	Central authority who manages the rights to access or change the database.	Open for the public but not all the information is accessible by them.
Secure	Very secure as each block has a copy of individual transaction.	Specific people have access and it is considered secure because all the participants are known.	Provides privacy for the transactions. Known entities and governs the rules who can have access to read the ledger.
Cost	High cost.	Cost lower than public blockchain.	Usually lower cost as compared to public blockchain.
Speed	Slow speed as each transaction has to be validated and synced with each node ¹ .	High speed due to limited number of participants.	High speed compared to public blockchain.
Consensus Protocol ²	Everyone can participate in throughout the consensus process.	Consensus mechanism supports large number of the participants.	The consensus process is controlled via pre-selected nodes.
Network Congestion	High network congestion.	Scales more easily compared there is a controlled process for joining consensus process.	Controlled by enterprise and having lower network congestion.
Block Propagation	The block size keeps increasing.	Few participants are involved.	Block size is controlled as only known participants are involved.

¹ Nodes are the computers/machines which are running the software.

² All the nodes on the network should agree on the state of blockchain that means creating a self-verification network.

Feasibility	Not a very feasible solution in terms of resources consumed and cost.	Easy to maintain and feasible solution in terms of cost and resources.	More feasible in cost but also dependent on the enterprise.
-------------	---	--	---

2.5 Blockchain based smart contracts

Smart contracts are an important part of blockchain applications. It is an agreement between the parties involved in the specified process. It is a computer protocol that meets certain rules, codes, and restrictions accepted by all network participants. For example, a smart business transaction or a financial contract contains all the terms and conditions agreed upon by all parties at the time of the transaction [25]. Contracts are always considered long-term and methods are used, whether contract or action.

The term smart contract can be a misleading term because these are not smart contracts or promises. In the context of blockchain, a smart contract is a simple publication on the blockchain that can accept or complete transactions from one address or another. (the operation may be rejected or require special characters to run) and may be based on the Immutable protocol. [26]. Smart contracts are designed as “computerized business processes that enforce the terms of a contract” (Szabo, 1994) and were first developed by cryptographer Nick Szabo. The main meaning and origin of the title of the contract is that some of the contract terms should be included in the program code according to the manner or difficulty of violation [27]. Smart contracts are often confused with Ricardian contracts, which are electronic systems and related to other legal contracts (Griggs, 2015). This is not the purpose of smart contracts because they do not need to be legal or connected to the outside in any way [28]. However, with the smart contracts of the Ricardian system, one can easily imagine interest in “outsourcing” the operation of legal contracts to smart contracts. Smart contracts for access control are the best option to consider when implementing distributed applications. This article uses smart contracts to manage access rights and different permissions on the network.

According to Szabo's definition of smart contract [29], a logical contract must have certain properties in order to be defined as a smart contract. These include: transparency, online governance, traceability and privacy. Observability (see use of the word “observability”)

means that contracting parties must be able to see the quality of each other's promises or demonstrate to other participants that their own status has been fulfilled. It can also be used for transparency of actions based on the logic in the contract; . Figure 2.4 shows a simple smart contract example.

```
1 pragma solidity >=0.4.22 <0.7.0;  
2  
3 contract SimpleSample {  
4     uint stateVar;  
5  
6     function set(uint x) public {  
7         stateVar = x;  
8     }  
9  
10    function get() public view returns (uint) {  
11        return stateVar;  
12    }  
13 }
```

Figure. 2.4 Simple example of a smart contract

The version of the solidity can be seen in the first section, pragma. It tells us that this contract will compile between the given versions of a compiler. That line `uint stateVar;` specifies a vector of state named `stateVar`. It could be seen that it is of the `uint` kind, meaning this is an unsigned 256-bit integer. To change `stateVar` it could call functions, or question it. Throughout this example two specified functions can be seen as:

Set the `stateVar`-value changes

Get `stateVar` value retrieved

Smart contracts also need to be verifiable and auditable in the case of a dispute. Eventually, smart contracts should be as private as possible, meaning that information and data access rights in an intelligent contract will only be open to the participants if necessary.

One might find that the objectives of the smart contracts just listed; transparency, online enforceability, verifiability and privacy lead in two separate directions. Privacy exercises control over the contracts with a view to restricting contact with third parties. The other three objectives, transparency, enforceability and verifiability, are diametrically opposed, allowing participants or auditors to have access to contract information. A balance must

therefore be found where outsiders are granted as little data and power as possible, but there is still the possibility of testing, tracking, and implementation. In 1997, Szabo's solution to the optimization issue was to trust an intermediary, a third party, like an auditor, before blockchain technology and developments in zero-knowledge proofs as well as stable multi-party computations.

2.6 Ethereum blockchain

Since its launch in 2015, Ethereum has been considered a promising yet new and very innovative platform, allowing the creation of distributed applications such as blockchain using Turing-complete programming languages running on a shared peer-to-peer network [30]. For this reason, a lot of work has been done in this field in the last two years. Ethereum is a distributed network based on public blockchain that provides functions for smart contracts [31]. It provides a virtual computer called the Ethereum Virtual Machine (EVM) as a runtime system for executing smart contracts [32]. The Ethereum network is a private blockchain network that uses a virtual machine (Ethereum Virtual Machine, EVM) to run smart contracts. Since the world runs solely on the blockchain in the form of virtual machines, the smart contracts of the node machines are isolated from the network, data systems or other processes. A high-level Turing-complete language has been developed to write smart contracts using Ethereum. Ethereum has driven the development of technology and expanded its operations. It is a complete network with its own web browser, programming language and trading platform. Most importantly, it helps users build equity applications on the Ethereum blockchain. The Ethereum blockchain is a great client when it comes to creating Dapps.

However, Solidity has now become a standard for other platforms with smart contracts. Syntactically strictness is similar to JavaScript, but written in a completely different style. Once the contract is written in Solidity, it is compiled into EVM bytecode and then sent to a specific Ethereum address. However, a custom JavaScript RPC library is used along with the Web API to implement and communicate with Ethereum's smart contracts. Smart contracts are still a new discipline as they were initiated by Ethereum blockchain technology and Solidity [33].

2.7 Public key-cryptography

The Ethereum blockchain platform uses a special elliptic curve encryption algorithm for its public key cryptography and a set of various mathematical parameters as specified by the US National Standards and Technology Institute (NIST). Elliptic curve cryptography encryption technique is a powerful cryptographic technique from a very well-known RSA (Rivest–Shamir–Adleman), and an evolutionary method [34]. RSA is a very popular asymmetric algorithm which is developed in 1977. It has been widely used in the network protocols such as SSH and SSL / TLS, and for email encryption, such as OpenPGP and S / MIME. The RSA algorithm is driven by the fact that 2 large numbers are very easy to multiply but it is very difficult to categorize large numbers. The development of the pair of keys is this algorithm's most complicated procedure, and that is what make it so different from the symmetric key encryption. There are the numerical steps for creating the key pair. There is another significant aspect of the RSA algorithm which is its capability to create a message signature digitally. With that kind of function the source of the message can be confirmed. To achieve that, the sender of the message signs the message with its encryption key. The recipient validates the digital certificate with the caller's public key, to validate the source of the text. The very first step of digital signature creation is the formation of a message hash. To build the hash you must apply a hashing algorithm to the text, the most widely used is SHA-256. Once this feature is implemented, the text is simplified to a significant size, 256 bits long. The overview of the encryption and decryption process of RSA algorithm can be seen in figure 2.5.

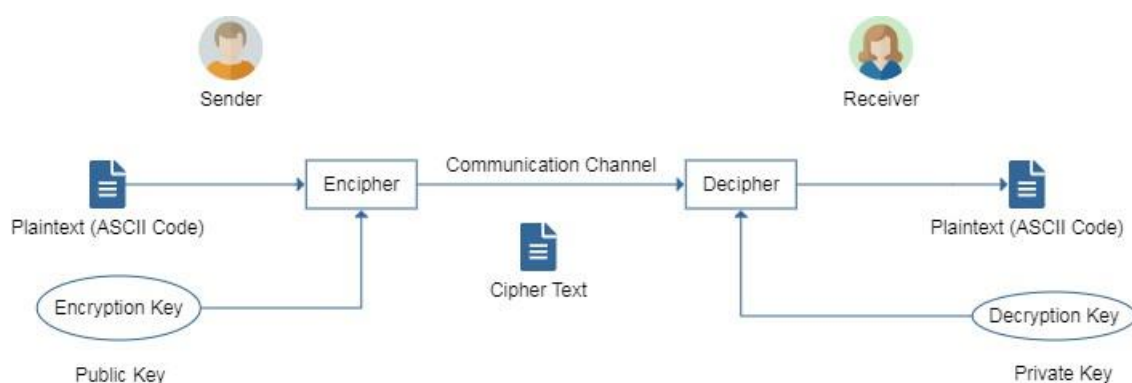


Figure. 2.5 Encryption and Decryption process in RSA algorithm

By using the mathematics behind elliptic curves, a technique used for public key encryption is to establish privacy between key pairs. ECC has grown steadily in popularity due to its potential to provide the same level of security as RSA (Rivest–Shamir–Adleman) with a relatively low key size [35].

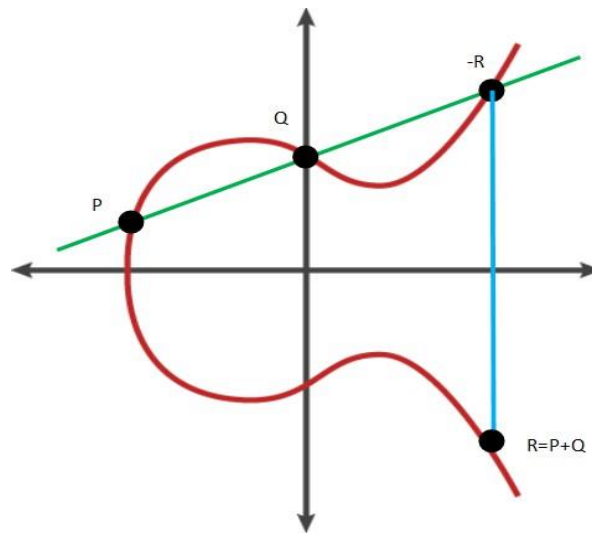


Figure. 2.6 Elliptic Curve (ECC). [39]

When working on the spatial plane, we can describe a group structure at any smooth cubic curve. In Weierstrass's normal form, such a curve will have one additional point at infinite space, O , at the particular emphasis that function as the identity of the group.

If X and Y are two main points on the graph then we can specifically define a third point, $X + Y$ initially, draw the line between X and Y as it can be seen in figure 2.7. This will usually intersect the cubic on a third point, Z as shown in the Figure 2.7.

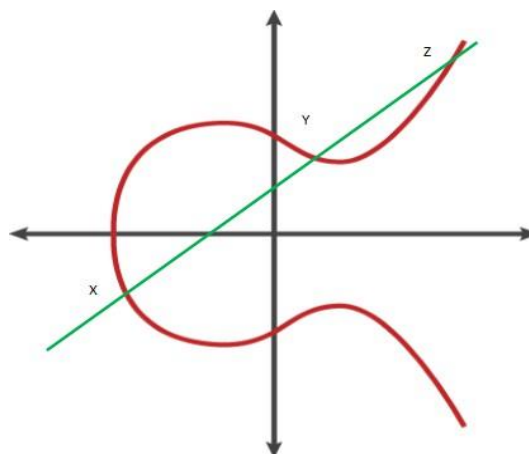


Figure. 2.7 Graph of curves. [39].

2.8 Ethereum virtual machine

EVM manages calculations and commitments in the case of blockchain network and follows assembly language with predefined instructions (opcodes) and parameters. So the contract is actually just one of the announcements processed by the EVM (Ethereum Virtual Machine). EVM can be thought of as a universal computer that has control over all smart contracts. Although it acts like a large computer or supercomputer, it is like a network of small machines that are constantly communicating.

All transactions on the Ethereum network, including the execution of smart contracts, are local and interoperate across all parts of the blockchain network. Each node analyzes and combines transactions sent by users into specific blocks and tries to add them to the blockchain network to get relevant results. This method is called the mining process, and miners are called nodes that participate in the network. To enable management of EVM resources, each instruction processed by EVM has a price associated with it (measured in Gas units). Operations that require more network traffic cost more fuel than operations that require less traffic.

This means that the denial of service will not affect the system as it will pass through the network by calculating the time spent by the user. Therefore, the purpose of natural gas is twofold. It encourages developers to write applications efficiently by preventing waste, while ensuring that miners get paid for the resources they contribute by working on applications. When paying for gas, there will be a small fee paid by Ether, the digital currency created on the Ethereum network, and the tokens that miners receive to trade and create blocks. Finally, Ethereum is known as the fuel of the Ethereum blockchain platform.

2.9 Ethereum-based smart contracts

Smart contracts are software that are built on the blockchain network and run as part of the verification of the transaction autonomously. A special development transaction will be conducted to create a smart contract in Ethereum platform, which will add a contract to the blockchain network. During this method, a unique address in the form of a 160-bit identifier is allocated to the contract and its code is submitted to the blockchain network [36]. A

smart contract, when successfully established, consists of a contract address, a balance of contracts, predefined executable code, and a state of a contract.

Let us just start with a simple example that determines a variable's value, and enables it to use for other contracts.

```
1 pragma solidity >=0.4.22 <0.7.0;
2
3 /**
4  * @title Storage
5  * @dev Store & retrieve value in a variable
6  */
7 contract Storage {
8
9     uint256 number;
10
11     /**
12     * @dev Store value in variable
13     * @param num value to store
14     */
15     function store(uint256 num) public {
16         number = num;
17     }
18
19     /**
20     * @dev Return value
21     * @return value of 'number'
22     */
23     function retrieve() public view returns (uint256){
24         return number;
25     }
26 }
```

Figure. 2.8 Smart contract code example.

The initializes with the Solidity version and tells that the source code has been written for the solidity version 0.4.22. For scripting languages, Pragma's are standard guidelines on how to handle the code.

A contract throughout the context of solidity is a set of code (its components) and information (its condition) that exists on the Ethereum blockchain at a particular address. In this code the uint establishes a variable of type unsigned 256-bit integer.

Smart contracts are usually implemented by blockchain network nodes, so it is not possible for a single entity to circumvent the rules specified in this code, as most participants would need to agree on this to happen. Smart contracts have the key advantage of being able to simplify the business logic of an enterprise and a system [37]. The move to automation of the contracts, in addition, cancels the consequences of human errors and misunderstandings which can result in legal disputes among different stakeholders involved in the system. Specific

interpretations may be subject to a legal contract or statute, but code is deterministic; there is no space for personal interpretations. A typical structure of a smart contract can be seen in figure 2.10.

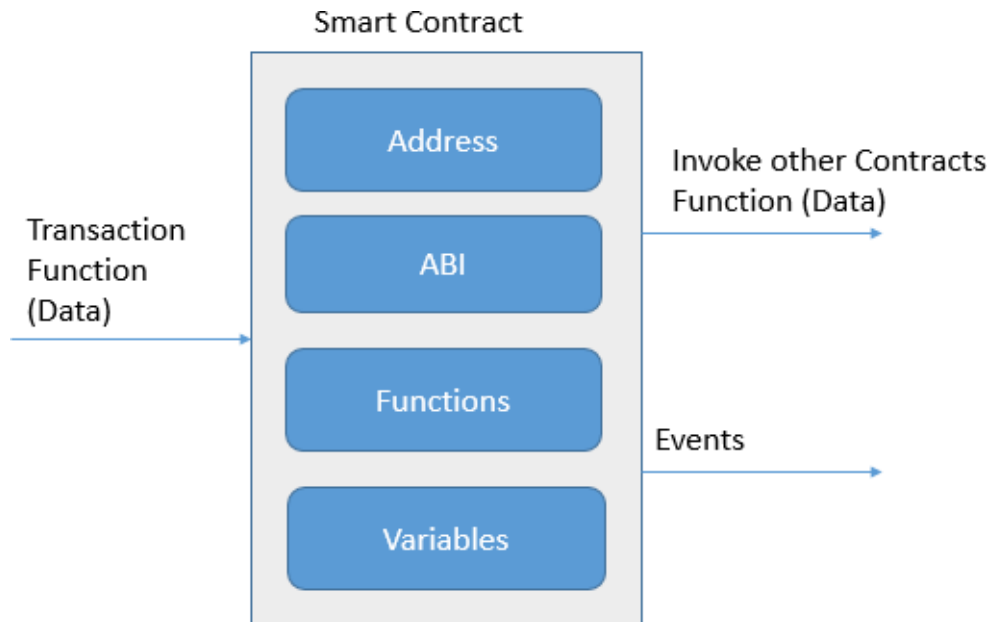


Figure. 2.9 Smart Contract Structure.

Through nodes submitting contract-invoking transactions to a specified contract address, different parties can then communicate with a specific contract. As a result of this, these can trigger any number of actions, such as reading and updating the contract state, interacting and carrying out other contracts, or transferring value to others. A contract-invoking payment must include the execution charge and a transfer of Ether from the caller to the client may also be required. It can also be described as input data for a function invocation. Once a transaction is accepted by the miners, the contract code is executed by all the network participants, taking into account the current blockchain status and input transaction data.

The network then agrees by participating in the consensus protocol on the output and the next contract state. Therefore, Ethereum can be regarded as a transaction-based state machine on a conceptual level, where its state is changed after each transaction happened.

2.10 Solidity

In Ethereum blockchain, smart contracts are typically written in higher-level languages and then converted to the bytecode on the EVM. High-level languages are Serpent which resembles a lot with Python, LLL, Viper (a Python-like language), and Solidity which is very much similar to Javascript [38]. In the early stages of the platform, LLL and Serpent were developed while Viper is currently under development to replace Serpent. Solidity is the most prominent and widely used language for the development of smart contracts [39]. Contracts are designed similar to classes in object-oriented programming languages when using Solidity for contract creation. As in conventional imperative programming, contract code consists of variables and functions that interpret and modify these. The Solidity language has a number of known peculiarities and a list of upcoming changes, meaning software now being written may not be fully functional with the upcoming update. There are a few programming best practices related to the design of smart contracts, gathered in the (relatively) short time Solidity was in use. The coding example of solidity has been given to understand the basic structs and mechanism of solidity program which is as follows;

The very first variable of that we must declare is address in the contract. This has a value of 160-bit, and stores the smart contract address. By accessing the public, it will let the variable access to other contracts that has been declared.

Mapping would then map the uint variables address (unsigned integers assigned to)

```
1 contract cryptoCoin {  
2     address public minter;  
3     mapping (address => uint) public balances;
```

Figure. 2.10 Creation of a contract

The next step is about declaring an event showing in figure 2.11. When the send function needs to execute this will be provoked. Ethereum clients could monitor and track the transactions by listening to these events and receiving arguments.

```
1 event Sent(address from, address to, uint amount);
```

Figure. 2.11 Event declaration in a contract

As shown in figure 2.12, once the contract has been created, the constructor will then execute:

```
1 constructor() public {  
2     minter = msg.sender;  
3 }
```

Figure. 2.12 Creation of a constructor in a contract

This contract has two functionalities as mint and send. Only one can call mint as the contract-creator. While doing so, one can create a given number of coins and can send them to another address.

The enable function call is to be used to define the constraints under which the adjustments should be switched back. In the figure shown below, it ensures that the minter really is the contract originator and describes the highest number of coins to be sent:

```
1 function mint(address receiver, uint amount) public {  
2     require(msg.sender == minter);  
3     require(amount < 1e50);  
4     balances[receiver] += amount;  
5 }
```

Figure. 2.13 Mint and send function

Unlike the mint, sending is accessible to everyone possessing coins. They can send a whole lot of tokens to somebody else by successfully executing it.

Unless the sender attempts to transfer more coins as compared to what they currently own, then the call for the required function will not be executed. An error occurred and the error message would pop up in this situation

```
1 function send(address receiver, uint amount) public {  
2     require(amount <= balances[msg.sender], "Balance too low!");  
3     balances[msg.sender] -= amount;  
4     balances[receiver] += amount;  
5     emit Sent(msg.sender, receiver, amount);  
6 }  
7 }
```

Figure. 2.14 Example of running a contract code

2.11 Smart contracts programming on Ethereum platform

Ethereum blockchain contract development requires a different approach to engineering than most web and mobile developers are familiar with [40]. In contrast to traditional programming languages, which accept a wide range of convenient data types for processing and manipulation, the programmer is responsible for deeper-level internal structure and data manipulation [41]. This implies that details that the developer may not be used to deal with must be addressed. For example, a developer would have to implement a lowercase string method, which are usually tasks that developers don't have to think about in other languages. Here is a simple smart contract example where the contract contains a constructor function and the message in figure 2.16. Function setMessage will change the state of message whenever a user wants to change its value.

```
1 contract Hello {  
2  
3     string public message;  
4  
5     function Hello(string initialMessage) public {  
6         message = initialMessage;  
7     }  
8  
9     function setMessage(string newMessage) public {  
10        message = newMessage;  
11    }  
12 }
```

Figure. 2.15 Simple smart contract example.

In addition, the Ethereum framework and Solidity [42] are constantly evolving at a rapid pace and the developer is facing a continuous transformation of application functionality and the security environment as new instructions are introduced and bugs and safety threats are discovered [43]. Developers need to consider that code written today will probably not be compiled in a couple of months or will need to be refactored at least.

2.12 Metamask

Ethereum has always been about discovering future innovation's potential. If we knew what it was good for, instead of a virtual machine, it would have shipped all those features. And the inventions continued to come. A MetaMask plugin is a script loaded over a protocol such as ENS, IPFS or Swarm that is checked and unauthorized [44]. By default, these scripts have zero rights, but will be able to request from MetaMask a number of important wallet APIs, via a

new API called the wallet API. The wallet API is an expansion of the classic ethereum or web3.currentProvider API, but with some additional features designed to make some of our favorite use cases simpler, such as layer 2 scaling techniques, and even more contract account support features. Metamask has been used to calculate the cost for a specific transaction on the ethereum blockchain for the distributed applications being implemented in this thesis.

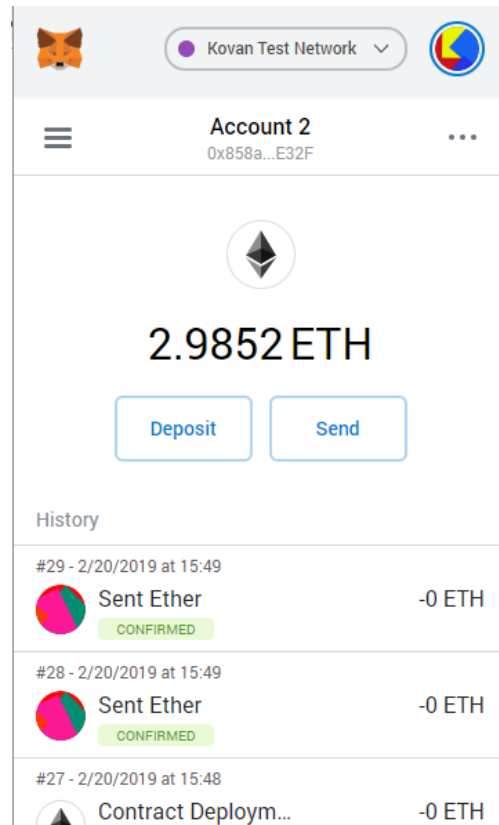


Figure. 2.16 Metamask Extension.

2.13 Etherscan

Etherscan is Ethereum blockchain's pioneer BlockExplorer. A BlockExplorer is essentially a search engine that allow users to search, confirm and verify transactions that happened on the Ethereum Blockchain effectively [45]. Figure 2.18 is an illustration of Etherscan transactions and blocks. In this thesis, Etherscan has been utilized to verify the transactions on the Ethereum Blockchain. Every transaction has been recorded, confirmed and verified using Etherscan for the smart contract applications implemented in the upcoming chapters.

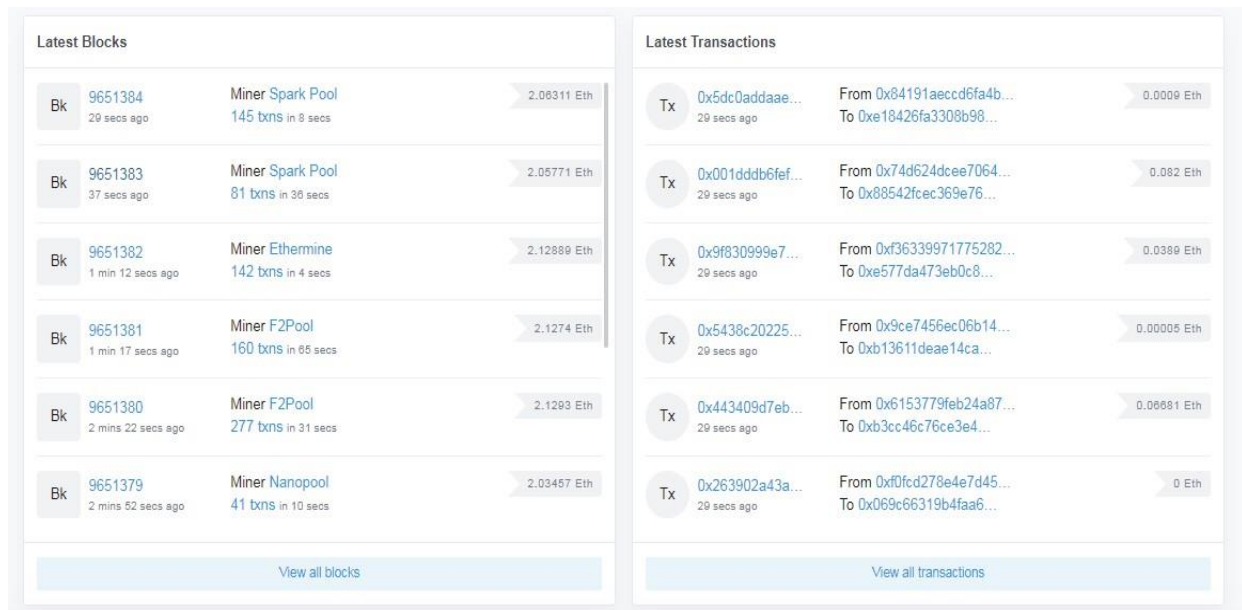


Figure. 2.17 Etherscan Transactions and Blocks.

2.14 Blockchain based smart contract applications

Ethereum blockchain platform makes it possible to develop and test smart contract apps or distributed applications (D-Apps) conveniently [46]. Public smart contracts allow start-ups to raise funds through Initial Coin Os (ICOs). On the other hand, big companies mainly want to take advantage of authorized smart contracts to incorporate their models and enforce enterprise procedures. Some of the common use cases include Fintech industry, Electronic Medical Record (EMR), IoT information management, supply chain and Energy sector. Other interesting applications like smart waste management, real estate, and ride-sharing arcade city are also available.

2.15 Conclusion

In this Chapter, we have briefly given the overview about the basic concepts of blockchain technology along its types and platforms. The foundation of blockchain technology has been discussed in details alongside Ethereum platform, solidity, Metamask, Etherscan and smart contracts. Different components and structures involved in the smart contract have been explained in detail. A brief introduction and explanation of cryptographic algorithms, hashing, and consensus techniques is provided in this chapter. This chapter also provides few examples on blockchain based smart contract applications which will be explained in detailed in the next chapters in terms of Healthcare and energy system application. The concepts presented here

will help to understand the next chapter which provides the literature review on blockchain based distributed applications mainly focused on healthcare applications and energy systems. This is a foundation technique chapter which provides all the details about the tools and techniques utilized in this thesis.

3 Literature review: Blockchain based Distributed applications

In this chapter, literature review has been conducted on existing blockchain based distributed application for Healthcare and Energy Systems. There has been detail provided on gaps in non-blockchain system. The usage of blockchain technology is making transaction histories more transparent. Since blockchain is a distributed ledger, rather than having individual copies of documents, all network participants have access to the same information. Only by consensus can that shared version be updated, which means everyone must agree on it. To amend a single transaction record, all future records would have to be changed as well, and the entire network would have to agree. As a result, data stored on a blockchain is more trustworthy, reliable, and transparent than the information stored in the existing Non-DLT systems. It is also accessible to all participants who have been granted permission. In this chapter we will discuss in details the existing literature on blockchain based applications while at the same time addressing the gaps in the existing non blockchain systems and the motivation to the work we have proposed for blockchain based distributed applications. All the basics concept of smart contracts, distributed applications and the tools and technologies we are using in our work has already been discussed in detail in the previous chapter which is the foundation technique chapter.

3.1 Traditional healthcare system vs Blockchain based healthcare infrastructure

Existing Health record systems were never intended to handle the complications of multi-institutional, lifelong medical records. Individuals' data becomes distributed among numerous organizations as they move between providers, making it difficult to access previous records. Patients encounter significant challenges in reading their results, fixing false data, and disseminating the content because caregivers, not patients, mostly handle the data. The scenario is similar to that of consumer finance, where a person may have multiple bank accounts, debit cards, debts, and investments but no centralized means to access and manage them. However, in the financial services space, there is a system in place to lubricate the rims. With health information systems, we are still lagging behind.

The volume of healthcare information are now steadily growing, yielding the enormous amount of data being generated. This reality relates closely to the emergence of software technologies and smart phones, and of course health records digitisation and clinical documentation. Healthcare data might contain very sensitive and important information. These healthcare data helps in improving healthcare outcomes, anticipating infectious diseases, gaining useful insights, preventing diseases, helping in lowering the healthcare costs and improving the overall quality of life. Keeping in view these aspects, healthcare information needs to be secure.

The emergence of healthcare apps, devices and digital transformation of medical records are rising exponentially. These medical healthcare data are collected, and used in legacy applications, which have serious concerned regarding mishandling of sensitive information. A resolution would then be required and this is where the blockchain technology emerges, as an innovative solution to make things simpler, more confidential and much more efficient.

The recognition of the key benefits of blockchain technology have been growing at a significant rate. This reality contributes in such a growing number of research studies related to the development of blockchain based healthcare applications. In most of these research findings new technologies have been created that can be classified on the basis of their goals such as: improving the insurance pay-outs process; facilitate the delivery of health records; promoting the medical and clinical studies and development of health care applications using the distributed ledger technology. These solutions aim to address emerging problems in conventional health care and data sharing for healthcare systems.

Conventional healthcare systems are centrally controlled: an entity is in place that monitors and manages all the information. Blockchain is built on the principle of consensus algorithm, where each node enables to evaluate the information is being exchanged, to whom and of all, each node does have a copy of all the data and information stored on the blockchain network. Furthermore, distributed systems also helps in reducing the transaction costs.

Medical healthcare information are classified as sensitive information which requires high level of privacy and transparency. Often, though, it is really needed

sometimes to share this information with other parties. This can be really challenging in the existing health-care systems due to a lack of standardization. Most systems do not have compliant data structures which preclude information sharing. Blockchain powered healthcare system improves system-to-system information sharing and is more effective in managing huge data volumes and different parties in the system. Blockchain enable data sharing system helps in the data exchange and integration between distributed apps and other systems efficiently. The blockchain based system allows real time updates in all the network nodes, streamlining the data sharing in the network.

Blockchain based smart contracts play a significant role in maintaining blockchain network's confidentiality and anonymity. There are conflicting rules and privileges in the existing healthcare systems which limit some certain party to access patient's data. A set of rules can be created with "smart contracts" to regulate the information about the patient's records. While doing so, the individual, who owns the health records, may choose to exchange medical-healthcare records with whoever he wants to. In addition, smart contracts are among the main features of blockchain crypto algorithms, which make a contribution pragmatically to the optimization of decentralized management, as it enables regulations and authorizations to be published in the code, thus instantaneously accomplished even without the need of any centralized system.

3.2 Existing blockchain based healthcare solutions and applications

In this section, we have conducted literature of existing Blockchain based healthcare frameworks. Although there are very few implementation of Blockchain based healthcare architectures and there is one very well known among them MedRec, which has been discussed in this chapter. The Legacy systems normally only end up sharing medical and healthcare resources structurally and are not fully compatible with external entities [47]. Nonetheless, there are multiple benefits of integrating these networks for integrated and better wellbeing, calling for interconnections between various organizations for researchers in health information technology [48]. One of most crucial issues is the low- and mid-organizational data exchange, which requires other entities, such as a physician or research institute, to have easily access to medical data obtained by a healthcare provider. Blockchain technology redefines data management and transparency in many Healthcare implementations. This is due

to its adaptability and secure exchanging and sharing of medical data. Blockchain technology is at the leading edge of many current developments in the healthcare industry [49].

With the advent of electronic health information, cloud storage, and patient information, a competitive market in health information management and effective services for patients to access and begin sharing their health information has emerged [50]. This section discusses blockchain-based applications in detail, including data sharing, data management, data storage, and EHR.

Use of new blockchain-based medical technology; It is divided into various levels such as information, blockchain technology, medical applications and stakeholders. A healthcare blockchain study was conducted in [51] and they wrote a discussion about how blockchain technology allows patient-centric management of organizational management information sharing in healthcare. In their research, they explored how blockchain technology could transform the healthcare industry by allowing digital access, patient identification across networks, management of bulk medical records, and immutable records. In another study on medical records [52], they used the Fabric Hyperledger platform to transfer medical records to the blockchain Hyperledger network. They use smartphones to collect this medical information. In their research, they tried to ensure that medical information was stored on the blockchain network. There is another project [53] that offers a better way to manage the quality of medical information using blockchain technology. Their research covers different types of research, and most of these studies discuss the health benefits and limitations of blockchain technology without providing evidence or evaluative control. They settled the debate on how blockchain can better manage cloud-based health data while maintaining data security and privacy.

There are different blockchain platform including permissioned and permissionless architectures. The authors in [54] identifies an approach to address the limitations of permission and permissionless blockchain networks. They have also used an instance of Hyperledger blockchain platform for the patient-controlled health data management system. There are numerous surveys conducted on healthcare blockchain possible solutions. In [55] the authors conducted a literature survey on healthcare management systems while proposing two algorithms for the network security. They have also suggested using a distributed ledger system for the better healthcare data management and to establishing the efficient regulations for the healthcare systems. Blockchain technology and IoT devices are

playing very vital role in the healthcare industry. The study in [56] proposes a medical data sharing system using blockchain and peer-to-peer networks named as MedChain. This system was designed for healthcare data generated through medical assessment and patient data gathered from IoT smart sensors and other mobile applications.

In another study [57], the authors analyze different healthcare management problems and how to use blockchain technology to solve them. In addition to current health research using business technology, they also talk about some medical applications where blockchain technology can play an important role in making the process work well. They also reported using network protocols to deploy IoT devices. Confidentiality and security of medical information is important. Litchfield et al. [58] pointed out the different problems of medical information security and personal access and said that blockchain is a solution to solve these problems. They also looked at health issues.

The patient's health information must be protected under all circumstances. Breach of patient information (name, address, etc.) is discussed in [59]. The main purpose of this article is to review the success of their plans and understand how their solutions benefit patients, doctors, and private cases, including third parties. Various medical applications using blockchain have been mentioned [60]. They talked about the importance of blockchain-based healthcare systems and how blockchain technology can create better healthcare. In another study [61] the authors stated how blockchain technology and smart contracts can benefit the healthcare industry by standardizing all layers. In their study, they said that the management of medical data is very important and that blockchain has the ability to reduce losses and protect data by preserving ledger data.

Blockchain technology can be an important tool for drug design and drug marketing. Cemil et al. Fundamentals of medication administration are discussed and how blockchain can be used to standardize the entire medication administration process. Throughout this work, they emphasized the difficulty of detecting counterfeit drugs and suggested that blockchain is a way to detect counterfeit products [62]. The human hand is very different and reflects the human body. Lee and Yang worked on nail control using blockchain technology and microscopes.

Using deep neural networks to monitor the performance of feature extraction algorithms. Blockchain technology is used as a way to protect user data and ensure security and privacy so that all transactions can be tracked and recorded by a ledger [63].

Ensuring data protection, processing, transactions, and managing their seamless integration is immensely important to any data-driven enterprise, particularly in health care where blockchain technology has the potential to address these critical issues in a robust and efficient manner. In [64] the authors, conducted a comprehensive study of latest literature on blockchain healthcare applications. To answer their research query they selected 65 research articles. Their study indicates that blockchain could be a potential technology for various healthcare case scenarios that includes the supply chain of drugs, clinical research, and electronic healthcare records management. However, they also analyzed the fact that more understanding of blockchain technology still needs to be developed and how it could best fit for different healthcare complex problems.

Innovation in healthcare has been slowed due to inefficiencies and heavy regulatory requirements. Azaria et al. discussed these regulatory issues which cause EMR system inefficiencies [65]. They have recommended blockchain-based solution recognized as MedRec to manage huge quantities of medical data in EMR system. They illustrated an innovative and unique approach to accessing healthcare records which offers a fair access log system for audit access. Using distributed ledger technology, MedRec allowed patients and doctors to share the medical data between different parties. They give people such as researchers, other health individual's incentives to take part in the mining process. MedRec enables the data to be anonymised and available to the miners as a reward for participating in the network.

In [66] the work states that how blockchain based smart contracts have the ability to fix various healthcare concerns. The authors took some initial steps in their work to incorporate blockchain technology for specific healthcare use cases and referred to numerous obstacles in adopting blockchain technology. They also worked out that creating blockchain-based applications will address healthcare problems more effectively.

Blockchain technology has many opportunities for medical scientists, health care practitioners and individuals [74]. It will enable both research and tissue engineering to create a single location for all health data, monitor personalized information directly and set permissions for fine-grained access to data [75]. The work [67] identified different blockchain applications for healthcare system₃₃ They outlined problems and challenges with the adoption

of blockchain technology and presented smart contracts for blockchain-based health care system.

Digital security is a big challenge because of hacking motives and privacy breaches. In [68] the authors, formulated consent governance in E-health environments and proposed blockchain as the most stable and reliable solution for handling health data. In this digital world age, access to personal information has become a major concern, with challenging aspects of security and privacy. This is possible in the area of eHealth where the health information management system for patients has to comply with many legislation while remaining accessible to duly authorized healthcare professionals. Because of its most common use-Bitcoin-most in the payment area must have heard of blockchain.

There are many advantages to the blockchain technology and distributed ledger system as discussed briefly in [69] that includes identity management, security of personal data, sensitive handling of information, elimination of third parties. With exception of centralized networks, the capability of the network continues even if single nodes break down. It increases confidence, as individuals do not assess the trustworthiness of the intermediary or other network participants. If people boost confidence within the system itself, that should be enough. The lack of intermediaries also facilitates the data security. As in the current practice of third parties collecting personal data, there is the possibility of security breaches. By using the blockchain, third parties may become redundant and effectively increase user protection. There was a report by the MIT Media Lab [70] highlighting the data protection aspects and the handling of personal information underline all the implementation of blockchain technologies. It is the significance of data processing which is secure – in the sense that it cannot be exploited. The data protection and privacy are another dimension of data security. For instance, Enigma is a decentralized, private information-guaranteed computing platform and a breakthrough on blockchain. Enigma's goal is to enable developers to build an end-to - end digital platform without a trusted intermediary. Enigma is indeed an extension of blockchain technology because processing and data management are not achieved inside the blockchain, rather the blockchain is an "interface" for protected multi - party computations performed by network-participating storage and computing nodes. Relevant data is split between different nodes, and various nodes work together to measure functions without leaking classified information towards the other nodes. In conclusion, "not a single party has any kind of access to the data in its entire duration; instead, each party has a meaningless piece of it (i.e., apparently arbitrary).

Blockchain holds the potential of creating a new data contract, a greater degree of personal data ownership, control and content delivery, through a network that enables the world to benefit from data collection. Within Google Maps, traffic congestion information is a direct example of the advantages of data aggregation: by incorporating location, travel pace and other important personally identifiable information, drivers leverage from the existing data pool to achieve shorter traffic times and avoid traffic jams. But Google attempts to integrate driver's personal location data to do this. BlockVerify, on the other contrary, is an illustration of a start-up using blockchain to assert proprietary information by verifying the origin of luxury goods, physical objects and by investigating the legal status of generic medicines, diamonds and electronics to resolve the issue of counterfeit goods. This type of security occurs because blockchain is decentralized so that it does not rely on a single authority for its maintenance, and therefore a single example of misappropriation that causes a failure does not affect the reliability of the records.

Another study [71] describes blockchain and ethereum as a secure platform for handling sensitive information of all kinds. It states that blockchain is a decentralized system. This has significant skill in solving market problems. The encryption secures the data in a blockchain transaction, and each transaction is linked to previous transactions or a database. Blockchain transactions are validated through algorithms on the nodes. A single person might not be able to make a transaction. Blockchains eventually have transparency, allowing each user to track the transactions at any time. Smart contract enforces a secure process which helps to prevent third party interruption. In [72] the authors used the cloud technology scenario and pick the cloud records as a data unit to easily classify user activity from source to collect data. By embedding the data into blockchain transactions, they develop and implement ProvChain, an architecture for cloud data provenance collection and verification. ProvChain operates mainly in three phases such as provenance data collection, origin data storage, and provenance data validation. The results of performance assessments show that ProvChain provides security features for cloud services and applications, including misleading provenance, consumer rights and low overhead durability. There are number of surveys conducted among numerous professionals about the conceptualisation of blockchain and the implementation of blockchain technology in healthcare institutions. Another study in [73] discussed how different business players are pursuing blockchain widely in the healthcare sector to improve their business operations. It can help improve patient outcomes, reduce costs and standardize the whole process.

This systematic review includes all the research studies that creates a new blockchain- based solution, algorithm, method, technique, or architecture to healthcare. Also included are review type research, discussion of possible blockchain uses and applications.

3.3 Discussion and motivation for a blockchain powered healthcare infrastructure

Medical researchers need detailed information to improve understanding of the disease, enable new treatments, rapid drug development and refinement, product lifespan, and historical treatment plans for patients [76]. Blockchain's decentralized information network will provide diverse information by involving patients from different cultures, cultural and economic backgrounds, and different industries. Since blockchain collects people's health information, it provides valuable information for clinical research [77].

Blockchain in healthcare can support the development of new “digital” medical applications that transcend new medical research and create new treatment options. Doctors and patients will have access to the same information and will be required to engage in collaborative, research-based clinical discussions, not ideals. This section examines existing blockchain-based healthcare applications. The smart contract scheme will be introduced in the next section. Among existing blockchain medical applications, no application can provide complete medical care based on distributed technology. The work presented in this article provides a framework for blockchain-based medical operations to participate in the medical ecosystem. Electronic health information exchange between different participants in the healthcare ecosystem (such as patients, doctors, and researchers) will promote healthier and more efficient collaboration. This personal information is provided only to approved and authorized users of the system. When looking at all health information, some users may only want to access some of the information and may not need to access all the health information mentioned in this article, it will help avoid the risk of disclosure of all sensitive information. Users of this information, as well as friends, in addition to accessing this information, still want to update some information and share this information with other friends by self-managing this model and monitoring all sensitive information in the system. Help them do this a lot Okay.

3.4 Blockchain based applications for energy Efficiency

Energy efficiency gains must increase by 2030 to meet the Environmental Sustainability Agenda. However, due to a number of market constraints, the adoption of energy efficiency solutions is gradual. By enabling transparent, decentralized, and tamper-resistant systems, blockchain technology has the ability to solve these constraints or perhaps radically revolutionize energy system architecture. A blockchain solution does, however, come with trade-offs that must be considered on a particular scenario. In this section, we address how to overcome the stated challenges to blockchain adoption and emphasize the importance of policy action to accelerate the development of pilot studies. Blockchain allows creative designs that help accelerate the adoption of energy saving initiatives by decentralizing system governance. A thorough literature review has been conducted on existing blockchain based applications in the energy system domain.

The use of Blockchain technology recently emerged as a significant technology in the energy sector's digital revolution and a number of international experts [139] [140] [141] have also identified the blockchain potential use cases for the energy eco-system. In addition, it will also facilitate energy consumers' ability to monetize their excess energy that could have come either from generation or energy savings.

The rapid pace of innovation in communications technology and the growing consumer interest in energy efficiency offer significant opportunities for transformation to a low emission energy system [78]. Distributed ledger technologies, especially blockchain, have recently gained considerable popularity in making the energy sector safer, more transparent and more efficient [79]. Blockchain has been researched as mentioned in the previous section, for several applications in the energy sector. It has been extensively discussed in connection with P2P energy trading and there are a number of articles available that describe this idea [80] [81] [82] [83] [84], a range of early product launches as well as [85] [86] [87] [88]. However, our literature review revealed that blockchain is still just an idea that is yet to be thoroughly investigated in terms of its application to energy efficiency. There is only a limited number of articles on this topic so the purpose of this section is to highlight those key literatures, media articles, blogs or any other relevant writings where the idea has been conceptualized.

Energy Service Companies (ESCOs) are looking for potential blockchain alternatives to overcome the energy performance contracting (EPC) complexity[89]. Over the last couple of years, the prevalence of EPC business models has increased significantly [90] and EPCs have become a popular method for improving energy efficiency in buildings. The problem with the EPC model is that it requires several stakeholders who maintain their own records of energy baseline data, implementation costs of technology, project expenditures, and the amount of energy savings achieved, which can generate conflicts between stakeholders when payment is due. It has even been pointed out that the smart contract functionality will substantially decrease transaction fees, and therefore ESCOs will have the opportunity to pursue smaller projects so the cost and time involved in setting up and administering each EPC will be reduced significantly. It will boost the number of ESCO projects, and the overall amount of energy savings that can be achieved as a result. A study by Gurcan et al. created a practical prototype where blockchain technology was applied to the EPC and removed the need for third-party audit committee to perform large volumes of benchmark and actual consumption data measurement and verification [91].

Ethan has addressed the interesting aspect of how blockchain may improve energy efficiency valuations. This includes a discussion on how to encrypt and share energy savings across a blockchain platform to improve the transparency of the energy efficiency market, information security, and service reliability. The American Council for Energy Efficient Economy (ACEEE) is also investigating how blockchain could be utilized to improve the measurement and verification process and how a more fluid energy market could be facilitated [92]. Toyo [93] stated how the application of blockchain technology could boost energy efficiency in the supply side and how it can tackle energy poverty through a decentralized energy network.

In the scope of energy-related certification schemes, a recent research explored the possibility for using blockchain to trade Certificates of Origin Guarantee (GoO), also referred to as Green Certificates. The regulator awards a green certificate to renewable energy producers for each Mega-Watt hour (MWh) of renewable energy generated from certified sources. Those green certificates document details of when it was produced, where, how, and by whom. This certificate also documents who owns the related renewable assets of the clean energy. The certificates may be transferred, bought, sold or withdrawn, but the processing process for such certificates is slow and opaque. The research carried out by Castellanos et al [94] demonstrates

that blockchain can be used to guarantee the validity of green certificates, increase system transparency and minimize transactional costs by eliminating any need for the third party regulators to manage the scheme.

The existing structure of energy regulation may face new challenges as a result of a decentralized system. The insights provided in this research, reveal that blockchain applications provide innovative organizational forms and advantages that have the potential to greatly alter and transform current energy systems. Blockchain technology could help small and large firms alike deliver energy-efficient products and services, providing innovative business models that could enhance energy efficiency in developing nations. Blockchain can improve accountability and cost-efficiency in these systems by decentralizing power. This research analysis reveals that blockchain technology can solve legacy system design constraints such lack of accountability, asymmetric information, high costs, and limited access to funding that are currently preventing the scaling up of energy efficiency solutions. Finally, whether and how blockchain-based energy solutions emerge in the highly regulated energy industry will be primarily determined by regulators.

3.5 Conclusion

In this chapter, detailed literature review has been conducted on Blockchain based distributed applications in the healthcare and energy sector. Existing available Blockchain based distributed applications in healthcare and energy systems have been discussed here. Using blockchain technology, privacy, security, availability and fine-grained control of data access rights can be ensured. The ultimate goal of using blockchain is to improve processes and thus the overall outcomes of the system. It can be concluded easily from the above discussion in the literature from the perspective of Healthcare and Energy system applications, that blockchain based systems will help in; reducing costs by using smart contracts which are embedded general purpose protocols to simplify procedures, reduce administrative burdens and remove intermediaries provides a better alternative to the non-blockchain systems. This will solve many of the current issues, including high administrative costs, lack of data security, and unaddressed privacy concerns.

4 Smart contract framework for healthcare management applications

Blockchain is transforming into a safe and efficient infrastructure for safe data exchange in applications such as the finance industry, operations management, food processing industry, the energy market, the Internet of Things and healthcare systems. Information sharing among health care and hospital systems is a key utilization of blockchain technologies in the medical eco-system. In this chapter, we have designed multiple healthcare ecosystem workflows using blockchain technology to effectively manage the data and processes. Using the ethereum blockchain, different medical workflows have been designed and implemented. This also involves accessing and managing a considerable amount of medical data. This work would facilitate the delivery of better health care services and cost optimisation whilst also multiple stakeholders involved in the medical system. The detailed implementation of all the medical work flows defining all the coding structures and functions executed in the smart contracts are included in the chapter 5 of this thesis.

In this chapter, using practical clinical databases, we examined the applicability of blockchain to the various healthcare workflows and the viability of existing blockchain implementation in specific healthcare eco-system use cases. Within the implementation of the medical workflows for the healthcare management, the associated costs for this system were estimated in terms of a feasibility study which is presented in this chapter. Blockchain technology has emerged recently as a crucial technology in the healthcare sector 's digital transition and numerous academic studies [131] [132] [133] have identified potential for blockchain in the health care ecological system. It is ready to revolutionize the way in which traditional medical systems and companies have been engaged in the healthcare sector over several years [110]. Information technologies (ICTs) and blockchain are the key technologies that enable healthcare institutions to be decentralized and digitized, and provide patients and service providers with modern and digitized healthcare ecosystems [134]. Blockchain data management applications create utilities for patients , doctors and healthcare institutes in the areas of patient record access and control, claims and payment management , medical IoT security management [135] research data authentication and financial audit exchange [136] and

openness. Real-time updates for distributed and encoded, decentralized blockchain network are done in these applications to understand, track, and manage medical information [137]. This also makes it easier for healthcare providers to restrict the unwanted person's access to confidential information.

Management of healthcare involves a number of activities such as management of finances, personnel, patients, legal issues, logistic support, inventory, etc. Medical workflows also include routine activities related to the treatment of patients, which can be depicted as a sequence of conditional acts. These are designed to provide stronger internal controls, enhance quality, compliance, profitability, and minimize risk, work cycles and overhead costs in hospitals and other providers of health care. In this chapter, multiple medical workflows are designed for various application areas of health care management systems.

This research introduces a smart contract healthcare framework for managing medical data, and streamlining complex medical procedures. We addressed state-of-the-art blockchain work in the field of healthcare, and introduced ethereum-based healthcare management solution. This research work also aims to indicate the prospective use of blockchain in healthcare and to demonstrate the challenges and possible directions of blockchain research.

4.1 System design and implementation framework Ethereum

The aim of our designed system is to facilitate different parties involved in the health care system including medical professionals, patients and healthcare insurance providers. This research thesis proposes an innovative new of decentralized data management framework using blockchain technology for managing Electronic Healthcare Records. The system architecture provides patients with extensive, unalterable logging and accessibility to their health records throughout different facilities and treatment care units. Using specific blockchain properties, this model manages data authentication, data retention, monitor changes for previous data records, updating data for clinicians and patients) and makes efficient data sharing in the system. It manages the records without having any central information repository; the modular framework architecture incorporates existing, local digital storage mechanisms for doctors, enabling interoperability and exchange of data among different stakeholders. Our objective is to develop a system which facilitate patients, providers and other stakeholders, over time, without creating the database that centralized the data and risked creating an attack on patient's information. Patient's electronic healthcare records contains

sensitive information. We have showed the patient EHRs hierarchy in figure 4.2. There are different permissions which shows who have access to what data in the system. Those permissions and the workflows are explained in detailed in this chapter. The detailed implementation of these data access rights and workflows have been given in the chapter 5 of this thesis. The platform implementation will be a decentralized application (DApp) that supports a private blockchain network at the back end, with a distributed file system (DFS). Ethereum has been used to implement a smart contract framework for blockchain in healthcare. This platform is open source, and presently one of the largest public blockchain networks with a community formed and a wide set of public DApps. The platform apparently uses a consensus proof-of - work (PoW) algorithm based Ethash, but in the immediate future, engineers are working to turn it into a proof-of - stake (PoS) scalability algorithm. Ideally a Delegated Proof-of-Stake for the creation of distributed applications, the consensus algorithm (DPoS) or Functional Byzantine Fault Tolerance (PBFT) is suitable. By matching DFS content with ledger registers, the DApp will have the potential to detect irregularities, unauthorized data insertions and missing entities. An Audit Timeline is labeled for each step. Functions, events, state variables, and modifiers are the essential elements of the smart contracts and are written in the language of the solidity programming. Remix and Kovan test network was used to build smart contracts on the testnet and testnet ethers to pay the transaction cost. The creation of smart contracts involves three stages, using Solidity programming to write, compile, and announce the contract on the network. The bytecode is created through the real-time Solidity compiler. Ethereum Wallet was used to announce smart contracts on the Ethereum Blockchain network. Figure 4.1 shows the overall mechanism of a smart contracts with Ethereum blockchain network, where the mining process has been excluded for the purpose of simplification. This smart contract has been constructed into machine-level byte code in which each byte reflects a function, and then posted as an EVM-1 transaction to the blockchain. A miner then picks it up, and confirms Block-1. When a user processes the response through the web interface, the EVM-2 queries and embeds the web-based data into Transaction tx and deploys it to the blockchain. In Block-2 the transaction tx status is changed. If node 3 decides to test the states that are stored in the contract, then it must synchronize the changes that tx triggers up to at least Block -2.

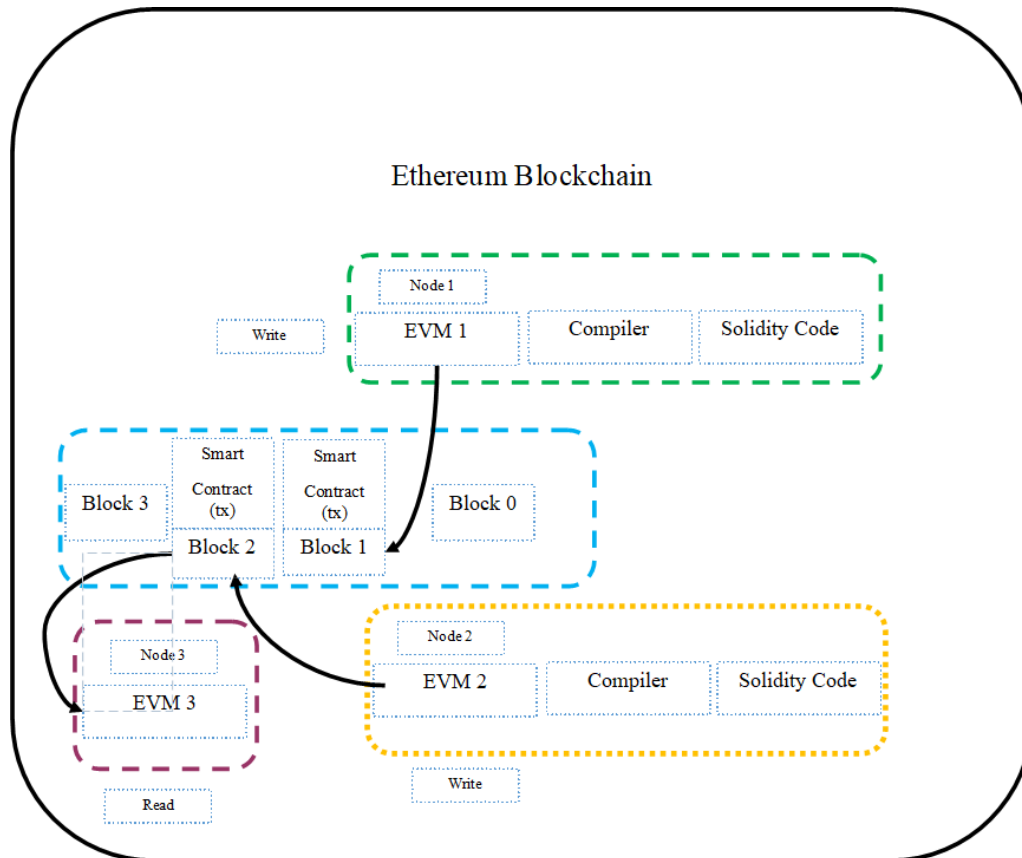


Figure. 4.1 Ethereum Smart Contract Mechanism. Reprinted with permission from Khatoun, A., Electronics 2020, 9(1), 94.

4.2 Medical Blockchain smart contracts

We leverage Ethereum's smart contracts to construct digital representations of actual medical records that are stored within individual nodes on the network. We are building contracts to include metadata, permissions and data validity of record ownership. Blockchain transactions of our network hold cryptographically signed instructions to handle certain properties. The contract's State-transition functions execute policies only through valid transactions that enforce data alternation. Such laws can be designed to implement any set of rules governing a specific medical record as long as it can be interpreted in a computational way. For example, a policy may involve the sending of separate consent transactions from patients and healthcare professionals before granting permission to a third party to access. Smart contracts were designed for different medical workflows and then data access permissions were managed between different entities in the healthcare ecosystem using Ethereum blockchain network. In

our system, we are managing an off-chain local database for the healthcare records. Hierarchy of electronic healthcare records (EHRs) can be seen in the figure 4.2.

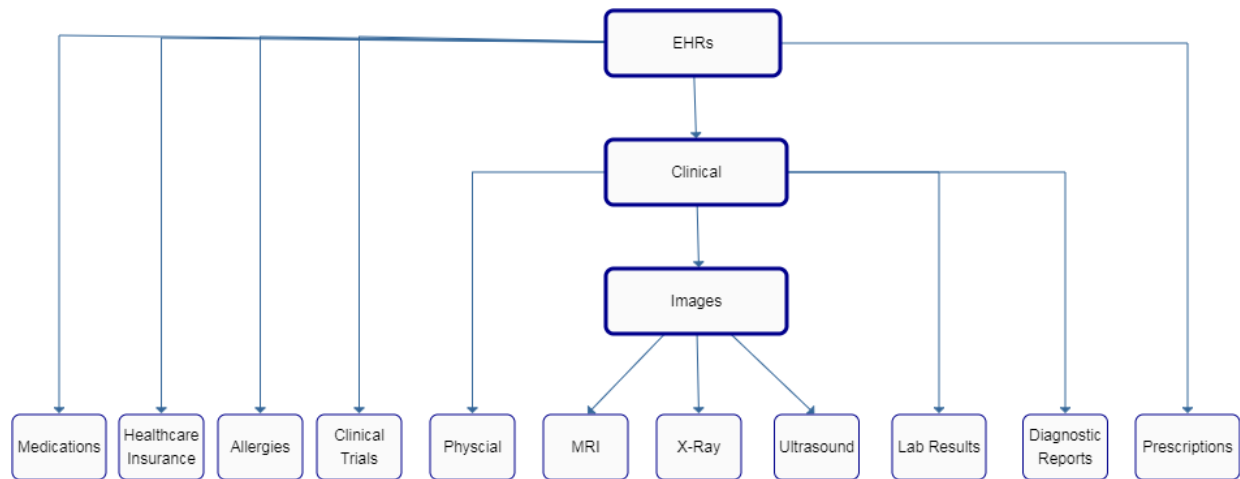


Figure. 4.2 Electronic Healthcare Records.

A smart contract, stored on blockchain technology has been developed and tested that have all the conditions from managing different permissions to accessing data as shown in Figure 4.3 and it can be seen that a number of stakeholders are involved in this scheme trying to perform various activities. This will create stronger interactions between patients and doctors with the help of smart contracts. The rules on data access rights are incorporated into smart contracts. This can also help monitor all behaviors with specific ids from their origin to their surrender. There will be no need for a centralized body to oversee and authorize the project because it can be handled directly via the smart contract that will greatly reduce the management process administration costs. All medical record data is stored in local database storage in order to preserve efficiency and economic viability, and the data hash is the data item of the chain's block.

The information transactions shall be signed with the private key (patient or doctor) of the owner. Data ownership and access rights exchanged by users of a peer-to - peer private network are the block material for the program. Blockchain technology encourages the use of smart contracts that allow us to automate and monitor such state changes (such as a shift in accessing rights or the birth of a new system record). We sign patient-provider relationships on an Ethereum blockchain via smart contracts that combine a medical record with accessing

permission rights and via providing data retrieval instructions (essentially information pointers and metadata) for the outside server execution to prevent tampering, we include a cryptographic hash of the blockchain record to ensure data integrity.

Providers may attach a record number associated with a particular patient, and patients can require sharing of records between providers. In both cases, the party receiving new information receives an automatic notification and may check the submitted record before approving or rejecting the data. That keeps the participants informed and engaged in the evolution of their records. This system prioritizes usability by also offering an assigned contract that aggregates links to all a user's patient-provider relationships, thus creating a new reference point for checking for any updates in medical history. We are using public key cryptography technique for the management of identity verification and using a DNS-like implementation structure that is mapping an already existing and widely accepted form of ID as person's name or their social security number to the Ethereum blockchain address of the user. After referring to the blockchain network to confirm different permissions via our system such as database authentication server, then a syncing algorithm will handle "off-the-chain" data exchange between patient's database and a provider's database.

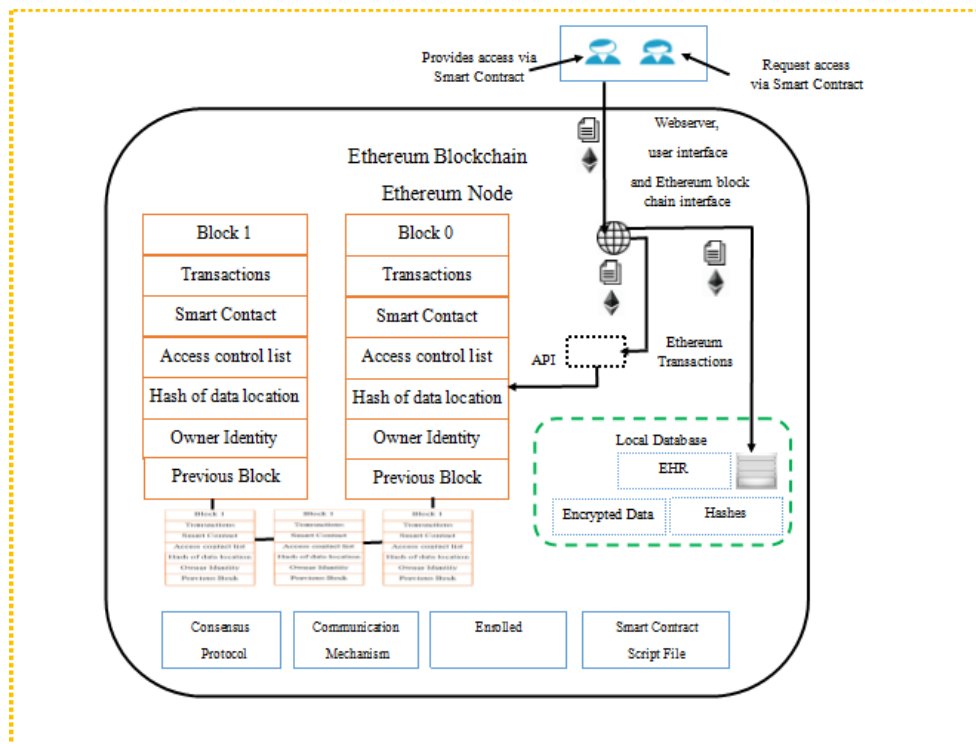


Figure. 4.3 The Schematic of the System workflow with smart contract controlled access.

Reprinted with permission from Khatoon, A., Electronics 2020, 9(1), 94.

4.3 System design and development

Different medical workflows were developed and enforced via the blockchain smart contract framework, involving unique medical procedures. This include the issuance of specific medical prescription for the treatment of complex diseases and their procedure such as care protocol for patients under surgery. The purpose of designing these smart medical contracts is to facilitate the overcoming of administrative inefficiencies for the patients, doctors and healthcare organization. This system will help in the collection, analysis and management of complex data and procedures in healthcare.

Algorithm 4.1: Patient Monitoring and updating records

Input: Ethereum address of the patient and all the other stakeholders involved in the system

Initialization of the process = Access approved

If Enrolment stage is finished

Then

 Allow all the transactions to be added in the network

 Mapping of data to the respective address

end

else

 Don't allow/accept unauthorized transactions

End

If Patient drop outs

Then Stop processing that further

 Update the records

 Notify/update the other peers in the network about the progress

End

Algorithm 4.2: Patient Monitoring in the event of Emergency

Input: Emergency case reported

If during the monitoring phase an emergency occurs
 & Ethereum Address = Primary doctor's EA /GP

Then

 Allow the Input details to be included as a valid transaction

End

else

 Don't allow/accept unauthorized transactions

End

If Ethereum Address = Specialist

 Approve the transaction from valid EA

End

else

 Don't accept unauthorized transactions

End

Algorithm 4.3: Reporting and Analysis

Input: Finalized the reports and update the EHRs

If Analysis and reporting is completed

 Accept the input as valid transaction

End

else

 Don't allow/accept unauthorized transactions

End

If Primary doctor/GP = EA **then**

Allow the accept/reject decision for the reports and analysis

else

Don't accept unauthorized transactions

End

4.3.1 The process flow of a smart contract for medical prescriptions

The key purpose is to improve the process of medical prescription handling by eliminating the long waiting period cycle, removing the fraud factor from the system and the human error rate caused by misunderstandings by the doctors. A doctor to write a prescription for the patient and needs to put it through a smart contract into the patient's healthcare records. The pharmacy then utilizes this prescription through the Ethereum blockchain smart contract, with the permission of the primary providers and the patients. After obtaining the prescription, the pharmacy then assigns the medication to the patient's healthcare records through smart contracts along its expiry date and dosage use, and then the medication is ready for patient selection. Medicine satisfaction among doctors and drug stores is generally coordinated by the smart contract app. Doctors spend less time discussing demands for medications or speaking directly to drug stores during a patient's visit.

As shown in Figure 4.4. data flow for the issuance of a medical prescription includes patient, primary doctor (GP), and pharmacy. It also contains prescription details which would include the medicine Id, date of expiry and patient Id.

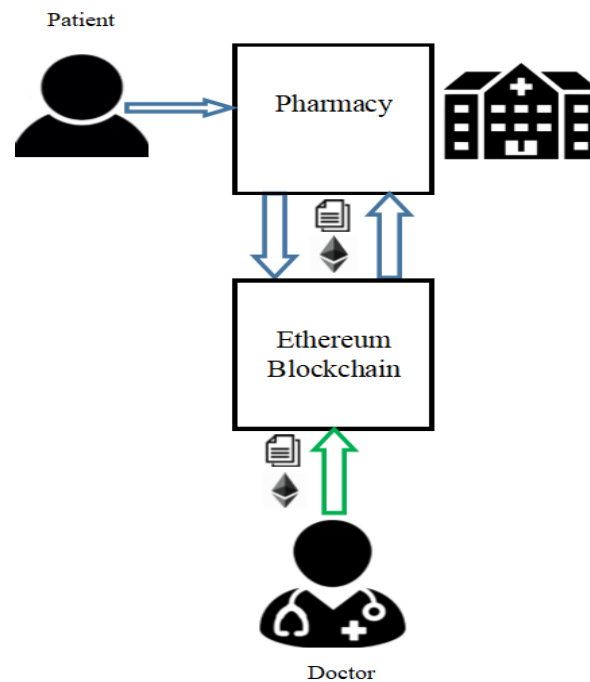


Figure. 4.4 The Smart contract for issuing and filing of medical prescriptions. Reprinted with permission from Khatoon, A., Electronics 2020, 9(1), 94.

4.3.2 Laboratory Test Results

The main goal is to share the information through smart blockchain contracts by allowing laboratories, doctors, emergency clinics and different parties involved in the system to effectively access and share the therapeutic information of a patient among different stakeholders as shown in Figure 4.5.

Here we consider a use-case in which a patient has to visits a blood test laboratory. After processing, the laboratory will put the outcomes into the patient records, the patient receives these information updates via Ethereum blockchain, a notification that now the test's processed results are available, and can either choose to enable the laboratory to encode the relevant information and place it on Ethereum blockchain. The patient grants approval to post the details on the blockchain. In the case of an emergency with the patient where he is unconscious, the emergency department may easily access patient details through Ethereum blockchain and provide personalized care.

By having allowed patient records to be posted on healthcare blockchain, a patient avoids having to either carry the laboratory results on their own or arrange for records to be faxed to various care providers. He also makes sure all of his health care professionals have the knowledge available to deliver the best medical treatment. Laboratories minimize printing

and mail or fax regulatory expenses for each test result to singular distributors. In addition, laboratories and patients have access to the healthcare blockchain, where they may obtain installments from protective firms advising the transferred information to process claims or from pharmaceutical organizations selecting the information to be used in contemplates. Consultants and emergency departments have free access to gather restorative information about their patients, reducing authoritative research and costs.

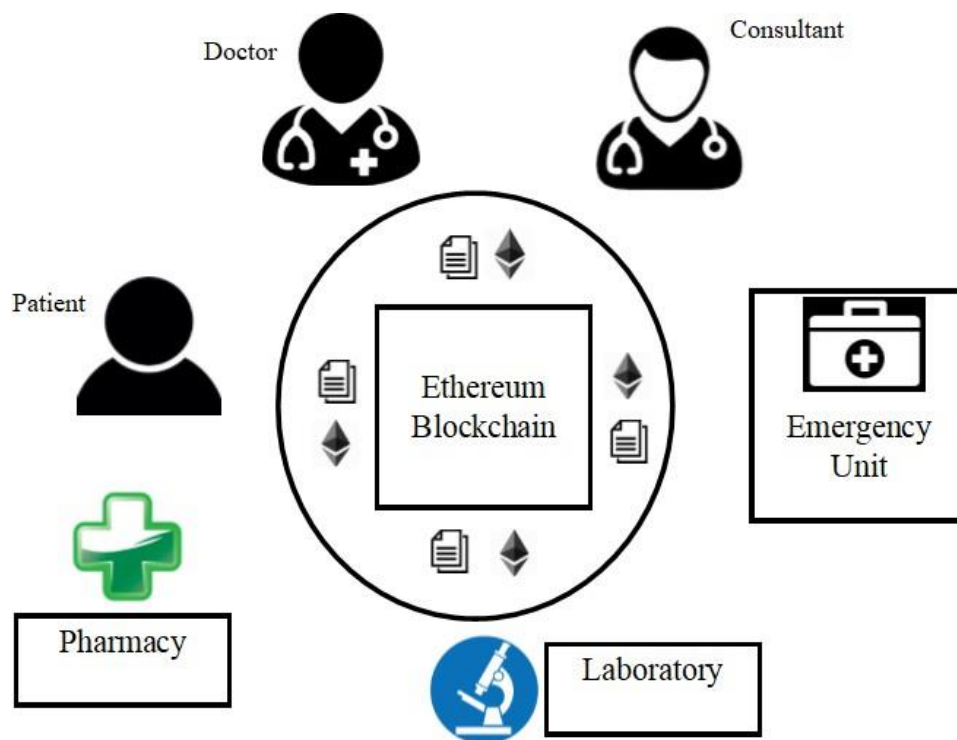


Figure. 4.5 Smart contract for sharing lab results. Reprinted with permission from Khatoon, A., Electronics 2020, 9(1), 94.

4.3.3 Communication between Patients and Service Providers

Under this use-case, as seen in Figure 4.6 the patient submits an application for a medical condition. It automatically adds that request through the smart contract system to the primary doctor. A doctor must consider the request and respond with a recommendation, and, where appropriate, refer the patients to the specialist for further care. Any patient information regarding treatment history should be reported on the EHR. Please note that patient records are maintained by a local database, where there are specific rules that can access the record to what extent and to what extent these rules are governed by the Ethereum blockchain smart contracts.

Another case in which the patient submits an application for a particular medical procedure. Accordingly, the strict structure of the agreement sends this application to the appropriate specialist. A doctor acknowledges the demand and respond appropriately with a recommendation, and where patients are forwarded with the specialist for further care. Any patient information about treatment history must be recorded on the EHR. Notice that a local database holds patient records where there are clear rules which can approach the record to what degree and how well these guidelines are implemented through the competent Ethereum blockchain contracts.

Patients who are seeking health information on a particular topic receive recommendations that are much more customized than those offered by a web search. Senior doctors are finding a new way to monetize their experience without having to overbook their schedules, whereas junior doctors can enter a new potential customer audience and develop their brand within their specialization. Payments motivate patients to receive Junior Physician recommendations.

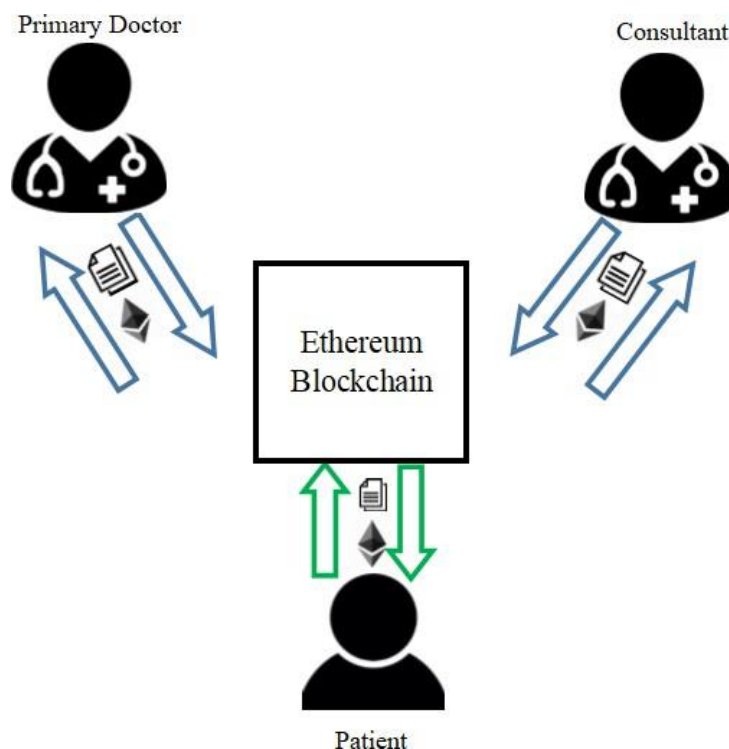


Figure. 4.6 Smart contract for enabling communication between patient and service provider. Reprinted with permission from Khatoon, A., Electronics 2020, 9(1), 94.

4.3.4 Healthcare reimbursement

The main aim is to speed up the reimbursement process for the medical healthcare system. In this, doctors will be able to continue to proceed with treatment quickly, instead of having to put their patient's treatment on hold while waiting for the payer to respond. Automated smart contract execution will supervise the entire process. Reducing-and eventually eliminating-the human effort to manually monitor and respond to inquiries for prior authorisation, and reducing appeals caused by misinterpretation of manually written prior authorisation forms.

Health Insurance Companies posts its policies through smart blockchain contracts which contain the policies used to ascertain authorization. A supplier then lodges a request for prior authorisation for a consultant appointment, treatment or prescription via Ethereum blockchain network. The payer's smart contract for a health policy automatically decides authorization using the patient's medical details processed by Ethereum blockchain and the request details. Authentication data are then immediately returned to the provider. Further, the patient, as well as any laboratories, pharmacies, specialist doctors and other stakeholder's involved in the system to whom the patient has delegated access, will also verify the authorization for insurance in real time. The whole process can be seen in Figure 4.7.

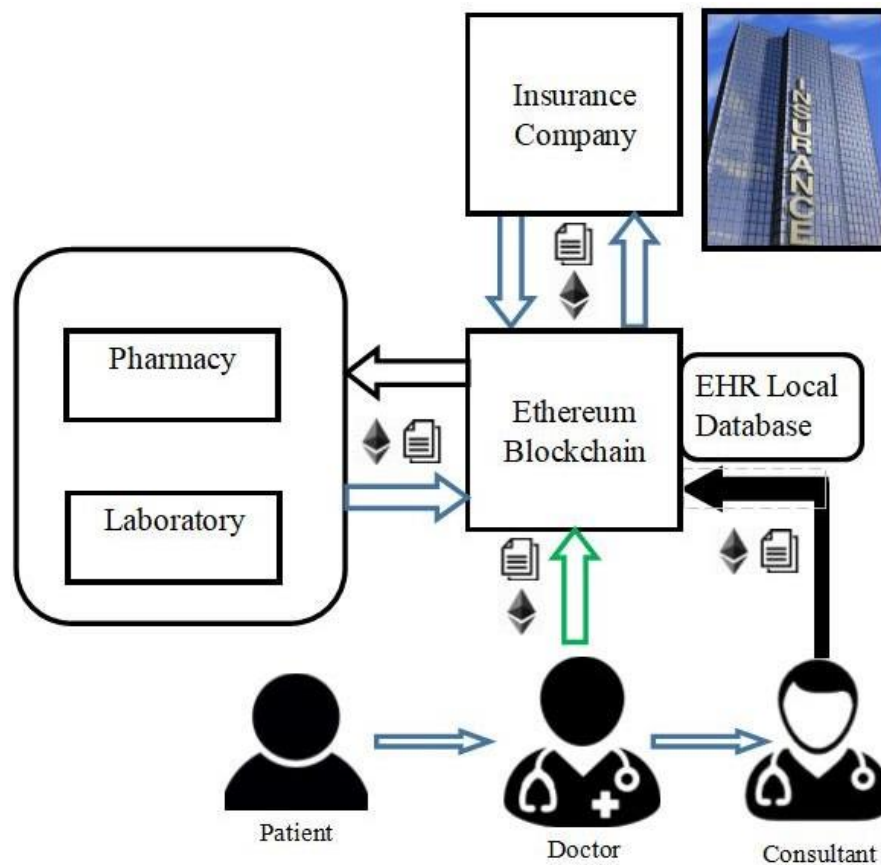


Figure. 4.7 Smart contracts for healthcare reimbursement. Reprinted with permission from Khatoon, A., Electronics 2020, 9(1), 94.

The automated prior authorisation process will result in considerable cost savings for payers, which already spends large sums on manually monitoring and responding to requests. Doctors can proceed with treatment quickly, rather than having to stop their patient's care while waiting for the payer's response. In fact, patients will be spared concerned about how their insurance will cover the medication their doctor recommends. With instant prior authorisation information available, doctors and patients can work easily with a care plan specially tailored to the patient's needs and adequate medical insurance coverage.

4.3.5 Ethereum Blockchain contracts for clinical trials

Providing healthcare, medical technology manufacturers and all the multiple stakeholders involves in the system throughout the processes of initialization, verification and validation of a trial with a quicker and more cost-effective alternative to the existing recruitment in the process of conducting clinical trials. This will also entails substantial expenditures in

purchasing patient contact information from independent data suppliers and carrying out extensive pull-marketing campaigns.

The main objective is to allow users to run clinical trial-related smart contracts on an Ethereum network leading to safer medicines and increased public interest in medical research. We will handle metadata in this process including protocol registration, pre-set study information, screening and enrolment logs through smart contracts.

A pharmaceutical company is searching for metadata stored on the Ethereum blockchain to identify possible patients for clinical trial inclusion as shown in Figure 4.8. The organization then sends a letter, including an application to read access to their medical records, to selected patients, including any related laboratory test results. If the patient provides access, a pharmaceutical company bill will be processed via smart contracts, awarding the patient part of the fee paid, and another portion to the laboratories which recorded the patient's correct test results.

Drug and medical device manufacturers will significantly reduce spending on data purchases and marketing efforts through direct targeting of qualifying customers. Patients, meanwhile, will gain access to alternative care options, in addition to obtaining compensation for engaging in trials. Laboratories responsible for delivering results would have a new way to monetize their data. The whole clinical trial processes includes different parties such as Review Board, FDA, Sponsor, Primary Investigator and lab scientist throughout the process.

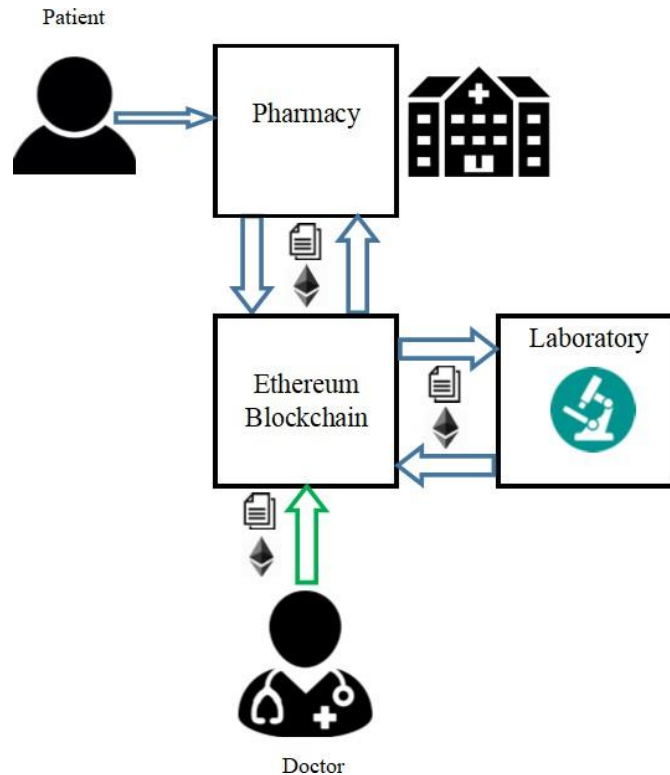


Figure. 4.8 Schematic diagram of Smart contracts for conducting clinical trials. Reprinted with permission from Khatoon, A., Electronics 2020, 9(1), 94.

4.3.6 Surgical procedure via smart contracts

In a busy clinical process, the procedure associated with surgery can be a huge burden. The EHR Surgical Workflow System addresses the needs of busy practices and converts a dynamic process into a simplified, all-in-one workflow. The practice could be fully integrated with EHR Surgical Workflow system via Ethereum blockchain smart contracts. This also allows administrators, billing, front desk operations, and other tasks to accomplish things from pre-operative medication care to post-operative patient management to support the overall workflow. Then, the details are seamlessly inserted into the patient's prior surgical record. Patient consent taking and initial assessment of the patient could be recorded through the smart contract features. Our process workflow consists of different activities associated throughout the patient surgery process. This requires pre-approval, medical certification, scheduling of surgical operations, pre-operative testing and consent to record. The visit is documented in the process, and treatment is registered and compensated. This would be useful

in revising the past surgical cases or the cancelled surgical procedures. Figure 4.9 and Figure 4.10 respectively display algorithmic workflow and the solidity smart contract components.

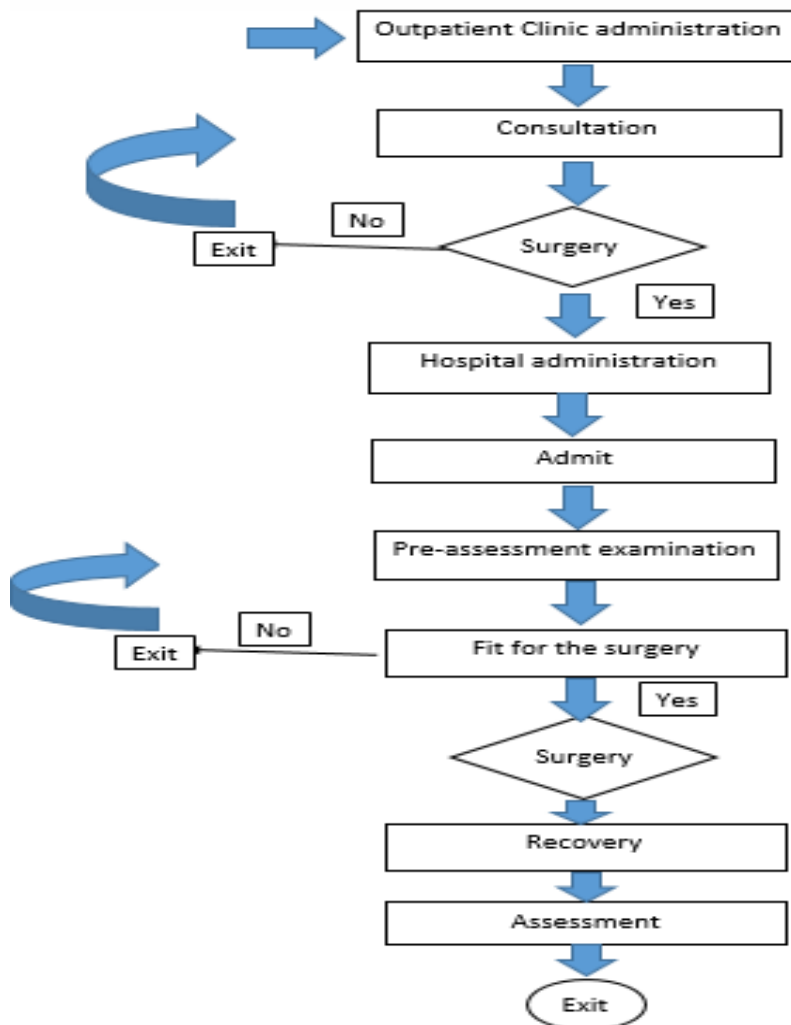


Figure. 4.9 Algorithmic workflow for a smart contract with surgery patients. Reprinted with permission from Khatoon, A., Electronics 2020, 9(1), 94.

```

1 //Contract Surgery
2 pragma solidity ^0.4.18;
3 contract Surgery {
4     address [] public consultant;
5     bool [] public consultantEnabled;
6     address [] public realtionships;
7     address public surgicalteam;
8     bool public sugicalteamEnabled;
9     address public patient;
10    bool public patientEnabled;
11    address public anesthesiologist;
12    bool public anesthesiologistEnabled;
13    modifier isowner () {
14        bool enable;
15        if (agentEnabled && msg.sender == agent) enable = true;
16        for (unit i = 0; i < consultant.length; i++) {
17            if (consultantEnabled[i] ) && msg.sender == consultant[i]) {

```

Figure. 4.10 Smart contract surgery.

4.4 Cost estimation

In terms of setting up and deploying a medical blockchain, an estimate of the costs associated with deploying smart contracts for healthcare needs to be made. The ultimate aim is to develop a program with all the advantages of blockchain that can offer a feasible electronic health system. In Ethereum blockchain, all programmable computations and calculations cost some sort of fees to avoid network abuse and to resolve other computational related problems. The fee is listed as gas in Ethereum blockchain to run all kinds of transactions. Gas in the Ethereum blockchain network refers to the payment or price value necessary for a successful transaction or contract execution on the Ethereum blockchain platform. The exact and accurate gas price is determined and calculated by the miners of the network, who could refuse to validate a transaction if the gas price does not meet their limit. All operations running on the Ethereum also including computations, message calls, smart contract creation / deployment and storage on Ethereum Virtual Machine (EVM) therefore require gas to perform all of these multiple tasks. To perform transactions on Ethereum virtual machine, if anyone wants to do some kind of activity on EVM, they must have unique amount of gas in their account. With any transaction there is a gas cap, and if there is any remaining gas it will return to the user account after the transaction has been completed. If a user has no valid balance account, he is unable to carry out any type of operation and is therefore considered invalid. In EVM Ethers, gas is purchased and the users on the network running the transactions can set their account gas limit for that particular transaction. But then again if they tend to approve and endorse the transaction or not, it is on the miner again. When a sender wants low gas price, charging for the gas will cost them high price and miners would be able to get great value and would be rewarded for the transactions. A miner then performs the computation to add that transaction to a block. A miner can then transmit the new block to the network after the successful execution of transactions. The gas utilizes during the broadcasting of smart contract depends on how complex the function of that specific smart contract is and also the number of stakeholders and interaction involved in the system.

4.5 Validation of the workflows with HSE datasets

We have used our smart contract workflow processes built to estimate the cost of implementation using actual healthcare datasets which we have taken from HSE Ireland. In ethereum, details of the blockchain transaction can be seen in Figure 4.11. The datasets are described in section A. In section B, using the actual datasets, the cost of deployment is calculated and plotted for different factors.

4.5.1 HSE Dataset

Datasets have been taken from the Health Service Executive (HSE) Ireland from their different archive system (<https://data.ehealthireland.ie/>) [138]. The Health Service Executive is responsible for delivering public funding for all people living in Ireland to the health and personal social services. In this work, all the outpatients, the waiting list of hospitals across different departments / hospital in Ireland were considered to be used. The waiting lists for the outpatient, hospital and day cases are managed by the National Treatment Purchase Fund (NTPF) from data collection to its validation phase. The OP's Waiting List study reveals the cumulative number of patients waiting for a first consultation appointment at a consultant-led outpatient clinic in the different time ranges. Each individual report is composed of the numbers waiting in each specialty per hospital. The numbers were aggregated under a 'Small Volume' heading to protect the confidentiality of individuals where < 5 patients are waiting in a particular specialty / hospital. All reports consist of monthly data over the course of a year.

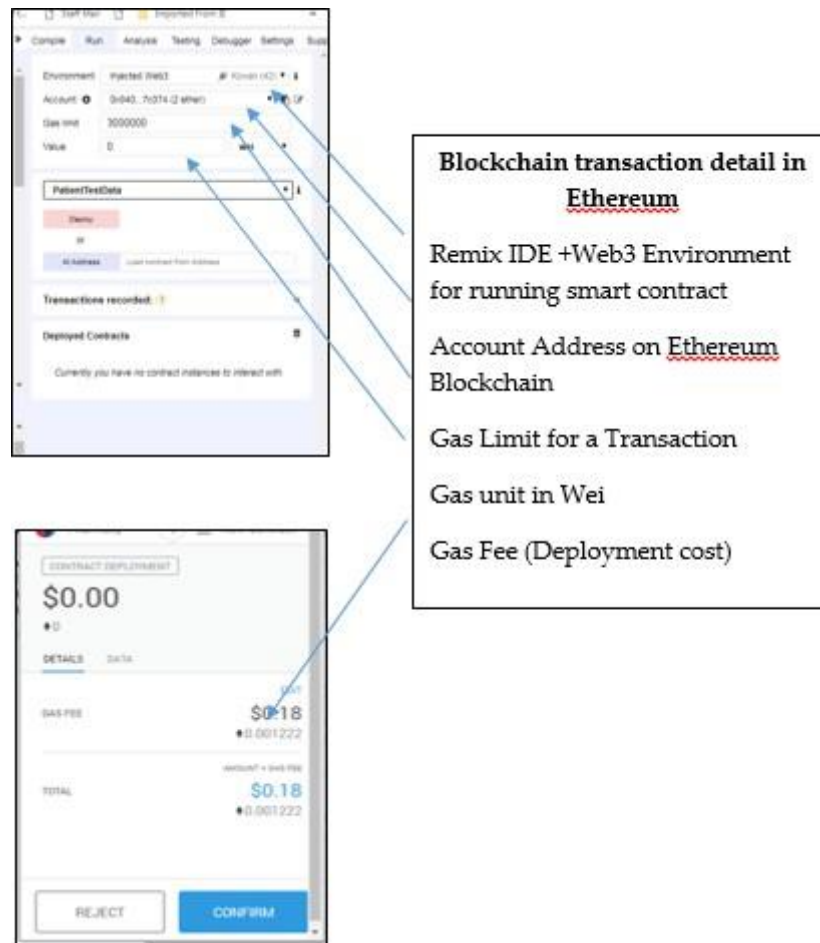


Figure. 4.11 Metamask extension for calculating smart contract cost.

The cost of creating, deploying and running of a smart contract needs ethers as a gas as seen in the figure 4.11. Whenever we need to broadcast a transaction on the network it needs a gas which can be measured in wei units. We are paying for the gas needed to run the transaction and function of a smart contract on the ethereum blockchain network via ethers using Metamask. MetaMask calls [eth estimateGas](#) on the Ethereum node. [eth estimateGas](#) basically measures the amount of gas used to run the transaction. It also depend on the block hash and block number that how much gas would be needed to run the specific smart contract transaction on ethereum blockchain.

Figure 4.12 below shows the county wise number of pharmacies, Figure 4.13 shows the number of transactions for different departments.

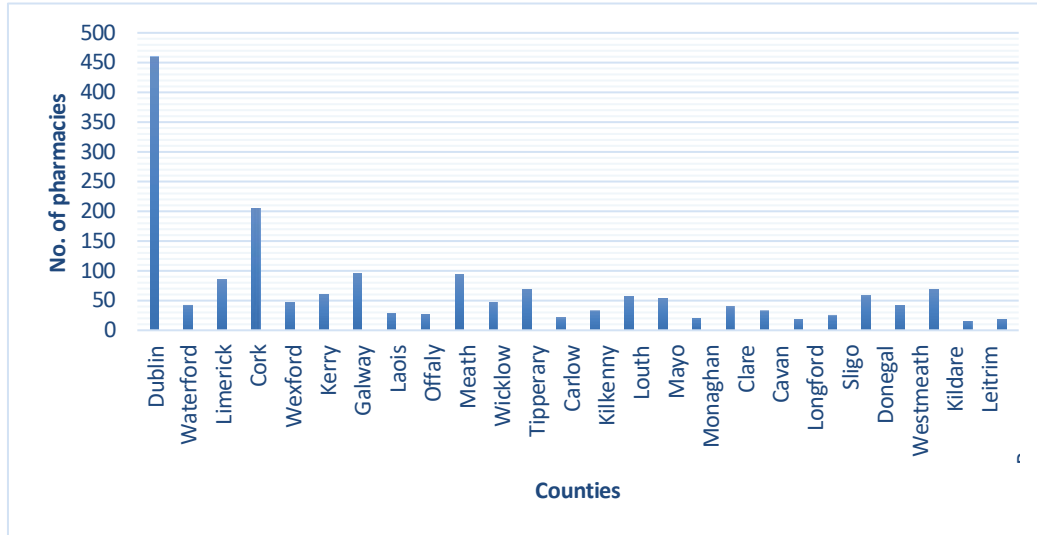


Figure. 4.12 Plot showing county wise pharmacy list from Ireland.

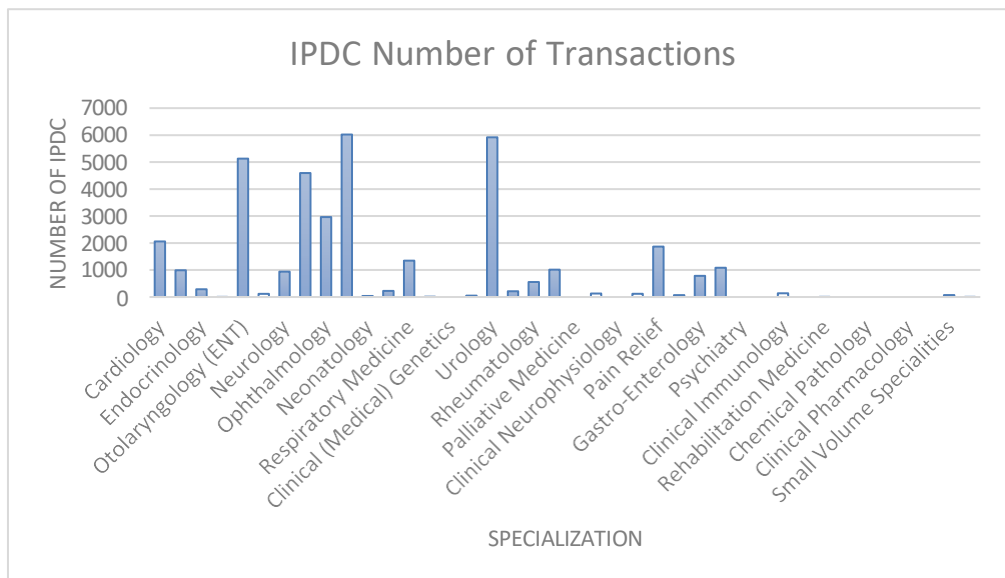


Figure. 4.13 Number of IPDC and their transaction across different departments/specialty.

4.5.2 Cost estimation using real datasets

The costs associated with implementing smart healthcare contracts need to be calculated in terms of the deployment of healthcare blockchain. The ultimate goal is to develop a system that will provide a sustainable electronic health network with all the advantages of blockchain. All

programmable calculations in Ethereum blockchain cost some fees to prevent network misuse and to solve other computational related problems. All activities, multiple computations, message calls, intelligent contract creation / deployment and storage on Ethereum Virtual Machine (EVM) therefore involves gas to perform all these certain tasks and activities.

The cost to deploy smart contracts for a healthcare management system has been compiled. There is cost known as Gas for running an operation on the Ethereum blockchain. All the transactions require 21,000 gas as the basic operational requirement. If a user interacts with Ethereum's smart contract, an additional gas associated with running and execution of those specific smart contract transactions will require 21,000 of the gas. The gas was compiled for medical smart contracts to enable contract deployment to communicate with the different contracts. More complex the smart contract functions / operations use more electricity, resulting in more fees. From the point of view of feasibility, it is very much clear and obvious from the results that the cost of smart contract deployment for healthcare management system is extremely low. As far as medical system is concerned, this expense is very affordable and everybody would like to pay this small charge to have control of their EHR and retain their medical data for life. Figure 4.14 indicates the expense of deploying smart contracts for each pharmacy, as our program estimates.

We have calculated the costs for patients in the general outpatients, paediatric clinic and surgical patients. The number of smart contract transactions and their related costs as calculated by our method are shown below in the Figures 4.14–4.29.

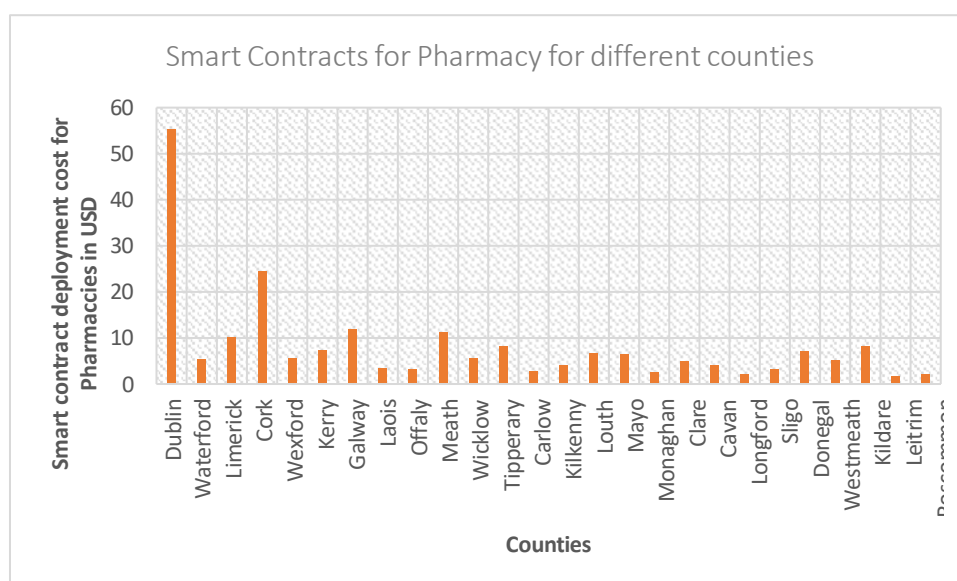


Figure. 4.14 Plot showing smart contract deployment cost for countywise pharmacies in Ireland.

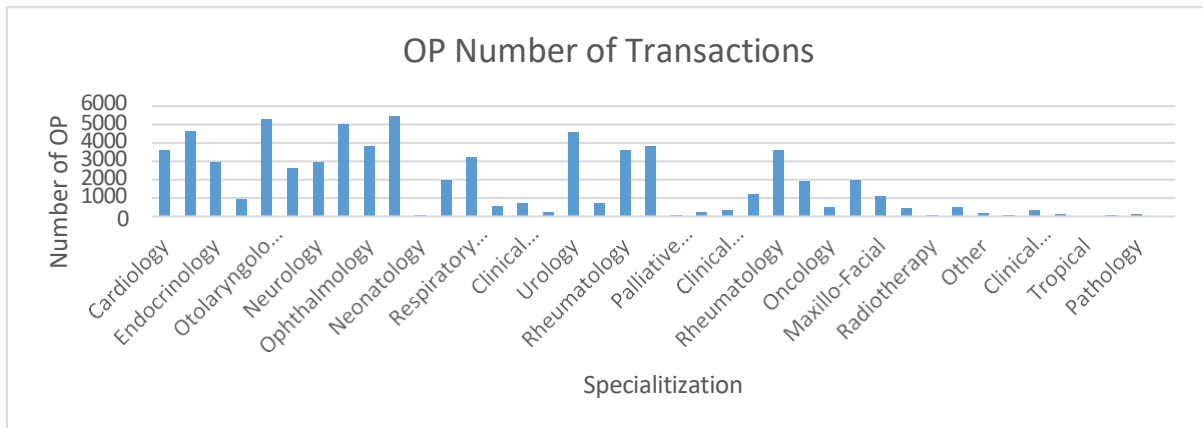


Figure. 4.15 Cost comparison among different smart contracts and entities.

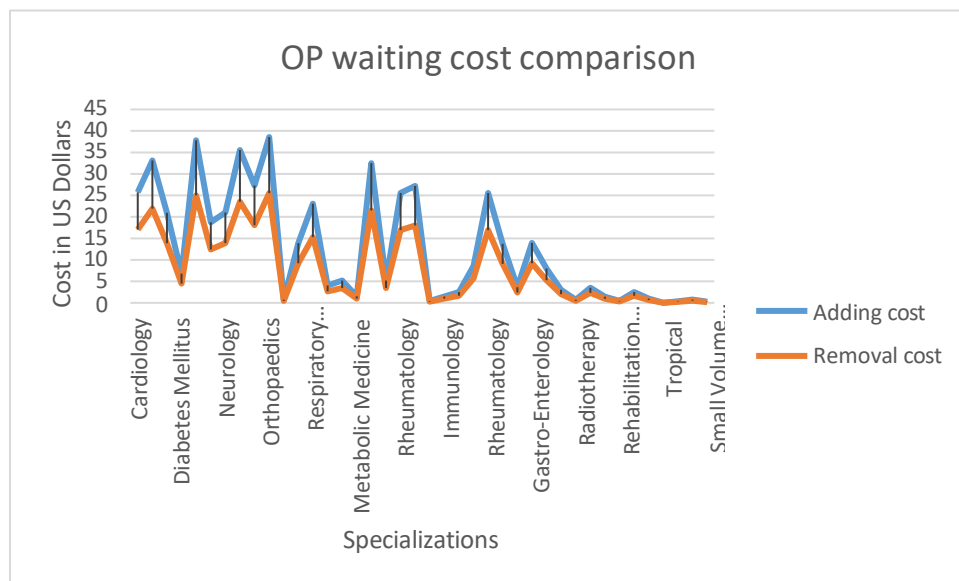


Figure. 4.16 Adding and removing entity cost for waiting list outpatients (OP) in the system across different departments/specialities.

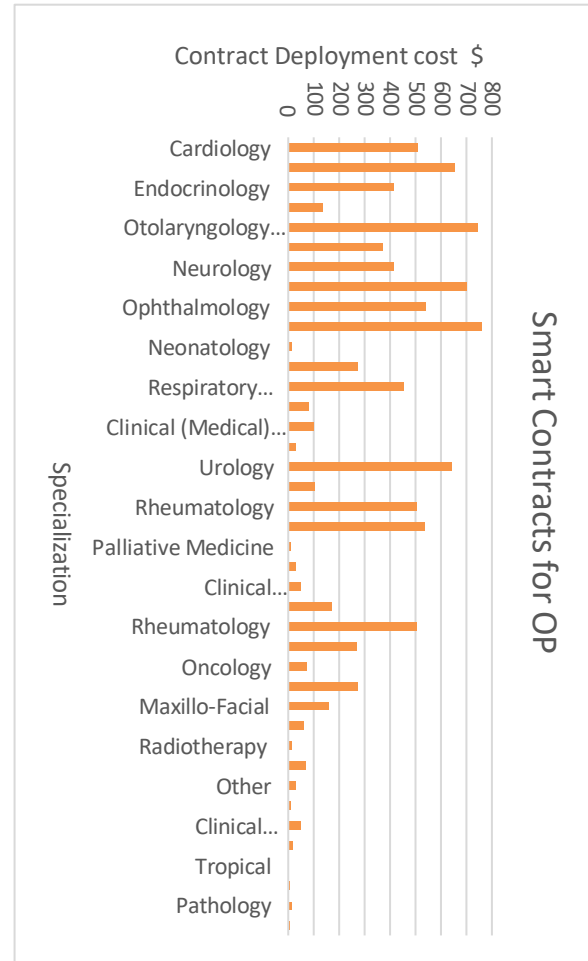


Figure. 4.17 Smart contract deployment cost for Outpatients (OP) across different departments/specialities.

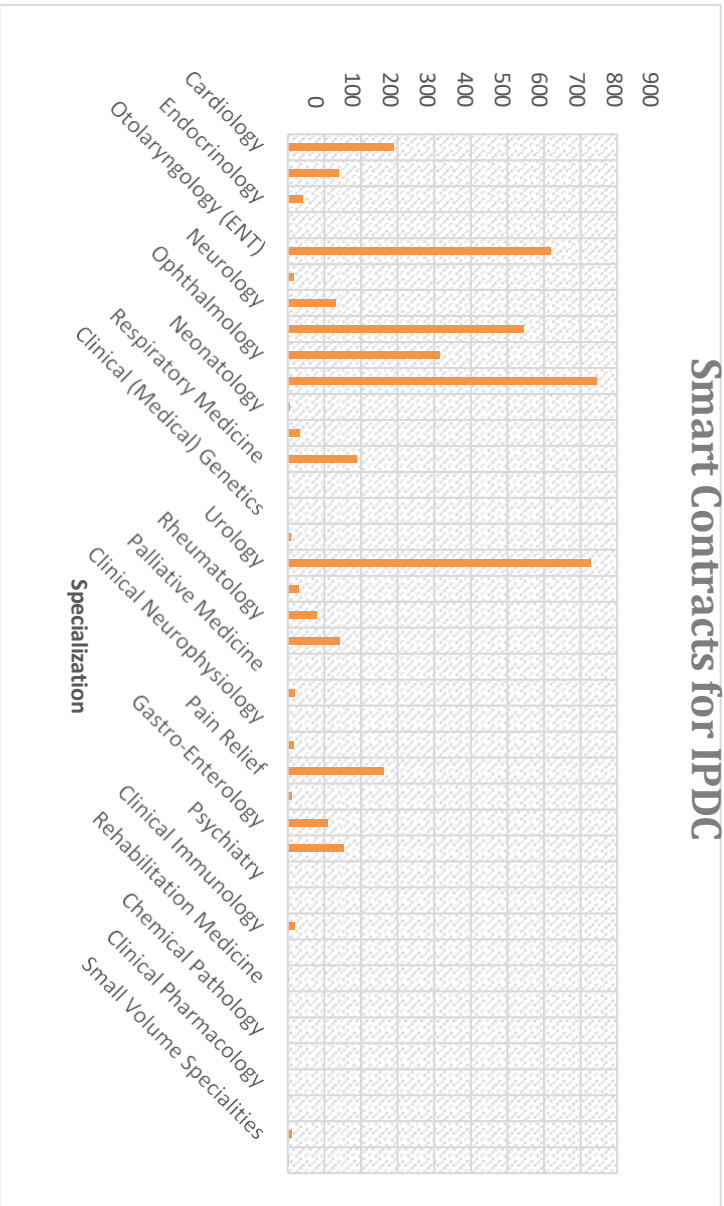


Figure. 4.18 Smart contract deployment cost for Inpatients and Day cases (IPDC) across different departments/specialities.

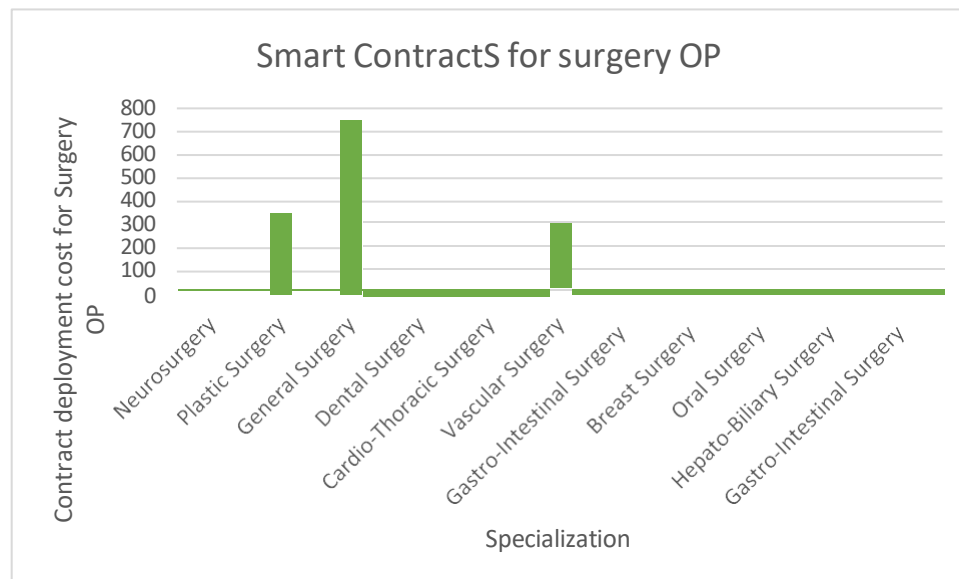


Figure. 4.19 Smart contract deployment cost for surgery outpatients across different departments/specialities.

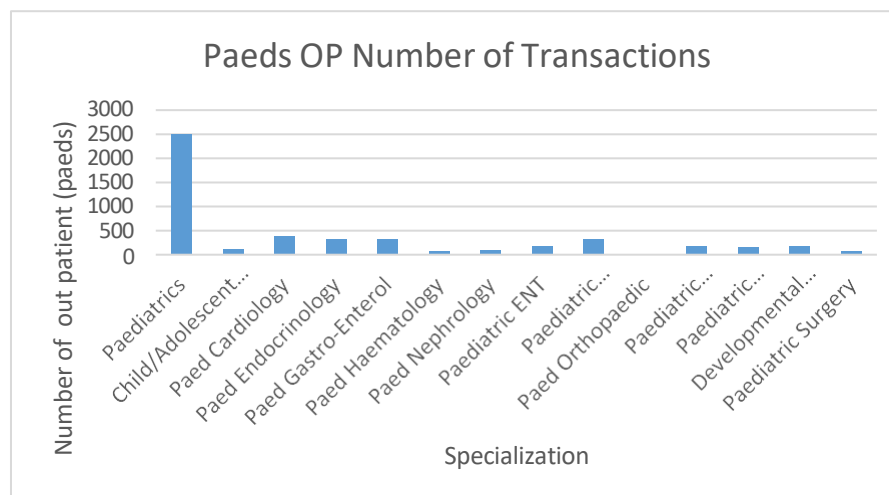


Figure. 4.20 Number of paediatric outpatients (OP) and their transaction detail across different departments/specialities.

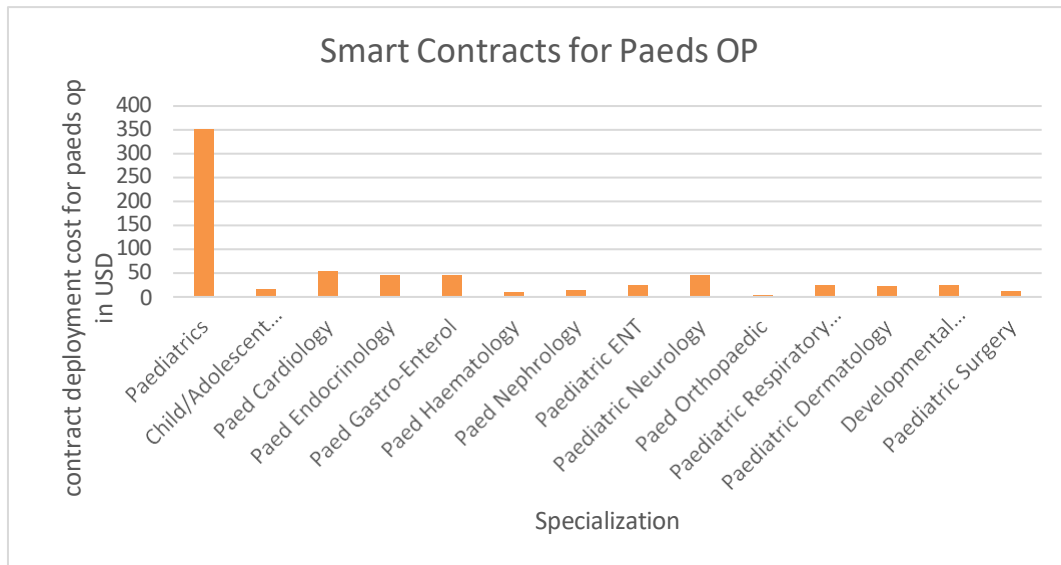


Figure. 4.21 Smart contract deployment cost for paed outpatient (OP) across different departments/specialities.

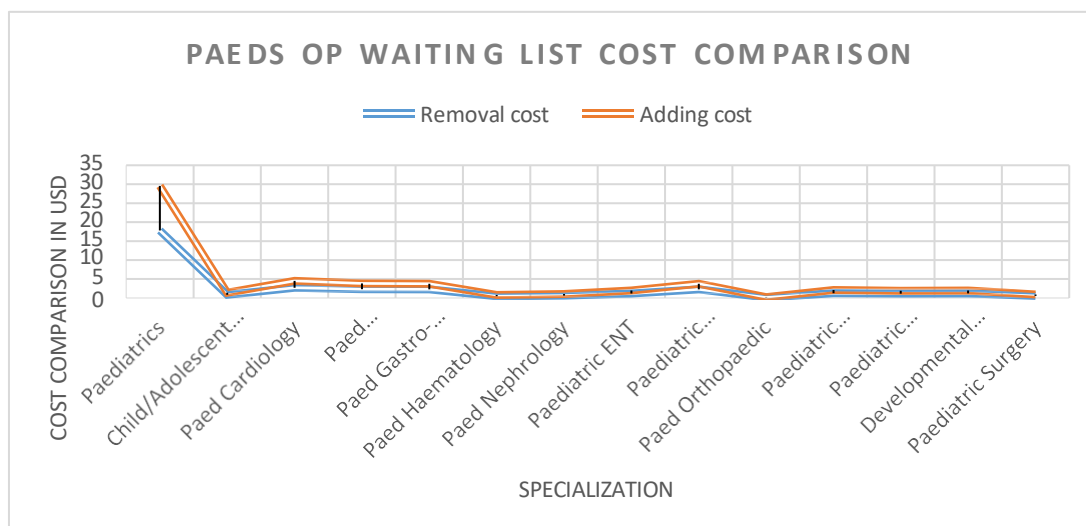


Figure. 4.22 Adding and removing entity cost for Paeds outpatients (OP) in the system across different departments/specialities.

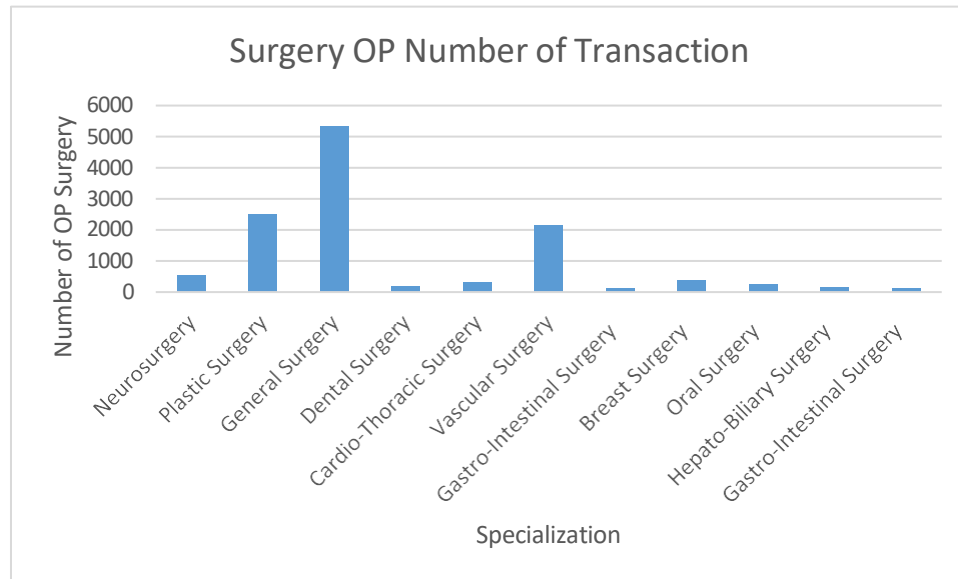


Figure. 4.23 Number of Outpatients (OP Surgery), smart contract deployment and their transaction detail across different departments/specialities.

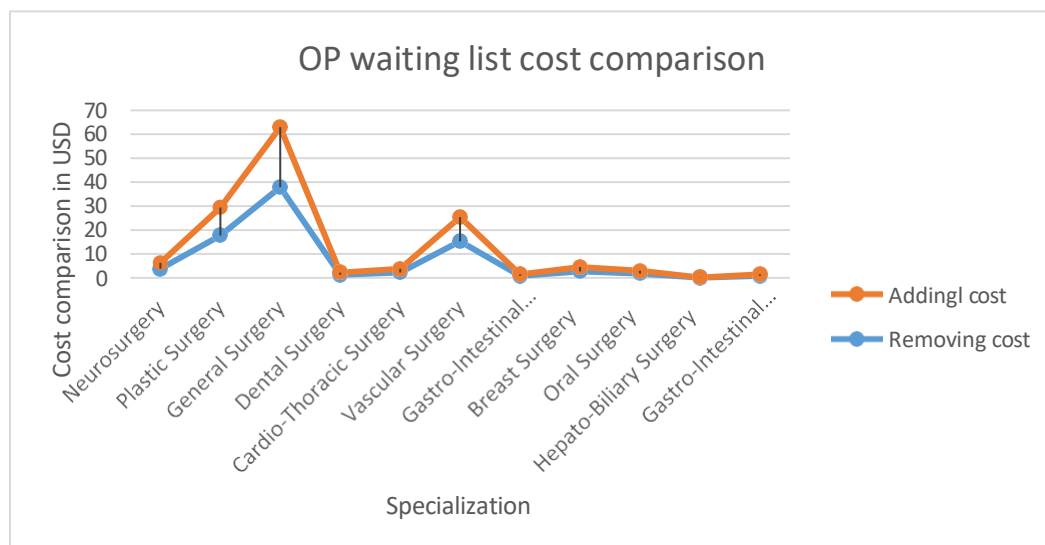


Figure. 4.24 Smart contract deployment cost comparison for Outpatients (OP Surgery) across different departments/specialties.

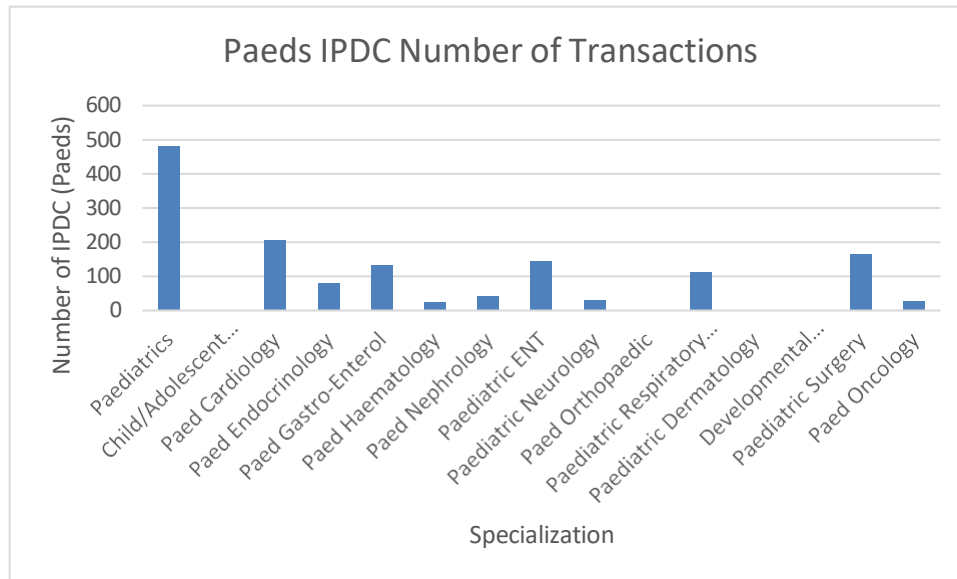


Figure. 4.25 Smart contract deployment cost for Inpatients and Day cases (IPDC Paeds) and their transaction detail across different departments/specialities.

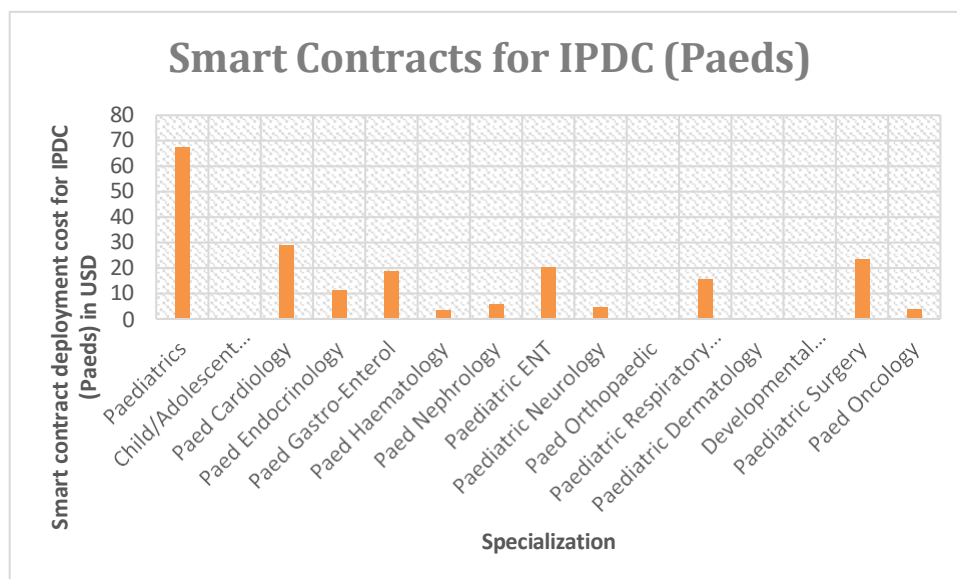


Figure. 4.26 Smart contract deployment cost for Inpatients and Day cases (IPDC Paeds) across different departments/specialties.

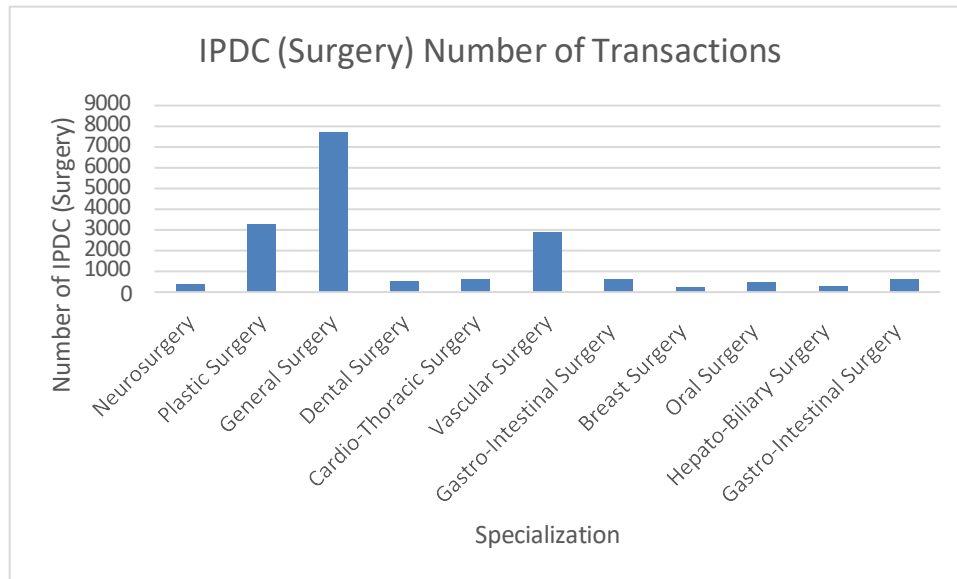


Figure. 4.27 Smart contract deployment cost for Inpatients and Day cases (IPDC Surgery) and their transaction detail across different departments/specialities.

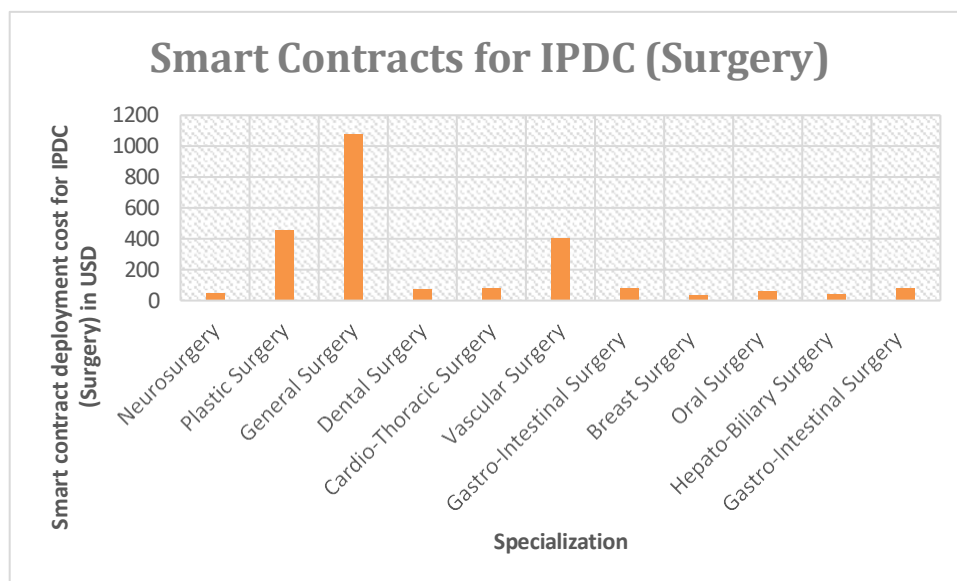


Figure. 4.28 Smart contract deployment cost for Inpatients and Day cases (IPDC Surgery) across different departments/specialities.

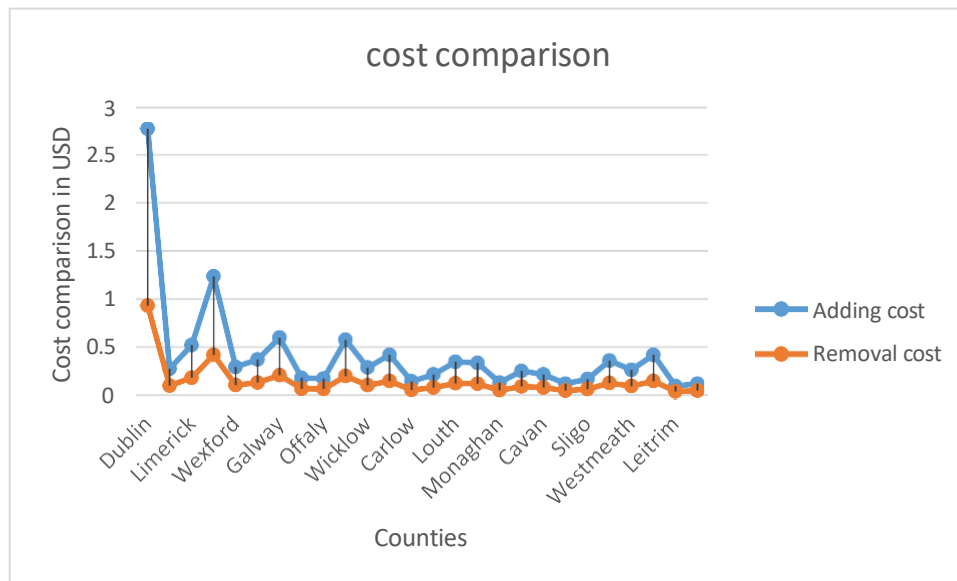


Figure. 4.29 Smart contract deployment cost for adding and removing of an entity across different counties.

4.6 Discussion

It is very well known that all patient records in conventional healthcare delivery models and systems, suppliers, labs, payers (i.e., insurance firms) and drug companies are held in various formats, so there is not at all standardization of the record keeping. This has contributed a lot to data breaches and the disarray we see in health information sharing today. Impoverished data-sharing infrastructure has also impeded advances in the drug discovery and public health research investigations and findings. Efforts to tackle this problem have primarily been focused on pushing a new universal standard around the ecosystem. These such attempts were unsuccessful, as they were quickly rejected by regulation, lobbying, and patient apathy. Owing to the lack of efficient collection and sharing of health data, the widespread acceptance of the concept of adjusting medical care to a patient's characteristics, desires and aspirations has been prevented. Personalized medicine and adequate treatment – or precision – has long been recognized as the future of healthcare, and industry operators have dedicated substantial resources to developing personalized healthcare opportunities, only to be stymied by the present system.

In this chapter, we have discussed the current needs, trends and requirements of the healthcare industry, the shortcomings of the present system, and given Ethereum-based

solutions for efficient healthcare management. Giving an overall overview of the state of the art personalized medicine, explaining the underlining issues with the existing healthcare system that hinder the introduction of personalized medicine and demonstrating how our built program provides solutions to these problems. We have also analyzed and calculated the practical cost of deploying smart contracts system for different health care scenarios and workflows, and found that with outpatient numbers the cost increases linearly. Health care departments such as paediatrics and general surgery costs are higher than others for these reasons.

4.7 Conclusion

Using the blockchain distributed technology, our blockchain based smart contract for healthcare management framework has shown how the concepts of decentralization can be applied to a large-scale data processing in medical environments and to expedite complex medical procedures. We demonstrated a revolutionary approach to the handling of medical records, offering traceability, connectivity and openness of the system through smart contracts. This program is structured to document consistency and granularity and allows for the exchange of patient data and opportunities to help the medical research program. We've suggested and designed possible applications of blockchain technology in health data management. From a medical perspective we have implemented a healthcare data management and sharing system based on the specified requirements in the medical eco-system. It is possible to ensure the utilization of blockchain technology, anonymity, protection, availability and fine-grained control of access to EHR data. The main aim of using blockchain as explained in this chapter is to improve the medical processes, and thus also improve the patient outcomes. Blockchain can help in many ways; reduce transaction costs by using smart contracts incorporating protocols for general purposes to simplify procedures, reduce administrative burdens and eliminate intermediaries. Many projects on blockchain are aimed at improving data collection, usage and exchange of health data from patients, researchers and sub-processors. Our proposed framework uses blockchain technology to build a system based on automated, distributed, stable, open and to provide a decentralized health-care ecosystem. This will encourage patients to freely and securely exchanging their medical records with physicians, hospitals, research organizations and other stakeholders involved in the system while maintaining absolute authority over the confidentiality of their medical healthcare data.

5 Blockchain Implementation of Ethereum Smart Contracts

In the blockchain research there are very few implementations of Blockchain-based smart contract systems. This practical aspect is considered in this chapter, while giving detailed description of the implementation of smart contracts that we introduced in chapter 4 of this thesis. The exchange of electronic medical data among different stakeholders in the healthcare eco-system, such as patients, physicians and researchers, will encourage greater and efficient integrated healthcare infrastructure. In order to make this possible we implemented a system for exchanging medical information based on permissions control mechanism over Ethereum blockchain based smart contract and different bits of information is being shared among various stakeholder of the system. All the healthcare information resides in the local database, and permission-related information has been stored on the Ethereum blockchain smart-contracts. In this chapter, implementations of smart contracts using Ethereum and Solidity are presented along with explanation of the code structure which are designed to automate the medical regulations. Also different workflows involving multiple stakeholders have been discussed. Structures of smart contracts are discussed in detail which shows the potential within a clinical data research network for managing data queries involving different workflows. Our proposed blockchain solution for health care extends the collection of clinical data to include data from groups of persons currently under-served by the health care system. The open data architecture of Blockchain makes the participation of "tricky-to-reach" users simpler, and more accessible for the general public.

5.1 Medical Smart Contract System

Here, we are taking the issuance of medical prescriptions as a first step to go into the implementation details of the system. A process diagram for issuing medical prescription has been shown in Figure 5.1, showing a medical prescription imitated by smart contracts. It is meant to be designed as so that the programmable components can be added a system, allowing for issuing and collection of a medicine, with expiry dates and patient ids.

Also very helpful in investigating the adverse effects of the drugs. There are three main parties involved in the system as doctors, patient and pharmacy, each of them having different permission access rights on the ethereum blockchain network.

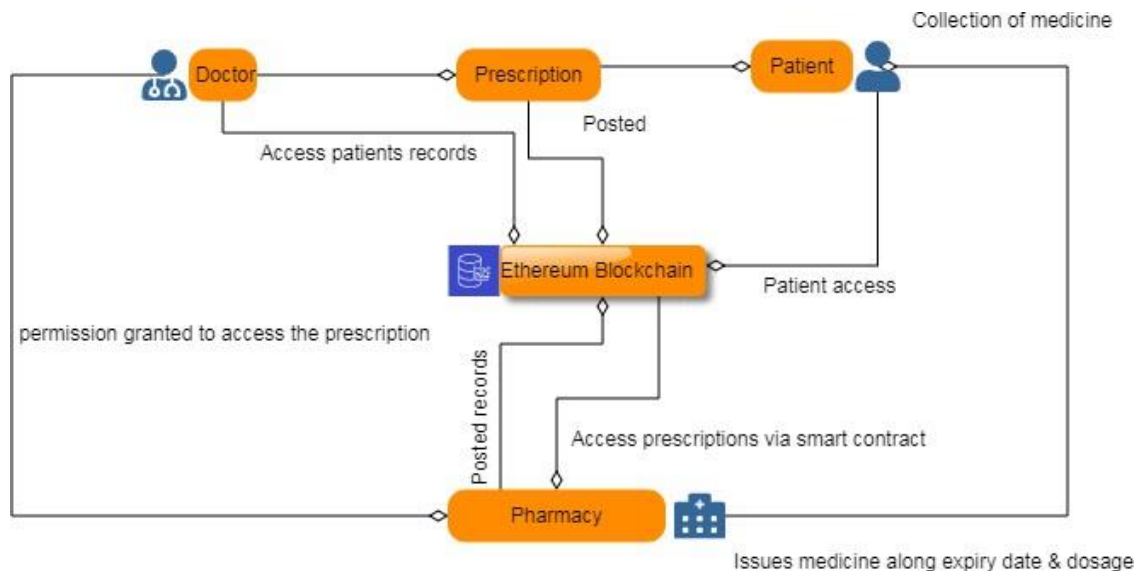


Figure. 5.1 Process flow diagram for issuing a medical prescription via smart contract.

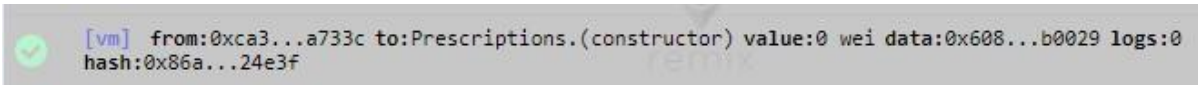
We are using Ethereum platform and wrote the smart contracts using solidity programming language. After compiling the code, we deployed and executed the smart contract code on the ethereum blockchain platform. Figure 5.2 shows a smart contract pseudo code for the issuance of medical prescriptions written in Solidity and executed on Ethereum which corresponds to the particular instance represented in figure 5.1.

```

1 Medical Prescriptions
2 pragma solidity ^0.4.15; //Version of a solidity, we are using
3
4 contract Prescriptions { // initialization of a smart contract
5 //Mapping referred to hash tables (initialized virtually)
6 // addresses referred to Ethereum address
7     mapping(address => bool) patients; // Mapping for the address to the patients
8     mapping(address => bool) GP; //Mapping for the address to the doctors
9     mapping(address => bool) Pharmacy; //Mapping for the address to the producers(pharmacy)
10 // structure for the Medicinebox; it holds expiry date, medicine id, dosage variables
11     struct MedicineBoxDef {
12         uint medicineboxId;
13         uint usedBeforeDate;
14         bool isUsed;

```

Figure 5.1 Pseudo code showing different stakeholder and their mapping addresses



```
[vm] from:0xca3...a733c to:Prescriptions.(constructor) value:0 wei data:0x608...b0029 logs:0
hash:0x86a...24e3f
```

Figure 5.2 Function executed with no error and the transaction has been successfully completed and the event happened

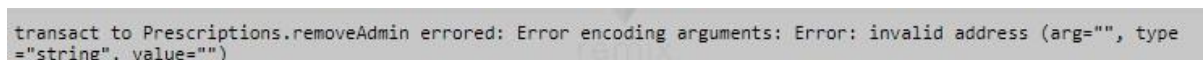
status	0x1 Transaction mined and execution succeed
transaction hash	0x6350ad3c42c6bb1f5c07e50b29c64363c85f610486868fe0448d46dcf4475f8f
contract address	0xdc04977a2078c8ffdf086d618d1f961b6c546222
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Prescriptions.(constructor)

Figure 5.4 Transaction mined and execution succeed as the testing modifiers where a function has been executed with no error as the required stakeholder was the assigned actor

gas	3000000 gas
transaction cost	882658 gas
execution cost	626794 gas
hash	0x6350ad3c42c6bb1f5c07e50b29c64363c85f610486868fe0448d46dcf4475f8f

Figure 5.5 Contract Execution cost shown in the figure upon the successful completion of the transaction

Testing modifiers: In Figure (5.6) function executed with no error as the required admin was the assigned actor while in figure (5.7) error appears when an intended actor has an invalid address



```
transact to Prescriptions.removeAdmin errored: Error encoding arguments: Error: invalid address (arg="", type="string", value="")
```

Figure 5.6 Function executed with no error

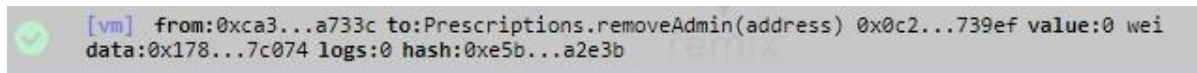


Figure 5.7 Error appears when an intended actor has an invalid address

5.2 Clinical Trials

A process flow diagram for conducting clinical trials have been shown in figure 5.8. Primary investigator initiate the study. FDA approves the application and gives approval of clinical trial. Sponsor create the contract and initiate the process. A more detailed description has been given in the previous chapter for the whole process. Algorithm 5.1 shows the clinical trial initiation process which involves number of steps as given below.

Algorithm 5.1: Clinical Trial process initiation

Input: Ethereum address of the patient and all the other stakeholders involved in the system

Process start, number of patients required, procedure protocols

If the application has been approve by the Investigational New Drug Authority

Then Allow the Input details to be included as valid transactions on the network

Initialization of the process = Access approved

End

else

Don't allow/accept unauthorized transactions

End

If Patient drop outs

Then Stop processing that further

Update the records

Notify/update the other peers in the network about the progress

End

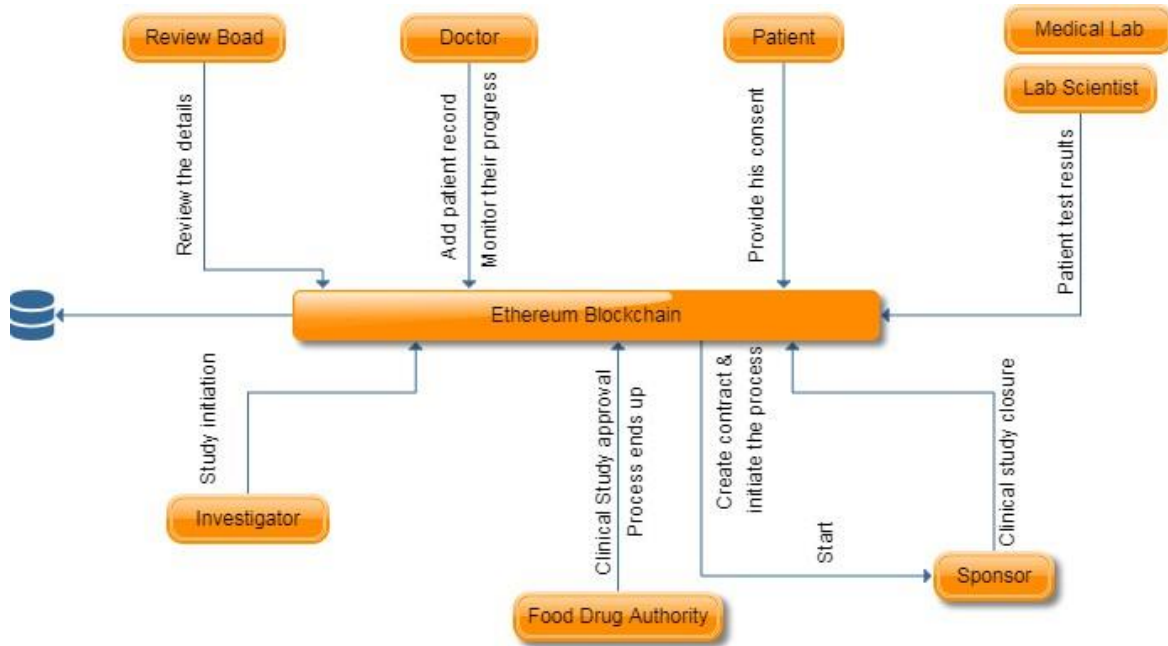


Figure 5.8 Process flow diagram for Clinical Trials

```

1 pragma solidity ^ 0.4.15; // Version of solidity, we are using
2
3 contract ClinicalTrials{ //Smart contract initialization
4
5     //mapping addresses of different participant involved in the process of Clinical Trials on Ethereum
6     mapping(address => bool) foodDrugsAuthority; // Mapping for the address to the food Drugs Authority;
7     mapping(address => bool) patients; // Mapping for the address to the patients
8     mapping(address => bool) RB; // Mapping for the address to the Review Board
9     mapping(address => bool) labScientist; // Mapping for the address to the lab scientist
10    mapping(address => bool) PrincipalInvestigator; // Mapping for the address to the Principal Investigator
11    mapping(address => bool) Sponsor; // Mapping for the address to the sponsor
12    mapping(address => bool) Doctor; // Mapping for the address to the doctor
13    address [] patientID;

```

Figure 5.9 Pseudo code showing different stakeholder and their mapping addresses for CTs

```

[vm] from:0xca3...a733c to:0xca35b7d915458ef540ade6068dfe2f44e8fa733c 0xca3...a733c
value:0 wei data:0x5da...0000 logs:0 hash:0x386...c26b8

```

Figure 5.10 Function executed with no error as the required admin was the assigned actor and the transaction has been successfully completed

5.3 Lab Test Results

A use case started when the patient visits a laboratory for the blood test. After all the processing, laboratory will put the patient results to his records via smart contracts access right given to them, the patient receives these notifications via Ethereum blockchain. A process diagram can be shown in the figure 5.11 explaining the whole process.

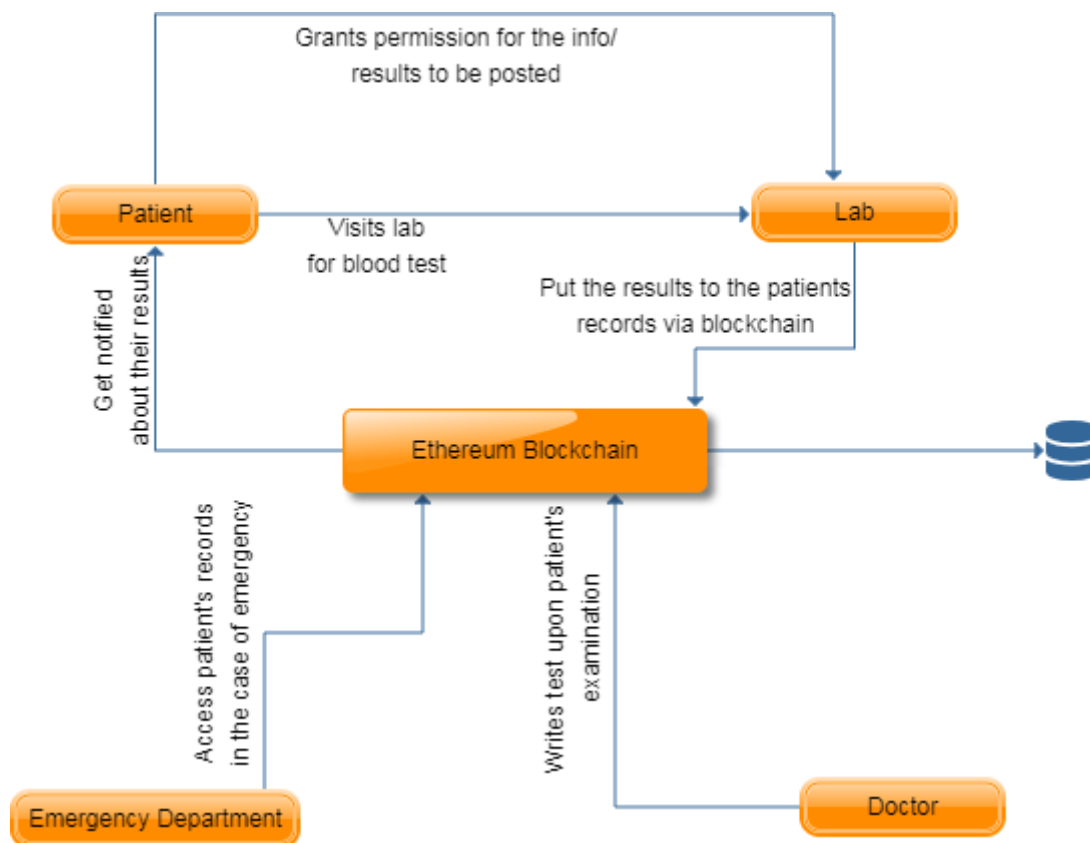


Figure 5.13 Process flow diagram for Lab Test Results

```

1 pragma solidity ^0.4.15;
2
3 contract LabResults{
4
5     mapping(address => uint[13]) Blood Test;
6
7     function setBloodResult (uint[13] memory bloodResults) public {
8         Blood[msg.sender] = bloodResults;
9     }
10
11     function getBloodResult () public view returns (uint[13] memory){
12         return Blood[msg.sender];
13     }
14
15 }
16
17 /*
18
19 Smart contract for storing test results data inside
20 the contract.

```

Figure 5.12 Pseudo code: Storing lab test results on the smart contracts

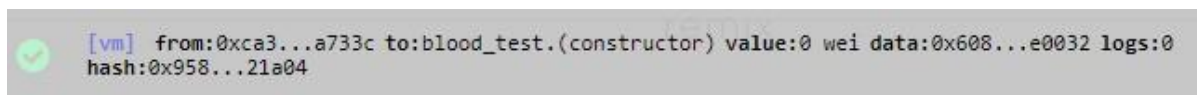


Figure 5.13 The event happened and the Function executed with no error hence the transaction has been successfully completed

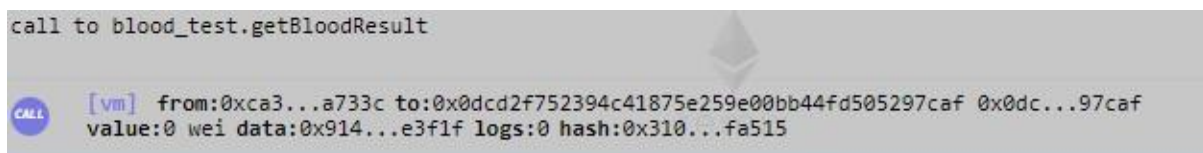


Figure 5.14 Call to the blood test for getting results, event happened and transaction successfully completed

5.4 Patient Consultant communication

To enable patient consultant communication and submitting a request for a medical condition. A process flow diagram has been shown in the figure 5.15. It starts with the submission request from patient for a specific medical treatment via Ethereum blockchain network. Primary doctor receives the request from the patient via smart contract on the network. After receiving the request, a primary doctor writes his recommendations and refer the patient to a specialist for further treatment via a blockchain. A consultant read those recommendation written by a

primary doctor and he proceed further with the further medication and treatment. Patient receives those recommendation via Ethereum blockchain. We have discussed this process flow in more detail in the chapter 4 of this thesis. Here we are very specific towards the logical flow of the smart contract system

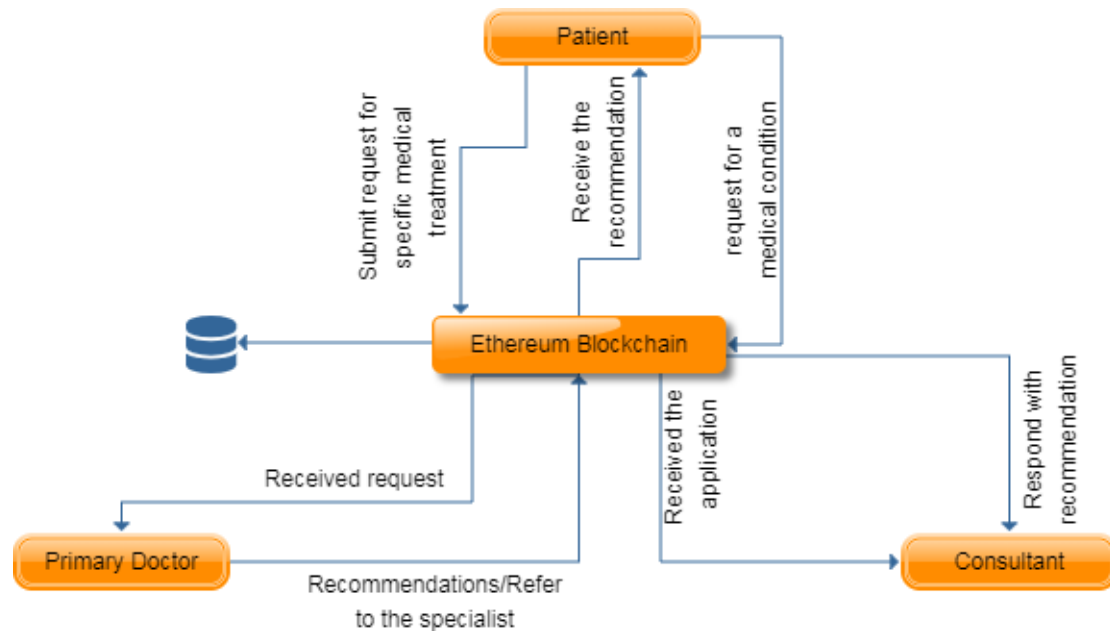


Figure 5.15 Process flow diagram for patient consultant and a physician communication and recommendations


```

1  pragma solidity ^0.4.15;
2
3  //Represents both a Patient and a consultant,
4  //Represents Primary Doctor,
5  //Represents Hospitals,
6  contract PatientConsultant {
7      address public agent;
8      bool public agentEnabled;
9      address[] public consultant;
10     bool[] public consultantEnabled;
11     address[] public relationships;
12
13     modifier isOwner() {
14         bool enable;
15         if(agentEnabled && msg.sender == agent) enable = true;
16         for(uint i = 0; i < consultant.length; i++) {
17             if(consultantEnabled[i] && msg.sender == consultant[i]) {
18                 enable = true;
19                 break;
20             }
21         }
22         if(!enable) revert();

```

Figure 5.16 Pseudo code showing different stakeholders

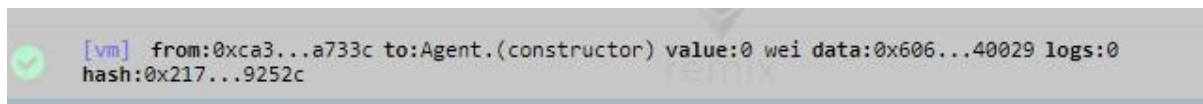


Figure 5.17 The event happened and the Function executed with no error hence the transaction has been successfully completed

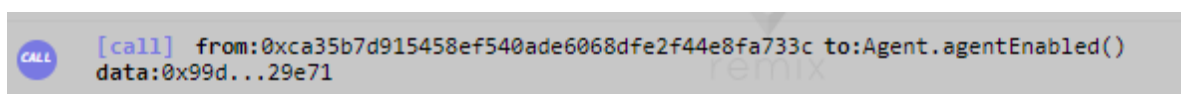


Figure 5.18 Call to the participant, event happened and transaction successfully completed

5.5 Health Insurance

Multiple stakeholders including physician, patient, pharmacy, lab and health insurance company involves in the system as seen by the process flow diagram. Each party connected via smart contract and putting every information on the Ethereum network. A diagram and a pseudo code have been given below in figure 5.19 and 5.20 respectively.

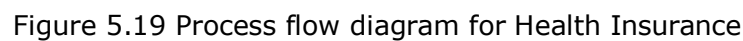


Figure 5.20 Pseudo code for Health Insurance

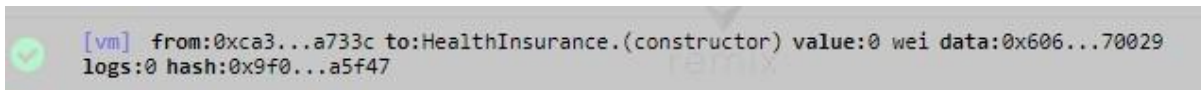


Figure 5.21 The event happened and the Function executed with no error hence the transaction has been successfully completed

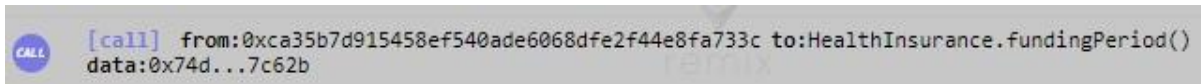


Figure 5.22 Call to the participant, event happened and transaction successfully completed

5.6 Surgery

Algorithm 5.2 shows the patient enrolment during surgical procedures. Getting consent for the patient to thoroughly monitoring and the initial assessment of the patients have been recorded on the blockchain as it can be seen from the figure 5.23. An algorithmic flow has been also discussed in the previous chapter.

Algorithm 5.2: Patient Enrolment

Input: Ethereum address of the patient and other information including consent forms

If All the information has been recorded and get approved

Then Allow the valid transactions to be added

Mapping of Patient's address

Update the network members about the progress

End

else

Don't allow/accept unauthorized transactions

End

If there is no consent

Then Stop processing that further

Notify/update the other peers in the network about the progress

End

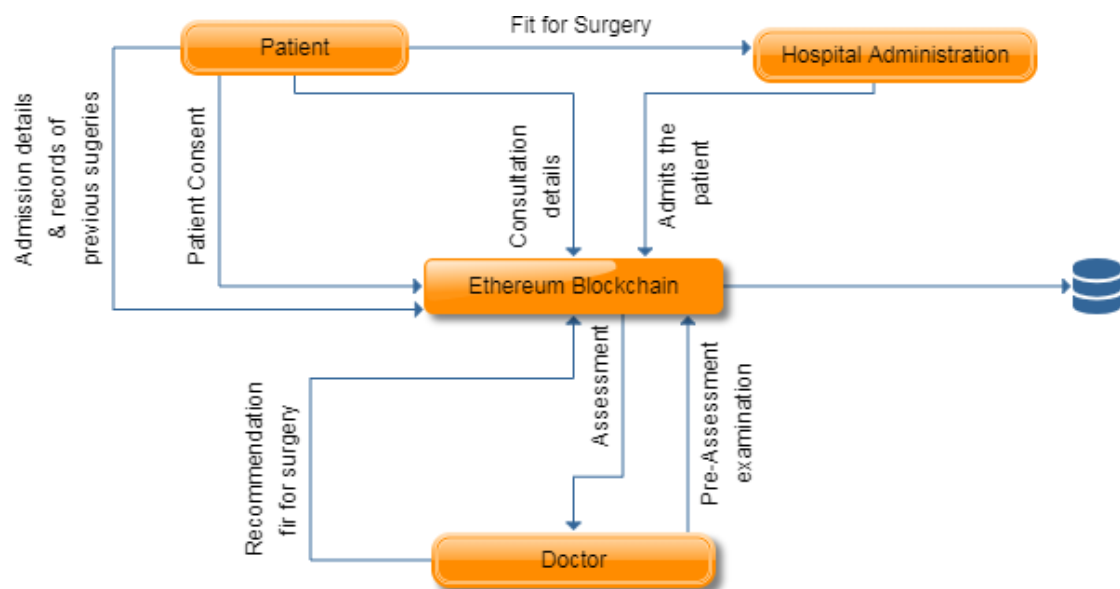


Figure 5.23 Process flow diagram for Surgery

```

1  pragma solidity ^0.4.15;
2
3  //Surgery
4  contract Surgery {
5      address public consultant;
6      bool public consultantEnabledEnabled;
7      address[] public relationships;
8      address [] public surgicalteam;
9      bool[] public surgicalteamEnabled;
10     address[] public patient;
11     bool[] public patientEnabled;
12     address anaesthesiologist;
13     bool[] public anaesthesiologistEnabled;
14
15
16     modifier isOwner() {
17         bool enable;
18         if(agentEnabled && msg.sender == agent) enable = true;
19         for(uint i = 0; i < consultant.length; i++) {
20             if(consultantEnabled[i] && msg.sender == consultant[i]) {
21                 enable = true;
22                 break;
23             }
24         }
25         if(!enable) revert();
26         _;
27     }
28
29     function Agent() public {
30         agent = msg.sender;
31         agentEnabled = true;

```

Figure 5.24 Pseudo code for the deployment of Surgery Smart Contract

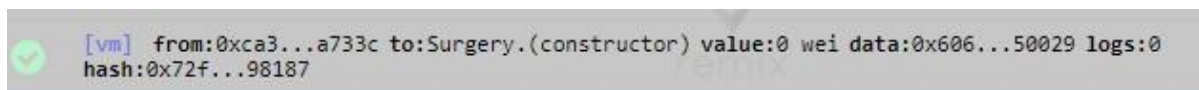


Figure 5.25 The event happened and the Function executed with no error hence the transaction has been successfully completed

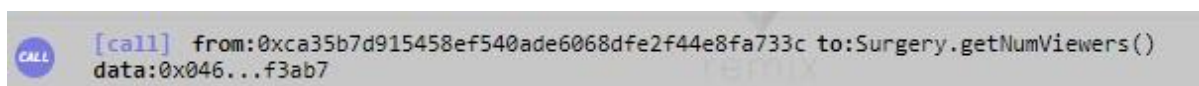


Figure 5.26 Call to the participant, event happened and transaction successfully completed

5.7 Conclusion

In this chapter, we have discussed different medical procedures and their implementation detail comprehensively. The aim of this chapter was to thoroughly discuss the structures, function and the components of the smart contract system designed and implemented for the healthcare applications. Different process flow diagram have been shown to explain the medical procedures and the treatment protocols and different interaction among different stakeholders involved in the system via Ethereum smart contract system in this thesis. This implementation of the Ethereum smart contracts would show the great potential in developing distributed applications (Dapps) for medical eco-system.

6 Blockchain smart contract system for Energy Efficiency applications

In this chapter, we have investigated the Blockchain trends in the energy sector and implemented Blockchain based smart contract for trading of energy saving certificates to enhance trust, privacy and transparency among energy efficiency market stakeholders. Blockchain technology is ready to disrupt almost every business strategic model and the energy industry is no exception. Energy companies around the world have already started to explore the use of blockchain technology among other applications in large-scale energy trading platforms, peer-to - peer energy trading markets, project financing, supply chain monitoring and asset management. Information and communications technology (ICTs) have recently begun to revolutionize the energy environment and now blockchain technology provides an additional opportunity to make the energy system faster, more efficient, more reliable and safer in the long run.

This work was done in a collaboration with IERC and Tyndall National Institute on introducing a new energy policy regulatory scheme where my main focus was to design and implement a smart contract system for the energy saving certificates. As I was looking into the blockchain based smart contract applications, we extended our work for the energy systems applications. This work is an additional contribution for the scope of this thesis. We looked more closely at the use of blockchain technology for its potential use in the energy efficiency industry and decided how it could make energy efficiency markets safer and more open in the longer term. This work explores in depth the key advantages of using blockchain in the energy efficiency market by introducing and analyzing two main case studies as appropriate for blockchain applications — I the UK Energy Company Obligation Scheme (ECO) and ii) the Italian White Certificate Scheme (IWCH). We discussed how the key issues surrounding energy efficiency savings trading — correct estimate of savings, stakeholder data transparency, and inefficient administrative processes — can be resolved by applying a smart contract framework centered on blockchain. This chapter presents the implementation of an intelligent contract framework for exchanging energy-saving certificates obtained via smart contract transactions on the Ethereum blockchain platform.

The energy sector is in transformation and the integration of distributed renewable energy sources into the existing centralized energy system is facing several challenges. Digital technologies like the Internet of Things (IoTs) [142] and blockchain system as enablers for the creation of a decentralized and democratized network of resources. Blockchain is being evaluated for various applications and systems in the energy sector as a means of solving protection and accountability issues and improving process efficiency by providing a decentralized authority framework, thereby creating a win-win scenario for all the stakeholders involved in the system. This research examines the application of blockchain technology to address the current challenges of the energy efficiency market and proposes a smart contract framework for exchanging energy-saving certificates on a transparent and stable digital transaction platform without any third party having to infer in the system.

Figure 6.1 shows main applications of blockchain based systems. For peer-to - peer energy trading [143] [144] [145], blockchain can provide a secure trading verification mechanism without requiring third party authentication. Having a centralized global blockchain network can also provide cross-border, seamless energy trading. Blockchain will enable prosumers to participate in the local energy market where they can rely on digital technology that can make transactions faster, easier, and cheaper than a conventional centralized energy system. It has also been tested in the charging facilities for electric vehicles (EVs) where it will allow access to all charging points for EV drivers through the creation of a network of EVs and charging stations and the development of such an simple payment and efficient settlement mechanism for all parties involved. Several energy firms are also pursuing blockchain technologies in supply and value chains with the aim of enhancing visibility and reducing the loss of assets from output to consumption. Project financing is also studied where blockchain is used to increase transparency and liquidity of pay-outs.

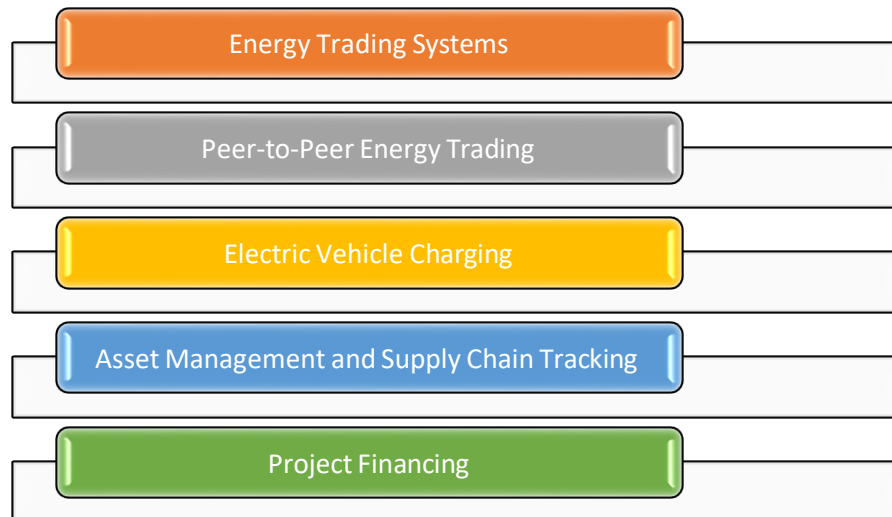


Figure. 6.1 Schematic of the Blockchain-based key energy applications. Reprinted with permission from Khatoon et al., *Energies* 2019; 12(17), 3317.

6.1 Smart Contract implementation for Energy Saving Certificates

In the previous sections of this chapter, we have briefly introduced smart contract features in the energy saving certificate management systems as a way to overcome issues such as third party reliance, improved data security, data audits and logs, and easy buying and selling of energy saving certificates. The smart contract system enabled by blockchain will help end users to securely trade their energy-saving certificates, offering to help one user achieve acknowledgement for their additional energy savings while at the same time allowing another user to fulfil their obligations. These will also help to monitor the energy saving certificates with their unique identification number from their origin to the end of the process. All permissions to access data are stored in the smart contracts by allowing authenticated users to access and control the data. Within this chapter the design of an energy saving certificate smart contract management system (Figure 6.2 and 6.3) has been prototyped using the Ethereum Blockchain framework.

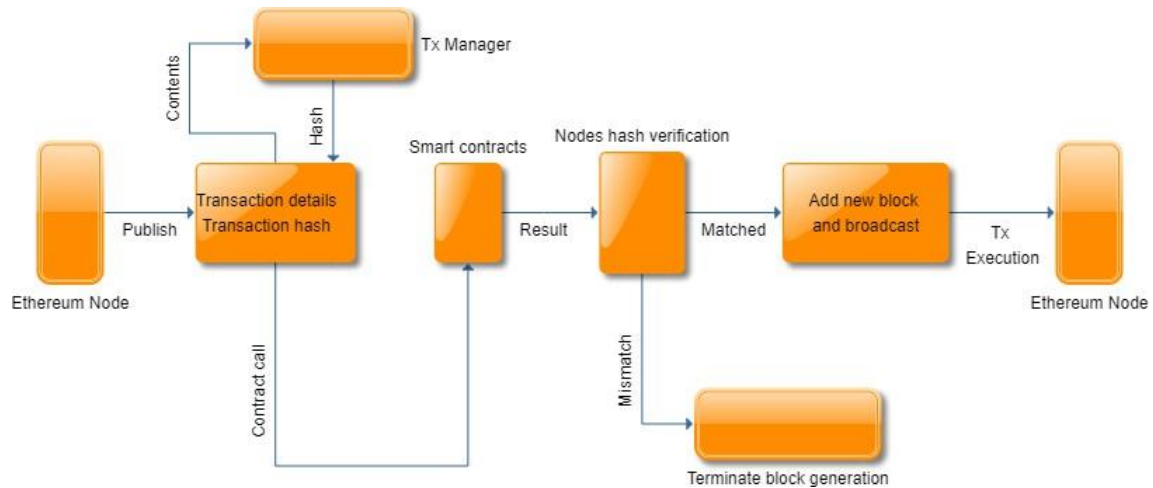


Figure. 6.2 Smart contract based peer-to-peer energy saving certificate trading system:
Consensus protocol

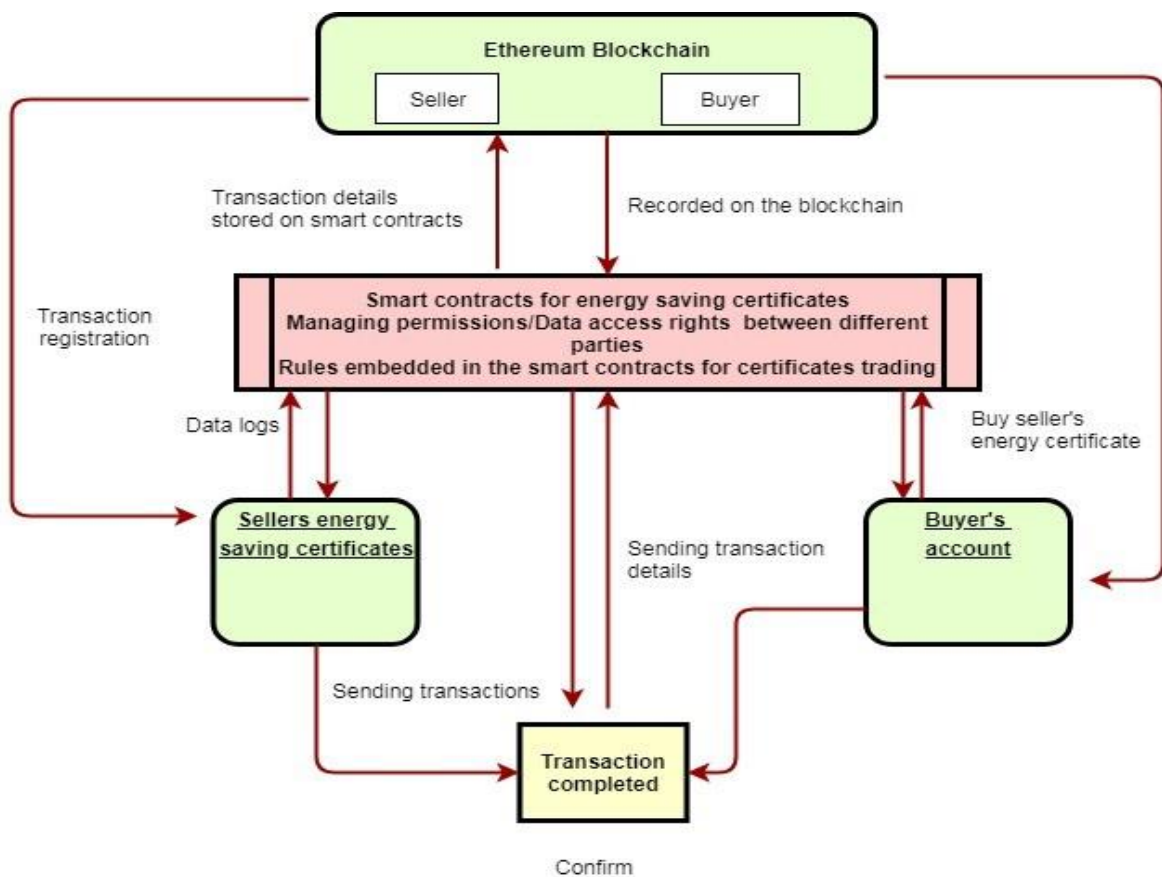


Figure. 6.3 Blockchain-based smart contract system for energy saving certificates.
Reprinted with permission from Khatoun et al., Energies 2019; 12(17), 3317.

The Kovan test network was used as an Ethereum wallet alongside Metamask. The Kovan test chain is basically a PoF blockchain for the Ethereum platform which uses the same technology as the Ethereum Mainnet blockchain. The aim of designing this smart contract system is to introduce such a platform where energy-saving certificates can be traded efficiently, eliminating the necessity of third parties. The smart contracts' key elements are represented in tasks, events, state variables, and modifiers. In Figure 6.4 which shows the main function of energy saving certificates, it maps the buyer, seller and governing body to the transaction. If the provider approves the request, the trading of energy certificates will go on further otherwise not. An Authorization algorithm has been given below which shows how the process initiated on the Ethereum network.

Algorithm: Authorization

Input: Ethereum address of stakeholders involved in the system

Initialization of the process = Access approved

If Initiation request approved

Add the record into the chain

Address Mapping for the stakeholders

Notify the other members in the network for enrolment of new members/peers

end

else

Don't accept transaction from unauthorized persons

End

Through the function Sell), (we initialize the contract, declare variables, functions and assign the owner as msg.sender. A modifier function, only Owner, has been used with the Sell) (function whenever the owner of the smart contract executes it and verifies the owner to sell the amount of energy overachieved). Solidity smart contract elements are well established in Figure 6.4 which shows how a smart contract was developed, and it is possible to see different interactions between various functions to run the transactions within the system. The very first line in the source code reveals that for solidity version 0.4.15, this program is written for. Pragma sets out the instructions provided to the compiler about how to handle the source code elements. The whole smart contract system presents a collection of functions and data (its

states), which resides on the Ethereum blockchain specific address. The owner is the administrator in charge of selling energy-saving certificates.

```
pragma solidity ^0.4.15;

contract energysaving certificates {

mapping (address => mapping (address => bool)) regulatory authority;

mapping (address => mapping (address => bool)) seller;

mapping (address => mapping (address => bool)) buyer;

event Overachieved (address tokenGet, uint amountGet, address tokenGive, uint amountGive,
uint expires, uint nonce, address user);

event Calculatesavings (address tokenGet, uint amountGet, address tokenGive, uint
amountGive, uint expires, uint nonce);

event Issuecertificates (address tokenGet, uint amountGet, address tokenGive, uint
amountGive, address get, address give);
```

Figure. 6.4 Components of a solidity smart contract. Reprinted with permission from Khatoon et al., *Energies* 2019; 12(17), 3317.

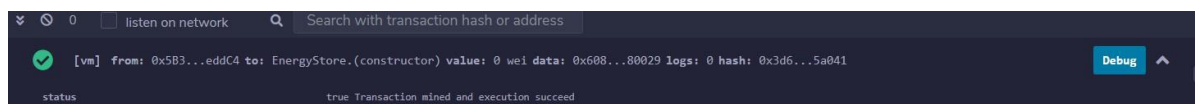


Figure 6.5 The event happened and the Function executed with no error hence the transaction has been successfully completed

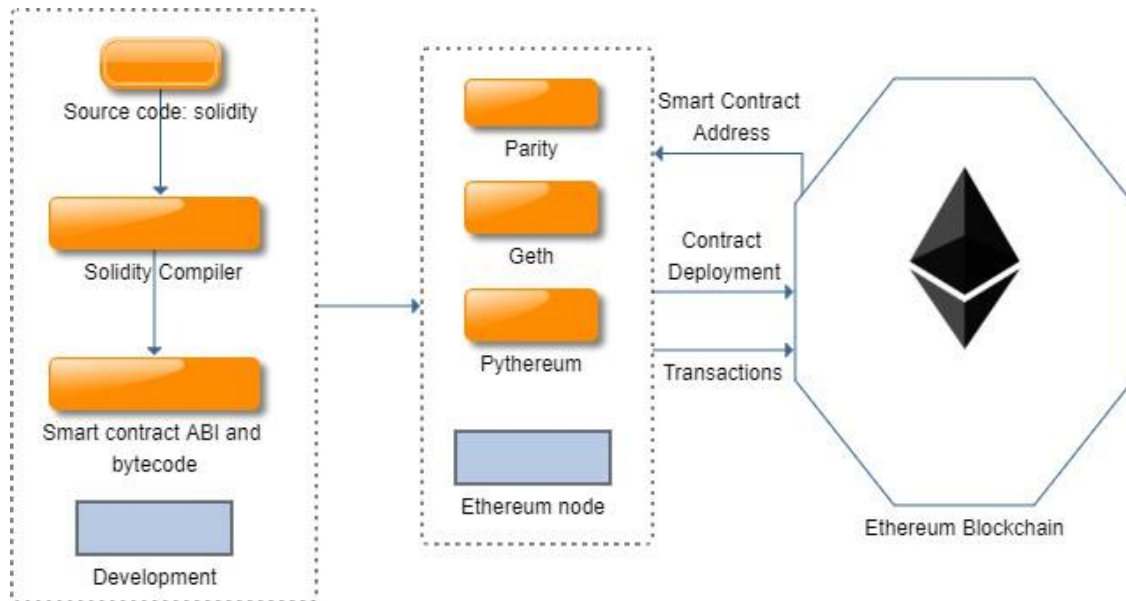


Figure. 6.6 Smart contract deployment on the Ethereum Blockchain.

The event happened and the function executed with no error hence the transaction has been successfully completed in figure 6.5. Smart contract deployment and the development process can be seen in figure 6.6. A smart contract is running on the Ethereum network as shown in figure 6.7, it also shows the transaction flow and how Metamask uses the owner's private key to sign the transactions. To verify the transaction and that all of the relevant information is stored for each transaction, we are using Etherscan. Etherscan is Ethereum's leading blockchain blockexplorer. A BlockExplorer is practically a search engine that helps the users to search, confirm, and validate Ethereum blockchain transactions. Figure 6.8 is an image taken for the blockchain transactions on the Etherscan. This data contains the level of complexity whilst also mining the block, the hash function of the transaction, the gas limit, and the gas used for the transactions to run on the Ethereum network; the nonce which is basically an arbitrary number ("used only once" — during the mined result) makes sure that all the data has been permanently stored on the blockchain. Whilst also giving the account details, one could see the specific details of the transaction on the Etherscan. The proposed approach has been implemented in the form of a smart contract on the Ethereum blockchain, as a distributed execution code. The trade algorithm has been written in solidity programming language and has been tested on the Ethereum blockchain network.

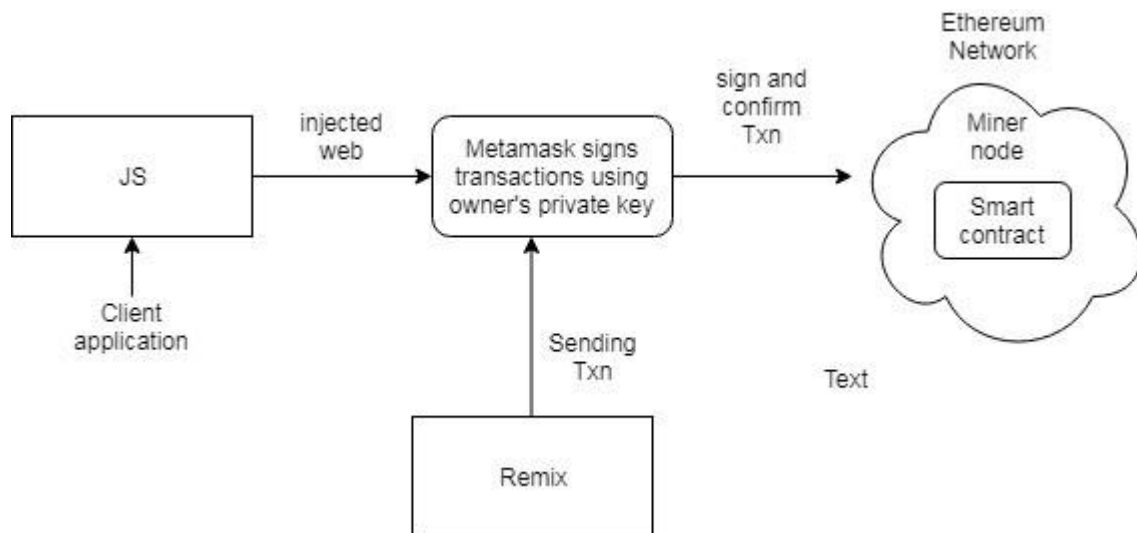


Figure. 6.7 Ethereum transactions workflow. Reprinted with permission from Khatoon et al., *Energies* 2019; 12(17), 3317.

Mined by:	0x0010f94b296a852aaac52ea6c5ac72e03afd032d (POA-Paritytech) in 16 secs
Block Reward:	5.00354826 Ether (5 + 0.00354826)
Uncles Reward:	0
Difficulty:	340,282,366,920,938,000,000,000,000,000,000,000,000,000
Total Difficulty:	3,677,308,016,815,390,000,000,000,000,000,000,000,000,000,000
Size:	9,904 bytes
Gas Used:	3,548,260 (44.35%)
Gas Limit:	8,000,000
Extra Data:	020405/Parity-Ethereum/1.33.0/li (Hex: 0xde830204058f5061726974792d457468657265756d86312e33332e30826c69)
Hash:	0xd543f54899cbd148cd4a4bc9d378ba9477d9282a87791c90d657a63270c72d37
Parent Hash:	0xf200cd7079530eb180a4c5e4d78184d26b790991bd636abb515c579282bfb258
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
Nonce:	0xb841edf85da56605a8c262f9e586472411a7f0bc02cbea642496d035b0e923eac05046c558e6fca0a3e70a0640005ba970da68030a97209fc02e812de7eb360879d401

Figure. 6.8 Blockchain smart contract transactions on Ethereum. Reprinted with permission from Khatoon et al., *Energies* 2019; 12(17), 3317.

6.2 Blockchain applications in the previous energy efficiency schemes

Blockchain technology has the potential to boost transparency and consumer trust and could be used to transform many initiatives for energy efficiency. It can provide consumers with an additional incentive to participate in energy efficiency and energy-saving campaigns by

enabling them to trade those savings and start generating additional funds through an automated process based on smart contracts.

The United Kingdom is enforcing its targets under Article 7 of the Energy Efficiency Directive through the implementation and administration of the (ECO) [150]. This imposes a burden on energy suppliers by introducing energy conservation programs to reduce energy sales by 1.5 per cent annually. Member States (EU directive) have adopted a range of approaches to achieving this objective, including the introduction of a White Certificate Scheme (WCS). To date, WCSs have been in some form implemented in the UK, France, Italy and (recently) Poland respectively. Specific deployment methods vary in each country but generally WCSs require that:

- White certificates are issued by the regulatory authority (normally issued by the energy regulators in the Member State) to verify that the energy consumption reduction has been accomplished.
- Obligatory entities (usually energy suppliers and/or distributors) must show that they may have accomplished their energy-saving obligations by submitting to the regulator sum of white certificates that suits their energy-saving goal at the end of every year.
- White certificates may be obtained by the agreed party either by the implementation of approved energy efficiency programs and the issuance of certificates directly by the regulator or by the acquisition of white certificates from a third party directly or through the spot market. Obligated parties who cannot return appropriate quantity of white certificates at the end of the year must pay a fine.
- The White Certificates spot market must be regulated by an independent entity and must register and verify all transactions that take place.

6.2.1 The Case Study 1: The Italian White Certificate Scheme (WCS)

Italian White Certificate Scheme (WCS) has been one of the most popular examples of a trading system designed to boost end-user energy efficiency. The White Certificate Scheme WCS is also stated to have the maximum potential to promote energy efficiency in Italian industries and is expected to achieve at least 60 per cent of the EU Directive 2012/27 / EU 2020 target [151]. The scheme imposes an obligation on electricity and gas distribution system operators (DSOs) with more than 50,000 customers in order to achieve an annual energy

saving target either by enforcing energy-efficient solutions among end users, or by purchasing white certificates from other DSOs equal to their obligation, or a combination of the two. Every white certificate is equal to one ton of oil equivalent (toe) and is provided by the regulator when additional energy savings compared to the aim are made. A basic block diagram of the Italian White Certificates scheme (WCS) can be seen in Figure 6.8 and it can be noticed that this scheme involves a range of stakeholders for different activities [152]. Dario Di Santo et al. have explained the detailed workings of this scheme in [153]. There are two significant mechanisms — measurement and verification (M&V), and white certificate issuance and trading. These are the complex processes in nature which are not entirely transparent. Blockchain technology will significantly boost the trust between the various stakeholders and making these processes more efficient and reliable [154].

A smart contract which would be stored on the blockchain network, could be built that may have all the terms from M&V to certificate trading as shown in Figure 6.9. The blockchain technology would allow end-users to exchange their white certificates easily and safely, helping one user gain appreciation for their additional energy savings while the other user can fulfill their obligation. It can also help monitor the white certificates from their origin to their surrender with its unique Id. There would be no need for a centralized entity to maintain and authorise trading as it can be managed directly through the smart contract that will significantly reduce trading management administration costs and can also motivate other smaller consumers who were previously unable to take part in the scheme due to high transaction costs. Blockchain will also improve the transaction speed, since trading approval by third parties will no longer be required.

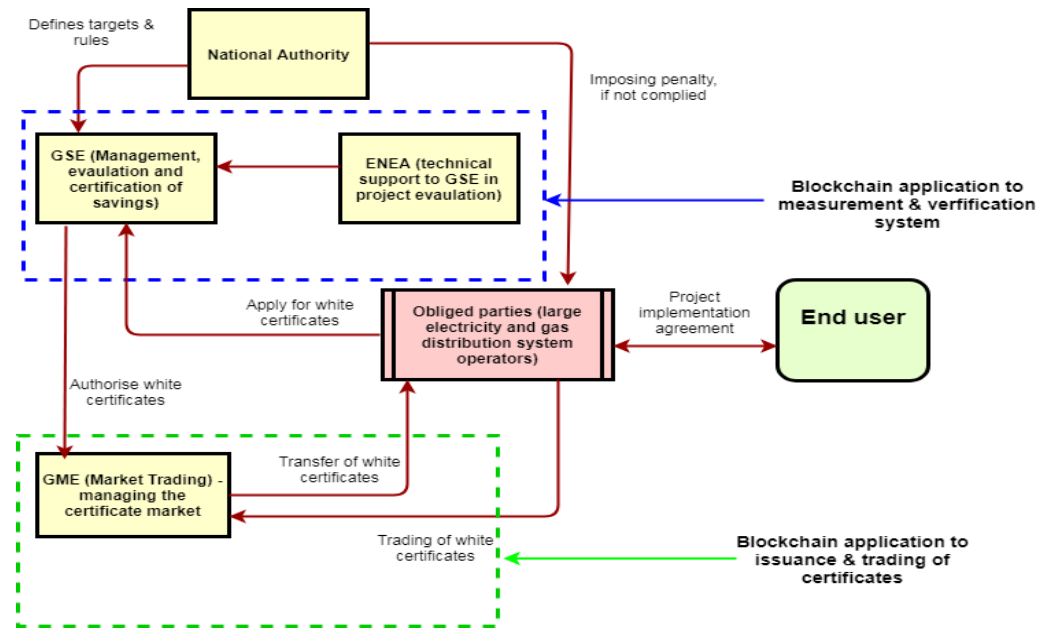


Figure. 6.9 Key stakeholder and processes in Italian White Certificate Scheme. .
Reprinted with permission from Khatoon et al., Energies 2019; 12(17), 3317.

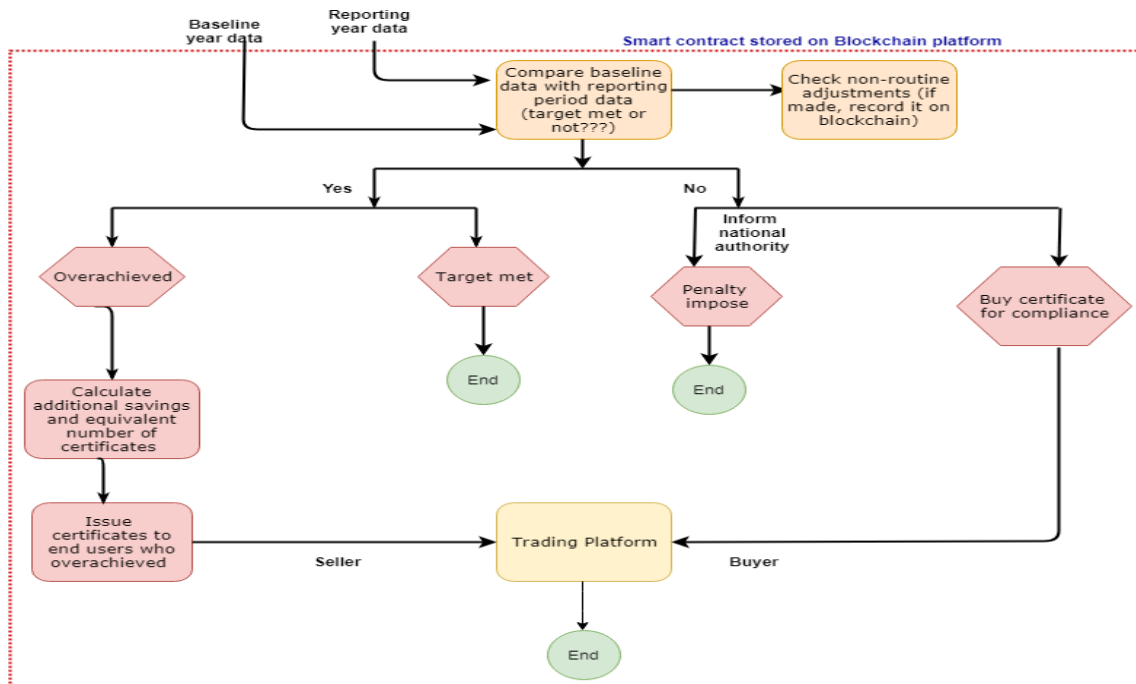


Figure. 6.10 Process flow under smart contract on the blockchain platform. Reprinted with permission from Khatoon et al., Energies 2019; 12(17), 3317.

6.2.2 The Case Study 2: The UK Energy Company Obligation Scheme (ECO)

Under Article 7 of the Energy Efficiency Directive, the UK is delivering its targets through the implementation and management of the Energy Company Obligation (ECO) scheme. This program places a specifications on energy suppliers with more than 250,000 domestic consumers who deliver more than 500 GWh of electricity or 1400 GWh of gas to promote and deploy energy efficiency measures at household [155]. The aim is to reduce energy consumption required to heat homes by implementing energy efficiency measures (such as insulation, more effective boilers and intelligent heating control systems) [156], Ultimately targeting energy deprivation elimination in disadvantaged households. The benchmarks for each compulsory energy supplier are set by the governing body, Ofgem, who is also responsible for deciding whether each supplier fulfills its obligations, audits the scheme, prevents deceitful compliance claims and reports advancement to the UK Government [157]. Energy suppliers have recently been allowed to exchange their obligations with other contracted suppliers and Ofgem is also responsible for managing the trade arrangements.

In order for this system to work properly and efficiently all the stakeholders in the value chain system including energy efficiency initiatives installers, energy suppliers and the UK government must support and trust Ofgem to implement the scheme safely, effectively and with honesty. While using this type of centrally controlled third-party system is the widely accepted method of ensuring transparency in the recent times through any supply chain, its weakness is that the system relies on the integrity and ability of those system operators to keep the data they manage secure. Therefore the system is open to failures because of organizational bias, external hackers or potential fraud. Blockchain may be used to tackle this issue.

Blockchain could be used to build a digital public decentralized ledger to record all the transactions relating to ECO delivery. A smart contract may indeed be built using the blockchain technology that records a qualified installer based on a set of verifiable requirements for any installation of an ECO measure at a home property. It can even be linked to energy consumption before and after deployment in order to demonstrate compliance with actual, rather than deemed, energy savings. By their design, the blocks on the ledger are connected, meaning that the new entry relies on the content of the previous block that prevents retroactive modification of any block because that would change all the subsequent entries. As each participant in the production chain can attach blocks to the blockchain and use their own digital signature to verify the validity of the transaction, peer-to - peer trading can take place

immediately between the installer and the energy supplier or even between the energy suppliers that enable them to transact their obligations directly with no need for a market operator to validate transactions. It will theoretically reducing the operating costs for the ECO system while also rising the degree of trust in the system at the same time.

6.3 Benefits of utilizing blockchain technology in the energy efficiency market

Energy efficiency already has great potential to bring the most positive effects. Energy Efficiency 2018 study by the International Energy Agency notes that enhancing energy quality will reduce energy bills to customers by more than \$500 billion per year [146]. As the technology such as blockchain progresses, it will give consumers the ability to exchange their excess electricity. Consumers will be driven further towards energy savings and improving their homes' energy efficiency as they will be given an extra additional benefit to monetize their excess energy. As the market for energy efficiency is projected to grow over time, blockchain technology could considerably improve the overall administrative procedures, openness of the system, cost and trust between various stakeholders. Some of the key advantages are shown and explained below in Figure 6.10.

6.3.1 Encryptions of the energy savings

Encryption is a method of converting digital data or other information to a code in order to avoid unauthorized access. Encrypting and exchanging of the energy savings over the blockchain has the potential to safeguard the market. Energy baseline and savings data are one of the energy efficiency market's most important assets as well as several transactions, from bank payments to amounts paid to energy service providers and technology companies, depend solely on this. Data security has become a significant problem in this digitized world and blockchain can provides opportunities to secure customer data on energy savings for a more safe energy efficiency markets. When gathering and checking energy savings, it is difficult to gain the confidence of customers. It involves high costs for energy control, estimation and verification, and this, combined with a lack of clarity in energy measurements, acts as an obstacle to energy efficiency contracting. By providing safe, independent verification of energy transaction data and savings, blockchain provides accountability and establishes trust with customers.



Figure. 6.11 Benefits of blockchain in the energy efficiency sector. Reprinted with permission from Khatoon et al., *Energies* 2019; 12(17), 3317.

6.3.2 Exchange of the energy savings

So far we have spoken about exchanging excess power production for peer-to - peer energy trading. But what if people in their locality want to trade energy savings? Can energy savings be built up and traded for a new energy-efficiency product that one would want to buy? Blockchain technology seems to have some opportunities here because energy savings data can be encrypted and stored on the blockchain platform to balance the energy bill or buy additional energy services.

6.3.3 Valuation of energy savings

Energy efficiency valuation has been very difficult, since the benefits of energy efficiency cannot be measured or evaluated technically in many cases. Blockchain, together with ICTs and process automation, may help to some degree in determining energy savings and their related benefits [147].

6.3.4 Increasing transparency

Since blockchain is a distributed ledger technology, digital data can be shared on a secure and tamperproof platform in a transparent manner. Interfering with the shared data on

the blockchain platform is a highly costly and technically impossible process. Blockchain is a trustless system so each data shared with the other blocks is verified by all the blocks in the chain, meaning that all the blocks will have data on energy savings [148] [149].

6.3.5 Lowering the transaction costs

Blockchain does not need intermediaries and the transaction may occur peer-to - peer directly which reduces process complexity and associated costs. In this way, the transaction cost of managing energy related contracts can be reduced considerably. In the case of the energy efficiency market, particularly in energy performance contracting, streamlining the transaction costs for ESCOs, banks, utilities and customers through a blockchain process can be reduced.

6.3.6 Increasing reliability

Trust is very important term in this new world , especially when it comes to storing of information when it can be stored either at a single point or in multiple account books belonging to different stakeholders without any automated processes. If information is stored at a single point, the time taken to gather the required information would make it very difficult to track and audit. Since blockchain is a trustless distributed ledger technology where information is recorded in different blocks, the overall system reliability can be significantly improved.

6.3.7 Increasing customer trust and security

Blockchain is made safe through its cryptography methods, which ensures that the energy saving data of consumers, information from financial institutions or data related to any stakeholder in the energy efficiency industry would be encrypted. Blockchain can also make the process automated rather than manual via smart contract features which can help increase consumer trust in the system.

6.3.8 Increasing the market success

Once the blockchain technology, such as energy performance contracting, is applied to the energy efficiency market, this can bring security , transparency, confidence, lower

operational costs, energy savings authorisation, and payments in an automated way. This will carry the energy efficiency market the next stage of growth. ICTs and blockchain can significantly reduce market obstacles and set a new energy efficiency trajectory for success.

6.4 Conclusions

Moving to a smart, integrated prosumers grid would require the implementation of new technology, as well as the opportunity to value energy conservation steps, so that the resulting savings can be shared equally and transparently. Blockchain technology offers an optimism for the energy sector that it will be possible to provide a safe and secure digital transaction system in which consumers can participate directly in the energy market. In this chapter we have addressed the use of blockchain for the energy efficiency market and some of the benefits that implementation of blockchain technology could bring to the stakeholders if appropriate structures could be introduced. The issues surrounding energy efficiency savings and trading markets, such as proper savings valuation, stakeholder data transparency, inefficient administrative procedures, and high energy-efficiency market complexities are very well known. Blockchain's potential application to address some of these major issues was explored by examining two case studies — the Italian White Certificate Scheme (WCS) and the UK Energy Company Obligation Scheme. This chapter also presents an algorithm designed for the trading of energy-saving certificates, which is implemented via a smart contract system based on the Ethereum blockchain. Unlike the other conventional energy saving certificate trading systems, our approach offers a decentralized, safe, automated, time-stamped and transparent trading platform among multiple users using blockchain technology.

There will still be challenges around the technology on its own that are currently being acknowledged such as scalability, performance, standardization, complexity, cost and skills. Given that a number of pilot projects are already underway to assess the usage of blockchain in a variety of energy-related applications, now is the best time to explore how the technology might be useful to the energy efficiency sector and to thoroughly examine the obstacles that exist before its commercialisation. This research work clearly suggests the technology's potential in the energy trading systems. While this technology has the ability to impact the energy efficiency market positively, we must also consider how future policy and regulatory models will look like and also what would be the position of the various stakeholders in the future energy efficiency market will shift.

In this work we have collaborated with International Energy Research Centre Cork and Tyndall National Institute on implementing new energy policy regulatory scheme. We were involved in the technical part of this work and our collaborators provided data on the energy policy side. We were looking into the Smart contract applications for medical healthcare management systems, we extended our work for the energy system applications. This chapter is an additional contribution to this thesis.

7 Conclusions and future directions

The work described in this paper demonstrates the design and development of smart contracts for blockchain applications. We have developed and implemented smart contracts for blockchain-based healthcare (health management in healthcare ecosystems) and utilities (increasing energy efficiency through the creation of smart contracts for energy savings certificates). In this article we also identify important topics, developments and new areas in medical and electrical research.

7.1 Smart contracts for Healthcare Management to facilitate Medical Eco-system

In this study, the feasibility of blockchain-based smart contracts for healthcare management is investigated. This research also suggests using blockchain technology for better data management in various fields, including healthcare. This may involve accessing and managing large amounts of medical information. When using the operational process of smart medical contract management, the relevant costs of the system are calculated as a result of a detailed study. Groups of transactions in the blockchain network use the hash value recorded in the previous block to combine links in the chain. Therefore, as a means of immutability, the security tools of the blockchain network have been improved. The longer (older) the blockchain, the more protected the information it contains is against changes. If the attacker tries to change the keys, the scratchpad will immediately become invalid because the hash value in the next block header will be completely different according to the hash function mechanism. Additionally, the network is often referred to as a decentralized ledger because the information stored in each part of the network operates on a separate network. When each block enters the system and becomes part of the chain, it plays an important role in connecting the previous block and the next block. The main function of each block is to collect, analyze and distribute the transactions of other blocks. This means that blocks in the chain cannot be deleted or modified because this will replace all subsequent blocks. It will work for research and personalized medicine by creating a repository for all health information, tracking personal information in real time, and organizing code access information at a granular level.

Health researchers need comprehensive data to improve understanding of disease, make clinical trial discoveries, rapidly develop drugs, and develop specific treatment plans determined by genetics, lifespan, and environment. When patients come from different cultures, health backgrounds, and different regions, our Ethereum-based blockchain data sharing network will collect a lot of data. In a long-term study, it provides a lot of information because the blockchain collects health information throughout the person's life. It will expand health data to include data from populations currently underserved or traditionally uninterested in research. Blockchain's open data ecosystem makes it easier for "hard to reach" businesses to participate and benefits the public. The initiative could support the development of new "smart" doctor apps that bypass the latest medical research and create new treatment options. This information is also available to doctors and patients who can collaborate with each other, learning to discuss science-based treatment rather than the best-case scenario as a feeling in the stomach.

In this article, we use blockchain technology, a smart contract-based healthcare management system, to show how the concept of distribution can be applied to big data in treatment and how to simplify the treatment process. We introduce a new approach to managing medical records that provides verification, collaboration, and accountability through smart contracts. The system is designed to track similarities and differences, allowing patient information to be shared and medical researchers to adopt the program. We present practical applications of blockchain technology in the management of medical records. From a medical perspective, we have created a need for data management and sharing models. Blockchain technology, transparency, security, availability and quality management of EHR data can be guaranteed. As stated in this article, the main purpose of using blockchain is to improve the medical process and therefore improve patient outcomes. Blockchain can help in many ways; Reduce transaction costs by using smart contracts in the process to simplify the process, reduce unnecessary costs and eliminate intermediaries in our scheme by using blockchain technology output to create an iterative, scalable, stable, open and decentralized repair ecosystem; . It will encourage patients to share their medical information openly and securely with doctors, hospitals, research institutions and other stakeholders.

Maintain the confidentiality of their medical information at all times. This will solve many of the current healthcare problems, including data silos, conflicts with legacy systems, lack of data processing and expensive printing, data security and privacy issues.

7.2 Blockchain based smart contract system for energy efficiency

Throughout this work, we discuss how key issues related to energy conservation (energy savings estimates, relevant data, and methods for which standard control is not good) can be addressed using a blockchain-based smart contract. The implementation of Ethereum-based smart contracts aims to trade electronic certificates recorded by executing smart contracts on the Ethereum blockchain. We discuss the advantages and impact of using blockchain in the field of energy use by presenting and discussing some research based on the potential use of blockchain - I UK Energy Company Liability and (ii) the Italian White Certificate Scheme (WCS)))

. Whether on the sales side or in native electronic business applications such as peer-to-peer energy trading, blockchain will enable a reliable printing process without the need for third-party authentication. Having a global blockchain infrastructure can also enable seamless cross-border trade. Blockchain will allow consumers to participate in the local electricity market, based on technology that is faster, cheaper and easier to trade than electricity in the middle. Blockchain is also being tested in electric vehicle (EV) charging stations, creating a network of EVs and charging stations, allowing EV drivers to access all charging stations and creating convenient payment and quality solutions for all parties involved. Some energy companies are also exploring the use of blockchain technology in the supply chain to increase transparency and reduce costs from supply to supply for consumption. The financial project where blockchain is used to increase the efficiency and effectiveness of the system and the income from payments is also being examined.

The transition to a smart, integrated prosumer grid requires the use of new technologies and the ability to leverage energy savings to reward benefits and the associated sharing and transparency.

Blockchain technology for the electronic market brings great prospects in creating a safe and reliable digital trading platform that allows consumers to directly participate in energy. In this report we discuss the use of blockchain in the electronics industry and some of the benefits that the use of this technology can bring to stakeholders that can be leveraged if the project is developed. The issues surrounding the energy conservation industry, such as required savings, relevant information, ineffective management systems, and complexity of the energy sector, are well known. Two studies, the Italian Free Certificate Scheme and the UK Energy Company Tariff Scheme, are exploring the possibility of using blockchain to solve some of these important problems. We also announced a system designed to trade energy savings certificates using a blockchain-based smart contract. and transparent transactions between different users using distributed trading tools.

7.3 Reflection and Impact Assessment

The smart contract based framework demonstrates how design concepts of decentralization and blockchain can lead to stable, interoperable systems. Using Ethereum smart contracts to facilitate a content-control network through various storage and provider sites, authentication log controls access rights while offering full record monitoring, auditability and data sharing to the parties involved. We demonstrated a revolutionary approach for accessibility of open APIs and network structure.

7.4 Future Work

In our current system, we use PoW and manage data off-chain due to cost and energy constraints. Because storing information in the supply chain is always expensive. We aim to use the (PoS) protocol in future work and store data on-chain instead of storing it in a local storage. But PoS is a big problem and it is not as easy as using PoW to get network approval. This allows nodes of the Ethereum network to agree on the current state of all data stored on the Ethereum blockchain, thus preventing certain types of business threats.

Ethash is a proof-of-work system that requires miners to compete in a trial-and-error game to obtain a random number for a block. Only valid blocks of random numbers can be added to the network. Miners will always only run the downloaded data and run the entire chain with some math operations (like miners) as they race to create a block.

At the most basic level, Proof of Stake and Proof of Work have the same end goal: helping the alliance reach a secure consensus. But there are some differences between the process and people: PoS for Stacked ETH de-emphasizes financial transactions. Validators are replacing miners in PoS. Validators contribute their ETH online to create new blocks. Validators don't work too hard to create blocks; Instead the algorithm selects them randomly. At some stage, if two-thirds of the validators agree, the block status will be declared final. Pros have to participate in all their stakes at this point, meaning they will lose everything if they try to participate in the future.

Unlike proof of work, consumer products do not require a large calculator because they are selective and not competitive. They don't need to mine blocks; All they have to do is create them when they need them and use the app when they don't. Evidence is the term for such evidence. One proof of this might be: "This block is good for us." Validators are rewarded for proposing new ideas and validating existing blocks. People could lose their shares if they try to prove illegal blocking. The basic process of starting the validator when there is enough stake is called proof of stake. To become a validator of Ethereum, users must deposit 32 ETH. Validators are assigned to randomly generated blocks and are responsible for double-checking and validating blocks they did not create. User authentication is also used to support authentication functionality. For example, users can lose all their funds if they go offline, get rejected, or are deliberately compromised. PoS is better when it comes to spending a lot of computing power. The future of this work lies entirely in the transition to (PoS) protocol.

References

- [1] “Cardano - Home of the Ada cryptocurrency and technological platform.” [Online]. Available: <https://www.cardano.org/en/home/>. [Accessed: 25-Mar-2020].
- [2] “Bitcoin: A Peer-to-Peer Electronic Cash System.” [Online]. Available: <https://bitcoin.org/en/bitcoin-paper>. [Accessed: 24-Mar-2020].
- [3] “Home | Ethereum.org.” [Online]. Available: <https://ethereum.org/>. [Accessed: 25-Mar-2020].
- [4] P. Deepak, M. Nisha, and S. P. Mohanty, “Everything You Wanted to Know About the Blockchain,” *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, 2018.
- [5] “What are Trustless Environments & How Cryptocurrencies Create Them ?” [Online]. Available: <https://blockonomi.com/trustless-environments/>. [Accessed: 25-Mar-2020].
- [6] “What is Blockchain?” [Online]. Available: <https://lisk.io/what-is-blockchain>. [Accessed: 25-Mar-2020].
- [7] M. Jakobsson and A. Juels, “Proofs of Work and Bread Pudding Protocols(Extended Abstract).” Springer US, pp. 258–272, 1999.
- [8] Z. Wan, D. Lo, X. Xia, and L. Cai, “Bug Characteristics in Blockchain Systems: A Large-Scale Empirical Study,” in *IEEE International Working Conference on Mining Software Repositories*, 2017, pp. 413–424.
- [9] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, “A detailed and real-time performance monitoring framework for blockchain systems,” in *Proceedings - International Conference on Software Engineering*, 2018, pp. 134–143.
- [10] “Blockchain: Everything You Need to Know.” [Online]. Available: <https://www.investopedia.com/terms/b/blockchain.asp>. [Accessed: 25-Mar-2020].
- [11] “Block hashing algorithm - Bitcoin Wiki.” [Online]. Available: https://en.bitcoin.it/wiki/Block_hashing_algorithm. [Accessed: 25-Mar-2020].
- [12] “Bitcoin Cash - Peer-to-Peer Electronic Cash.” [Online]. Available: <https://www.bitcoincash.org/>. [Accessed: 25-Mar-2020].
- [13] “Bitcoin Puzzle Worth 2.1 BTC STILL Unsolved, Find New Clues Here.” [Online]. Available: <https://bitcoinist.com/bitcoin-puzzle-worth-2-1-btc-still-unsolved-find-new-clues-here/>. [Accessed: 25-Mar-2020].
- [14] “Proof-of-Work vs. Proof-of-Stake - HydroMiner - Medium.” [Online]. Available:

- <https://medium.com/@hydrominer/proof-of-work-vs-proof-of-stake-7b3afe24f0cc>.
[Accessed: 25-Mar-2020].
- [15] "Peercoin — The Pioneer of Proof of Stake." [Online]. Available:
<https://www.peercoin.net/>. [Accessed: 25-Mar-2020].
- [16] "Home | Monero - secure, private, untraceable." [Online]. Available:
<https://www.getmonero.org/>. [Accessed: 25-Mar-2020].
- [17] "XRP | Ripple." [Online]. Available: <https://ripple.com/xrp/>. [Accessed: 25-Mar-2020].
- [18] "Buy Binance Coin | Buy BNB | Buy Binance Coin with Credit Card | Binance.com." [Online]. Available: <https://www.binance.com/en/buy-Binance-Coin>. [Accessed: 25-Mar-2020].
- [19] "EOSIO - Blockchain software architecture." [Online]. Available: <https://eos.io/>.
[Accessed: 25-Mar-2020].
- [20] "Tether – Stable digital cash on the Blockchain." [Online]. Available:
https://tether.to/?__cf_chl_jschl_tk__=b1913042d380bf14ca2b13c04df5c8f1af13b7ae-1585175857-0-AU9TL7_54PS7gaaC-15mCwIasWUzTe33Dfq_Tz1ARJmBJHRO5zHo2crYG5_D4zlSTr0dq4rWZDZB3FTBXMHV8rtOHzuSz3FbGGxWfAx8fyXSvcWnXZ0awtoGsMPRxgUGG8xL_DE9ubKTYbdmORbBJvyCE14U-seAbHWJZRAi8XSUEngK7Zlw14khM6ta-1WDewukzYo_fodpek264Z47j0JFPuzL5WOi65sUwWb8ztIjE-Ux10DkoKI3eFYpGU8mzIos7m3rCbw5v1hCNkOrI. [Accessed: 25-Mar-2020].
- [21] "Stellar - an open network for money." [Online]. Available: <https://www.stellar.org/>.
[Accessed: 25-Mar-2020].
- [22] "Dash - Dash is Digital Cash You Can Spend Anywhere." [Online]. Available:
https://www.dash.org/?__cf_chl_jschl_tk__=3074aa005757ec111f908f14b3d1e51a6094671e-1585175637-0-ASWYPw59Zwz-8hi9rf_gTzNMvH8QmJWt2YcSWJoL-0fAb88hLxFf-PjQ2d0XFRKskk0gyZhNCwwEiPzJPMLdat9CMLgkaYtiZA4VtAxf6kBQ-o8FMhPQHNYKY_XwYCazCOfqYwDk0z74DryMUGg2d8k8xTyqQEv1bDUORZw0l5KZ_0MNfLBW9L4xrjfPPExTDVnFklK_2ZTF0Pkxolk2cgU_4bITKJX6zDnhhDV-O7vtDALkgoy_ydoCJ0YxLmf6VktWgN-qQOW_bbksqhLTxdw. [Accessed: 25-Mar-2020].
- [23] "Litecoin - Open source P2P digital currency." [Online]. Available:
<https://litecoin.org/>. [Accessed: 25-Mar-2020].

- [24] “(6) The difference between a Private, Public & Consortium Blockchain. | LinkedIn.” [Online]. Available: <https://www.linkedin.com/pulse/difference-between-private-public-consortium-collin-thompson/>. [Accessed: 24-Mar-2020].
- [25] G. A. Oliva, A. E. Hassan, and Z. M. Jiang, “An exploratory study of smart contracts in the Ethereum blockchain platform,” *Empir. Softw. Eng.*, pp. 1–41, Mar. 2020.
- [26] N. Grech, L. Brent, B. Scholz, and Y. Smaragdakis, “Gigahorse: Thorough, Declarative Decompilation of Smart Contracts,” in *Proceedings - International Conference on Software Engineering*, 2019, vol. 2019-May, pp. 1176–1186.
- [27] R. Tonelli, G. Destefanis, M. Marchesi, and M. Ortu, “Smart Contracts Software Metrics: a First Study,” Feb. 2018.
- [28] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2016, vol. 24-28-October-2016, pp. 254–269.
- [29] N. Szabo, “Formalizing and securing relationships on public networks,” *First Monday*, vol. 2, no. 9, Sep. 1997.
- [30] M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, “Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact,” *Futur. Gener. Comput. Syst.*, vol. 102, pp. 259–277, Jan. 2020.
- [31] I. Grishchenko, M. Maffei, and C. Schneidewind, “Foundations and Tools for the Static Analysis of Ethereum Smart Contracts.” Springer International Publishing, pp. 51–78, 2018.
- [32] “The Ethereum Virtual Machine — How does it work? - MyCrypto - Medium.” [Online]. Available: <https://medium.com/mycrypto/the-ethereum-virtual-machine-how-does-it-work-9abac2b7c9e>. [Accessed: 25-Mar-2020].
- [33] “1. What Is Ethereum? - Mastering Ethereum [Book].” [Online]. Available: <https://www.oreilly.com/library/view/mastering-ethereum/9781491971932/ch01.html>. [Accessed: 25-Mar-2020].
- [34] “Elliptic Curve Cryptography - KeyCDN Support.” [Online]. Available: <https://www.keycdn.com/support/elliptic-curve-cryptography>. [Accessed: 25-Mar-2020].
- [35] “Elliptic Curve Cryptography: a gentle introduction - Andrea Corbellini.” [Online]. Available: <https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/>. [Accessed: 25-Mar-2020].
- [36] S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, and Y.

- Alexandrov, “SmartCheck: Static analysis of ethereum smart contracts,” in *Proceedings - International Conference on Software Engineering*, 2018, pp. 9–16.
- [37] “Smart Contracts: The Future of Blockchain? Mason Hayes Curran.” [Online]. Available: <https://www.mhc.ie/latest/blog/smart-contracts-the-future-of-blockchain>. [Accessed: 25-Mar-2020].
- [38] “JavaScript | MDN.” [Online]. Available: <https://developer.mozilla.org/en-US/docs/Web/JavaScript>. [Accessed: 25-Mar-2020].
- [39] “Solidity — Solidity 0.6.4 documentation.” [Online]. Available: <https://solidity.readthedocs.io/en/v0.6.4/>. [Accessed: 25-Mar-2020].
- [40] “Solidity: Why You May Want to Learn This Ethereum Smart Contract Language - Bitcoin EU.” [Online]. Available: <https://bitcoin.eu/solidity-why-you-may-want-to-learn-this-ethereum-smart-contract-language/>. [Accessed: 25-Mar-2020].
- [41] “Ethereum for Developers | Ethereum.org.” [Online]. Available: <https://ethereum.org/developers/>. [Accessed: 25-Mar-2020].
- [42] “Introduction to Smart Contracts — Solidity 0.6.4 documentation.” [Online]. Available: <https://solidity.readthedocs.io/en/v0.6.4/introduction-to-smart-contracts.html>. [Accessed: 25-Mar-2020].
- [43] “A 101 Noob Intro to Programming Smart Contracts on Ethereum.” [Online]. Available: <https://medium.com/@ConsenSys/a-101-noob-intro-to-programming-smart-contracts-on-ethereum-695d15c1dab4>. [Accessed: 25-Mar-2020].
- [44] “Introducing Web3 Plugins - MetaMask - Medium.” [Online]. Available: <https://medium.com/metamask/introducing-the-next-evolution-of-the-web3-wallet-4abdf801a4ee>. [Accessed: 25-Mar-2020].
- [45] “Ethereum (ETH) Blockchain Explorer.” [Online]. Available: <https://etherscan.io/>. [Accessed: 25-Mar-2020].
- [46] Y. Hu, M. Liyanage, A. Mansoor, K. Thilakarathna, G. Jourjon, and A. Seneviratne, “Blockchain-based Smart Contracts - Applications and Challenges,” pp. 1–26, 2018.
- [47] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control,” *J. Med. Syst.*, vol. 40, no. 10, pp. 1–8, Oct. 2016.
- [48] “Intelligent Computing, Information and Control Systems: ICICCS 2019 - Google Books.” [Online]. Available: <https://books.google.ie/books?id=EMO3DwAAQBAJ&pg=PA528&lpg=PA528&dq=Lemieux,+V.L.+Trusting+records:+Is+Blockchain+technology+the+answer?+Rec.+M>

anag.+J.+2016,+26,+110–

139&source=bl&ots=sdEanEVLlm&sig=ACfU3U28vZ1ImmLC8WpjphVYPb9P9UQh1w&hl=en&sa=X&ved=2ahUKEwie2Zzz4rLoAhUaXRUIHYgXDJIQ6AEwAHoECAYQAQ#v=onepage&q=Lemieux%2C V.L. Trusting records%3A Is Blockchain technology the answer%3F Rec. Manag. J. 2016%2C 26%2C 110–139&f=false. [Accessed: 24-Mar-2020].

- [49] M. N. Kamel Boulos, J. T. Wilson, and K. A. Clauson, “Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare,” *International Journal of Health Geographics*, vol. 17, no. 1. BioMed Central Ltd., 05-Jul-2018.
- [50] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, “Using Blockchain to Enable Untrusted Business Process Monitoring and Execution,” *Int. Conf. Bus. Process Manag.*, pp. 329–347, 2016.
- [51] W. J. Gordon and C. Catalini, “Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability,” *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224–230, 2018.
- [52] D. Ichikawa, M. Kashiya, and T. Ueno, “Tamper-resistant mobile health using blockchain technology,” *JMIR mHealth uHealth*, vol. 5, no. 7, pp. 1–10, 2017.
- [53] A. A. Vazirani, O. O’Donoghue, D. Brindley, and E. Meinert, “Implementing blockchains for efficient health care: Systematic review,” *J. Med. Internet Res.*, vol. 21, no. 2, pp. 1–12, 2019.
- [54] S. Rouhani and L. Butterworth, “MediChain TM : A Secure Decentralized Medical Data Asset Management System,” no. Section II.
- [55] H. Wu and C. Tsai, “Toward Blockchains for Health-Care Systems,” *IEEE Consum. Electron. Mag.*, vol. 7, no. July, pp. 65–71, 2018.
- [56] B. Shen, J. Guo, and Y. Yang, “MedChain: Efficient healthcare data sharing via blockchain,” *Appl. Sci.*, vol. 9, no. 6, 2019.
- [57] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, “Blockchain technology in healthcare: A comprehensive review and directions for future research,” *Appl. Sci.*, vol. 9, no. 9, pp. 1–28, 2019.
- [58] A. T. Litchfield, A. Khan, " A And Khan, and A. Khan, “CONF-IRM) 5-2019 Review of Issues in Healthcare Information Management Systems and Blockchain Solutions,” vol. 1, 2019.
- [59] J. Vora *et al.*, “BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records,” *2018 IEEE Globecom Work. GC Wkshps 2018 - Proc.*, pp. 1–6,

- 2019.
- [60] A. Petre, "Blockchain use cases in healthcare," *LinkedIn Pulse*, vol. 111, pp. 1–41, 2017.
- [61] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives," *Cryptography*, vol. 3, no. 1, p. 3, 2019.
- [62] F. Jamil, L. Hang, K. H. Kim, and D. H. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," *Electron.*, vol. 8, no. 5, pp. 1–32, 2019.
- [63] S. H. Lee and C. S. Yang, "Fingernail analysis management system using microscopy sensor and blockchain technology," *Int. J. Distrib. Sens. Networks*, vol. 14, no. 3, 2018.
- [64] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.
- [65] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, 2016.
- [66] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Design of blockchain-based apps using familiar software patterns with a healthcare focus," *Proc. 24th Conf. Pattern Lang. Programs*, p. 19, 2017.
- [67] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain utilization in healthcare: Key requirements and challenges," *2018 IEEE 20th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2018*, pp. 1–7, 2018.
- [68] Jp. Genestier *et al.*, "Blockchain for Consent Management in the eHealth Environment: A Nugget for Privacy and Security Challenges," *J Int Soc Telemed eHealth*, vol. 5, pp. 24–25, 2017.
- [69] M. Nofer, P. Gomer, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, 2017.
- [70] D. Shrier, W. Wu, and A. Pentland, "Blockchain & Infrastructure," *MIT Connect. Sci. Eng.*, pp. 1–18, 2016.
- [71] R. Stephen and A. Alex, "A Review on BlockChain Security," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 396, no. 1, 2018.
- [72] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with

- Enhanced Privacy and Availability,” *Proc. - 2017 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. CCGRID 2017*, pp. 468–477, 2017.
- [73] T. K. Mackey *et al.*, ““Fit-for-purpose?” - Challenges and opportunities for applications of blockchain technology in the future of healthcare,” *BMC Med.*, vol. 17, no. 1, pp. 1–17, 2019.
- [74] M. Greenberger, “Block what? The unrealized potential of blockchain in healthcare,” *Nurs. Manage.*, vol. 50, no. 5, pp. 9–12, May 2019.
- [75] K. V. O. Rabah, “Challenges & Opportunities for Blockchain Powered Healthcare Systems: A Review.” 2017.
- [76] I. Radanović and R. Likić, “Opportunities for Use of Blockchain Technology in Medicine,” *Appl. Health Econ. Health Policy*, vol. 16, no. 5, pp. 583–590, Oct. 2018.
- [77] A. Khatoon, “A Blockchain-Based Smart Contract System for Healthcare Management,” *Electronics*, vol. 9, no. 1, p. 94, Jan. 2020.
- [78] “The strategic business value of the blockchain market | McKinsey.” [Online]. Available: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>. [Accessed: 24-Mar-2020].
- [79] A. Khatoon, P. Verma, J. Southernwood, B. Massey, and P. Corcoran, “Blockchain in Energy Efficiency: Potential Applications and Benefits,” *Energies*, vol. 12, no. 17, p. 3317, Aug. 2019.
- [80] “Implementation of Blockchain on Peer-to-Peer Energy Trading.” [Online]. Available: <https://www.blockchain-council.org/blockchain/what-is-blockchain-how-does-it-relate-to-p2p/>. [Accessed: 24-Mar-2020].
- [81] “Blockchain and the Rise of Peer-to-Peer Power Markets - Microgrid Media.” [Online]. Available: <http://microgridmedia.com/blockchain-distributed-peer-peer-energy-markets/>. [Accessed: 24-Mar-2020].
- [82] M. R. Alam, M. St-Hilaire, and T. Kunz, “Peer-to-peer energy trading among smart homes,” *Appl. Energy*, vol. 238, no. October 2018, pp. 1434–1443, 2019.
- [83] M. Andoni *et al.*, “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” *Renew. Sustain. Energy Rev.*, vol. 100, no. February 2018, pp. 143–174, 2019.
- [84] F. P. (Fereidoon P. Sioshansi, *Consumer, prosumer, prosumer : how service innovations will disrupt the utility business model.* .
- [85] “First European energy trade over the blockchain.” [Online]. Available:

- <https://enerchain.ponton.de/index.php/11-first-european-energy-trade-over-the-blockchain>. [Accessed: 24-Mar-2020].
- [86] “Scaling up blockchain for peer-to-peer energy trading | Engerati,” <https://www.engerati.com/>.
- [87] “New York neighbours power up blockchain-based Brooklyn Microgrid.” [Online]. Available: <https://www.siliconrepublic.com/machines/brooklyn-microgrid-blockchain-energy-networks>. [Accessed: 24-Mar-2020].
- [88] C. Zhang, J. Wu, C. Long, and M. Cheng, “Review of Existing Peer-to-Peer Energy Trading Projects,” *Energy Procedia*, vol. 105, pp. 2563–2568, 2017.
- [89] “How can blockchain save energy? Here are three possible ways. | ACEEE.” [Online]. Available: <https://www.aceee.org/blog/2018/10/how-can-blockchain-save-energy-here>. [Accessed: 24-Mar-2020].
- [90] “ESCO contracts – Energy Service Companies (ESCOs) – Analysis - IEA.” [Online]. Available: <https://www.iea.org/reports/energy-service-companies-escos-2/esco-contracts>. [Accessed: 24-Mar-2020].
- [91] O. Gurcan, M. Agenis-Nevers, Y. M. Batany, M. Elmtiri, F. Le Fevre, and S. Tucci-Piergiovanni, “An Industrial Prototype of Trusted Energy Performance Contracts Using Blockchain Technologies,” *Proc. - 20th Int. Conf. High Perform. Comput. Commun. 16th Int. Conf. Smart City 4th Int. Conf. Data Sci. Syst. HPCC/SmartCity/DSS 2018*, no. July, pp. 1336–1343, 2019.
- [92] “Blockchain and energy efficiency: a match made in heaven? | ACEEE.” [Online]. Available: <https://www.aceee.org/blog/2018/04/blockchain-and-energy-efficiency>. [Accessed: 24-Mar-2020].
- [93] “IPEEC - Blockchain technology brings innovative ways to achieve energy efficiency.” [Online]. Available: <https://ipeec.org/bulletin/82-blockchain-technology-brings-innovative-ways-to-achieve-energy-efficiency-.html>. [Accessed: 24-Mar-2020].
- [94] J. A. F. Castellanos, D. Coll-Mayor, and J. A. Notholt, “Cryptocurrency as guarantees of origin: Simulating a green certificate market with the Ethereum Blockchain,” *2017 5th IEEE Int. Conf. Smart Energy Grid Eng. SEGE 2017*, pp. 367–372, 2017.
- [95] J. Lee and H. Kim, “in the Internet of Things,” no. july 2017, pp. 134–136, 2020.
- [96] W. Ejaz and A. Anpalagan, *Internet of Things for Smart Cities: Overview and Key Challenges BT - Internet of Things for Smart Cities: Technologies, Big Data and Security*. 2019.
- [97] C. Li and L. Zhang, “A Blockchain Based New Secure Multi-Layer Network Model

- p for Internet of Things,” pp. 33–41, 2017.
- [98] M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA*, vol. 0, pp. 1–6, 2016.
 - [99] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, “Internet of Things, Blockchain and Shared Economy Applications,” *Procedia Comput. Sci.*, vol. 58, pp. 461–466, 2016.
 - [100] A. Gervais, G. O. Karame, K. Wüst, and H. Ritzdorf, “On the Security and Performance of Proof of Work Blockchains Vasileios Glykantzis Srdjañ Capkun,” *Bitcoin.org*, 2017.
 - [101] D. Mendez Mena, I. Papapanagiotou, and B. Yang, “Internet of things: Survey on security,” *Inf. Secur. J.*, vol. 27, no. 3, pp. 162–182, 2018.
 - [102] “USING BLOCKCHAIN TO SUPPORT PROVENANCE IN THE INTERNET OF THINGS,” 2017.
 - [103] M. Banerjee, J. Lee, and K. K. R. Choo, “A blockchain future for internet of things security: a position paper,” *Digit. Commun. Networks*, vol. 4, no. 3, pp. 149–160, 2018.
 - [104] M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” *J. Inf. Secur. Appl.*, vol. 38, no. February, pp. 8–27, 2018.
 - [105] N. Fabiano, “Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation,” *Athens J. Law*, vol. 3, no. 3, pp. 201–214, 2017.
 - [106] O. Ala-Peijari, “Bitcoin The Virtual Currency: Energy Efficient Mining of Bitcoins. Master’s Thesis,” pp. 12–16, 2015.
 - [107] X. Zhu, “Autonomic Identity Framework for the Internet of Things,” 2017.
 - [108] S. Kornmesser, “Theoretizität im logischen empirismus und im strukturalismus - Erläutert am fallbeispiel des neurobiologischen konstruktivismus,” *J. Gen. Philos. Sci.*, vol. 39, no. 1, pp. 53–67, 2008.
 - [109] N. Fabiano, “The Internet of Things ecosystem : the blockchain and privacy issues . The challenge for a global privacy standard,” vol. 2060, 2017.
 - [110] C. Decker, C. Decker, and R. Wattenhofer, “Information propagation in the Bitcoin network Information Propagation in the Bitcoin Network,” *13-th IEEE Int. Conf. Peer-to-Peer Comput.*, no. August, pp. 1–10, 2016.
 - [111] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things : Challenges

- and Solutions.”
- [112] D. W. Kravitz and J. Cooper, “Securing User Identity and Transactions Symbiotically : IoT Meets Blockchain,” 2017.
 - [113] G. Zyskind, O. Nathan, and A. Pentland, “bok%3A978-1-4899-7537-9,” *Ieee*, pp. 180–184, 2015.
 - [114] J. A. Dev, “Bitcoin mining acceleration and performance quantification,” *Can. Conf. Electr. Comput. Eng.*, pp. 1–6, 2014.
 - [115] F. Kaup, P. Gottschling, and D. Hausheer, “PowerPi: Measuring and modeling the power consumption of the Raspberry Pi,” *Proc. - Conf. Local Comput. Networks, LCN*, pp. 236–243, 2014.
 - [116] A. Khatoon and P. Corcoran, “Privacy concerns on Android devices,” in *2017 IEEE International Conference on Consumer Electronics, ICCE 2017*, 2017.
 - [117] A. Khatoon and P. Corcoran, “Android permission system and user privacy-A review of concept and approaches,” in *IEEE International Conference on Consumer Electronics - Berlin, ICCE-Berlin*, 2017, vol. 2017-Sept.
 - [118] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” in *IEEE Access*, vol. 4, no. , pp. 2292–2303, 2016.,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
 - [119] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Sciascio, “Semantic Blockchain to Improve Scalability in the Internet of Things,” 2017.
 - [120] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, “The Blockchain-Based Digital Content Distribution System,” *Proc. - 2015 IEEE 5th Int. Conf. Big Data Cloud Comput. BDCloud 2015*, pp. 187–190, 2015.
 - [121] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of things: The road ahead,” *Comput. Networks*, vol. 76, pp. 146–164, 2015.
 - [122] A. Bahga and V. K. Madiseti, “Blockchain Platform for Industrial Internet of Things,” pp. 533–546, 2016.
 - [123] L. C. Ankit Songara, “Blockchain : A Decentralized Technique for Securing Internet of Things,” *Int. Conf. Emerg. Trends Eng. Innov. Technol. Manag. (ICET EITM-2017)*, no. October, pp. 2–5, 2017.
 - [124] M. Pustišek and A. Kos, “Approaches to Front-End IoT Application Development for the Ethereum Blockchain,” *Procedia Comput. Sci.*, vol. 129, pp. 410–419, 2018.
 - [125] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, “FairAccess: a new Blockchain-based access control framework for the Internet of Things,” *Secur. Commun.*

- Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.
- [126] J. Kreku, V. Vallivaara, K. Halunen, and J. Suomalainen, “Evaluating the efficiency of blockchains in IoT with simulations,” *IoTBDs 2017 - Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, no. April, pp. 216–223, 2017.
 - [127] A. Beikverdi and J. Song, “Trend of centralization in Bitcoin’s distributed network,” *2015 IEEE/ACIS 16th Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel/Distributed Comput. SNPD 2015 - Proc.*, pp. 1–6, 2015.
 - [128] G. Di Battista, V. Di Donato, M. Patrignani, M. Pizzonia, V. Roselli, and R. Tamassia, “Bitcoveview: Visualization of flows in the bitcoin transaction graph,” *2015 IEEE Symp. Vis. Cyber Secur. VizSec 2015*, pp. 1–8, 2015.
 - [129] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” *Inf.*, vol. 8, no. 2, 2017.
 - [130] R. Dennis and G. Owen, “Rep on the block: A next generation reputation system based on the blockchain,” *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015*, pp. 131–138, 2016.
 - [131] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, “Blockchains everywhere - A use-case of blockchains in the pharma supply-chain,” *Proc. IM 2017 - 2017 IFIP/IEEE Int. Symp. Integr. Netw. Serv. Manag.*, pp. 772–777, 2017.
 - [132] S. R. Bryatov and A. A. Borodinov, “Blockchain technology in the pharmaceutical supply chain: Researching a business model based on Hyperledger Fabric,” *CEUR Workshop Proc.*, vol. 2416, pp. 134–140, 2019.
 - [133] L. A. Linn and M. B. Koo, “Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research,” *ONC/NIST Use Blockchain Healthc. Res. Work.*, pp. 1–10, 2016.
 - [134] R. Dennis and G. Owen, “Rep on the block: A next generation reputation system based on the blockchain,” *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015*, pp. 131–138, 2016.
 - [135] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” *IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC*, vol. 2017-Octob, pp. 1–5, 2018.
 - [136] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, “Metrics for assessing blockchain-based healthcare decentralized apps,” *2017 IEEE 19th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2017*, vol. 2017-Decem, pp. 1–4, 2017.

- [137] “US20150332283A1 - Healthcare transaction validation via blockchain proof-of-work, systems and methods - Google Patents.” [Online]. Available: <https://patents.google.com/patent/US20150332283A1/en>. [Accessed: 25-Mar-2020].
- [138] “Welcome - HSE Open Data.” [Online]. Available: <https://data.ehealthireland.ie/>. [Accessed: 24-Mar-2020].
- [139] C. Burger, A. Kuhlmann, P. Richard, and J. Weinmann, “Blockchain in the energy transition. A survey among decision-makers in the German energy industry,” *Ger. Energy Agency*, p. 41, 2016.
- [140] World Energy Council and PwC, “The Developing Role of Blockchain,” p. 22, 2017.
- [141] I. Renewable Energy Agency, “Aggregators: Innovation landscape brief,” 2019.
- [142] and E. K. Saraju P. Mohanty, Uma Choppali, “Everything you wanted to know about smart cities,” *IEEE Consum. Electron. Mag. Electron.*, vol. 10, pp. 409–410, 2016.
- [143] “First European energy trade over the blockchain.” [Online]. Available: <https://enerchain.ponton.de/index.php/11-first-european-energy-trade-over-the-blockchain>. [Accessed: 25-Mar-2020].
- [144] T. Sousa, T. Soares, P. Pinson, F. Moret, T. Baroche, and E. Sorin, “Peer-to-peer and community-based markets: A comprehensive review,” *Renew. Sustain. Energy Rev.*, vol. 104, no. June 2018, pp. 367–378, 2019.
- [145] P. Verma, B. O'Regan, B. Hayes, S. Thakur, and J. G. Breslin, “EnerPort: Irish Blockchain project for peer- to-peer energy trading,” *Energy Informatics*, vol. 1, no. 1, 2018.
- [146] “Market Report Series energy efficiency 2018 Market Report Series energy efficiency 2018.”
- [147] “How Blockchain Improves the Energy Management Systems Sector | INN.” [Online]. Available: <https://investingnews.com/innspired/using-blockchain-to-improve-the-energy-management-systems-sector/>. [Accessed: 25-Mar-2020].
- [148] “How blockchain can make the world more energy efficient | World Economic Forum.” [Online]. Available: <https://www.weforum.org/agenda/2017/09/blockchain-energy-efficiency-finance>. [Accessed: 25-Mar-2020].
- [149] “Blockchain to increase efficiency and transparency in the energy sector | Commodity Inside.” [Online]. Available: <https://commodityinside.com/blockchain-can-increase-efficiency-transparency-energy-sector/>. [Accessed: 25-Mar-2020].
- [150] “Energy efficiency directive | Energy.” [Online]. Available: <https://ec.europa.eu/energy/topics/energy-efficiency/targets-directive-and->

rules/energy-efficiency-directive_en. [Accessed: 25-Mar-2020].

- [151] “The Italian White Certificates Scheme - D.Rotiroti, GSE.” [Online]. Available: <https://www.slideshare.net/gserinnovabili/the-italian-white-certificates-scheme-drotiroti-gse>. [Accessed: 25-Mar-2020].
- [152] F. Testa, “Italian Energy Efficiency White Certificate Scheme ” “Thanks to the Energy Efficiency Certificates (TEE), an innovative and pioneering system, we have achieved from 2005 to 2013 annual energy savings of 5Mtoe/year and incentivised more than €22 billion investments in energy efficiency.”
- [153] D. Di Santo, V. Venturini, D. Forni, and E. Biele, “The white certificate scheme : the Italian experience and proposals for improvement,” pp. 249–260, 2011.
- [154] “Best Blockchain Cryptocurrency Trading Platform in Singapore.” [Online]. Available: <https://newconomy.media/news/singapore-builds-solar-energy-trading-platform-on-blockchain>. [Accessed: 25-Mar-2020].
- [155] “Energy suppliers | Ofgem.” [Online]. Available: <https://www.ofgem.gov.uk/environmental-programmes/eco/energy-suppliers>. [Accessed: 25-Mar-2020].
- [156] P. R. S. A-e, “Energy Company Obligation (ECO3): Measures table,” no. January, p. 2020, 2020.
- [157] “About the ECO scheme | Ofgem.” [Online]. Available: <https://www.ofgem.gov.uk/environmental-programmes/eco/about-eco-scheme>. [Accessed: 25-Mar-2020].
- [158] A. Outchakoucht and J. P. Leroy, “Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things,” vol. 8, no. 7, pp. 417–424, 2017.
- [159] “CONNECTING MULTIPLE DEVICES WITH BLOCKCHAIN,” 2017.