CLOUD-BASED PAYMENT SYSTEMS VS BLOCKCHAIN BASED PAYMENT SYSTEMS

A Thesis Submitted
In Partial Fulfilment of the Requirements
for the Degree of

MASTER OF COMPUTER APPLICATIONS

By

Chirag Tyagi
(University Roll No. 2000290140038)
Astha Chauhan
(University Roll No. 2000290140034)
Divyanshu
(University Roll No. 2000290140044)

Under the Supervision of
Dr. Arun Kumar Tripathi
Professor

Submitted to

DEPARTMENT OF COMPUTER APPLICATIONS
KIET Group of Institutions, Ghaziabad
Uttar Pradesh-201206

(MAY 2022)

CERTIFICATE

Certified that **Chirag Tyagi (Enrollment No. 200029014005723)**, **Astha Chauhan (Enrollment No. 200029014005719), and Divyanshu (Enrollment No. 200029014005729)** have carried out the project work having "**CLOUD-BASED PAYMENT SYSTEMS VS BLOCKCHAIN BASED PAYMENT SYSTEMS**" for Master of Computer Applications from Dr. A.P.J. Abdul Kalam Technical University (AKTU**)** (formerly UPTU), Technical University, Lucknow under my supervision. The project report embodies original work, and studies are carried out by the student himself / herself and the contents of the project report do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Date:

Chirag Tyagi (University Roll No. 2000290140038)
Astha Chauhan (University Roll No. 2000290140034)
Divyanshu (University Roll No. 2000290140044)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date:

Dr. Arun Kumar Tripathi
Professor
Department of Computer Applications
KIET Group of Institutions, Ghaziabad

Signature of Internal Examiner **Signature of External Examiner**

Dr. Ajay Shrivastava
Head, Department of Computer Applications
KIET Group of Institutions, Ghaziabad

ABSTRACT

In the current scenario, one of the most popular systems for the transaction through electronic and cloud mediums is the ‘Online-Payment-System (OPS)’. The problem with this system is the involvement of a third party that may compromise the security of data and may also result in a slow transaction, while their transaction charges are also not constant. Our proposed system uses Blockchain that works on distributed ledger technology which further eliminates the need for a central authority to check any kind of manipulation in the data. Blockchain technology facilitates peer-to-peer transfer or payment without the involvement of third-party gateways. One of the key features of this technology is that every block comprises its hash as well as the hash of the previous block, no one can tamper with the records on the blockchain and thus it eliminates all the existing drawbacks of the current system. Against this background, in this paper, we propose a payment system using smart contracts which are based on blockchain technology and are self-executing contracts with all the terms and agreements written into lines of code which further makes the transactions trackable and irreversible. In this system details of all the transactions via blockchain network are visible to everyone present in the network and are also stored in the blockchain safely while ensuring data integrity. Therefore, the proposed system provides a safe and efficient way for transactions thus contributing to a good user experience which proves the significance of this research.

ACKNOWLEDGEMENTS

Success in life is never attained single handedly. My deepest gratitude goes to my thesis supervisor, **Dr. Arun Kumar Tripathi** for his guidance, help and encouragement throughout my research work. Their enlightening ideas, comments, and suggestions.

Words are not enough to express my gratitude to Dr. Ajay Kumar Shrivastava, Professor and Head, Department of Computer Applications, for his insightful comments and administrative help at various occasions.

Fortunately, I have many understanding friends, who have helped me a lot on many critical conditions.

Finally, my sincere thanks go to my family members and all those who have directly and indirectly provided me moral support and other kind of help. Without their support, completion of this work would not have been possible in time. They keep my life filled with enjoyment and happiness.

Chirag Tyagi

Astha Chauhan

Divyanshu

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

List of Chapters

CHAPTER 1

INTRODUCTION

OVERVIEW

In the current scenario, one of the most popular systems for the transaction through electronic and cloud mediums is the ‘Online-Payment-System (OPS)’. The problem with this system is the involvement of a third party that may compromise the security of data and may also result in a slow transaction, while their transaction charges are also not constant.

Being cloud based it possesses certain drawbacks like third party involvement, extra gateway charges, comparatively slower and much more whereas blockchain tends to make transaction free from all the drawbacks of the current system.

Blockchain is a distributed database that is shared across all of the nodes of a computer network is what is known as a blockchain. A blockchain may be thought of as an electronic database that holds information in a digital format. Blockchains are probably best recognised for their vital function in cryptocurrency systems like Bitcoin, in which they are used to keep a public ledger of transactions that is both safe and decentralised. The innovation that is brought about by a blockchain is that it ensures the accuracy and safety of a record of data and establishes confidence without the requirement of a third party that can be relied upon.

The way in which data is organised is one of the primary distinctions that can be drawn between a traditional database and a blockchain. A blockchain organises the data it stores into groups, which are called blocks, and each block can store a specific set of data. When a block's storage capacity is used up, it is sealed off and connected

to the block that came before it. This creates a chain of data that is referred to as the blockchain. Blocks have varying capacities. All of the newly received data that comes after a block that has just been added to the chain is assembled into a newly formed block, which, after it is complete, is likewise added to the chain.

With a database, the data is often organised into tables, but in a blockchain, the data is organised, as the name of the technology suggests, into chunks that are connected together called blocks. When implemented in a decentralised manner, this data structure inevitably generates an irreversible data timeline. When a block is completely filled, the information contained inside it is immutable and is added to this timeline. When a new block is added to the chain, that block receives a precise time stamp that is associated with its addition to the chain.

1.1 History of blockchain

A brief history of Blockchain is discussed as follows:

- In **1991**, Stuart Haber and W Scott Stornetta were the first to define a cryptographically safe chain of blocks. These researchers were looking for a Computational Practical Solution for time-stamping digital documents so they couldn't be tampered with or misdated. As a result, both scientists collaborated to create a system based on cryptography. The time-stamped papers are kept in a Chain of Blocks in this system.

- **In 1992,** Nick Szabo, a computer scientist, is working on 'bit gold,' a decentralised digital money.

- **In 2000,** Stefan Konst presented his cryptographic protected chain theory, as well as implementation suggestions.

- **In 2008,** A white paper describing the model for a blockchain was published in 2008 by developer(s) acting under the pseudonym Satoshi Nakamoto. In his white paper "A Peer to Peer Electronic Cash System," Satoshi Nakamoto proposed the notion of "Distributed Blockchain." He tweaked Merkle Tree's concept to develop a system that is more secure and keeps track of data

exchange history. His system uses a peer-to-peer time stamping network. Blockchain became the backbone of cryptography as a result of his system's success.

- **In 2009,** Nakamoto created the first blockchain as the public database for bitcoin transactions.

- **In 2014,** The potential of blockchain technology for other financial and inter-organizational transactions is investigated when it is divorced from the currency. The term "blockchain 2.0" is used to refer to uses other than money.

The Ethereum blockchain architecture incorporates computer programmes that represent financial assets such as bonds into the blocks. These are referred to as smart contracts. Figure 1.1 shows history of the blockchain technology diagrammatically.

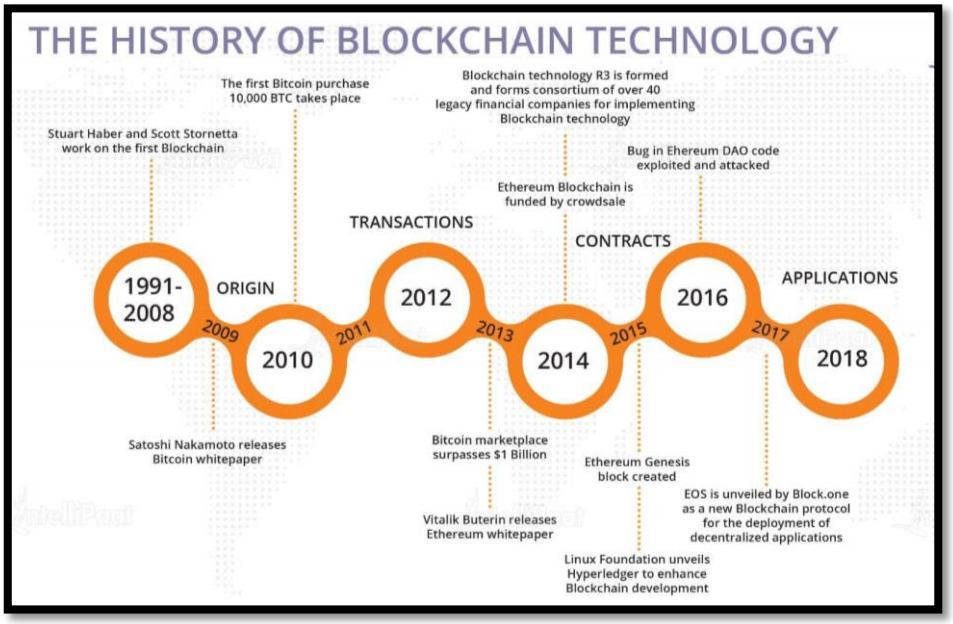

Figure 1.1: History of blockchain

Important points about Blockchain:

- **Bitcoin's role:** Nakamoto designed bitcoin as a type of payment that could be transmitted peer-to-peer without the need for a central bank or other authority to manage and maintain the ledger, similar to how actual cash may be. They

published their foundational essay in 2008 and launched the original code in 2009. While bitcoin was not the first online money to be proposed, it was by far the most successful version, since it solved various challenges in the area.

- The blockchain is the engine that operates Nakamoto's bitcoin ledger; the original and biggest blockchain is the one that still manages bitcoin transactions today.

- **The second generation:** After bitcoin, Ethereum is the second most popular blockchain implementation. Ethereum not only distributes the ether money, but it also allows for the storing and execution of computer code, enabling smart contracts. Ripple is a public ledger-based real-time gross settlement system, currency exchange, and remittance network.

1.2 Consensus Algorithm

The consensus algorithm is a method through which all peers in a Blockchain network reach a consensus on the current state of the distributed ledger. Consensus algorithms achieve blockchain network resilience and create trust amongst unknown peers in a distributed computing environment in this way. In essence, the consensus protocol ensures that every new block added to the Blockchain is the one and only version of the truth that all nodes in the Blockchain agree on. The Blockchain consensus protocol has several specific goals, including reaching an agreement, collaboration, cooperation, equal rights for all nodes, and each node's mandatory participation in the consensus process. As a result, a consensus algorithm seeks to identify a common ground that benefits the entire network. Figure 1.2 shows consensus protocol properties.

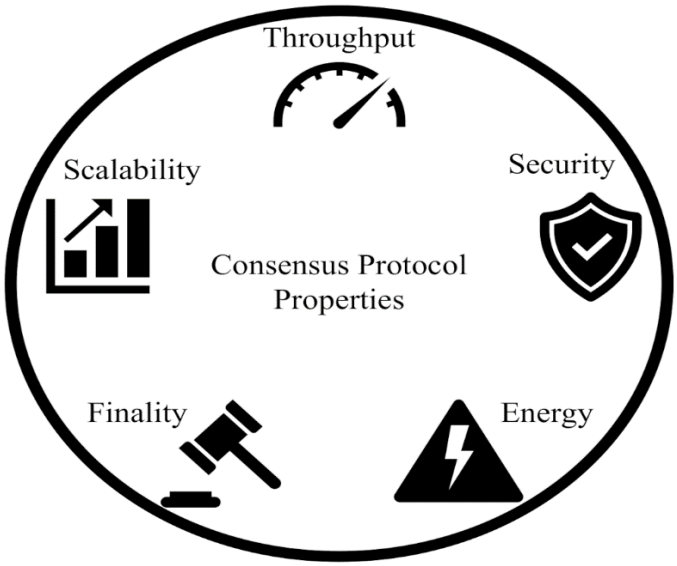

Figure 1.2: Consensus Protocol Properties

Consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Burn (PoB), among others, are utilised by blockchain to offer security.

1.2.1 Proof of Work (PoW)

"In order to produce new blocks in the Bitcoin blockchain, the Proof of Work consensus process requires solving a computationally difficult puzzle." The process is colloquially known as'mining,' and the nodes in the network that participate in mining are known as 'miners.' The motivation for mining transactions is derived from economic payoffs, in which competing miners are rewarded with 12.5 bitcoins (at the time of writing this article; this reward will be lowered by half its present value over time) and a modest transaction fee." Figure 1.3 shows the working of the Proof of Work Algorithm

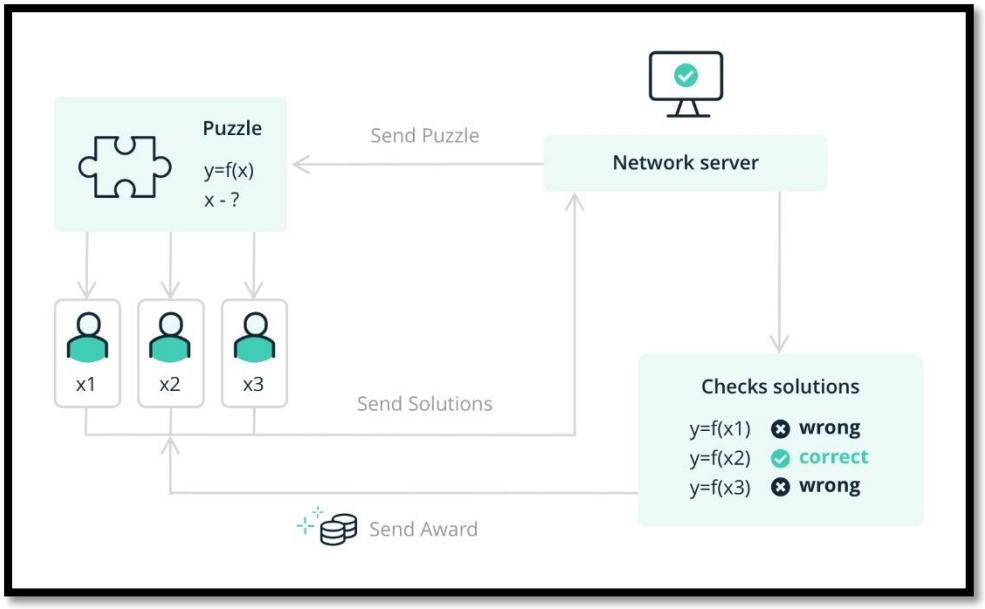

Figure 1.3: Working of Power of Work Algorithm

1.2.2 Proof of Stake (PoS)

The proof-of-stake concept allows cryptocurrency owners to stake coins and set up their own validator nodes. Staking is the act of pledging your coins to be used for transaction verification. While you stake your coins, they are locked up, but you may unstack them if you wish to swap them.

When a block of transactions is ready for processing, the cryptocurrency's proof-of-stake mechanism selects a validator node to evaluate it. The validator verifies that the transactions in the block are correct. If this is the case, they upload the block to the blockchain and collect cryptocurrency incentives for their efforts. However, if a validator suggests adding a block with incorrect information, they will be penalized by losing some of their staked holdings. Figure 1.4 shows the working of Proof of Stake Algorithm

Figure 1.4: Proof of Stake

1.2.2.1 Difference between Proof of Work and Proof of Stake

Difference between Proof of Work and Proof of Stake is shown in the Table 1.1.

Table 1.1: Difference between Proof of Work and Proof of Stake

S. No.	**Proof of Work (PoW)**	**Proof of Stake (PoS)**
1.	The likelihood of mining a block is determined by the amount of computing labour performed by the miner.	The likelihood of mining a block is determined by the amount of computing labour performed by the miner. The likelihood of validating a new block is dependent by the amount of stake a person has (how many coins they possess).
2.	The amount of computer labour performed by the miner determines the possibility of mining a block. The possibility of a new block being validated is determined by the amount of	The validator does not receive a block reward; instead, they receive a network charge.

	stake a person holds (how many coins they possess).	
3.	Miners must compete to solve complex riddles using their computer processing power to add each block to the chain.	As the block maker, there is no competition. An algorithm based on user stake selects the winner.
4.	To introduce a malicious block, hackers would require 51 percent of the processing power.	Hackers would need to hold 51% of all bitcoin on the network, which is very impossible.
5.	Proof of work systems use less energy and are less expensive, but they are more reliable.	Proof of Stake systems are far less expensive and energy efficient than POW systems, although they are less proved.
6.	Specialized equipment for increasing processing power.	A standard server grade unit is more than sufficient.
7.	Purchase of hardware requires an initial cost.	Initial investment to acquire a share and establish a reputation.
8.	Bitcoin is the most well-known cryptocurrency using a Proof-of-Work consensus building mechanism that employs the most well-known proof-of-work function, SHA256.	EOS (EOS), Tezos (XTZ), Cardano (ADA), Cosmos (ATOM), and Lisk are among cryptocurrencies that employ distinct versions of proof-of-stake consensus (LSK).

Figure 1.5 shows the difference between Proof of Work and Proof of Stake graphically.

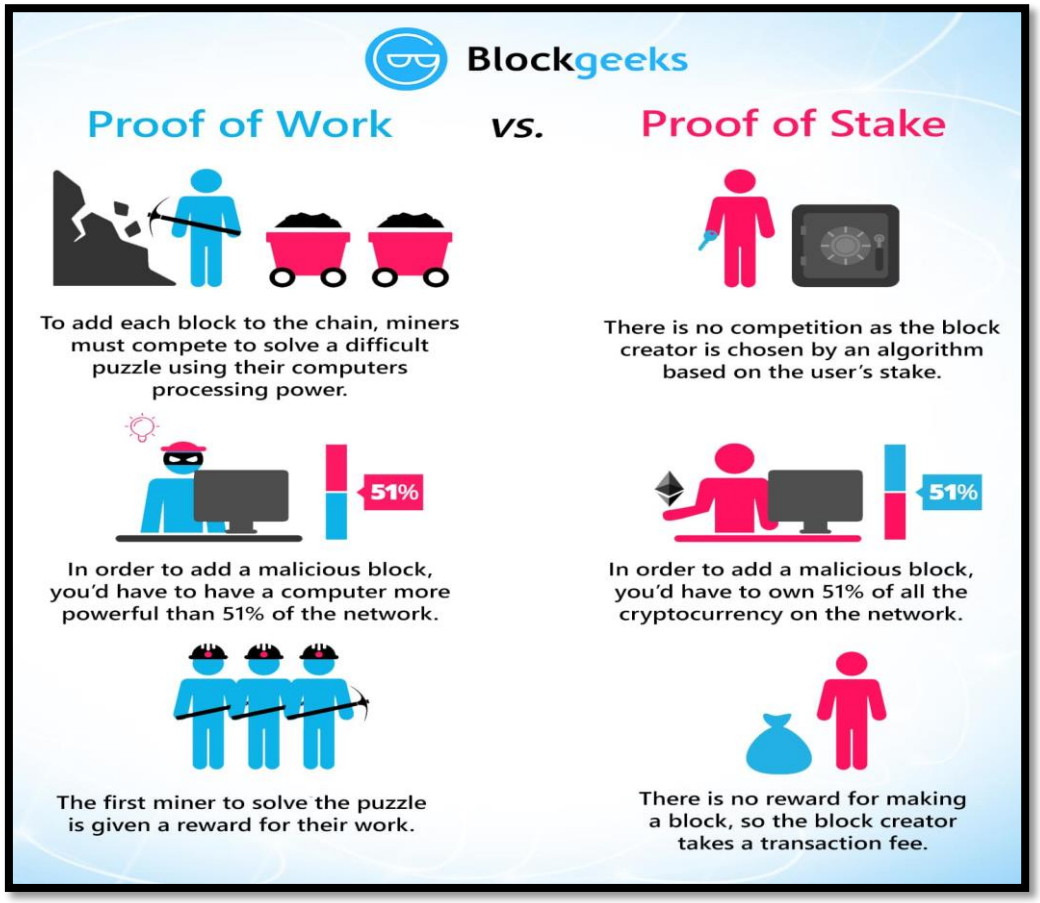

Figure 1.5: Proof of Work Vs Proof of Stake

1.2.3 Practical Byzantine Fault Tolerance (PBFT)

pBFT attempts to create a viable Byzantine state machine replication that can function even in the presence of rogue nodes in the system.

In a pBFT-enabled distributed system, nodes are ordered progressively, with one node serving as the primary (or leader node) and the rest serving as secondary (or the backup nodes). It is important to note that any eligible node in the system can become the primary by switching from secondary to primary (typically, in the case of a primary node failure). The objective is for all honest nodes to contribute to obtaining an agreement on the state of the system using the majority rule.

A realistic Byzantine Fault Tolerant system can work if the greatest number of malicious nodes is less than or equal to one-third of all nodes in the system. The system gets more secure as the number of nodes increases.

pBFT consensus rounds are divided into four phases:

a. The client initiates communication with the principal (leader) node.
b. The request is disseminated to all secondary (backup) nodes by the primary (leader) node.
c. The nodes (main and secondary) provide the required service and then respond to the client.
d. The request is properly fulfilled when the client receives'm+1' answers with the same result from various nodes in the network, where m is the maximum number of defective nodes permitted.

Figure 1.6 shows the working of the pBFT.

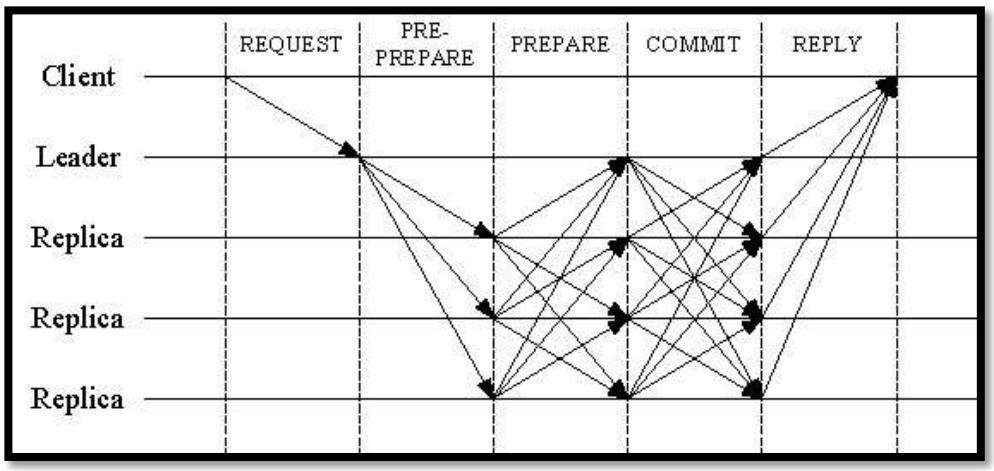

Figure 1.6: Working of pBFT

1.2.4 Proof of Burn (PoB)

By burning the money, miners reach a consensus in the Proof of Burn (PoB) procedure. It is a way for permanently eliminating cryptocurrencies from common use. In such cases, the practise of burning coins is utilised to validate transactions. As a result, the greater the number of coins burned by a miner, the more likely the block will be added to the network.

PoB utilises less energy than the proof of Work (PoW) system. Furthermore, unlike PoS systems, PoB does not require miners to stake their currencies in order to add a new block to the network.

Figure 1.7 shows the working of Proof of Burn

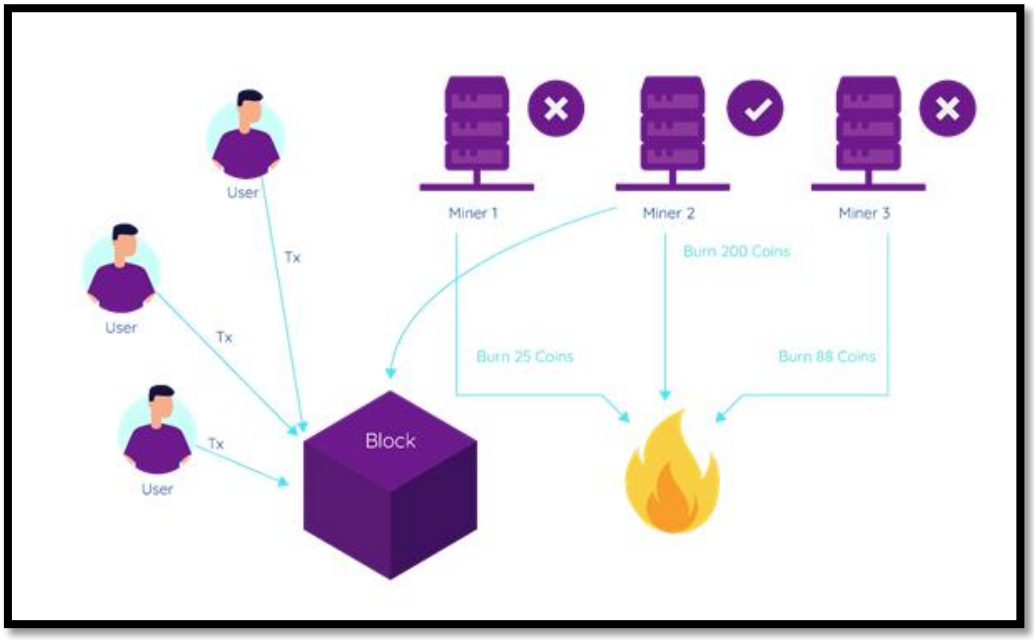

Figure 1.7: Working of Proof of Burn

1.3 Hashing in Blockchain

When discussing blockchain technology, the phrase "hashing" or "hash" is frequently used. Hashing is the translation and creation of input data of arbitrary length into a fixed-length string by a specified method. The Bitcoin hash algorithm is SHA-256, which stands for Secure Hashing Algorithm 256 bits. Because the original data cannot be recovered by decryption, this approach is a one-way cryptographic function.

The use of a cryptographic hash function can help to avoid fraudulent transactions, duplicate spending in blockchain, and password storage. But what exactly is Bitcoin hash, and what does it have to do with this context? In summary, this is a one-of-a-kind number that cannot be duplicated according to the method. As a result, it is widely used to validate the validity of a file. To put it another way, when a hashed file changes, its hash changes as well. And each consecutive hash is linked to the preceding hash, guaranteeing that all blocks are consistent.

Figure 1.8 depicts the working of hash in blockchain.

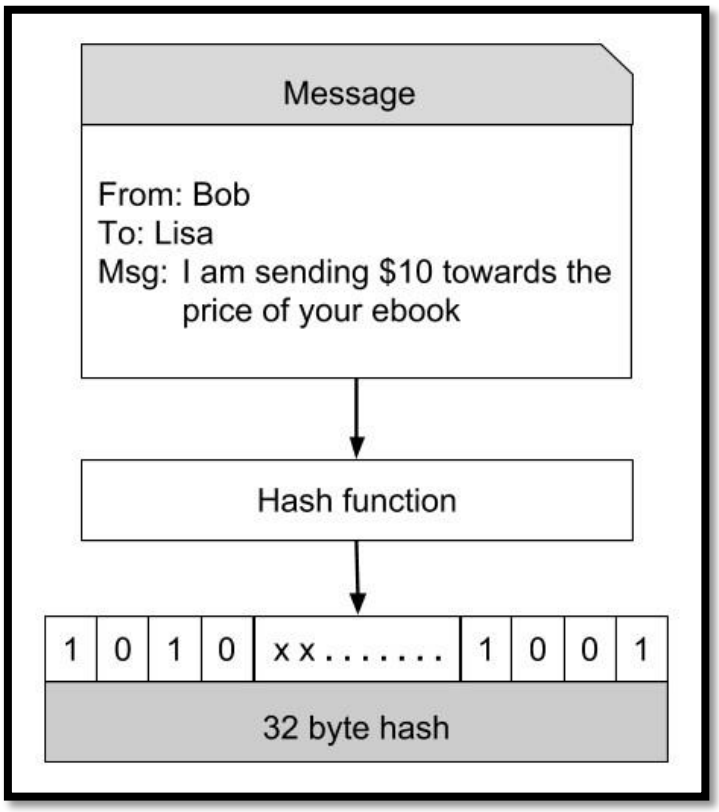

Figure 1.8: Working of Hash

Figure 1.9 shows the basic blockchain structure.

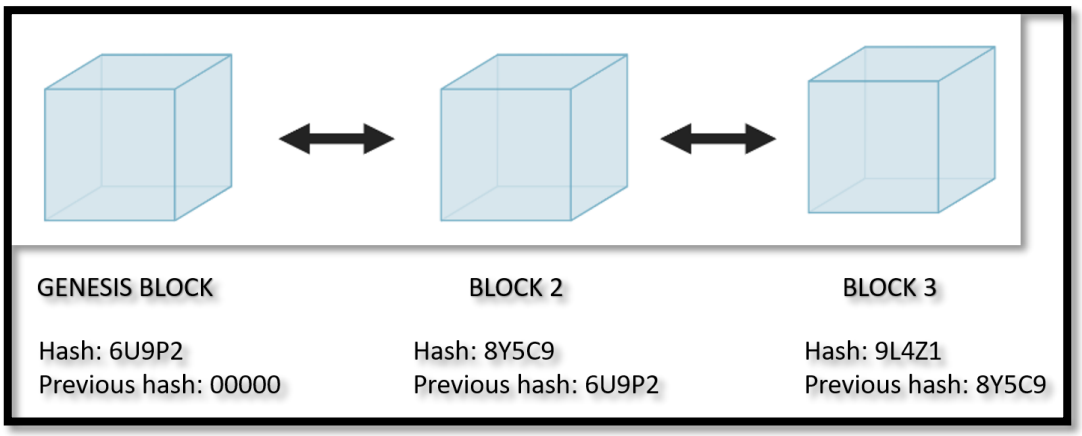

Figure 1.9 Blockchain structure

1.4 Types of Blockchain

Blockchains are majorly divided into 4 types:

1.4.1 Public blockchain

There are no constraints on a public blockchain. Anyone with an internet connection may join the network and begin verifying blocks and sending transactions. In most cases, such networks provide some sort of incentive to users who validate the blocks.

In any case, for transaction validation, this network often employs Proof of Work or Proof of Stake consensus techniques. It is, in fact, a "Public" network.

It was the model proposed by Satoshi Nakamoto in 2009. You may call it the mother of all technologies. Later, corporate organisations became interested in blockchain technology, changing the nature of the decentralised ledger and introducing private blockchains.

One may download the protocol at any moment in a public blockchain architecture, and you will not require permission from anybody. The public blockchains represent the perfect paradigm that has made the IT sector so profitable.

As a result, it is fully decentralised, with no single entity controlling the ecosystem. A private blockchain, on the other hand, may only be edited and amended by the entity that owns it.

A public blockchain eliminated the need for a third party. The system has its own inherent flow, much like a moving river. The flow channel is not controlled by anybody, yet everyone utilises it. So, how can you define it simply? A digital public ledger that is self-governed, totally decentralised, and autonomous. It's similar to the concept of democracy of, by, and for the people!

1.4.2 Permissioned or private blockchain

Private blockchains, such as Ripple and Hyperledger, are faster because they have a smaller user base, which means it takes less time to achieve a consensus to validate a transaction. Private blockchains are easily scalable and can process thousands of transactions per second.

A private blockchain uses a centralised network to speed up the transaction process. A centralised network creates the issue of trust, which is addressed by a public blockchain. The legitimacy of a transaction cannot be confirmed on private networks and is dependent on the reliability of the authorised nodes.

Furthermore, fewer nodes make the network more vulnerable to malicious assaults.

Because it is difficult to track the persons involved, the anonymity of public blockchains has made it a popular go-to transaction mechanism for criminal activity in the darknet.

1.4.3 Federated or consortium blockchain

Anyone with an internet connection can view public blockchains or open blockchains. Private blockchains are typically used by businesses to solve business cases and provide corporate software solutions. The consortium blockchain, which is more of a private type of distributed ledger, is a mix of the previous two blockchains. The major goal of a consortium blockchain is to increase cooperative effects in order to tackle the ongoing issues of a certain sector. Consortium blockchain may be used by organisations with shared aims to improve transparency, accountability, and workflow.

According to the Deloitte analysis, nearly 74% of firms are opting for blockchain consortiums. Many blockchain platforms are promoting themselves as the foundation for different organisational solutions. Instead of beginning from scratch, consortium blockchain allows the new kid on the block to join the current framework and exchange information. This technology enables enterprises to

collaborate to identify answers, saving time and money on development. Federated blockchains are another name for consortium blockchains.

1.4.4 Hybrid blockchain

A hybrid blockchain is a distinct form of blockchain technology that combines elements of both public and private blockchains or attempts to use the best features of both public and private blockchain solutions.

In a hybrid blockchain, transactions and data are rendered private but may be validated as necessary, for as by granting access via a smart contract. Private information is stored within the network but may still be verified.

Even if a private company owns the hybrid blockchain, it cannot alter transactions. A hybrid blockchain enables organisations to set up a private, permission-based system alongside a public, permissionless system, allowing them to control who has access to specific data stored in the blockchain and which data is made public.

When a user joins a hybrid blockchain, they have total network access. Unless they participate in a transaction, the user's identity is safeguarded and shielded from other users. The opposite party is then informed of their identification. The following table provides a detailed comparison among these three blockchain systems:

Table 1.2: Comparison between Public, Private, Hybrid and Consortium Blockchain

	Public (permissionless)	**Private** (permissioned)	**Hybrid**	**Consortium**
ADVANTAGES	+ Independence + Transparency + Trust	+ Access control + Performance	+ Access control + Performance + Scalability	+ Access control + Scalability + Security
DISADVANTAGES	– Performance – Scalability – Security	– Trust – Auditability	– Transparency – Upgrading	– Transparency
USE CASES	▪ Cryptocurrency ▪ Document validation	▪ Supply chain ▪ Asset ownership	▪ Medical records ▪ Real estate	▪ Banking ▪ Research ▪ Supply chain

3.5 Blockchain Architecture

The following are the fundamental blockchain architecture components:

a. **Node** – Within the blockchain architecture, a node is a user or machine (each has an independent copy of the whole blockchain ledger)
b. **Transaction** – the smallest building block of a blockchain system (records, information, etc.) that serves the blockchain's function.
c. **Block** – A block is a data structure that stores a collection of transactions that are sent to all network nodes.
d. **Chain** – A chain is a specified succession of blocks.
e. **Miners –** Miners are nodes that execute block verification before adding anything to the blockchain structure.
f. **Consensus (consensus protocol)** – It is a collection of rules and procedures for carrying out blockchain activities.

Any new record or transaction on the blockchain necessitates the creation of a new block. Each record is then verified and digitally signed to confirm its authenticity. This block should be validated by the majority of system nodes before being uploaded to the network.

Figure 1.10 shows the architecture of blockchain.

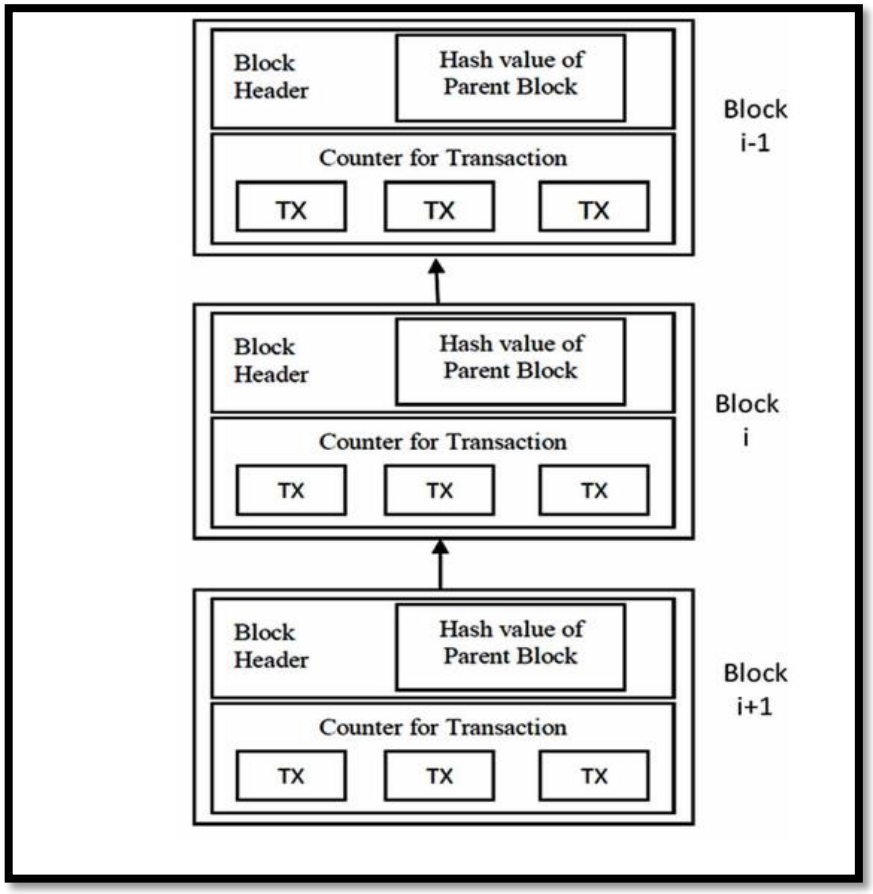

Figure 1.10: Blockchain Architecture

1.6 Scope of Research

The main focus of this research is to come up with an alternative transaction method other than current cloud-based transactions to enable payment transfer between two parties. In this proposed system we have used a smart contract which are deployed on the Ethereum blockchain to create a secure transaction possible between two parties.

1.7 Research Methodology

a. Referencing Blockchain research papers, smart contracts, and speaking with a Blockchain developer.
b. The existing cloud-based approach has significant shortcomings, including security flaws, privacy concerns, and expensive management costs.

c. The idea is to create a smart contract for enabling transaction between two parties so as to remove the drawbacks in the current system like third party involvement, time-consuming process, etc.

1.8 Thesis Outline

Chapter 1 describes blockchain technology, its advantages, the working of blockchain technology, how blockchain secures itself with the help of consensus algorithms, and how it is used in transaction. Chapter 2 is dedicated to the literature review whereas in Chapter 3 smart contracts and it's use in blockchain is discussed. Chapter 4 presents the deployment of smart Contracts in transaction using the Ethereum blockchain and Chapter 5 describes the long-term environmental aims, i.e. how the proposed system would benefit society where Chapter 6 gives the conclusion and Chapter 7 tells about the possible future work regarding the proposed system and Chapter 8 contains the references of the research papers.

CHAPTER 2

LITERATURE REVIEW

A literature review covers published material in a certain topic area, as well as information published within a specific time period.

A literature review can be as basic as a summary of the sources, but it generally follows an organizational structure and incorporates summary and synthesis. A summary is a recap of the source's main information, but a synthesis is a reorganization or reshuffling of that material. It might provide a fresh take on old material or merge new and old perspectives. It might also chart the intellectual evolution of the field, including key controversies. Depending on the circumstances, the literature review may assess the sources and advise the reader on the most topical or relevant. Some of them are discussed below.

- Zibin Zheng, Shaoan Xie, et al. [1], discussed about blockchain in their paper, the backbone of Bitcoin, has recently gained a lot of attention. Blockchain functions as an immutable record that enables for decentralised transactions. Blockchain-based applications are emerging in a variety of industries, including financial services, reputation systems, and the Internet of Things (IoT), among others. However, many hurdles of blockchain technology, including as scalability and security issues, have to be solved. This paper provides an in-depth look of blockchain technology. First, the author's present an explanation of blockchain architecture before comparing some common consensus methods utilised in various blockchains. In addition, technological

hurdles and recent improvements are briefly discussed. They also discussed potential blockchain future trends.

- Maher Alharby, Amjad Aldweesh, et al. [2], discussed Smart contracts on the blockchain which are computer programmes that codify an agreement between untrustworthy people. If certain circumstances are satisfied, smart contracts are performed on a blockchain system, eliminating the need for a trusted third party. Blockchains and smart contracts have gotten a lot of interest in recent years, including from academics. Authors conduct a thorough mapping investigation of all peer-reviewed technology-oriented smart contract research. Authors are interested in two things: providing a review of the scientific literature and identifying academic research trends and adoption. Authors solely look at peer-reviewed scientific articles to see how academic academics have adopted smart contract technology and produced scientific results. Authors acquired all research articles from the major scientific databases and identified 188 relevant publications using the systematic mapping approach. These articles were divided into six categories: security, privacy, software engineering, application, performance and scalability, and other smart contract-related subjects. Authors discovered that most of the articles (approximately 64 percent) fit under the applications and software engineering categories. In comparison to our 2017 study [1,] authors see an eightfold rise in the number of relevant publications, with a significant shift toward smart contract applications.

- Karthikeya Thanapal, Dhiraj Mehta, et al. [3], discussed that increasing the number of records is possible using blockchain, where each record is connected via cryptography. Every block in the chain comprises a timestamp, transaction data, and a cryptographic hash of the preceding block. This is a secure system that will eventually replace the present online payment system. A modern internet payment gateway is vulnerable to hackers, who can meddle with the network and cause money loss. Not only that, but the transaction must pass through various payment systems, which takes time and increases the likelihood of the transaction failing. So, our solution would use blockchain,

which enables online transactions, allowing online payments to be transmitted directly from one party to another without going through a financial institution and in a safe manner. This technology lets two parties to conduct online transactions using cryptographic evidence without relying on or trusting a third party. Author utilises a proof of work technique to record transactions, making it computationally hard for an attacker to modify. Digital signatures are one component of the solution for maintaining the security and integrity of data stored on a blockchain.

- Yinghui Zhang, Robert H, et al. [4], discussed about Deng Outsourcing services, as an appealing cloud computing business model, typically include online payment and security concerns. Mutual mistrust between consumers and outsourced service providers may stymie cloud computing's widespread adoption. Nonetheless, most existing payment systems only take into account a certain type of outsourced service and rely on a trusted third-party to ensure fairness. In this article, we offer BCPay, a blockchain-based fair payment framework for cloud computing outsourcing services, in order to provide safe and fair payment of outsourcing services in general without relying on any third-party, trusted or not. Authors discussed BCPay's system architecture, requirements, and adversary model first, then describe its design in depth. Our security research shows that BCPay achieves Soundness and Robust Fairness, which means that the fairness is impervious to eavesdropping and malleability attacks. Furthermore, our performance study reveals that BCPay is quite efficient in terms of transaction volume and calculation cost. Authors also build a blockchain-based verifiable data possession scheme in cloud computing and a blockchain-based outsourced computation protocol in fog computing as illustrative uses of BCPay.

- Jingyu Zhang, Siqi Zhong, et al. [5], discussed in their paper that many attempts are now being made to ensure data privacy protection and reliable information tracing, but conventional solutions are still subject to information loss, privacy leakage, and other threats until blockchain technology emerges. To assure the security and dependability of data kept in a distributed network,

blockchain can record historical data by constructing a collaboratively maintained and tamper-resistant public ledger. It realises a decentralised network architecture, which has the potential to deliver innovative solutions to various industries, including information tracing and privacy protection. Blockchain technology has increasingly drawn the interest of all industries in recent years, and this paper outlines the existing blockchain-based systems and applications. Authors primarily examine blockchain traceability technology applications in many areas, blockchain decentralised applications, and other blockchain applications in data security protection, in that order. This work may create new chances and difficulties for the future development of different sectors.

- HuaqunGuo, XingjieYu, et al. [6], discussed in their paper about decentralization, autonomy, integrity, immutability, verification, fault-tolerance, anonymity, auditability, and transparency are all desired characteristics of blockchain technology. In this paper, author first conduct a more in-depth survey of blockchain technology, specifically its history, quantitative comparisons of consensus algorithms, details of cryptography in terms of public key cryptography, Zero-Knowledge Proofs, and hash functions used in the blockchain, and a comprehensive list of blockchain applications. Furthermore, the security of blockchain is emphasised in this study. Author investigate blockchain security using risk analysis to provide comprehensive blockchain security risk categories, analyse real-world attacks and flaws against blockchain, and review newly established blockchain security remedies. Finally, the difficulties and research trends for more scalable and secure blockchain systems for big deployments are discussed.

- Mohammad Rasheed Ahmed, Kandala Meenakshi, et al. [7], discussed in their paper about payment mechanisms which have changed dramatically as Internet technology has advanced, from entity exchange to Internet banking. Almost every industry has undergone the transition from traditional to digital technology. Making payments has become easier than ever with the introduction of online payment and digital wallet systems, and with the

increasing demand for such services, the number of consumers using fast money transfer systems is rapidly expanding. However, the current online payment system includes flaws such as a single point of failure, lack of transparency, and an insider problem. Furthermore, security in such online payments is critical in order to reduce risks and cost inefficiencies. This paper proposes a private and permissioned Blockchain-based Payment System for the Indian banking industry. The suggested architecture is based on the Istanbul Byzantine Fault Tolerance (IBFT) consensus and addresses bank interaction with the system.

- Tharaka Hewa, Yining Hu, Kandala Meenakshi, et al. [8], discussed in their paper that throughout the previous few decades, the industrial and computing research setting has seen numerous revolutions. The blockchain-based smart contract has sparked great academic interest due to distinctive properties such as decentralised transaction storage, autonomous execution of contract instructions, and decentralised trust formation. Blockchain-based smart contracts have the potential to revolutionise the working architecture of practically all businesses, resulting in higher service standards. Blockchain-based smart contracts have applications ranging from industrial applications such as cryptocurrency systems to logistics, agriculture, real estate, energy trading, and so on. Blockchain decentralisation is one of the most significant advances in technological research since the Internet of Things (IoT) and edge computing gained traction. A variety of study is being conducted to examine the prospects for smart contracts and blockchain technology to be used to many businesses. It is critical to identify the technological features of blockchain-based smart contracts in order to develop and sharpen the capabilities that are now available. The purpose of this study is to identify the important technical elements of blockchain-based smart contracts, as well as the accompanying future research paths.

- X. Liang, S. Shetty, Kandala Meenakshi, et al. [9], discussed in their paper that cloud data provenance is metadata that tracks the history of a cloud data object's creation and actions. Data accountability, forensics, and privacy all

rely on secure data provenance. In this work, author propose a blockchain-based decentralised and trustworthy cloud data provenance architecture. Blockchain-based data provenance can give tamper-proof records, provide data accountability transparency in the cloud, and aid to improve the privacy and availability of provenance data. To gather provenance data, author employ the cloud storage scenario and the cloud file as a data unit to identify user actions. By incorporating provenance data into blockchain transactions, author develop and build ProvChain, an architecture for collecting and verifying cloud data provenance. ProvChain works in three stages: (1) collecting of provenance data, (2) storage of provenance data, and (3) validation of provenance data. According to the results of the performance study, ProvChain delivers security characteristics such as tamper-proof provenance, user privacy, and dependability with little overhead for cloud storage applications.

- X. Wang, X. Xu, L. Feagan, S. Huang, L. Jiao, et al. [10], discussed in their paper that the real-time gross settlement system (RTGS) is the foundation of interbank payment transactions. The extraordinary growth of large-value wholesale payments has compelled financial institutions to create inter-bank payment systems (IBPS) with better levels of throughput, security, and stability. This intriguing method to IBPS orchestration makes use of developing blockchain technology, which has been successfully used to provide distributed trust and secrecy for a variety of financial industry applications. However, blockchain is not a panacea for IBPS, which faces several issues because of high-value transactions. Financial institutions anticipate not just a straightforward transition from traditional RTGS to a blockchain platform, but also a decentralised system with improved secrecy, instruction settlement finality, a liquidity preservation mechanism, and more efficient gridlock resolution mechanisms. Author provide an end-to-end IBPS prototype built on the Hyperledger Fabric enterprise blockchain platform in this article. For interbank payment activity, the prototype enables gross settlement, impasse resolution, and reconciliation. As part of the early study for the Ubin Project, this prototype has been shown to deliver a better degree of payment settlement service.

- Salar Ahmadisheykhsarmast, Rifat Sonmez, et al. [11], discussed in their paper that Project participants must be paid on time for construction projects to be completed successfully; unfortunately, the construction sector globally suffers from inadequate payment procedures. Existing research investigated the causes and implications of the payment dilemma, but relatively few studies suggested solutions. This article introduces SMTSEC, a unique smart contract payment security solution designed to eliminate or reduce payment concerns in the construction industry. The SMTSEC maintains the security of construction contract payments using an automated computerised system based on a decentralised blockchain. An actual construction project is used to investigate the potential contributions and limits of the proposed SMTSEC. The SMTSEC's key value is that it provides a new mechanism for timely and transparent payment of construction projects by assuring security of payment for works in progress without the administrative fees and responsibilities of trusted middlemen such as attorneys or banks.

- Lin Zhong, Qianhong Wu, et al. [12], discussed in their paper that off-chain payments are a critical strategy for increasing the scalability of blockchain-based cryptocurrencies. However, because tokens locked in off-chain channels cannot be transferred from one channel to another, current off-chain payment systems have capacity limitations. Author's offer a secure large-scale immediate payment (SLIP) method in this paper to boost the capacity of blockchain networks. The SLIP mechanism connects some of the off-chain channels with an aggregate signature scheme, allowing tokens locked in these channels to move from one to the next. As a result, the quantity of tokens distributed in these channels is the sum of all locked-in tokens rather than the minimum locked-in tokens. In other words, it enhances the negotiability of tokens trapped in these linked off-chain channels. Furthermore, because payers may accumulate signatures gradually, payees only need to check a line of transactions once in each transaction, whereas nodes (miners) that maintain the blockchain system only need to validate all transactions once, making the SLIP system incredibly efficient. Authors demonstrated that the SLIP system is secure if the underlying blockchain system is secure and aggregate signature

fulfils aggregate chosen-key security. Finally, evaluations demonstrate that the SLIP system has a far bigger capacity than the Lightning Network.

- H. Singh and A. Dubey, et al. [13], discussed in their paper that traditional electronic payment methods have challenges with ensuring safety, trust, and accuracy. Blockchain technology has the potential to address these issues. The bibliometric trends of blockchain technology and electronic payments research show that China, Chinese authors, and Chinese universities dominate the subject. China was followed by the United States of America. The main journals were IEEE Access and Lecture Notes in Computer Science. Future research might concentrate on expanding the use of blockchain technology in electronic payments, and future researchers could concentrate on papers and resources from China and the United States of America for knowledge updates and research collaborations**.**

- S. Joseph and S. Karunan, et al. [14], discussed in their paper that Blockchain, the underlying technology underpinning Bitcoin, is a new industry technology. Blockchain has the potential to improve existing corporate processes by making them more democratic, transparent, secure, and efficient. Banking industry are the first to capitalise on this technology's disruptive potential. The Indian banking system is one of the most complicated bank payment systems on the planet. The present infrastructure utilised by Indian banks is a real-time gross settlement system with a centralised design. Transaction processing is sluggish and cumbersome as a result of this centralised design. It also results in a significant quantity for security and recovery considerations. The real-time gross settlement system necessitates a high level of security, robustness, and performance. The primary goal is not to migrate from old systems to blockchain platforms, but to create a system that provides security, secrecy, and a decentralised money lending mechanism. A unique method is suggested here that enables a decentralised banking system and services based on the Ethereum blockchain platform. Using distributed ledger technology, the system supports several services such as money deposit, money transfer, and loan checking, among others.

- N. P. Pravin, K. P., et al. [15], discussed in their paper that people's lives have been transformed as digital technology has advanced. Many dangers and scams have been found in the financial sector. Banking systems employ centralised databases, which allows attackers easy access to data and renders the system unsafe. The disadvantage of this centralised system may be mitigated by restructuring the system through the use of blockchain technology without the need of tokens. For storing and accessing data in a database, blockchain employs a decentralised design. This lowers compromised database attacks. Transactions made using blockchain technology are validated by each block in the chain, making the transaction more secure and allowing the financial system to operate more quickly.

- Lin Zhong, Qianhong Wu, Jan Xie, et al. [16], discussed in their paper that in the present blockchain systems, ever-increasing transaction fees, severe network congestion, and poor transaction rates limit their widespread adoption. Author propose a secure versatile light payment (SVLP) system to alleviate this problem. The SVLP uses only a digital signature algorithm and a one-way function, and its security is comparable to that of existing blockchain systems such as Bitcoin and Ethereum. The suggested approach consumes very little power since payers and payees only need one-way functions to complete repeated transactions, rather than the costly digital signature algorithms. Furthermore, the payment and refunding methods are adaptable. This is because the denomination in our scheme is divisible, and users do not need to check the preimages on the lengthy chain one by one. Finally, because the transaction may be performed off-chain and offline, it can be utilised in rural places or areas affected by natural disasters when communication infrastructure is lacking or damaged. All of these characteristics show that our strategy is both practical and adaptable.

- Mohanty, Debasis, et al. [17], discussed in their paper that interoperability protocols are required for blockchain-technology uptake due to the widely fragmented blockchain and cryptocurrency environment. The immediate

consequence of interchain interoperability is automated cryptocurrency switching. A comprehensive study of the available literature on Blockchain interoperability and atomic cross-chain transactions was conducted. Author researched many blockchain interoperability options, including industrial solutions, classified them, defined the major mechanisms employed, and provided numerous examples for each category. Author concentrated on atomic transactions across blockchains, often known as atomic swap. Furthermore, author investigated contemporary atomic swap implementations as well as architectural approaches, and author derived research difficulties and obstacles in cross-chain interoperability and atomic swap. Atomic swap may quickly transfer tokens while drastically lowering related costs without the use of centralised authority, facilitating the construction of a sustainable payment system for greater financial inclusion.

- C. V. N. U. B. Murthy, M. L. Shri, et al. [18], discussed in their paper that blockchain technology is a distributed ledger with data records covering all information of transactions carried out and disseminated across network nodes. All transactions in the system are validated by consensus procedures, and once recorded, data cannot be changed. Blockchain technology is the enabling technology for Bitcoin, a prominent digital cryptocurrency. "Cloud computing is the technique of storing, managing, and processing data on a network of remote computers housed on the internet rather than a local server or a personal computer." It still faces several issues such as data security, data management, compliance, and dependability. In this post, author discussed some of the major difficulties that the cloud faces and provided solutions by combining it with blockchain technology. Author will conduct a quick review of previous studies focusing on blockchain integrating with the cloud to demonstrate their superiority. In this study, authors also created an architecture that integrates blockchain and cloud, demonstrating the connection between blockchain and cloud.

- J. Sidhu, et al. [19], discussed in their paper that while Bitcoin [Nak] solved the double spend problem and offered work with timestamps on a public

ledger, it has not yet expanded the capabilities of a blockchain beyond a transparent and public payment system. Satoshi Nakamoto's first reference client had a decentralised marketplace service that was eventually discontinued owing to a lack of resources [Deva]. Author built on Nakamoto's vision by developing a set of commercial-grade services that support a wide range of business use cases, such as a fully developed blockchain-based decentralised marketplace, secure data storage and transfer, and unique user aliases that connect the owner to all services controlled by that alias.

- F. Gao, L. Zhu, et al. [20], discussed in their paper that a component of V2G networks, EVs receive power not only from the grid but also from other EVs and may regularly send the power back to the grid. Payment records in V2G networks may be used to extract user habits and make better decisions about power supply, scheduling, pricing, and consumption. However, sharing payment and user information presents major privacy concerns, on top of the current problem of safe and dependable transaction processing. In this paper, author propose a blockchain-based payment method for V2G networks that allows data exchange while protecting sensitive user information. The method presents a registration and data maintenance procedure based on a blockchain approach, which maintains user payment data confidentiality while allowing payment audits by privileged users. Our concept is deployed using Hyperledger to ensure its practicality and efficacy.

- Qinghua Lu, Xiwei Xu, et al. [21], discussed in their paper that blockchain-based payments have piqued the interest of everyone from amateurs to corporations to regulatory authorities as the game-changing use of blockchain technology. Blockchain enables quick, safe, and cross-border payments without the use of intermediaries like banks. Because blockchain technology is still in its early stages, systematic knowledge that provides a holistic and comprehensive view on creating blockchain-based payment applications has yet to be produced. If such information could be produced in the form of a collection of blockchain-specific patterns, architects may utilise those patterns to develop a blockchain-enabled payment application. As a result, in this paper,

author first define a token's lifetime before presenting 12 patterns that address essential elements of allowing token state transitions in blockchain-based payment systems. The lifecycle and annotated patterns give a payment-focused systematic perspective of system interactions as well as guidance on how to apply the patterns effectively.

- N. El Madhoun, F. Guenane, et al. [22], discussed in their paper that NFC technology is now employed in contactless payment applications, with NFC payment capabilities available in credit/debit cards, smartphones, and payment terminals. As a result, an NFC payment transaction is carried out in a straightforward and practical manner. EMV is a security protocol that applies to both contact and contactless payment systems. However, during an EMV payment transaction, this standard does not enforce the following two major security limitations between a client payment device and a payment terminal: (1) mutual authentication and (2) confidentiality of sensitive financial data transferred. Because the transaction is done via NFC radio waves in an open environment, these flaws pose a significant danger in the case of NFC payment. Contact payment reduces risk since the transaction is completed in a closed environment by putting the card into the terminal. Author presents a novel security protocol for NFC payment transactions based on a Cloud architecture in this study. Author use the Scyther tool, which gives formal proofs for security protocols, to validate this proposal.

- Z. Wang, et al. [23], discussed in their paper that computing is causing a big change in e-business. Software, platforms, and infrastructure arrive on the Internet one after the other, extending the electronic business chain and becoming the most recent paradigm known as entire e-business. This thesis proposes a cloud computing-based online payment method after examining cloud computing theories and the constraints of existing online payment models. The mode's organisational structure, technical architecture, and business processes have been designed and analysed to serve as references for establishing collaboration with the "four chains" - commerce chain, capital

chain, logistics chain, and government chain - and realising the integration of banking system and entity industry system.

- S. Wang, Y. Wang, et al. [24] discussed in their paper that today, an increasing number of businesses and people are outsourcing their data to cloud storage systems. Data deduplication is an important technology for lowering the storage costs of cloud storage systems. The customer can outsource the data files to the cloud storage server and pay for them in a cloud storage system using deduplication technology. One of the most important difficulties in the cloud deduplication storage system is fair remuneration. Currently, a number of safe deduplication encryption algorithms have been developed to ensure client data privacy. However, most contemporary fair payment solutions produce payment tokens using standard electronic currency systems, which necessitates the employment of a trusted authority to avoid double-spending. Trusted authority will become payment system bottlenecks. To address this issue, author propose a new decentralised fair payment mechanism for cloud deduplication storage systems using Ethereum blockchain technology in this study. The new protocol takes use of blockchain technology's decentralisation by allowing direct transactions without the need of trusted third parties. If a malevolent circumstance happens in the new protocol, the system may ensure fair payment by pre-storing penalty money in the smart contract. Author novel procedure is practical, according to both safety and experimental evaluations.

- X. Lei, T. Xie, et al. [25] discussed in their paper that bitcoin (BTC) payments have grown in popularity among retailers and service providers in recent years. A BTC transaction (tx) requires six confirmations (one hour) to be validated, excluding it from fast-pay situations. In theory, a shorter waiting time period enhances the likelihood of a successful double-spending assault. To overcome this issue, author propose the BTCFast scheme, which supports quick BTC transfers. BTCFast is a unique, decentralised, escrow-based system built on top of blockchains with programmable smart contracts (PSC) (e.g. Ethereum, EOS). Author create a smart contract (PayJudger) to operate as a trustworthy payment judger, ensuring the tx fairness. Furthermore, author design a payment

judging method based on proof-of-work (PoW) for PayJudger to decide a BTC payment dispute. Our theoretical and practical results suggest that BTCFast may cut the waiting time to less than 1 second while maintaining equivalent security to the present strategy (i.e., waiting for six confirmations) and incurring no additional operating fees.

- Y. Li, et al. [26] discussed in their paper that while smart contracts have enabled a wide range of applications in many public blockchains, such as Ethereum, their security flaws have raised a growing number of risks to the ecosystem's stability. In actuality, many external assaults against smart contracts are the consequence of failed payments using digital assets such as bitcoins. While a growing number of research papers have been published on such issues, many of them have used pattern-based heuristics (e.g., reentrancy) to detect payment-related assaults, which can result in a significant number of false positives and negatives. In order to overcome these constraints and improve payment security on blockchain, we established a new class of payment attacks in this work, namely, unfair payment attacks (UP). UP conceptually encompasses a broader spectrum of payment assaults than previous heuristics. Furthermore, author emphasised the SAFEPAY generic architecture for comprehensively detecting UP. The essential finding is a new security invariant called fair value exchange (FVE), which simulates the fairness of blockchain payments between several participants. SAFEPAY, in particular, explores the transaction space of a given smart contract methodically and generates a restricted set of transaction sequences. SAFEPAY reports a UP assault for each sequence after an FVE violation is established. SAFEPAY for Ethereum has been further instantiated and used in real-world smart contracts. In the empirical examination, SAFEPAY was able to detect previously unknown UP assaults while efficiently avoiding false alarms when compared to other analysers in the literature.

- X. Zhao and Y. -W. Si, et al. [27] discussed in their paper that academic certificates are still commonly awarded on paper nowadays. Traditional certificate verification is a time-consuming, labor-intensive, and even costly

procedure. In this research, author offer NFTCert, a novel NFT-based certificate system that allows for the construction of linkages between a legal certificate and its owner through a Blockchain. Author explain the NFTCert framework's implementation in this paper, covering schema definition, minting, verification, and revocation of NFT-based certificates. In addition, we incorporate a payment mechanism into the minting process, allowing NFTCert to be utilised by a broader audience. As a result, NFTCerts participants do not need to rely on cryptocurrencies for transactions. When compared to existing Blockchain-based systems, the proposed framework is meant to provide usability, authenticity, secrecy, transparency, and availability features.

- Y. Chen, X. Li, et al. [28] discussed in their paper that the transaction throughput and latency of blockchain-based coins are severely constrained. A payment channel, which facilitates trust-free payments between two peers without draining the blockchain's resources, is a possible solution to this problem. A connected payment channel network (PCN) allows payments to be made between two peers via a number of intermediary nodes that forward and charge for the payments. However, most existing ideas merely employ the shortest path as the transaction path, causing frequently repeated channels to be soon depleted. Furthermore, the majority of existing PCNs are virtually exclusively designed for payments between two parties, resulting in limited application scenarios. The two-party PCNs cannot perform simultaneous payments when several payments use the same intermediate channel. In this study, author offer a multi-party payment channel (MPC) network, a payment channel proposal that permits several payments over the same intermediate channel at the same time, considerably increasing payment channel application possibilities. Furthermore, our channel selection and transaction conversion tactics can improve transaction success rates. Author build the MPC network in the Truffle-based simulated blockchain network and lightning network, and a significant number of trials validate the usefulness of our approach.

- C. Wu, J. Xiong, et al. [29] discussed in their paper that in its most basic form, a smart contract is a piece of computer programme code comprising associated

economic transactions and algorithms. This is essentially the computerization of the previously agreed-upon contract between the participants. When certain circumstances are met, this customised contract agreement is immediately evaluated and implemented. Smart contracts are utilised not just in financial transactions, but also in many sectors of social life. Although smart contract technology offers distinct advantages, it is still in its early phases of development, with numerous issues yet to be resolved. This article first quickly covers the blockchain development process before focusing on the research progress of blockchain 2.0-smart contracts. Second, the associated ideas of smart contracts are explained, as well as the functioning mechanism of smart contracts and the challenges that smart contracts confront. Finally, in response to these issues and quandaries, the relevant remedies and concepts are described, and the future difficulties and development patterns of smart contracts are studied and evaluated.

- Mahmoud Saleh Obaid, et al. [30] discussed in their paper that Mobile payments are becoming the preferred way of payment for a growing number of clients. Providing an effective security mechanism for mobile payments in public networks is a difficult challenge for device manufacturers and network service providers. Although most mobile payment applications make payments simple and quick, customers must contend with new security risks. Because users must conduct money transactions over an open network, their sensitive data is put at danger, allowing advisories to launch attacks and steal user identifying information. Recent payment applications, such as Google-pay and phone-pay, have effectively addressed security concerns; nonetheless, these apps may be vulnerable to internal assaults since data is centralised, and apps must obtain authorization from bank servers to conduct transactions. Author establish a protected transaction pattern utilising blockchain technology in the proposed system, which addresses the limitations of the present system. Our money is converted into bitcoins and stored in a separate wallet. The wallet is installed on the mobile devices. Payment or transaction between two consumers without previous approval. To protect data privacy from attackers, the suggested System employs a decentralised data server. During the

transaction, author transmit funds directly through the blockchain wallet, bypassing the bank. For online payment transactions, the suggested solution proved to be secure and efficient. Because it is protected against cyber attackers or hackers, data can be kept in different blocks, making it difficult to identify specific data. This eliminates the disadvantage of traditional mobile payments.

- X. Pei, L. Sun, et al. [31] discussed in their paper that while multiple party computation (MPC) has been proposed for over two decades, author have yet to see implementations that make MPC or its derivatives a tangible reality. Difficulties originate from recurring security and trust difficulties, which often manifest as data leakage, sloppy computation, and payment denial, among other things. Many solutions rely on a third party to coordinate parties co-working; however, each participant must completely trust the third party and entrust the source data and payment to it. In this research, author propose a blockchain-based protocol for efficient MPC without the need for a trusted third party. A zero-knowledge coordinator handles collaboration and work scheduling, while smart contracts manage user requests and secure payment. Cryptography techniques are used to maintain secrecy, privacy, and verifiability. All data is transported and computed in the encryption state, and only the user who has paid may decode the computation result.

- Zhaoxuan Li, Rui Zhang, et al. [32] discussed in their paper that the smart contract is gaining popularity as a basic component of the blockchain. However, the regular occurrence of smart contract security incidents demonstrates that smart contract security must be improved. It is yet unclear how to ensure both the secrecy of contract execution and the accuracy of computation outputs at the same time. One potential option is to use secure multi-party computation (SMPC) technology to construct smart contracts. However, a concern has been overlooked in previous SMPC-based contract execution schemes: the attacker can conduct the same procedure as the reconstructor to recover the secret, resulting in the disclosure of users' privacy. As a result, in order to address this issue throughout the smart contract operation process, this research proposes an improved homomorphic

encryption method with a minimal public key size, low ciphertext length, and good encryption efficiency. Then, a contract execution system combined with SMPC and homomorphic encryption (SMPC-HE for short) is developed, which can guarantee contract execution privacy while also ensuring the correctness of calculation results, and also makes smart contract execution fairer. Finally, theory and empirical findings show that our approach is safe, efficient, and has a minimal space overhead.

- X. Luo, W. Cai, et al. [33] discussed in their paper that because crypto currency users are compelled to relinquish their private keys to the exchange, traditional centralised token exchanges (CEX) are criticised for their security and privacy vulnerabilities. In contrast, a decentralised token exchange (DEX) overcomes this problem by adding a trading gas cost and delay to the system. To combine the benefits of CEX and DEX, a hybrid decentralised token exchange (HEX) has been suggested. However, current HEX is still plagued by two flaws. The first issue is that it is inconvenient for a trader who has to swap tokens frequently within a specific time frame because it is time-consuming and costly. The second problem is the possibility of Ethereum network congestion caused by the exchange's excessive simultaneous transactions. Author suggests a payment channel-based HEX in this research, which extends current systems by introducing a new payment channel layer to assist frequent traders and relieve network congestion.

- P. Frauenthaler, M. Sigwart, et al. [34] discussed in their paper that current blockchain relay systems need the destination blockchain to validate each relayed block header immediately. When establishing these relays across Ethereum-based blockchains, where verifying block headers on-chain is computationally difficult, this results in significant running costs. To address these restrictions, author provide an unique relay system that combines a validation-on-demand pattern with economic incentives to lower the cost of running a relay across Ethereum-based blockchains by up to 92 percent. Decentralized interoperability between blockchains such as Ethereum and Ethereum Classic becomes possible with this relay method.

- D. Kaid and M. M. Eljazzar, et al. [35] discussed in their paper that motivated by the current disruption in changing sectors through blockchain, this research investigates the impact of combining blockchain and Enterprise Resource Planning systems on the relationships between supply chain participants. Distributors aim to automate payments with retailers under certain conditions in order to establish a smooth integration, which may be accomplished using smart contracts on a blockchain network. In this research, author investigate the use of QR codes to manage such scenarios in the supply chain business, namely between distributors and retailers. Then, author look at how blockchain may help in these situations. Furthermore, a prototype is constructed and developed using Hyperledger Composer to highlight the benefits of blockchain in a supply chain. This prototype emphasises the increased value blockchain may have on the relationship between the two supply chain participants, while also giving additional capabilities to help both sides create the necessary trust.

CHAPTER 3

SMART CONTRACTS

INTRODUCTION

Transactions between participants in present systems are often centralized, necessitating the engagement of a trusted third party (e.g., a bank). However, this might lead to security vulnerabilities (such as a single point of failure) and expensive transaction costs. To address these concerns, blockchain technology has evolved, allowing untrusted organizations to connect with each other in a distributed manner without the intervention of a trusted third party. Blockchain is a distributed database that records all network transactions that have ever occurred. Blockchain was first launched for Bitcoin (a peer-to-peer digital payment system), but it has since grown to be utilized for the development of a wide range of decentralized applications. Smart contracts are an intriguing application that can be developed on top of blockchain.

Smart contracts are essentially programs that run when certain criteria are satisfied and are recorded on a blockchain. They are often used to automate the implementation of an agreement so that all participants may be confident of the conclusion instantly, without the participation of an intermediary or time lost. They can also automate a workflow by automatically activating the next activity when certain circumstances are satisfied.

3.1 A Brief History of Smart Contracts

Nick Szabo, an American computer scientist, is thought to have first used the term smart contract in an article in 1994. He wrote (Szabo, 1994): A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart-contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.

Since the 1990s, computer scientists and mathematicians have created the technical tools to automate contracts. More to the point some technology to enable early and rudimentary form of smart contracts already existed at the time when Szabo was sharing his thoughts with the world. Example of such technology is the DigitCash by Chaum et al. (1988), a payment system that protected users' privacy.

Furthermore, Szabo believed that to make smart contracts more valuable to society they need to be: verifiable, observable, and enforceable. In this way, smart contracts would be part of the fabric of society which would in turn lower legal barriers, slash transaction costs, cut the time to execute the contract, and provide an opportunity to create new types of businesses. Szabo was spot on in his predictions: today, as smart contracts develop and replace some traditional contracts, they are reducing costs and speed up execution, as the example of the bike has shown.

3.2 Importance of Smart Contracts

Developers may use smart contracts to create a wide range of decentralized apps and coins. They're utilized in anything from new financial tools to logistics and gaming experiences, and they're kept on a blockchain just like any other cryptocurrency transaction. Once a smart-contract software is put to the blockchain, it cannot be modified or reversed (although there are some exceptions).

Smart-contract-powered apps are also known as "decentralized applications" or "dapps," and they include decentralized finance (or DeFi) technology, which aspires to revolutionize the financial sector. DeFi applications enable bitcoin users to conduct complicated financial activities – saving, lending, and insurance — without the

involvement of a bank or other financial institution, and from anywhere in the globe. Some of the most prominent smart-contract-powered applications available today include:

a. Uniswap: A decentralized exchange that allows users to trade various types of cryptocurrencies using smart contracts without any central authority regulating the exchange rates.
b. Compound: A platform that leverages smart contracts to allow investors to earn interest and borrowers to get loans instantaneously, eliminating the need for a bank in the middle.
c. USDC: A cryptocurrency that is linked to the US dollar via a smart contract, making one USDC equal to one US dollar. UDDC is a stablecoin, which is a newer type of digital currency.

So, how would you put these smart contract-enabled instruments to use? Assume you have some Ethereum that you want to swap for USDC. You may put some Ethereum into Uniswap, which will automatically discover the best exchange rate, conduct the deal, and send you your USDC via smart contract. You could then invest part of your USDC in Compound to lend to others and earn an algorithmically calculated interest rate — all without utilizing a bank or other financial institution. Swapping currencies in traditional finance is costly and time consuming. Individuals lending their liquid assets to strangers on the other side of the planet are not easy or secure. However, smart contracts enable all of these possibilities, as well as a wide range of others.

3.3 Smart Contract Limitations

One of the intrinsic drawbacks of smart contracts is that the blockchains on which they run are isolated networks, which means that blockchains have no built-in connectivity to the outside world. Smart contracts cannot communicate with external systems to validate the occurrence of real-world events without external connection, nor can they access cost-effective computational resources. Smart contracts, like computers without Internet access, are severely restricted in the absence of real-world connectivity. They cannot, for example, ascertain the price of an asset before

conducting a deal, check the average monthly rainfall before paying out a crop insurance claim, or verify that products have arrived before settling with a supplier. To construct hybrid smart contracts, Oracles connect inputs and outputs to blockchains.

As a result, the biggest advancement in the blockchain business is programmable smart contracts that interact with real-world data and traditional systems outside of a blockchain, extending the inputs and outputs utilised inside smart contract logic. These hybrid smart contracts integrate on-chain code with off-chain infrastructure, such as triggering a smart contract with external data or settling a contract off-chain on a traditional payment rail, using safe middleware known as an oracle. Figure 3.1 shows oracles connect input and outputs to blockchains to create hybrid smart contracts

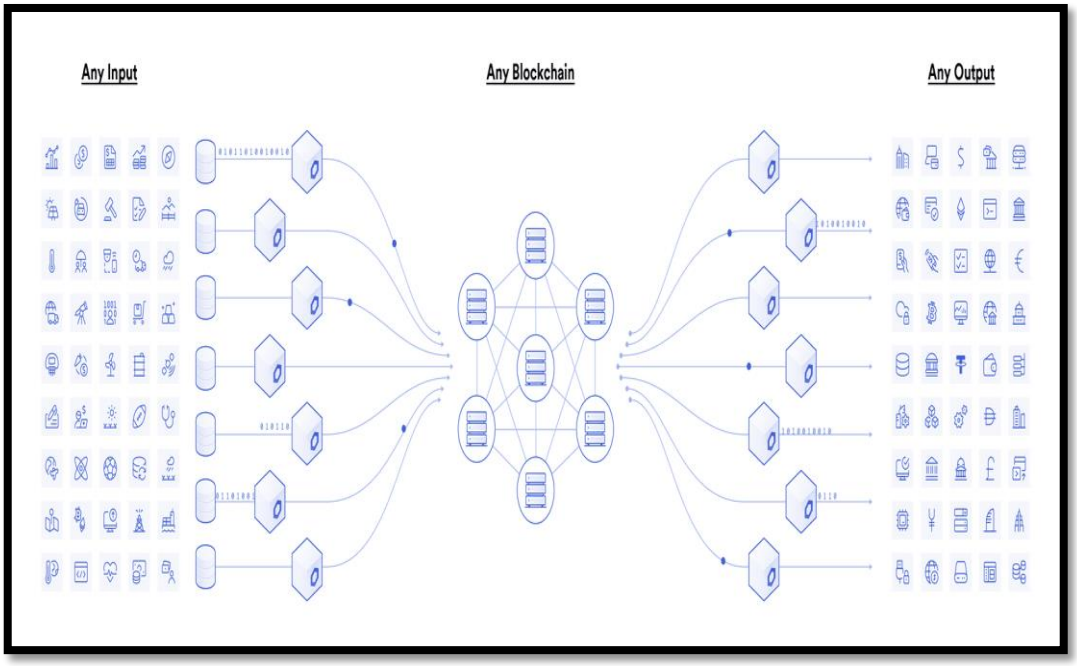

Figure 3.1 Oracles connect input and outputs to blockchains to create hybrid smart contracts

Thus, the major evolution underway in the blockchain industry is programmable smart contracts that connect with real-world data and traditional systems outside a blockchain, expanding the inputs and outputs used within smart contract logic. These hybrid smart contracts use secure middleware known as an oracle

to combine on-chain code with off-chain infrastructure e.g., trigger a smart contract with external data or settle a contract off-chain on a traditional payment rail.

3.4 Working of Smart Contract

Smart contracts operate by executing basic "if/when...then..." phrases encoded into blockchain code. When preset circumstances are met and validated, a network of computers conducts the activities. These activities might include transferring payments to the proper parties, registering a vehicle, providing alerts, or issuing a ticket. When the transaction is completed, the blockchain is updated. This implies that the transaction cannot be modified, and the results are only visible to persons who have been granted permission. One such example of smart contracts working is shown in the below figure 3.2.

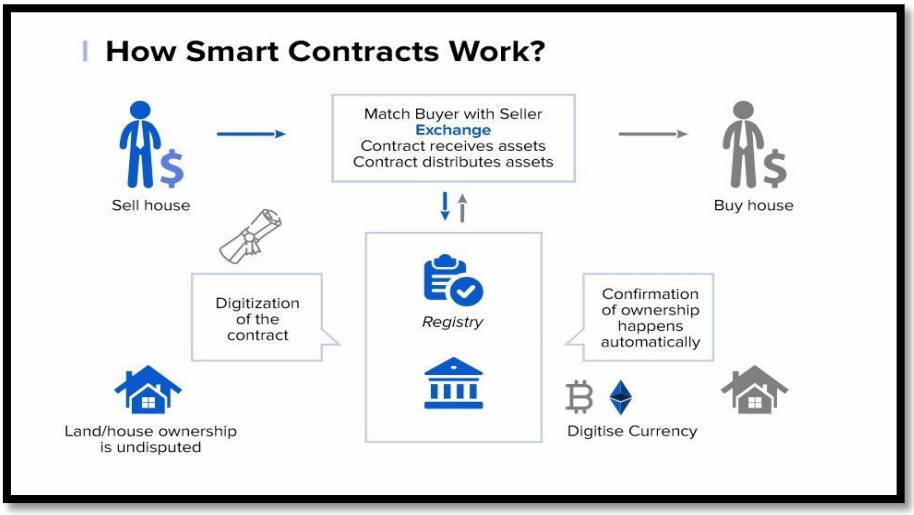

Figure 3.2 Working of Smart Contracts

A smart contract can have as many specifications as necessary to reassure the participants that the work will be executed correctly. Participants must identify how transactions and associated data are represented on the blockchain, agree on the "if/when...then..." rules that govern those transactions, investigate all conceivable exceptions, and design a framework for resolving disputes in order to set the terms.

The smart contract can then be coded by a developer; however, firms that use blockchain for business are increasingly providing templates, web interfaces, and other online tools to facilitate smart contract construction.

3.5 Benefits of smart contract

a. **Speed, efficiency and accuracy:** When a condition is satisfied, the contract is instantly executed. Because smart contracts are digital and automated, there is no paperwork to handle, and no time wasted correcting errors that frequently occur when filling out forms manually.
b. **Trust and transparency:** There is no need to question if information has been manipulated for personal gain because there is no third party engaged and encrypted records of transactions are transmitted between participants.
c. **Security:** Blockchain transaction records are encrypted, making them extremely difficult to hack. Furthermore, because each record on a distributed ledger is linked to the preceding and subsequent entries, hackers would have to modify the entire chain to change a single record.
d. **Savings:** Smart contracts eliminate the need for middlemen to conduct transactions, as well as the time delays and fees that come with them.

3.6 Platform for Smart Contracts

There are several different blockchain systems that support the development and deployment of smart contracts (e.g., NXT, Ethereum, and Hyperledger Fabric). A number of different platforms provide a variety of features that may be utilized for constructing smart contracts. These features include contract programming languages, contract code execution, and various levels of security. Certain platforms offer support for high-level programming languages, which are required for the development of smart contracts.

Bitcoin is a public blockchain platform that may be used to perform transactions involving cryptocurrencies, while having a relatively limited computer capabilities. Bitcoin was created by Satoshi Nakamoto. The scripting language utilized by Bitcoin is stack-based and bytecode. Using the programming language of bitcoin,

it is not possible to write a smart contract with a complex logic chain. This is a significant limitation. To allow smart contracts to perform as intended on Bitcoin's blockchain, significant adjustments would have to be made to both the mining operations and the mining incentive schemes.

NXT is a blockchain platform that is completely open-source and operates solely on a consensus mechanism known as proof-of-stake. It incorporates a number of different smart contracts that are still active at the moment. However, it is not a Turing-complete system, which means that users are limited to making use of the pre-existing templates and cannot install individualized smart contracts.

The first blockchain platform designed specifically for the development of smart contracts is Ethereum. With the assistance of a Turing-complete virtual computer that goes by the name of the Ethereum virtual machine, it enables more sophisticated and individualized smart contracts (EVM). The Ethereum Virtual Machine (EVM) serves as the runtime environment for smart contracts. Each node in the Ethereum network runs its own version of EVM and follows the same set of instructions. The high-level programming language Solidity is used to develop smart contracts; the compiled version of the contract code is then converted into EVM bytecode and uploaded to the blockchain so that it may be executed there. Ethereum is now the most popular development platform for smart contracts. It is also capable of being utilized for the building of a wide variety of decentralized apps (DApps) in a number of different industries.

Hyperledger Fabric is a permissioned blockchain, which means that only a collection of business-related organizations can join in through a membership service provider. The network of Hyperledger Fabric is built up from the peers whose are owned and contributed by those organizations. This is in contrast to the public blockchain, which allows any party to participate in the network. Examples of public blockchains include Bitcoin and Ethereum. IBM has proposed Hyperledger Fabric, an open-source enterprise-grade distributed ledger technology platform that also enables smart contracts. Hyperledger Fabric was developed by IBM. Modularity and adaptability are provided for a diverse range of industry use cases by this solution. Plug-and-play components allow Hyperledger Fabric's flexible design to suit the wide variety of use cases that are common in business settings.

There are various ways in which Ethereum and Hyperledger Fabric smart contracts are not identical. Although Solidity is a well-known programming language, Hyperledger Fabric allows multi-language smart contracts, including Go, Java, and JavaScript. Ethereum smart contracts are written in Solidity. In Ethereum, the contract code is included across a transaction, which is then propagated in the peer-to-peer network; any miner who gets this transaction is able to execute it in its local virtual machine. Contract code execution is accomplished by including the code in a transaction. When a transaction is made by an application using Hyperledger Fabric, the transaction can only be processed and signed by a limited number of peers that have been defined (endorsing peers). Following receipt of the transaction proposal from the application, each of these endorsing peers separately carries it out by calling the chain-code that the transaction refers to Chain code is executed in an isolated container environment (like Docker) with the purpose of ensuring its safety. Table 3.1 gives the comparison of smart contract platforms.

Table 3.1: Comparison of Smart contract platforms

Comparison of smart contract platforms

Title	Ethereum	Fabric	Corda	Stellar	Rootstock
Execution environment	EVM	Docker	JVM	Docker	VM
Turing completeness	Turing complete	Turing complete	Turing incomplete	Turing incomplete	Turing complete
Applications of smart contracts	General	General	Digital currency	Digital currency	Digital currency
Supported languages	Solidity, Serpent, LLL, Mutan	Java, Golang	Java, Kotlin	Python, JavaScript, Golang, PHP	Solidity
Permission	Public	Private	Private	Consortium	Public
Consensus algorithms	PoW (soon moving to PoS)	PBFT	Raft	SCP	PoW
Data model	Account-based	Key-value pair	Transaction-based	Account-based	Account-based

CHAPTER 4

DEPLOYMENT OF SMART CONTRACTS IN THE PROPOSED SYSTEM

Overview

Our proposed system is a blockchain-based Transaction system. Prior to the discovery of the blockchain, cloud based system played a major role in enabling the transactions between two parties. But it had certain drawbacks and that's when Smart Contracts came into picture.

Smart contracts are essentially programmes that run when certain criteria are satisfied and are recorded on a blockchain. They are often used to automate the implementation of an agreement so that all participants may be confident of the conclusion instantly, without the participation of an intermediary or time lost.

Other blockchain based payment systems used The Proof of Work (PoW) consensus process consumes more energy, however we abolished PoW in our suggested system, which employs the Proof of Stake (PoS) consensus algorithm for the consensus mechanism.

We employed smart contracts in the proposed solution to eliminate any third parties. We utilised ethers to deploy the smart contracts on the Ethereum blockchain network. Smart contracts are a collection of computer programmes written in solidity language that function as an agreement between two parties. One smart contract-based system is used in the proposed study. The paper includes 2 actors, a sender and a receiver.

4.1 **Sequence Diagram**

Sequence Diagrams are interaction diagrams that show how processes take place. They record the interaction of items within the framework of a partnership. Sequence Diagrams are time focused, and they graphically express the sequence of the interaction by utilising the vertical axis of the diagram to indicate time, what messages are conveyed, and when. Figure 4.1 shows sequence diagram for the proposed system.

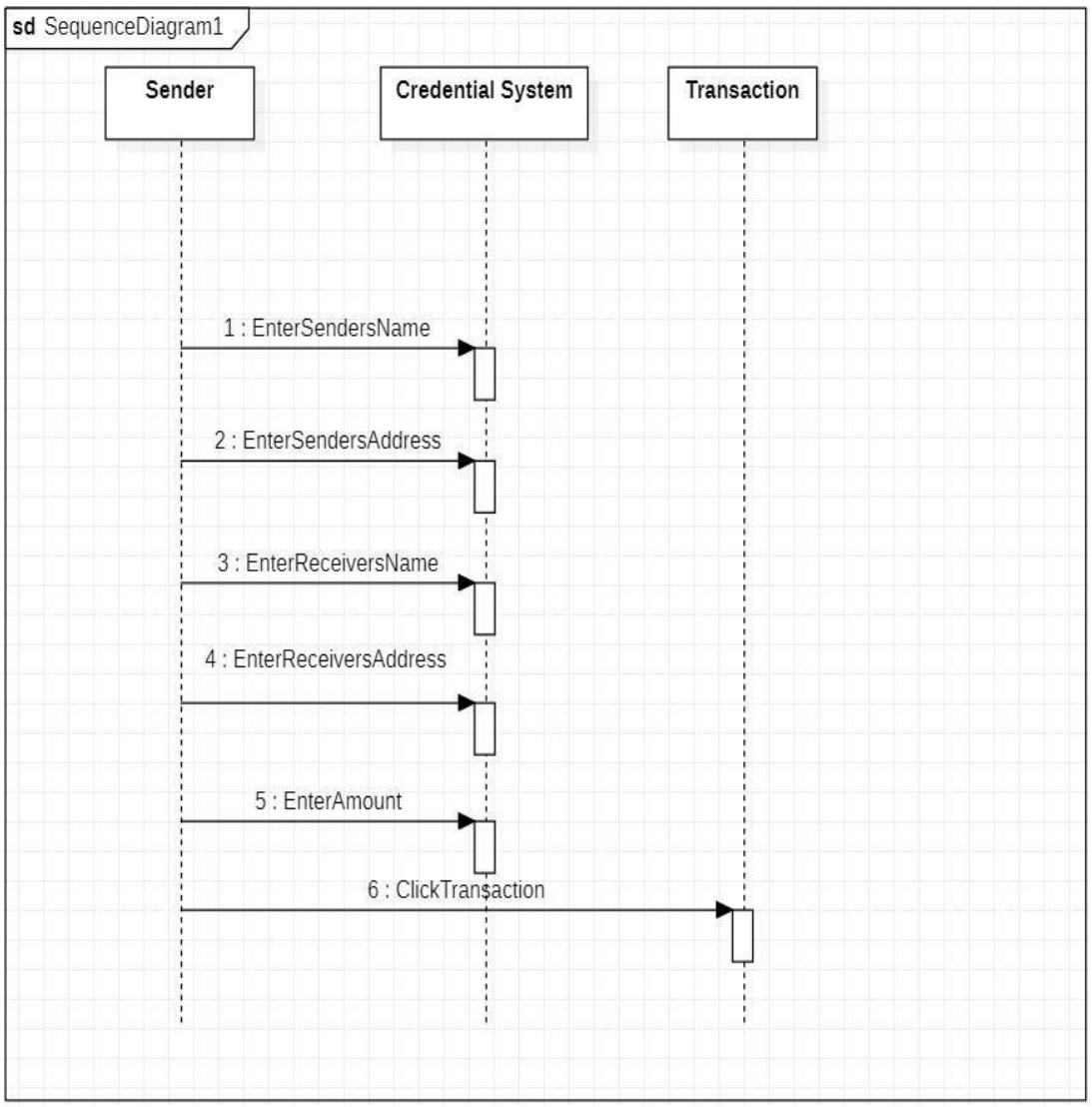

Fig 4.1: Sequence Diagram for transaction through Blockchain

4.2 **WORKING**

The set of rules or the algorithm which is being used in this research paper is mentioned below:

4.2.1 ALGORITHM

An algorithm is a well-defined collection of instructions for solving a certain issue. It accepts a collection of inputs and outputs the desired result.

START

STEP 1: Declare contract name ‘transaction’
STEP 2: Declare the structure of the contract
STEP 3: Declare the address of the sender in the contract
STEP 4: Map the address with the structure of the contract
STEP 5: Call the constructor for sending the data
STEP 6: Set the permissions
STEP 7: Enable the event of contract
STEP 8: Call a function to set the information in the contract
END

4.3 **SENDER TO RECEIVER SMART CONTRACT**

The smart contract in our proposed system consists of the following fields:
(i) Sender’s name (ii) Receiver’s name
(iii) Sender’s wallet address
(iv) Receiver’s wallet address
(v) Amount

Where the wallet address is a 32 bit long unique address assigned to every wallet by default. Objective of this smart contract is to facilitate a transaction between sender and receiver. Figure 2.1 shows the code of the smart contract.

```
pragma solidity ^0.4.25;
//Declare contract having the name 'transaction'.
contract transaction{
    //Declare the structure of the contract.
    struct TransactionInfo{
        string Name_of_Sender;
        string Name_of_Receiver;
        address Receiver;
        uint Amount;
    }
    address public Sender; //Declare address of sender in the contract.

    //Maping the address with structure of contract.
    mapping(address => TransactionInfo) public transactioninfos;
        //Call a constructor for sending the data.
    constructor() public{
        Sender = msg.sender;
        }
    //Set the permission
    modifier onlySender(){
        require(msg.sender == Sender,
    "Only Sender can set these parameteres."
    );
    _;
    }
        //Enable the event of the contract.
    event trans(string Name_of_Sender, string Name_of_Receiver, uint Amount, address Receiver);
    //Call a function to set the information in the contract.
    function setTransactionInfo(address _Sender, string Name_of_Sender, string Name_of_Receiver, uint Amount,address Receiver)
        onlySender public{
            transactioninfos[_Sender] = TransactionInfo(Name_of_Sender, Name_of_Receiver, Receiver, Amount);
        emit trans(Name_of_Sender, Name_of_Receiver, Amount,Receiver);
    }
}
```

Figure 4.2 Smart contract code

Figure 4.3 shows the output of this code when it's executed, and which is accessible to everybody.

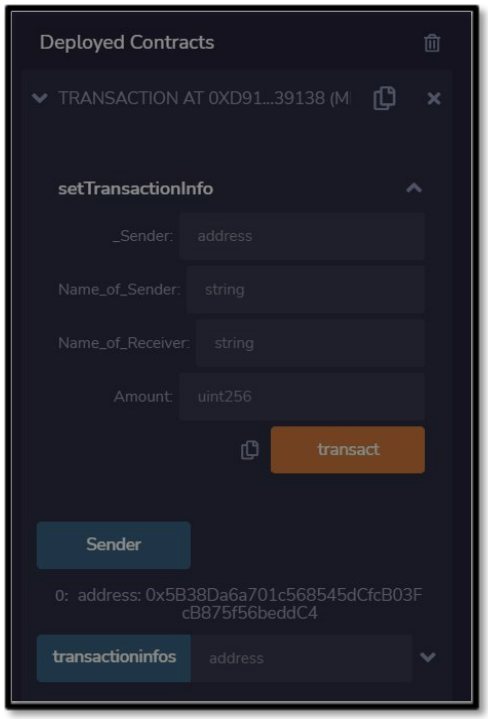

Figure 4.3 Interface of transaction

In the figure 4.4 deployment result of the transaction process is shown:

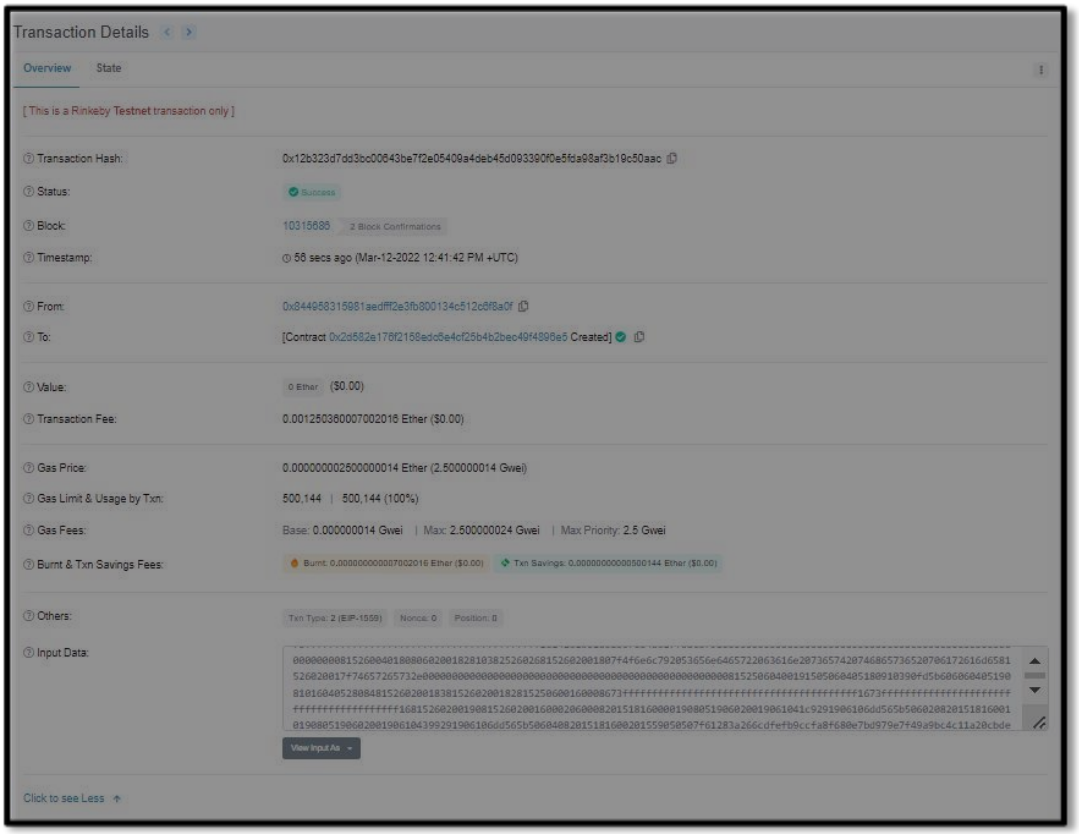

Figure 4.4 Deployment result of transaction between sender and receiver

CHAPTER 5

SUSTAINABLE DEVELOPMENT GOALS

OVERVIEW

The Sustainable Development Goals (SDGs) or Global Goals are a set of 17 interconnected global goals intended to serve as a "roadmap to a better and more sustainable future for all."

The United Nations General Assembly (UN-GA) established the SDGs in 2015, with the goal of achieving them by 2030. They are contained in a UN-GA Resolution known as the 2030 Agenda, sometimes known informally as Agenda 2030. The SDGs were designed as the future global development framework to supersede the Millennium Development Goals, which were completed in 2015.

4.2 **The 17 Sustainability development goals**

4.3 **No Poverty**

End poverty in all its forms everywhere

4.4 **Zero Hunger**

End hunger, achieve food security and improved nutrition and promote sustainable agriculture.

5.1.3 **Good Health and Well-being**

Ensure healthy lives and promote well-being for all at all ages.

5.1.4 **Quality Education**

Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all

5.1.5 **Gender Equality**

Achieve gender quality and empower all women and girls.

5.1.6 **Clean Water and Sanitation**

Ensure availability and sustainable management of water and sanitation for all.

5.1.7 **Affordable and Clean Energy**

Ensure access to affordable, reliable, sustainable and modern energy for all.

5.1.8 **Decent Work and Economic Growth**

Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all.

5.1.9 **Industry, Innovation and Infrastructure**

Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation.

5.1.10 **Reduced Inequality**

Reduce inequality within and among countries.

5.1.11 **Sustainable Cities and Communities**

Make cities and human settlements inclusive, safe, resilient and sustainable.

5.1.12 **Responsible Consumption and Production**

Ensure sustainable consumption and production patterns.

5.1.13 **Climate Action**

Take urgent action to combat climate change and its impacts.

5.1.14 **Life Below Water**

Conserve and sustainably use the oceans, seas and marine resources for sustainable development

5.1.15 **Life on Land**

Protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reverse land degradation and halt biodiversity loss.

5.1.16 **Peace and Justice Strong Institutions**

Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels.

5.1.17 **Partnerships to achieve the Goal**

Strengthen the means of implementation and revitalize the global partnership for sustainable development

Figure 5.1 shows sustainable development goals.

Figure 5.1: Sustainable Development Goals

Our project focusses on the **ninth goal** of the UN Sustainable Goal which is "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation".

5.2 The Ninth Goal

The targets which come under this goal are:

- Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well- being, with a focus on affordable and equitable access for all.
- Promote inclusive and sustainable industrialization and, by 2030, significantly raise industry's share of employment and gross domestic product, in line with national circumstances, and double its share in least developed countries.
- Increase the access of small-scale industrial and other enterprises, in particular in developing countries, to financial services, including affordable credit, and their integration into value chains and markets
- By 2030, upgrade infrastructure and retrofit industries to make them sustainable, with increased resource-use efficiency and greater adoption of clean and environmentally sound technologies and industrial processes, with all countries taking action in accordance with their respective capabilities
- Enhance scientific research, upgrade the technological capabilities of industrial sectors in all countries, in particular developing countries, including, by 2030, encouraging innovation and substantially increasing the number of research and development workers per 1 million people and public and private research and development spending
- Facilitate sustainable and resilient infrastructure development in developing countries through enhanced financial, technological and technical support to African countries, least developed countries, landlocked developing countries and small island developing States 18
- Support domestic technology development, research and innovation in developing countries, including by ensuring a conducive policy environment for, inter alia, industrial diversification and value addition to commodities
- Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020

With our research, we wish to upgrade the technological capabilities of industrial sectors in all countries, in particular developing countries, including, by 2030, encouraging innovation and substantially increasing the number of research and development workers per 1 million people and public and private research and development spending.

CHAPTER 6

CONCLUSION

The major goal of this research paper is to show how blockchain technology can be used to create a more efficient and secure transaction system, as well as how blockchain can be used to address the challenging process of handling sensitive transaction details between sender and receiver using smart contracts.

Blockchain is a well-known technology that has aided in the resolution of a wide range of challenges in a variety of industries. It's a technology that's tamper-proof, transparent, and secure. Blockchain is a potentially powerful and revolutionary technology since it reduces risk, eliminates fraud, and promotes transparency in a scalable manner for a wide range of applications. It's a distributed ledger of records that's verified by a global network of computers. The records are governed by a large community rather than a single central authority, and no single person has control over the records. This technology uses consensus mechanisms for security purposes. The data is encrypted using extremely advanced algos, and only the legal owner has access to it. The consensus algorithms which are used in blockchain are Proof of Work (PoW), Proof of Stake (PoS), Proof of Burn, etc.

In Blockchain it’s nearly impossible to tamper with the data as it is stored in a block and each block of the blockchain contains its Hash value and the Hash value of the previous block so, when anyone tries to change the data or tamper with a block then the block will be rejected because its Hash value will change. Blockchain is used in a wide range of areas such as supply chain, healthcare, cryptocurrency exchange, banking, law enforcement, voting, internet of things, real estate, digital Ids, etc.

In transaction, blockchain technology ensures safety of the transaction details. Limitations like third party involvement, delay in payment process, gateway charges, and much more which are associated with the current transaction method through cloud-based payment systems are rectified using the approach of blockchain.

The proposed system talks about the use of blockchain and smart contracts in transaction.

In conclusion, blockchain-based online payment transactions have been successfully implemented, which aims to secure the entire process. The one-way hashing algorithm aids in the secure transmission of data to miners, who then use the proof of stake mechanism to validate transactions based on the hash value sent. The validated transactions are subsequently placed in the blockchain, where they cannot be tampered with once they have been stored. As a result, the application seeks to provide a safe online transaction procedure by overcoming threats such as man-in-the-middle attacks and eliminating third-party gateways, making the entire process of online money transfer faster.

CHAPTER 7

FUTURE WORK

Future research will be devoted to the development of a user-friendly graphic user interface that will further improve the overall experience of the user as well as to explore the possibility of switching from Ethereum blockchain to Hyperledger.

REFERENCES

4.3 Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang "An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends", IEEE International Congress on Big Data, 2017, DOI:10.1109/BigDataCongress.2017.85.

4.4 Maher Alharby, Amjad Aldweesh, Aad van Moorsel, "Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research, International Conference on Cloud Computing Big Data and Blockchain (ICCBB), 2018, DOI: 10.1109/ICCBB.2018.8756390.

4.5 Karthikeya Thanapal, Dhiraj Mehta, Karthik Mudaliar, and Bushra Shaikh "Online Payment Using Blockchain", ITM Web of Conference, DOI:10.1051/itmconf/20203203007.

4.6 Yinghui Zhang, Robert H. Deng, Ximeng Liu, Dong Zheng "Blockchain based Efficient and Robust Fair Payment for Outsourcing Services in Cloud Computing", Information Sciences, 2018, DOI: 10.1016/j.ins.2018.06.018.

4.7 Jingyu Zhang, Siqi Zhong, Tian Wang, Han-Chieh Chao, Jin Wang, "Blockchain-based Systems and Applications: A Survey," Journal of Internet Technology, vol. 21, no. 1, pp. 1-14, Jan. 2020.

4.8 HuaqunGuo, XingjieYu "A survey on blockchain technology and its security", Institute for Infocomm Research, 2022, DOI: 10.1016/j.bcra.2022.100067.

4.9 Mohammad Rasheed Ahmed, Kandala Meenakshi, Mohammad S. Obaidat, Ruhul Amin, Pandi Vijayakumar "Blockchain Based Architecture and Solution for Secure Digital Payment System", IEEE International Conference on Communications, 2021, IEEE International Conference on Communications, DOI: 10.1109/ICC42927.2021.9500526.

4.10 Tharaka Hewa, Yining Hu, Madhusanka Liyanage, Salil S. Kanhare, Mika Ylianttila "Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research", IEEE Access, 2021, DOI:10.1109/ACCESS.2021.3068178.

4.11 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," 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2017, pp. 468-477, DOI: 10.1109/CCGRID.2017.8.

4.12 X. Wang, X. Xu, L. Feagan, S. Huang, L. Jiao and W. Zhao, "Inter-Bank Payment System on Enterprise Blockchain Platform," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 614-621, DOI: 10.1109/CLOUD.2018.00085.

4.13 Salar Ahmadisheykhsarmast, Rifat Sonmez "A smart contract system for security of payment of construction contracts", ISSN 0926-5805, DOI: 10.1016/j.autcon.2020.103401.

4.14 Lin Zhong, Qianhong Wu, Jan Xie, Zhenyu Guan, Bo Qin "A secure large-scale instant payment system based on blockchain", ISSN 0167-4048, DOI: 10.1016/j.cose.2019.04.007.

4.15 H. Singh and A. Dubey, "Electronic Payments based on Blockchain Technology. A Bibliometric Review", 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2021, pp. 1574-1577, DOI: 10.1109/ICAC3N53548.2021.9725363.

4.16 S. Joseph and S. Karunan, "A Blockchain Based Decentralized Transaction Settlement System in Banking Sector", 2021 Fourth International Conference on Microelectronics, Signals & Systems (ICMSS), 2021, pp. 1-6, DOI: 10.1109/ICMSS53060.2021.9673610.

4.17 N. P. Pravin, K. P. Anil, S. M. Sunil, M. S. Kundlik and P. A. Suhas, "Block chain technology for protecting the banking transaction without using tokens", 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020, pp. 801-807, DOI: 10.1109/ICIRCA48905.2020.9183333.

4.18 Lin Zhong, Qianhong Wu, Jan Xie, Jin Li, Bo Qin, "A secure versatile light payment system based on blockchain", 2019, DOI: 10.1016/j.future.2018.10.012.

4.19 Mohanty, Debasis, Divya Anand, Hani M. Aljahdali, and Santos G. Villar "Blockchain Interoperability: Towards a Sustainable Payment System", 2022, DOI: 10.3390/su14020913.

4.20 C. V. N. U. B. Murthy, M. L. Shri, S. Kadry and S. Lim, "Blockchain Based Cloud Computing: Architecture and Research Challenges", IEEE Access, vol. 8, pp. 205190-205205, 2020, DOI: 10.1109/ACCESS.2020.3036812.

4.4 J. Sidhu, "Syscoin: A Peer-to-Peer Electronic Cash System with Blockchain-Based Services for E-Business", 26th International Conference on Computer Communication and Networks (ICCCN), 2017, pp. 1-6, DOI: 10.1109/ICCCN.2017.8038518.
4.5 F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan and K. Ren "A Blockchain-Based Privacy- Preserving Payment Mechanism for Vehicle-to-Grid Networks", IEEE Network, vol. 32, no. 6, pp. 184-192, November/December 2018, DOI: 10.1109/MNET.2018.1700269.
4.6 Qinghua Lu, Xiwei Xu, H.M.N. Dilum Bandara, Shiping Chen, Liming Zhu "Patterns for Blockchain-Based Payment Applications", 26th European Conference on Pattern Languages of Programs, 2021, DOI: 10.1145/3489449.3490006.
4.7 N. El Madhoun, F. Guenane and G. Pujolle, "A cloud-based secure authentication protocol for contactless-NFC payment," 2015 IEEE 4th International Conference on Cloud Networking (CloudNet), 2015, pp. 328-330, DOI: 10.1109/CloudNet.2015.7335332.
4.8 Z. Wang, "Research on Cloud Computing-Based Online Payment Mode," 2011 Third International Conference on Multimedia Information Networking and Security, 2011, pp. 559-563, DOI: 10.1109/MINES.2011.41.
4.9 S. Wang, Y. Wang and Y. Zhang, "Blockchain-Based Fair Payment Protocol for Deduplication Cloud Storage System," in IEEE Access, vol. 7, pp. 127652-127668, 2019, DOI: 10.1109/ACCESS.2019.2939492.
4.10 X. Lei, T. Xie, G. -H. Tu and A. X. Liu, "An Inter-blockchain Escrow Approach for Fast Bitcoin Payment," 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), 2020, pp. 1201-1202, DOI: 10.1109/ICDCS47774.2020.00148.
4.11 Y. Li et al., "Protect Your Smart Contract Against Unfair Payment," 2020 International Symposium on Reliable Distributed Systems (SRDS), 2020, pp. 61-70, DOI: 10.1109/SRDS51746.2020.00014.
4.12 X. Zhao and Y. -W. Si "NFTCert: NFT-Based Certificates With Online Payment Gateway", 2021 IEEE International Conference on Blockchain (Blockchain), 2021, pp. 538-543, DOI: 10.1109/Blockchain53845.2021.00081.
4.13 Y. Chen, X. Li, J. Zhang and H. Bi, "Multi-Party Payment Channel Network Based on Smart Contract", IEEE Transactions on Network and Service Management, 2022, DOI: 10.1109/TNSM.2022.3162592.
4.14 C. Wu, J. Xiong, H. Xiong, Y. Zhao and W. Yi, "A Review on Recent Progress of Smart Contract in Blockchain," in IEEE Access, vol. 10, pp. 50839-50863, 2022, DOI: 10.1109/ACCESS.2022.3174052.
4.15 Mahmoud Saleh Obaid "Mobile Payment Using Blockchain Security", Journal of Applied Science and Engineering, Vol. 24, No 4, Page 687-692, DOI:10.6180/jase.202108_24(4).0025.
4.16 X. Pei, L. Sun, X. Li, K. Zheng and X. Wu, "Smart Contract Based Multi-Party Computation with Privacy Preserving and Settlement Addressed", 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2018, pp. 133-139, DOI: 10.1109/WorldS4.2018.8611588.
4.17 Zhaoxuan Li, Rui Zhang & Pengchao Li "A Secure and Efficient Smart Contract Execution Scheme", Web Services – ICWS 2020 (pp.17-32), 2020, DOI: 10.1007/978-3-030-59618-7_2.
4.18 X. Luo, W. Cai, Z. Wang, X. Li and C. M. Victor Leung, "A Payment Channel Based Hybrid Decentralized Ethereum Token Exchange", 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019, pp. 48-49, DOI: 10.1109/BLOC.2019.8751454.
4.19 P. Frauenthaler, M. Sigwart, C. Spanring, M. Sober and S. Schulte, "ETH Relay: A Cost-efficient Relay for Ethereum-based Blockchains", 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 204-213, DOI: 10.1109/Blockchain50366.2020.00032.
4.20 D. Kaid and M. M. Eljazzar, "Applying Blockchain to Automate Installments Payment between Supply Chain Parties", 2018 14th International Computer Engineering Conference (ICENCO), 2018, pp. 231-235, DOI: 10.1109/ICENCO.2018.8636131.