CHAPTER 1

INTRODUCTION

Blockchain is a ground-breaking technology that has skyrocketed in popularity recently. It is a distributed, decentralised ledger that enables safe transaction recording without the use of middlemen. Double spending is a significant problem for blockchain technology, though, as it could endanger its security and legitimacy. The practise of using the same cryptocurrency more than once results in double spending, which is a fraudulent transaction. In this project report, we will explore the double spending problem in blockchain technology. We will delve into the technical aspects of the problem, including its causes and possible solutions. Furthermore, we will analyze the implications of double spending on the security and trustworthiness of blockchain networks. This report aims to provide a comprehensive understanding of the double spending problem in blockchain and its impact on the broader ecosystem. We will also explore the current state of research in this area, including the latest techniques and approaches to address this problem. Finally, we will provide insights and recommendations for future research directions in this field. Overall, this report will serve as a valuable resource for individuals and organizations interested in blockchain technology and its potential applications.

1.1 Problem Statement

The well-known double-spending problem in digital currency systems has been made worse by the development of blockchain technology. Double-spending is avoided in typical digital currency systems like PayPal and Venmo by a central authority that authenticates and verifies each transaction. However, there is no central authority in a decentralised blockchain network, and participants across the network validate transactions.

Participants in a blockchain network must concur on the legitimacy of each transaction and make sure the same digital currency unit is not used twice in order to prevent duplicate spending. This is accomplished through a consensus process, which can be in the form of Proof-of-Work or Proof-of-Stake, among others.the process of creating a trust chain in a blockchain to prevent double spending. A double-spend issue occurs when a malevolent user pays money to another user and then, before that money is deducted from his account and spread throughout the network, conducts another transaction with it. The Trust chain a procedure to avoid this problem.

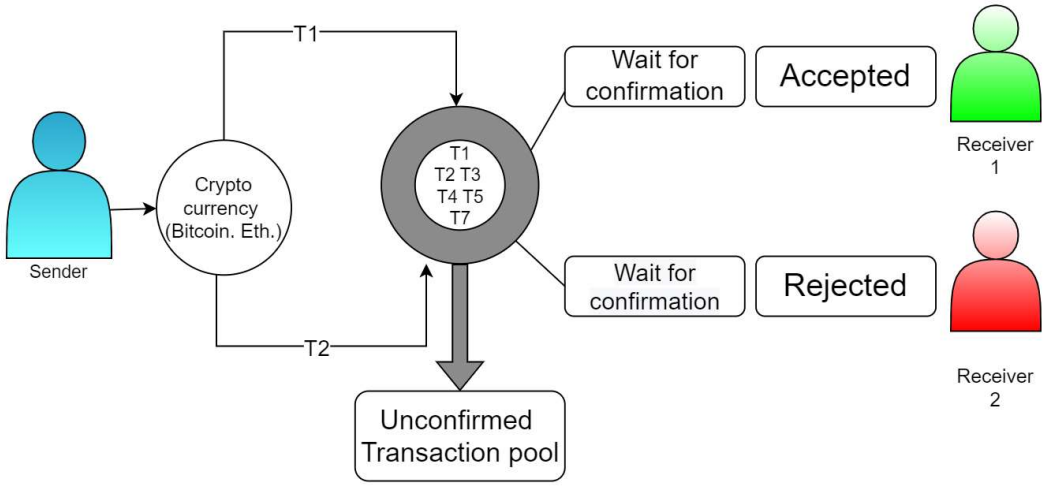

Fig. No.1.1.1. Double Spending Problem

1.2 Project Overview

The objective of this project is to as we see the proof-of-work consensus model is an elegant method used by permission-less digital currencies like Bitcoin to deal with the double spending issue. Unfortunately, the need for a single, consistent global state cannot grow and necessitates extras like leaders or supervisory servers. The goal of all three blockchain technologies is to enable reliable transactions at scale. The issue is that, to yet, researchers have failed to develop and use a self-organizing mechanism to foster trust that is resistant to all known methods of attack. So, our objective is Double spending problem where we will Optimizing in transaction security and management.

1.3 Expected Outcome

Review paper submitted to CISES Conference 2023

Acceptance Notification: By 30th April

Develop a network observe model which can detect double spending problem with better accuracy and develop a peer alert system to authenticate a transaction. Develop trust between sender and receiver so then can accept digital currency and save sender and receiver's time.

1.4 Hardware & Software Specifications

For the implementation of the project, following things would be used.

Hardware Requirements

- **CPU**: Intel Core i5 or any 3rd generation Computer
- **RAM**: 8GB
- **Storage**: At least 1 GB free storage.
- **Basic I/O**: using generic keyboard and mouse.
- **Display**: Standard monitor

Software/Framework/Tools

- **OS**: Windows Operating System
- **Language**: Node.js
- **Libraries**: Elliptic library and Random Nonce Generator
- **IDE**: VS Code

1.5 Other Non-Functional Requirements

Other non-functional requirements of the project include:
Availability - The model for prevent double spending problem can be available in to access in all the systems.

Usability - The proposed model is easy to use for digital transaction in blockchain technology.

Reliability- The probability of the software functioning faultlessly for a fixed period is called reliability.

Maintainability- This means how long it usually takes, how easy it is, and how rapidly a software can be fixed or restored after an error occurs.

Recoverability- It is the capability of a software to recuperate from a crash or failure and recommence regular functioning.

Performance- A system's performance is determined by how quickly it can respond to a given user's action while managing a specific workload.

Serviceability- This feature shows how simple it is to provide service when it is required.

1.6 Report Outline

In Chapter 1 the problem statement is presented, the project overview, expected outcome and hardware and software requirements.

The emphasis of Chapter 2 is on earlier work, related studies, a review of the literature, a suggested system, and a feasibility assessment.

Chapter 3 focuses on the suggested model, how it works, the requirements, the users, and the approach that will be used to create our solution.

The findings and experimental analysis of our system are presented in Chapter 4.

The entire study is concluded in Chapter 5, which discusses the system's potential future application.

CHAPTER 2
LITERATURE SURVEY

2.1 Existing Work

The double-spending problem is a critical challenge that must be addressed for digital currencies and decentralized systems to gain widespread adoption. Ongoing research in this area is focused on developing innovative and efficient solutions that can balance the security and performance requirements of these systems.

Steffen et al.,[1]. The authors evaluate the proposed system using a prototype implementation and demonstrate its effectiveness in managing access control in a decentralized social network. The evaluation shows that the proposed system can provide a more flexible and efficient approach to access control in decentralized systems, and can help address the challenges associated with managing identities and permissions in a distributed environment.

Yadav et al.,[2]. The authors argue that current property transaction systems are often centralized, inefficient, and prone to fraud and errors, and that a decentralized system based on DLT could address these issues. They proposed consensus mechanism is based on a trust model that assigns trust scores to participants based on their behavior and performance. The authors argue that this trust-based approach can improve the reliability and scalability of the consensus mechanism, and can help prevent attacks such as double-spending and Sybil attacks.

Yadav et al.,[3]. The authors argue that current land transaction systems are often inefficient, error-prone, and subject to fraud, and that a DLT-based system could address these issues by providing transparency, security, and immutability. They developed a DLT-based land transaction system that uses a trusted nodes consensus process as a viable way to enable secure and transparent land transactions.

Sergey, et al.,[4]. The authors propose a framework for evaluating blockchain systems that includes several dimensions, such as security, scalability, performance, and interoperability. They also suggest a set of evaluation criteria that can be used to assess each dimension. The suggested framework offers a comprehensive method for assessing blockchain systems and may be used to pinpoint the advantages and disadvantages of various blockchain platforms.

Yadav, et al.,[5]. The authors evaluated their proposed approach by implementing a prototype system using the Hyperledger Fabric blockchain platform and conducting experiments to measure its performance. According to their findings, the proposed approach can greatly increase

the efficiency of the land register system by reducing the amount of storage needed and hastening the processing of transactions.

Rahul, et al.,[6]. The author of this study explored the relationships between the three DSTs, SR, OLAP, and ARM, in terms of semantics. They determine that the data interpretation, visualization, and individualized decision-making capabilities of SR, OLAP, and ARM processes complement one another. The suggested mappings demonstrate the similarities between OLAP and ARM in terms of statistical reasoning, exploratory data analysis methods, and decision support problem-solving strategies. Based on these conclusions, they examined the present challenges in SR, OLAP, and ARM separately. Additionally, many next-generation hybrid decision support technologies will benefit from being designed using the semantic correspondences between the three DSTs.

Yadav, et al.,[7]. The authors highlight the importance of having an efficient and secure system for managing land records, and note that the use of DLT can help to achieve this. They suggest a consensus algorithm built on the PBFT algorithm, which they claim is more effective and scalable than existing consensus algorithms used in DLT-based land record management systems.

Malik, et al.,[8]. The paper presents a detailed analysis of the various trust management schemes that have been proposed in the context of blockchain-based supply chain management. The authors discuss the advantages and disadvantages of each scheme and identify the key challenges that need to be addressed to achieve effective trust management in supply chain management. The authors also present their own proposal for a trust management system called TrustChain, which is designed to address the key challenges identified in the literature review. The TrustChain system uses a combination of blockchain technology and IoT devices to provide secure and transparent trust management in supply chain management.

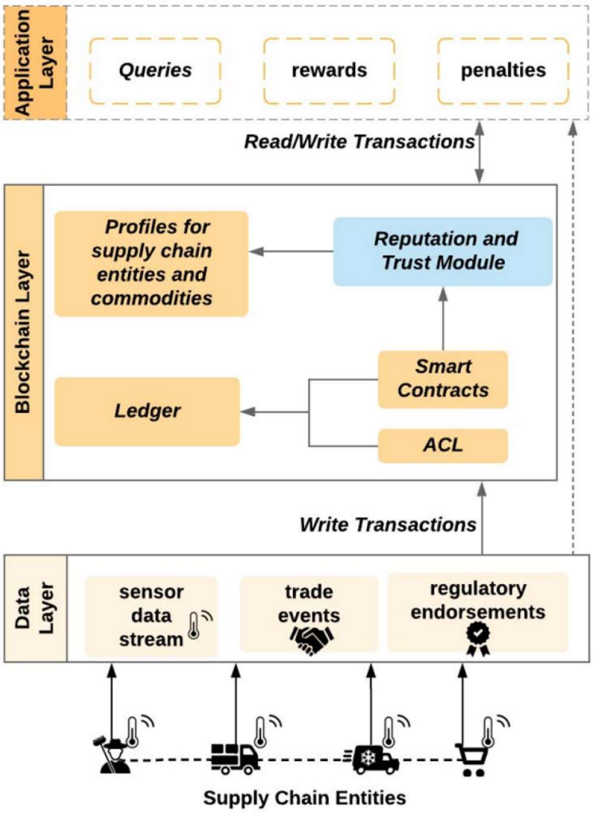

Fig. 2.1.1. Three-layered structure of the TrustChain framework [8].

Kaboli, et al.,[9]. The authors conducted an experiment involving three supply chain partners: a supplier, a manufacturer, and a retailer. They used a simulation model to simulate a supply chain, where the inventory replenishment decisions were made based on trust levels between the partners. The study found that trust plays a significant role in inventory replenishment decisions, and higher levels of trust lead to better inventory replenishment performance. The authors also identified various factors that affect trust, such as communication, transparency, and reputation.

Six et al.,[10]. The authors reviewed 105 articles and identified 27 distinct patterns related to the design of decentralized applications using blockchain technology. They classified the patterns into four categories: Data Management Patterns, Interaction Patterns, Process Patterns, and Security Patterns. In the Data Management Patterns category, the authors found patterns related to data storage, data sharing, and data validation. In the Interaction Patterns category, the authors found patterns related to user interaction, smart contract interaction, and blockchain network interaction. In the Process Patterns category, the authors found patterns related to process execution, event handling, and data processing. Finally, in the Security Patterns category, the authors found patterns related to access control, data privacy, and data integrity.

Ragh et. al.,[11]. In the retail sector, the author discusses several applications of blockchain technology, including supply chain management, loyalty programs, and product identification. The article also covers the advantages of utilizing blockchain technology, such as increased transparency, improved traceability, and reduced fraud. Furthermore, the paper highlights the challenges and limitations of implementing blockchain technology in the retail industry. These include technical challenges, lack of standardization, and regulatory barriers.

Feras et. al.,[12]. The author presents a summary of blockchain technology and some potential advantages for the railway sector, such as increased security, transparency, and efficiency. The article then presents the mobility and speech recognition prototype, It aspires to enhance the passenger experience by offering personalized services and real-time information. The prototype employs a smart contract to carry out passenger requests and is based on blockchain technology. The article describes how the prototype works, including the use of speech recognition and natural language processing to interpret passenger requests, and the application of blockchain technology to make sure that requests are processed securely and quickly. The author suggests that blockchain technology could help to improve the efficiency and security of railway systems, as well as enhance the passenger experience through personalized services.

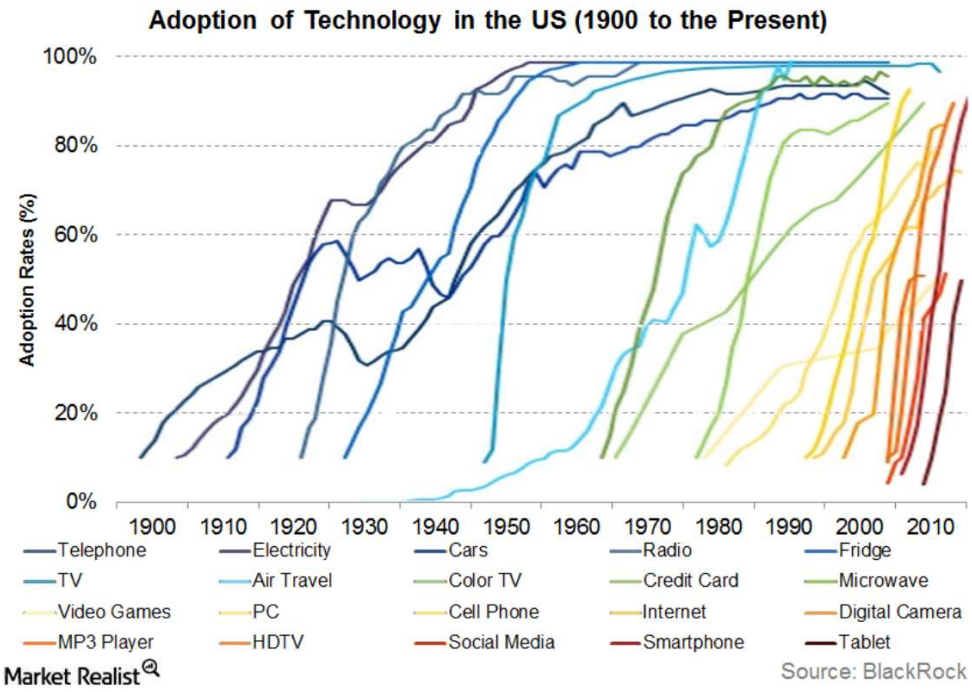

Fig. 2.1.2. Different Adoption rates of blockchain technology and innovation in the US since 1900 [12].

Pascal et. al.,[13] The paper goes on to describe the technical details of the proposed bare metal

crypto terminal, including its hardware components and software architecture. The terminal is designed to be highly secure, with features such as an embedded secure element, biometric authentication, and encrypted communication protocols. The author also discusses the potential applications of the bare metal crypto terminal, including its use in decentralized finance (DeFi) applications, smart contract execution, and secure key management.

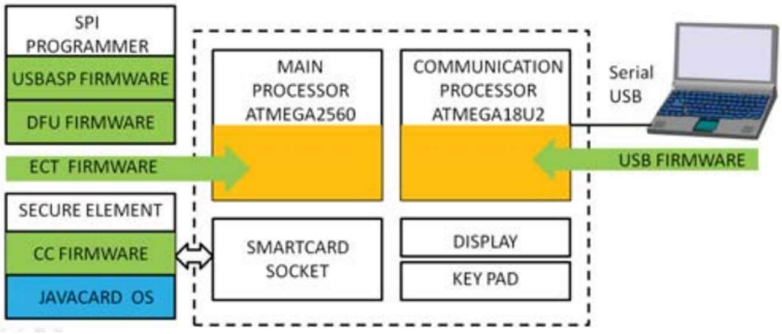

Fig. 2.1.3. Crypto Terminal Components & Firmware [13].

Hrvoje et. al.,[14] After reviewing the existing research on the use of blockchain technology for digital archives, the author proposed a fresh strategy that makes use of blockchain's benefits while avoiding data immutability's disadvantages. They suggest a hybrid blockchain architecture-based digital archive management system that employs smart contracts to control access and permissions to the digital archives. The system allows for the creation of multiple "layers" of digital archives, each with its own access control and retention policies.

Oliver et. al.,[15] The author of this article provides a detailed explanation of the three most common consensus methods used in blockchain systems: Byzantine Fault Tolerance (BFT), Proof of Work (PoW), and Proof of Stake (PoS). The authors also discuss the challenges associated with achieving consensus in a distributed system and the trade-offs between different consensus mechanisms. In addition to consensus mechanisms, the authors cover the technical details of transaction validation in blockchain systems, including the role of digital signatures and public key cryptography. They also explain how smart contracts work, and how they can be used to automate complex business processes.

Satoshi et. al.,[16] The paper describes the use of a distributed timestamp server to verify the order of transactions, a proof-of-work system to prevent double-spending and ensure security, and a peer-to-peer network to enable transactions between users. Additionally, it puts forth the idea of "blocks" that include several transactions and are added to a blockchain, which acts as a public database of all system transactions.

Yifan et. al.,[17] The paper addresses the issue of trust in software-defined networking (SDN)

systems, which are becoming increasingly popular due to their flexibility and programmability. For the purpose of ensuring the reliability of SDN network nodes, the authors propose a blockchain-based trust chain assessment methodology. The proposed method utilizes a blockchain-based trust chain to store and manage the trust values of SDN network nodes. The trust chain is generated and updated by each node based on its interactions with other nodes in the network. The authors also provide a simulation of the suggested method to analyze how well it performs in terms of determining trust and identifying attacks.

Long et.al.,[18] The authors explain that blockchain technology relies on a decentralized network of nodes that verify and record transactions. This network is maintained through economic incentives, such as rewards for miners who validate transactions and earn cryptocurrency as a reward in the study, The economics of blockchain systems are investigated in relation to the effects of the proof-of-work and proof-of-stake consensus algorithms. In this post, we discussed how cryptocurrencies fit into the blockchain ecosystem and how they could be used as a store of value, a medium of exchange, and a unit of account.

Ryuya et. al.,[19] The author focuses to the problem of surveillance camera video fabrication and the possible repercussions, such as false accusations or the failure to find the actual offenders. The suggested approach is inserting the video footage into a blockchain network, which can guarantee the data's integrity and guard against any manipulation or alteration. Digital signatures are created using hash functions and saved in the blockchain together with the original video data as part of the approach. They offer a thorough explanation of the suggested solution, covering both its technical details and procedures for execution. Also covered are the benefits of employing blockchain technology for data protection in this context, including decentralized data storage, immutability, and network transparency.

Upul et. al.,[20] The authors designed Blockchain privacy problems will be addressed by TrustChain by isolating user data from transaction data, allowing users to have control over their data and decide who can access it. They provide a detailed analysis of TrustChain's architecture, describing the role of each component and its interactions with the other components. They also evaluate TrustChain's performance in terms of latency, throughput, and resource utilization, and compare it to existing blockchain architectures.

Table 2.1.1. Summary of Literature Survey.

Authors/Year	Name of the paper	Objectives	Summary
Steffen, Rainer, and Rudi Knorr (2005)	A trust based delegation system for managing access control.	They provided a cutting-edge delegation system that explains digital trust between users using tokens that are cryptographically safeguarded	For ubiquitous applications, the delegation system that is being discussed enables a safe and user-friendly trust-based access control method. More permission restrictions, such as increased context awareness or permissions that are only granted in certain circumstances, will be the subject of future study.
Yadav, Amrendra Singh, Nikita Singh, and Dharmender Singh Kushwaha (2022)	A scalable trust based consensus mechanism for secure and tamper free property transaction mechanism using DLT	Numerous flaws and gaps in the current system might result in conflicts and corruption.	The distributed and secure P2P network infrastructure for real estate transactions is suggested in this article. Transparency is increased and risks are decreased when property transactions are shared via a block-chain.
Yadav, Amrendra Singh, Shivani Agrawal, and Dharmender Singh Kushwaha.(2022)	Distributed Ledger Technology-based land transaction system with trusted nodes consensus mechanism	Blockchain technology is a new choice for many financial applications that require a secure and immutable transactions system.. The land registry is one such application. It is laborious to manage transactions for land registration. It's extremely unsafe and vulnerable to fake land records, problems with verification, middlemen, etc.	It has been proposed to manage real estate transactions using a blockchain-based system. The proposed framework aims to fix the problems with the existing land registration system. The suggested technology, which is built on a blockchain, may be used to map every aspect of property transactions.

Smetanin, and Sergey (2020)	Blockchain evaluation approaches :State-of-the-art and future perspective.	The business focus is now changing away from examining the technology's potential and toward developing solutions based on distributed ledger technology, signalling that the current growth in interest in blockchain-based systems is already hitting a tipping point.	We identified current problems and possible solutions for blockchain simulation approaches, such as the need for multiple benchmarks for trustworthy model comparison, accessibility to historical representative blockchain system data, evaluating the effect of abstractions on model accuracy, examining relationships between blockchain characteristics, utilising machine learning, and a lack of expertise.
Yadav, Amrendra Singh, Nikita Singh, Dharmender Singh Kushwaha (2022)	Sidechain: storage land registry data using blockchain improve performance of search records	His study suggests the main chain and side chain as two distinct sorts of blockchains. Non-transactional data, including images, contracts, PDFs, and other related material, is saved in the sidechain while publicly viewable metadata is kept in the mainchain.	The registration office uses the summary file to search records in the main chain in order to get block hashes and property record numbers. Based on the property record number, it searches for similar records and gives the buyer access to those records.
Sharma, Rahul, et al. (2022)	Towards Unification of Statistical Reasoning, OLAP and Association Rule Mining	Online analytical processing (OLAP) and association rule mining both have their own distinct goals and purposes.	The development of several next-generation hybrid decision support systems will benefit from the semantic similarities between the three DSTs.
Yadav, A. S.,(2021)	The efficient consensus algorithm for land record management	It is built on blockchain technology, with the goal of streamlining the registration process by bringing all registrar	In this work, two consensus techniques for the IPFS-based property registration transaction system are compared. We have used IPFS to build blockchain on several

	system	offices under one framework.	hosts in order to do this.
Malik, Sidra, (2019)	Trust chain: Trust management in blockchain and iot supported supply chains	The use of statistical reasoning was one of these tools that was widely used to explain data-driven conclusions. Later, we saw the development of OLAP and association rule mining, both of which have different aims and objectives.	The framework also offers a reputation model that is asset- and agent-based, enables smart contracts for automation and efficiency, and may assign participants to different products with different reputations.
Kaboli, Amin(2012)	An experimental study of the relationship between trust and inventory replenishment in triadic supply chain	They account for two separate types of blockchain system trust: supplier and consumer trust.	They consider the dynamics of player trust in the game and the relationship between that trust and the decision to restock inventories, both of which have received little attention in earlier research.
Six, Nicolas, Nicolas Herbaut, and Camille Salinesi(2022)	Blockchain software patterns for the design of decentralized applications.	A distributed ledger made up of blocks and supported by a network of peers, each of whom has a copy of the ledger, is the basis of the blockchain technology.	By creating a taxonomy to help categorise newly created patterns, mapping and describing the body of literature on blockchain-based patterns within the taxonomy, and identifying research gaps that could be filled in future studies, this study also advances the state of the art for blockchain-based patterns.

2.2 Proposed System

Network observers: The We proposed a model for the cryptocurrency blockchain transactions to prevent double spending attack in blockchain network. The risk of using the same cryptocurrency tokens twice within a blockchain network is known as the "double spending problem." In a conventional payment system, a centralised body makes sure that funds cannot be used again. However, in a decentralized blockchain network, there is no central authority to prevent double spending. When a user initiates a transaction in a blockchain network, All network nodes receive a broadcast of the transaction. The transaction is then validated by these nodes to make sure the sender has enough bitcoin tokens to finish it. If the transaction is legitimate, it is recorded in a block and added to the blockchain. If a malicious user tries to double spend by creating two incompatible transactions, the network nodes may accept one while rejecting the other. This could lead to a scenario where the same cryptocurrency tokens are used twice, decreasing their value for the recipient and jeopardising the blockchain's integrity. To address the issues with the current system, we developed a network observer that can track anomalous transactions carried out without authority. In addition, we proposed a peer warning mechanism that notifies the sender and receiver nodes of the unauthorised transaction by relaying a message from the fraudulent node to them.

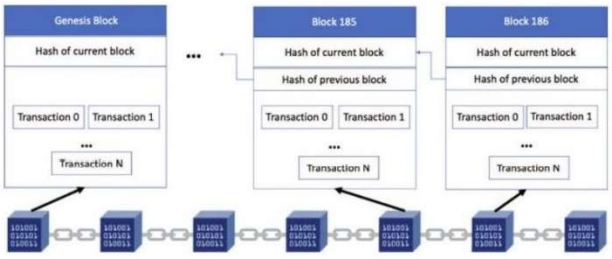

Fig. 2.2.1. Blockchain Architecture.

Network observers: Each pair of nodes has a network observer placed in betweenThe sender node notifies the neighbouring node with the transaction's value, transaction ID, and sender. The adjacent node will then transmit this to the appropriate forward node after completing the transaction process. This continues until the recipient node receives the funds. The observers in each pair of nodes keep track of the user ids, the number of transactions, and the amounts issued by each user. An observer can use this record to calculate the frequency of node communications in its node pair based on the volume of transactions issued by the user. If the frequency is higher than required, the anomaly will be noted, the transaction will be terminated, and a return acknowledgement will be sent to

the sender node.

Peer Alert Systems: When a network observer detects an anomaly at one of the transaction steps between a node-pair, the surrounding nodes are alerted to the fraudulent transaction. This will let the neighbouring nodes cut off their connections to the fraudulent node pair so that their transactions can be carried out over other secure paths.

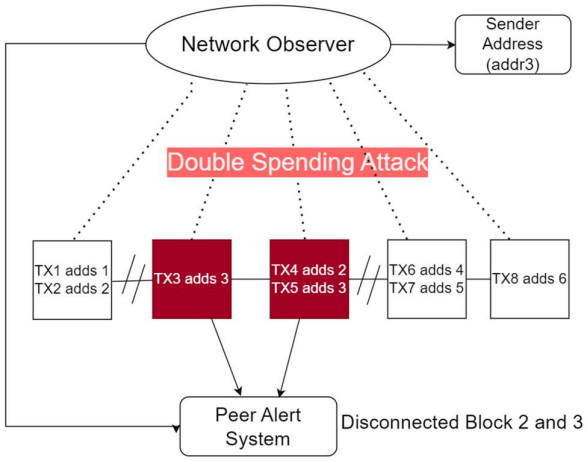

Fig. 2.2.2. Network Observer and Peer Alert System Model.

2.3 Feasibility Study

Technical feasibility: The main technologies and tools associated with the project are:

- Any standard PC or laptop
- Windows Operating System or Ubuntu or MacOS.
- Node.js Version 19.0.1 or above
- NPN installed.
- A programming device like a laptop or a computer.
- Programming tools that are freely available.
- Programming individuals

CHAPTER 3

SYSTEM DESIGN & ANALYSIS

3.1 Project Perspective

The blockchain represents a breakthrough in computer science that has the potential to lower the cost of building and sustaining trust for both people and companies. By eliminating the need for a neutral central authority, blockchain technology enables collaboration between individuals who don't really trust one another. The chain of trust that arises from this approach. Because the prior software would not have performed it if it had been unlawfully altered, the final software can be trusted to have certain qualities. The prior software is reliable because it wouldn't have loaded if its signature weren't legitimate. Each layer is guaranteed to be trustworthy by the one before it, all the way back to the trust anchor.

3.2 Performance Requirement

Performance requirements for blockchain systems are critical to ensuring the system can handle a large volume of transactions while maintaining security, integrity, and availability. Here are some of the key performance requirements for blockchain systems:

Scalability: Blockchain systems must be designed to handle a high volume of transactions, including spikes in traffic. This requires scalability measures that allow for horizontal scaling of the system across multiple nodes or vertical scaling through the addition of more computing power.

Speed: Transaction processing speed is critical for blockchain systems, especially for those supporting time-sensitive use cases such as real-time payments. The system must be designed to process transactions quickly, ideally in a matter of seconds or minutes.

Consensus Algorithm Efficiency: Consensus algorithms are at the heart of blockchain systems and must be designed to be efficient and effective. They should be able to reach consensus quickly and with minimal computational overhead.

Network Latency: Network latency is a significant factor that can impact the performance of blockchain systems. Minimizing network latency is critical to ensure that transactions are

processed quickly and that the system is available and responsive.

Security: Blockchain systems must be designed with security as a primary concern. The system should be resilient against various types of attacks, including 51% attacks, double-spending, and other forms of cyber attacks.

Fault Tolerance: Blockchain systems should be designed to be fault-tolerant, meaning they can continue to operate even if a portion of the network goes offline or is compromised. This requires redundancy measures such as backup nodes or multiple copies of the blockchain.

Storage Efficiency: As the blockchain grows, it can become challenging to store all transactions in a single ledger. Blockchain systems should be designed to optimize storage efficiency, including compression and data management techniques.

Overall, performance requirements for blockchain systems are critical to ensuring the system can handle the demands of its use case. By addressing scalability, speed, consensus algorithm efficiency, network latency, security, fault tolerance, and storage efficiency, blockchain systems can provide a reliable, secure, and efficient solution for various applications.

3.3 System Features

Using network observers and peer-alert systems, we provide a technique for preventing double-spending attacks in bitcoin blockchains.

Network observers are used to track abnormal transactions carried out without authorization in order to address flaws with the current system. A peer alert system is also created so that the message is transmitted from the fraudulent node to the sender and receiver nodes to inform them of the unauthorized transaction.

3.4 Methodology and Testing Process

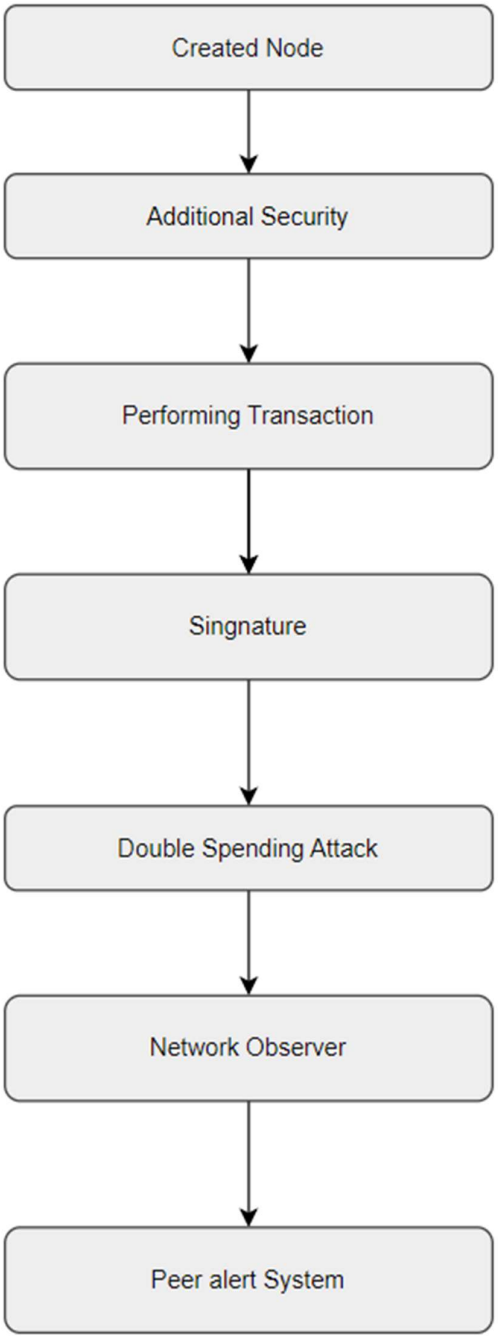

Fig. No.3.4.1 Methodology

3.4.1. Created Nodes

To start the initial blockchain, we created nodes using node.js and after using the command line or terminal to access the directory, use the following command: node.js for CryptoBlockchain.

3.4.2. Additional Security

A random nonce generator will be used to create the hash in order to boost security. Additionally, a difficulty index is used to add extra zeros to the generated hash, which increases the mining time complexity and lengthens the time required to mine individual blocks. A two-fold validation process is used for every pair consisting of the current block and its preceding block on the cryptocurrency blockchain to validate it as well.

- The current block's hash is recalculated using the same nonce, and the values of the original and recalculated hashes are compared.
- The hash of the present block and the block that came before it are compared.
- The validation function produces an error if one of these two processes reveals a discrepancy.

3.4.3. Performing Transaction

In order to carry out transactions between the intended sender and recipient blocks or nodes, their addresses must be mined. This allows the transaction amount to be subtracted from the sender node and added to the receiver node. Starting with a null amount transaction for the genesis block, an array keeps track of all the pending transactions for each block and then saves each new transaction.

As an example, consider the following scenario: The first block delivers 100 bitcoin units to the second block. 50 bitcoin units are returned to the first block by the second block in turn. The transaction array will therefore include information on the transactions with the amounts null, 100, and 50, respectively. A mining reward of 100 points is applied to the balance of a certain genesis block after each successful transaction.

```
Starting the miner...
Block Mined: 00006eb226eb57af646715ce400947bb0e9afcf621933c1764eaf3ed8053965e
Timestamp: 1670410714608
Block successfully mined!
Block Mined: 0000941c20d3b97ac547e76d43f01d4a8c92071e7d98bd9df3c5e095b8925d3d
Timestamp: 1670410728214
Block successfully mined!
Block Mined: 0000c517beeb9dbe29ae5a770f0b76745bc9f4afc9df594570a3f8b3d8da50cd
Timestamp: 1670410732404
Block successfully mined!
Block Mined: 0000f5d920ca87291a43c5274dbbc5207f2054ad9d41c68d34eff643dbc92a5a
Timestamp: 1670410733573
Block successfully mined!
```

Fig. No.3.4.3 Performing Transactions

3.4.4. Signature

Every transaction is signed with a signature to verify that it is unique. This signature is formed using the private and public key and the block hash derived using the elliptic library (based on elliptic curve cryptography). Additionally, every transaction is authenticated using this as a security measure. The next graphic shows a transaction with 10 bitcoins coming from the genesis block and a receipt of 100 bitcoins from the genesis block.

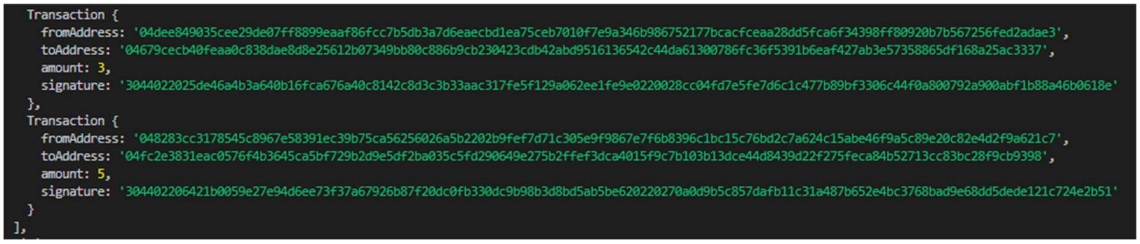

Fig. No.3.4.4 Signature

3.4.5. Double Spending Attack

Attack with Double Spending A double spending attack happens when a sender tries to carry out the identical transaction (for the same amount) twice, but with two distinct receivers, even when his starting balance is insufficient to cover both transactions.

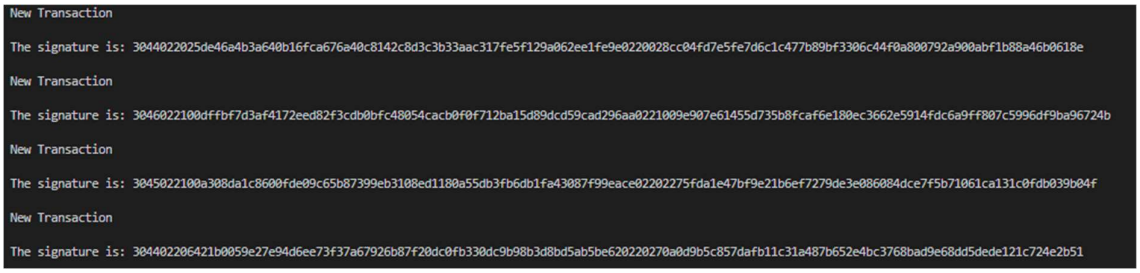

Fig. No.3.4.5 Double Spending Attack

3.4.6. Network Observer

In a blockchain, a network observer will look up the total number of pending transactions from a specific sender address. A transaction aborted error will be displayed and the user will be given the option to either cancel the most recent transaction with the same amount or try performing the transaction again later if the payment amount of two pending transactions from that address is the same and the total amount is higher than the sender's starting balance.

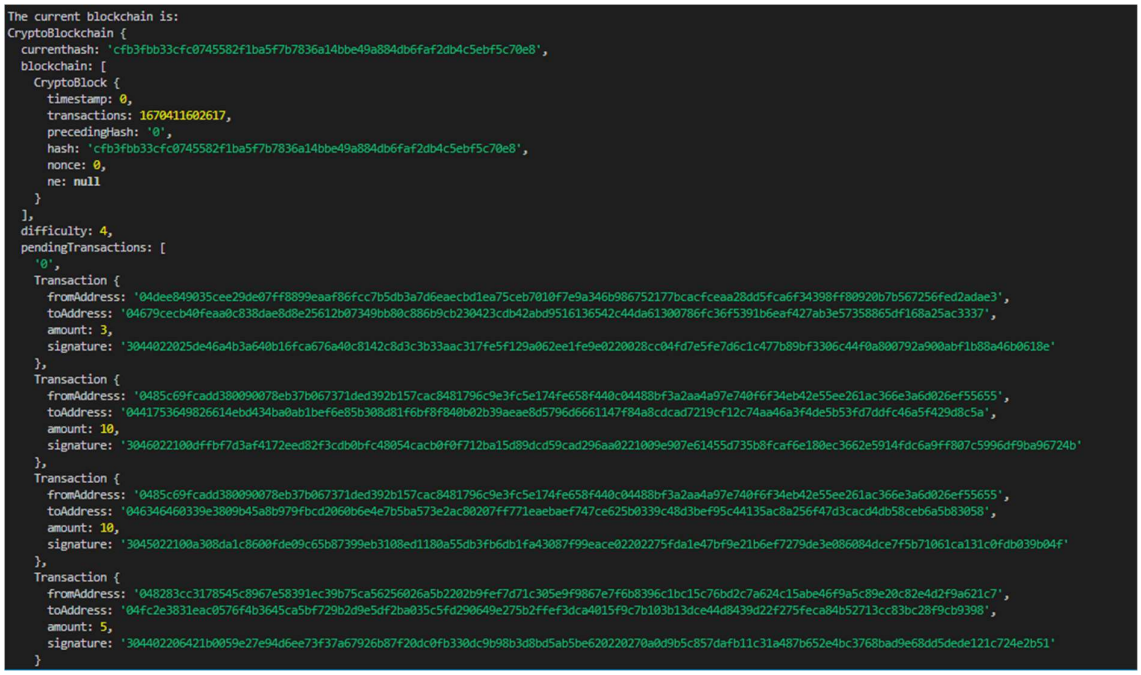

Fig. No.3.4.6 Network Observer

3.4.7. Peer Alert System

Peer Alert Systems: The nearby blocks are informed in order to detach from the block where the fraudulent transaction or double spending attack occurred. Any upcoming transactions scheduled for this block are diverted to alternate routes, and its nearby blocks cut off communication with it. The sender (who intended to carry out the double spending attack) will either be temporally blocked before being allowed to make any new transactions again, or they must withdraw one of the transactions within a certain timeout period.

Fig. No.3.4.7 Peer Alert System

In the blockchain, a double spending attack takes place. The network observer issues an error and requests the user to cancel the most recent transaction or risk suspension. Following this, the peer alert system will cut off connections between legitimate blocks and other blocks, alerting nearby blocks.

3.5 Test Cases

Descriptions:

Test Case ID	1
Test Case Name	Create a blockchain with additional security
Test Case Description	Test the blockchain with additional security
Steps	1. Run node.js code 2. Check nonce and signature of blocks
Expected Results	Blockchain successfully created with additional security.
Actual Results	successful

Test Case ID	2
Test Case Name	Perform a transaction between Sender and Receiver
Test Case Description	Mining between two nodes
Steps	1. Perform Transaction 2. Check if mining is started or not
Expected Results	Successfully performed transaction
Actual Results	successful

Test Case ID	3
Test Case Name	Unique transaction
Test Case Description	Check every block created with a unique signature
Steps	1. Perform Transaction 2. Check if block is created with

	Signature
Expected Results	Blockchain successfully created unique signature.
Actual Results	successful

Test Case ID	4
Test Case Name	Network observer
Test Case Description	Check if network observer working in blockchain
Steps	1. Run node.js code 2. Check if network observer detects pending transaction
Expected Results	Network observer showed difficulty for pending transaction.
Actual Results	successful

Test Case ID	5
Test Case Name	Alert system
Test Case Description	Test if peer alert system is notifying other block.
Steps	1. Perform a double spending attack 2. Check if neighboring blocks are getting alert.
Expected Results	Terminate their connections
Actual Results	successful

CHAPTER 4
RESULTS AND OUTPUTS

The double spending assault reduces the number of transactions from four to two (the transactions involved in the attack are cancelled). Due to the fact that the previous hash is one of the factors used to determine the current hash of any block, the peer warning system will invalidate the previous hash of blocks that had fraudulent blocks before them.

This block is changed to a new genesis block with a preceding hash of "0" in order to solve the problem of having a null preceding hash. This will also result in the creation of a new current hash that may be used to carry out the same transaction as previously (Change of transaction route).

Finally, once the blockchain has only been used for authorized transactions, those transactions are executed and the balances of each address are updated appropriately.

4.1 Proposed Model Output

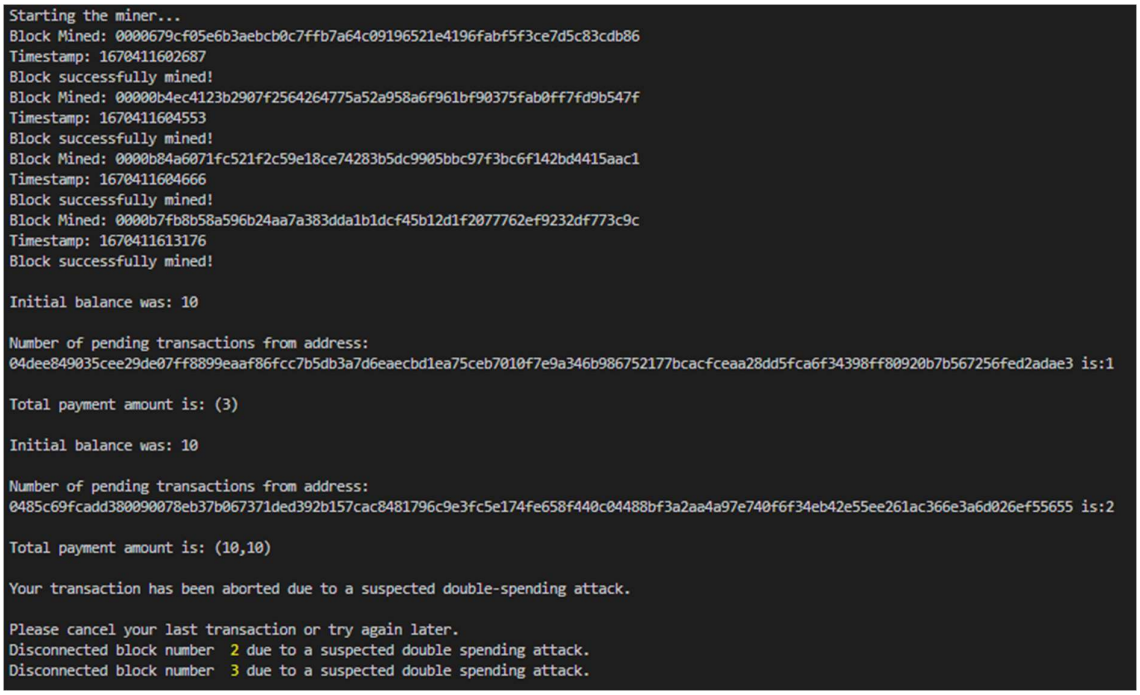

Fig. No.4.1.1 Proposed Model Output

CHAPTER 5
CONCLUSION

5.1 System Usability

Blockchain technology continues to face a major obstacle in the form of the double spending issue. Due to its decentralised structure, blockchain is vulnerable to double spending attacks because there is no central authority to authenticate transactions. Researchers and developers have proposed a variety of solutions, including as Proof of Work (PoW), Proof of Stake (PoS), Byzantine Fault Tolerance (BFT), Directed Acyclic Graph (DAG), and other consensus mechanisms, to address this problem. Additionally, other approaches have been proposed, such as centralized checkpointing, double-spending detection algorithms, and transaction verification through trusted parties. While these solutions have been shown to be effective in mitigating the double spending problem, there are still research gaps that need to be addressed. A comprehensive evaluation framework is necessary to compare and assess the various approaches and their effectiveness in preventing double spending attacks. Additionally, more study is required to comprehend the problem's economic and game-theoretical components, which can help in the design of more durable and resilient solutions. Moreover, the scalability of existing solutions is another research gap that needs to be addressed. As blockchain technology continues to gain popularity and adoption, the demand for fast and efficient transactions will continue to grow. Therefore, it is important to investigate the scalability of existing solutions and explore new solutions that can meet the needs of a large-scale decentralized system. In conclusion, the development of efficient consensus mechanisms, exploration of hybrid consensus mechanisms, integration of off-chain solutions, and investigation of new security models are crucial steps toward mitigating the double spending problem and ensuring the integrity and trustworthiness of decentralized systems. The resolution of these research gaps will provide a more robust foundation for blockchain technology, enabling it to be more widely adopted across industries and applications.

5.2 Future Scope

The proposed model is expected to be used To increase security in a blockchain system where users can trust on digital currency (bitcoin) payments by have an authorized successful transaction detail. We used network observers to monitor transactions inside each pair of nodes, keeping track of user ids, the number of transactions they issued, and the total amount of those transactions, in order to increase the security of blockchain transactions. Based on the quantity of transactions that the user has issued, the network observer will determine the frequency of node communications in its node pair. If the frequency (amount) exceeds what is necessary. The transaction will be cancelled and users will receive a message stating that it was unsuccessful due to a double-spending attack.

We intend to investigate our network to give better results with different upscaling factors by increasing the training data.

We also intend to train the model for more epochs to obtain better results.

REFERENCES

[1] Rainer Steffen, Rudi Knorr “A Trust Based Delegation System For Managing Access Control” Fraunhofer Institute for Communication Systems, Hansastrasse 32, 80686 Munich, Germany.

[2] Yadav, Amrendra Singh, Nikita Singh, and Dharmender Singh Kushwaha. "A scalable trust based consensus mechanism for secure and tamper free property transaction mechanism using DLT." International Journal of System Assurance Engineering and Management 13.2 (2022): 735-751.

[3] Yadav, Amrendra Singh, Shivani Agrawal, and Dharmender Singh Kushwaha. "Distributed Ledger Technology-based land transaction system with trusted nodes consensus mechanism." Journal of King Saud University-Computer and Information Sciences 34.8 (2022): 6414-6424.

[4] Sergey Smetanin, Aleksandr Ometov , Mikhail Komarov, Pavel Masek and Yevgeni Koucheryavy "Blockchain evaluation approaches: State-of-the-art and future perspective." Sensors 20.12 (2020): 3358.

[5] Yadav, Amrendra Singh, Nikita Singh, and Dharmender Singh Kushwaha. "Sidechain: storage land registry data using blockchain improve performance of search records." Cluster Computing 25.2 (2022): 1475-1495.

[6] Sharma, Rahul, et al. "Towards Unification of Statistical Reasoning, OLAP and Association Rule Mining: Semantics and Pragmatics." International Conference on Database Systems for Advanced Applications. Springer, Cham, 2022.

[7] Amrendra Singh Yadav, Swati Shikha, Sulaksh Gupta and Dharmender Singh Kushwaha "The efficient consensus algorithm for land record management system." IOP Conference series: materials science and engineering. Vol. 1022. No. 1. IOP Publishing, 2021.

[8] Malik, Sidra, et al. "Trust chain: Trust management in blockchain and iot supported supply chains." 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019.

[9] Amin Kaboli, Naoufel Cheikhrouhou, Maryam Darvish and Rémy Glardon "An experimental study of the relationship between trust and inventory replenishment in triadic supply chain." Proceedings of the POMS world conference. 2012.

[10] Nicolas six, Nicolas Herbaut, and Camille Salinesi. "Blockchain software patterns for

the design of decentralized applications: A systematic literature review." Blockchain: Research and Applications (2022): 100061.

[11] Ragh Satya Sai Medida “Scope of blockchain technology in the retail industry” International Journal of Computer Engineering & Technology (IJCET) volume 11, issue 3, may-june, 2020, pp. 26-30, article id: ijcet_11_03_003.

[12] Feras Naser “The Potential Use Of Blockchain Technology In Railway Applications An Introduction Of A Mobility And Speech Recognition Prototype” 2018 ieee international conference on big data.

[13] Pascal Urien "introducing innovative bare metal crypto terminal for blockchains and bigbang paradigm" 9 78-1-7281-1542-9/19 2019 IEEE.

[14] Hrvoje Stancic and Vladimir Bralic “Digital archives relying on blockchain: overcoming the limitations of data immutability” Computers 2021, 10, 91. https://doi.org/10.3390/computers10080091

[15] Oliver Kattwinkel, Michael Rademacher “Technical Fundamentals of Blockchain Systems” Isbn: 978-3-96043-081-0, Digital Object Identifier: 10.18418/978-3-96043-081-0 (2020).

[16] Satoshi Nakamoto “Bitcoin: A Peer-To-Peer Electronic Cash System” https://bitcoin.org/bitcoin.pdf (2009).

[17] Yifan Liu, Bo Zhao, Xiaofei Li, Shuo Wang, Bin Zhang and Zhenpeng Liu “A Trust Chain Assessment Method Based On Blockchain For Sdn Network Nodes” 2019 IEEE International Conference on Smart Internet of Things (SmartIoT).

[18] Long Chen, Lin William Cong, and Yizhou Xiao “A Brief Introduction to Blockchain Economics” 2021 World Scientific Publishing Company https://doi.org/10.1142/9789811220470_0001.

[19] Ryuya Uda “Data Protection Method with Blockchain against Fabrication of Video by Surveillance Cameras” ICBCT'20, March 12–14, 2020, Hilo, HI, USA 2020 Association for Computing Machinery.ACM ISBN 978-1-4503-7767-6/20.

[20] Upul Jayasinghe , Gyu Myoung Lee ,Áine MacDermott, and Woo Seop Rhee “TrustChain: A Privacy Preserving Blockchain with Edge Computing” Hindawi Wireless Communications and Mobile Computing Volume 2019, Article ID 2014697.

ANNEXURE I

Review Paper for the said project has been **accepted** in *2nd IEEE-International Conference on Computational Intelligence and Sustainable Engineering (CISES-2023)*.

Paper Title:

A Review on Double Spending Problem in Blockchain

Abstract:

The double-spending problem in blockchain technology is a significant challenge that threatens the integrity and trustworthiness of decentralized systems. This problem occurs when a user attempts to spend the same cryptocurrency unit twice, leading to a situation where the blockchain network must decide which transaction to accept and which to reject. One of the most urgent problems with blockchain technology is the issue of double spending, as it undermines the fundamental principles of trust and transparency that underlie decentralized systems. Various factors can contribute to the double-spending problem, including network latency, malicious actors, and the consensus mechanism used to validate transactions. This study investigates the many approaches put out to solve the double-spending issue in blockchain technology. The proof-of-work consensus mechanism, which necessitates network users to carry out difficult calculations in order to validate transactions, is one of the most popular alternatives. The proof-of-stake consensus technique is an additional remedy, which relies on participants staking their cryptocurrency units to validate transactions. While both mechanisms have their advantages and disadvantages, they are not foolproof and can be vulnerable to attacks. Emerging technologies, like multi-party computation and zero-knowledge proofs, are being investigated in addition to current solutions to the double-spending issue. Overall, this paper highlights the critical nature of the double-spending problem in blockchain technology and evaluates the existing and emerging solutions to the issue.

Authors:

Abhishek Kumar, Bashant Kumar Sah, Tushar Mehrotra and Gaurav Rajput

Abhishek Kumar
<2019005482.abhishek@ug.sharda.ac.in>

Fwd: CISES-2023 #8260- Acceptance

2 messages

Mr. Tushar Mehrotra (SSET Assistant Professor) <tushar.mehrotra@sharda.ac.in> Wed, Apr 26, 2023 at 9:50 AM

To: Abhishek Kumar <2019005482.abhishek@ug.sharda.ac.in>, Basant Kumar <2019007919.basant@ug.sharda.ac.in>

---------- Forwarded message ---------
From: **Tushar mehrotra** <tusharmehrotra9@gmail.com>
Date: Wed, Apr 26, 2023, 9:49 AM
Subject: Fwd: CISES-2023 #8260- Acceptance
To: <tushar.mehrotra@sharda.ac.in>

---------- Forwarded message ---------
From: **CISES2023** <conf.cises@glbitm.ac.in>
Date: Tue, Apr 25, 2023, 4:24 PM
Subject: CISES-2023 #8260- Acceptance
To: <abhishek@ug.sharda.ac.in>, <bashant@ug.sharda.ac.in>, <tusharmehrotra9@gmail.com>, <gauravrajput31@gmail.com>

Dear Author,

Greetings from G L Bajaj, India!

We are pleased to inform you that your paper **ID: 8260** with Title: " **A Review on Double Spending Problem in Blockchain**", submitted to the 2nd International Conference on Computational Intelligence and Sustainable Engineering Solution (CISES-2023), has been **Accepted**. The Conference is scheduled to be held from 28th April 2023 to 30th April 2023.

ANNEXURE 2

Research Paper for the said project has been **Communicated** in *20th India Council International Conference (INDICON-2023)*.

Paper Title:

A Trust Based Blockchain For Digital Transactions

Abstract:

The quantity and quality of interactions with the entity being trusted are often the determinants of trust. A web service's or the Internet's level of successful and failed interactions determines how much confidence may be placed in it. Within the setting of chains of trust when an agent is authorized to promote a service, effective interactions are used to simulate trust. Since the agent must first communicate with the provider and then with the person requesting the service, this is known as a "trust chain." Four different forms of modelled and simulated interactions employ five suggested trust theorems. It is demonstrated that in order for trust to increase, interaction times must eventually approach infinity; as a result, trust could never be total in practice term.

Authors:

Abhishek Kumar, Bashant Sah, Tushar Mehrotra

Abhishek Kumar
<2019005482.abhishek@ug.sharda.ac.in>

Fwd: INDICON-2023 submission 18

1 message

Abhishek Kumar <abhishekbth99@gmail.com>
To: 2019005482.abhishek@ug.sharda.ac.in

Thu, May 4, 2023 at 2:56 AM

---------- Forwarded message ---------
From: **INDICON-2023** <indicon2023@easychair.org>
Date: Thu, 4 May 2023 at 02:41
Subject: INDICON-2023 submission 18
To: Abhishek Kumar <abhishekbth99@gmail.com>

Dear authors,

We received your submission to INDICON-2023 (20th India Council International Conference):

Authors : Abhishek Kumar and Bashant Kumar Sah
Title : A Trust Based Blockchain For Digital Transactions
Number : 18

The submission was uploaded by Abhishek Kumar <abhishekbth99@gmail.com>. You can access it via the INDICON-2023
EasyChair Web page

https://easychair.org/conferences/?conf=indicon2023

Thank you for submitting to INDICON-2023.

Best regards,
EasyChair for INDICON-2023.