A Review on Double Spending Problem in Blockchain

Abhishek Kumar
Department of Computer Science and Engineering
Sharda School of Engineering & Technology, Sharda University,
Greater Noida,Uttar Pradesh, India
abhishekbth99@gmail.com

Bashant Kumar Sah
Department of Computer Science and Engineering
Sharda School of Engineering & Technology, Sharda University,
Greater Noida,Uttar Pradesh, India
basantsah1438@gmail.com

Tushar Mehrotra
Assistant Professor
Department of Computer Science and Engineering
Sharda School of Engineering & Technology, Sharda University,
Greater Noida,Uttar Pradesh, India
tusharmehrotra9@gmail.com

Gaurav Kumar Rajput
Assistant Professor
College of Computing Sciences & IT,
Teerthanker Mahaveer University
Moradabad
gauravrajput31@gmail.com

2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES) | 979-8-3503-2391-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/CISES58720.2023.10183579

***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.**

Keywords—Cyber Security, Blockchain, Cryptocurrency, Digital Archive, Database, Networking, Trust Evaluation.

I. INTRODUCTION

Blockchain technology has emerged as a revolutionary innovation that offers decentralized and transparent systems for storing and transferring data and value. It has gained significant traction in recent years, with applications ranging from cryptocurrencies to supply chain management, voting systems, and more. However, a fundamental issue known as the double-spending problem poses a danger to the reliability and integrity of blockchain technology. When a user tries to spend the same cryptocurrency unit twice, thus making a duplicate of the original transaction, this is known as double-spending. This problem is a result of the decentralized nature of blockchain technology, which allows multiple nodes in the network to validate transactions. If not addressed properly, the double-spending problem can undermine the fundamental principles of trust and transparency that underlie decentralized systems. Various factors contribute to the double-spending problem, including network latency, malicious actors, and the consensus mechanism used to validate transactions. The consensus mechanism is a critical component of blockchain technology that ensures that all nodes in the network agree on the order and validity of transactions. However, if the consensus mechanism is compromised, it can allow a malicious actor to double-spend cryptocurrency units. Over the years, The double-spending issue in blockchain technology has been addressed in a number of ways. 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. The double-spending problem is still a major obstacle for blockchain technology, despite these fixes, and new approaches like zero-knowledge proofs and multi-party computation are being investigated to solve it. Consequently, the purpose of this paper is to give a general overview of the double-spending issue with blockchain technology, its causes and consequences, and evaluate the existing and emerging solutions to the issue. Given the importance of addressing the double-spending problem, researchers and developers have proposed various solutions to mitigate the issue. However, these solutions are not foolproof, and the problem persists. Therefore, further research and innovation are needed to develop more effective solutions to address the double-spending problem in blockchain technology. The purpose of this paper is to present a thorough review of the double-spending issue in blockchain technology, examining its causes and consequences and evaluating the existing and emerging solutions to the issue. The paper will also highlight the limitations and challenges associated with existing solutions and identify potential future research directions in this critical area. In summary, the double-spending problem remains a significant challenge in blockchain technology, undermining its integrity and trustworthiness. While various solutions have

been proposed to address the issue, For decentralised systems to be secure and reliable, more research and innovation are required to create more efficient solutions. The report will also emphasise the requirement for additional investigation and invention to guarantee the security and dependability of decentralised systems.

II. Literature Review

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. A DLT-based land transaction system they designed with a trusted nodes consensus mechanism offers a promising means of facilitating safe and open 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 proposed framework provides a holistic approach to evaluating blockchain systems and can be used to identify the strengths and weaknesses of different 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]. This paper's author discussed the semantic connections between the three DSTs, SR, OLAP, and ARM. 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.

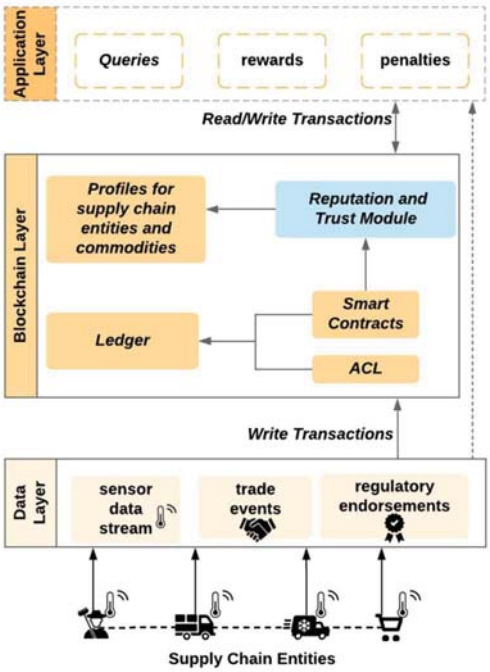

Fig. 1. Three-layered structure of the TrustChain framework [8].

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 programmes, and product identification. The article also covers the advantages of utilising 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 personalised 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.

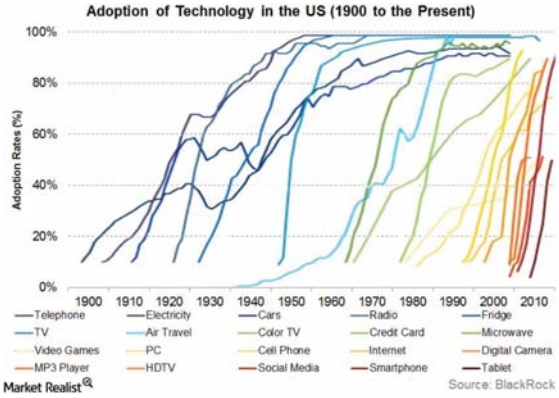

Fig. 2. Different Adoption rates of blockchain technology and innovation in the US since 1900 [12].

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.

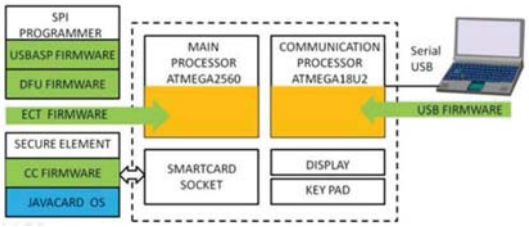

Fig. 3. Crypto Terminal Components & Firmware [13].

Hrvoje et. al.,[14] The author analysed the body of research on the use of blockchain technology for digital archives and then offered a novel approach that takes advantage of the advantages of blockchain while getting around the drawbacks of data immutability. 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 most prevalent consensus techniques used in blockchain systems, such as Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT), are thoroughly explained by the author in this study. 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 suggest a trust chain assessment approach based on blockchain technology. 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 analyse 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 impact of proof-of-work and proof-of-stake consensus algorithms on the economics of blockchain systems is examined. The function of cryptocurrencies in the blockchain ecosystem and their potential as a medium of trade, a store of value, and a unit of account were covered in this article.

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 decentralised 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 I. 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.	This article proposes a distributed and secure P2P network infrastructure for real estate transactions. Using the block-chain to share the storage of property transactions improves system transparency and reduces hazards.
Yadav, Amrendra Singh, Shivani Agrawal, and Dharmender Singh Kushwaha.(2022)	Distributed Ledger Technology-based land transaction system with trusted nodes consensus mechanism	A new option for many financial applications that need a safe and unchangeable transactions mechanism is blockchain technology. 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 issues and potential solutions for blockchain simulation approaches, including the need for multi-task benchmarks for reliable model comparison, access to historical blockchain system data that is representative, assessing the impact 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	Both online analytical processing (OLAP) and association rule mining have emerged, each with specific purposes and objectives.	the semantic resemblances among the three DSTs will be useful in the creation of a few next-generation hybrid decision support systems.
Yadav, A. S.,(2021)	The efficient consensus algorithm for land record management system	It is built on blockchain technology, with the goal of streamlining the registration process by bringing all registrar offices under one framework.	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 hosts in order to do this.
Malik, Sidra, (2019)	Trust chain: Trust management in blockchain and iot supported supply chains	Among these technologies, statistical reasoning was frequently utilised to clarify data-driven conclusions. Later, we witnessed the rise of association rule mining and online analytical processing (OLAP), both of which have distinct purposes and goals.	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	We take into account two different kinds of trust: customer and supplier trust.	Second, take into account the dynamics of trust in the game and the link between trust and the choice to replenish inventory, which hasn't been well explored in previous studies.
Six, Nicolas, Nicolas Herbaut, and Camille Salinesi(2022)	Blockchain software patterns for the design of	The blockchain technology is a distributed ledger made up of blocks, which is supported by a network of	This study also advances the state of the art for blockchain-based patterns by developing a taxonomy that will aid in categorising newly developed patterns, mapping and describing the body of literature on blockchain-based patterns within the
	decentralized applications.	peers, each of whom possesses a copy of the ledger.	taxonomy, and identifying research gaps that could be filled in future studies.

III. PROPOSED MODEL

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. The transaction is included in a block and added to the blockchain if it is valid. The network nodes may accept one transaction while rejecting another if a fraudulent user attempts to double spend by generating two conflicting transactions. This can create a situation where the same cryptocurrency tokens are spent twice, leading to a loss of value for the recipient and undermining the integrity of the blockchain. We proposed a network observer that can follow anomalous transactions carried out without authorization in order to fix the problems with the current system. Additionally, we suggested a peer warning system that passes the message from the fraudulent node to the sender and receiver nodes in order to alert them of the unauthorised transaction.

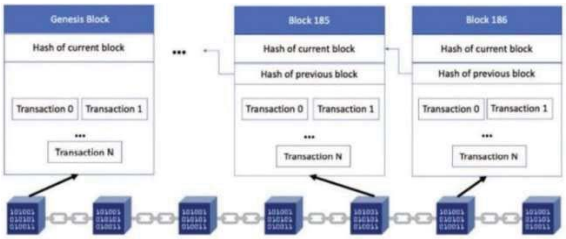

Fig. 4. Blockchain Architecture.

Network observers: Each pair of nodes has a network observer placed in between. The transaction amount, transaction ID, and sender information are sent to the nearby node by the sender node. After completing the transaction process, the nearby node will then pass this to the matching forward node. This keeps on till the recipient node gets the money. The user ids, number of transactions, and amounts issued by each user are tracked by the observers within each pair of nodes. Based on the quantity of transactions issued by the user, an observer can use this record to determine the frequency of node communications in its node pair. The anomaly will be recorded, the transaction will be cancelled, and an acknowledgement will be issued back to the sender node if the frequency is higher than what is necessary.

Peer Alert Systems: The surrounding nodes are made aware of the fraudulent transaction when a network observer notices an irregularity at one of the transaction steps between a node-pair. So that their transactions may be carried out over

other secure pathways, this will assist the neighbouring nodes in cutting off their connections with the fraudulent node pair.

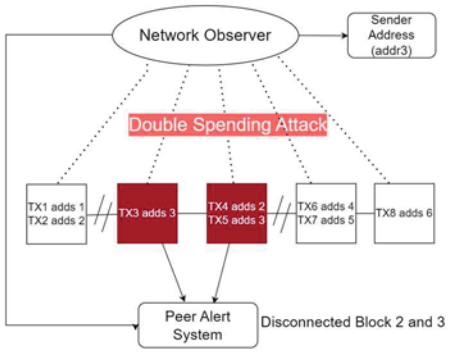

Fig. 5. Network Observer and Peer Alert System Model.

Implementation of proposed mode: Firstly, we run a program to start the initial blockchain in node JS and After navigating to the directory using the command line or a terminal, we execute the next command, node CryptoBlockchain.js. It will construct nodes as follows:

```
The current blockchain is:
CryptoBlockchain {
  currenthash: '0000a0edcfe4285c12726fdd88c42736d49016b4358c47e58ea4e06b9a3796cb',
  blockchain: [
    CryptoBlock {
      timestamp: 0,
      transactions: 1682020737929,
      precedingHash: '0',
      hash: 'a645fc624f155de6ab0f03699472787bd91376f25e0674b3e99fa3d8ab57e687',
      nonce: 0,
      ne: null
    },
    CryptoBlock {
      timestamp: 1682020738000,
      transactions: [Array],
      precedingHash: 'a645fc624f155de6ab0f03699472787bd91376f25e0674b3e99fa3d8ab57e687',
      hash: '00000128f8242dc0f681b26edd777a7880472f0936174a09fdcff969e0177651',
      nonce: 159968,
      ne: null
    },
    CryptoBlock {
      timestamp: 1682020752511,
      transactions: [Array],
      precedingHash: null,
      hash: '0000a0edcfe4285c12726fdd88c42736d49016b4358c47e58ea4e06b9a3796cb',
      nonce: 84063,
      ne: null
    }
```

Fig. 6. Initial Cryptocurrency Blockchain.

For additional security a random nonce generator is used, that will be used in the hash creation. Moreover, to increase A difficulty index is used to add extra zeros to the computed hash, which increases the mining time complexity and 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.

1. The original and recomputed hash values of the current block are compared after the hash has been recalculated using the same nonce.

2. The hash of the current block is compared to the hash of the block before it.

The validation method produces an error if one of these two processes reveals a discrepancy.

```
CryptoBlockchain {
  currenthash: '0000a0edcfe4285c12726fdd88c42736d49016b4358c47e58ea4e06b9a3796cb',
  blockchain: [
    CryptoBlock {
      timestamp: 0,
      transactions: 1682020737929,
      precedingHash: '0',
      hash: 'a645fc624f155de6ab0f03699472787bd91376f25e0674b3e99fa3d8ab57e687',
      nonce: 0
      ne: null
    },
    CryptoBlock {
      timestamp: 1682020738000,
      transactions: [Array],
      precedingHash: 'a645fc624f155de6ab0f03699472787bd91376f25e0674b3e99fa3d8ab57e687',
      hash: '00000128f8242dc0f681b26edd777a7880472f0936174a09fdcff969e0177651',
      nonce: 159968,
      ne: null
    },
    CryptoBlock {
      timestamp: 1682020752511,
      transactions: [Array],
      precedingHash: null,
      hash: '0000a0edcfe4285c12726fdd88c42736d49016b4358c47e58ea4e06b9a3796cb',
      nonce: 84063,
      ne: null
    }
  ],
  difficulty: 4
```

Fig. 7. Blockchain integrated with additional functionalities.

Here, the black highlights represent the random nonces used to compute the hash for each new block added, and the red highlights represent the appended zeros based on the difficulty index. Before changing any of the blocks, we should observe and record the output of the verify chain validity function, which should return true, indicating that the blockchain is legitimate.

We are currently conducting transactions. The addresses of the intended sender and destination blocks or nodes are mined in order to carry out transactions between them. This allows the transaction value to be added to the receiver node and subtracted from the sender node. Beginning with the genesis block's null amount transaction and continuing to store each subsequent transaction, an array holds the records of all pending transactions for each block. The first block transfers 100 bitcoin units to the second block as an illustration. The second block then gives the first block back 50 bitcoin units. Because of this, the transaction array will include information about the transactions with amounts of 0, 100, and 50, respectively. A mining reward of 10 points is applied to the balance of a particular genesis block after each successful transaction.

```
smashingCoin.createTransaction( new Transaction("addr1","addr2",100));
smashingCoin.createTransaction( new Transaction("addr2","addr1",50));

console.log("Starting the miner...");
smashingCoin.minePendingTransactions("myAddress");
console.log("Your balance is: "+smashingCoin.getBalanceOfAddress('myAddress'));

console.log("Starting the miner again...");
smashingCoin.minePendingTransactions("myAddress");
console.log("Your balance is: "+smashingCoin.getBalanceOfAddress('myAddress'));
```

Fig. 8. Program to perform transaction.

```
Starting the miner...
Block Mined: 0000353965b0a2eca880ea43429032ae609f72ce536fe6615bc1057061b8b671
Timestamp: 1682050350796
Block successfully mined!
Block Mined: 00002bf03ab686bee11f268d1afcf7123a953c038b148c2d73f0b0bfab0d7dcd
Timestamp: 1682050376019
Block successfully mined!
```

Fig. 9. Performing Transaction in Blockchain.

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 the genesis block receiving 10 cryptocurrency units in exchange for 3 cryptocurrency units from another block.

```
Transaction {
  fromAddress: '04dee849035cee29de07ff8899eaaf86fcc7b5db3a7d6eaecbd1ea75ceb7010f7e9a346
b986752177bcacfceaa28dd5fca6f34398ff80920b7b567256fed2adae3',
  toAddress: '04b9b89e4dbeffabedc5081fef54f3f65540f86ee9b04a9d709b5777ad04889e157132318
419afe2b9570ed2fd6e27f79b8b8b53b10af6b81c4963900e13cf48ab',
  amount: 3,
  signature: '3046022100d711f2575595f504ddb004abf9b38cc0d1475e379b235981fbcb89446361dde
b022100ef34284b08a9c6a384bf3c13ae4e6a59d6bb0d12175f05fb5a789b09114a8114'
},
Transaction {
  fromAddress: '0485c69fcadd380090078eb37b067371ded392b157cac8481796c9e3fc5e174fe658f44
0c04488bf3a2aa4a97e740f6f34eb42e55ee261ac366e3a6d026ef55655',
  toAddress: '04651603030f5d80b64770ec9fb95738514f412d92816bb08d296ac483b03fe2f836bf91e
724aa716b1d1913a01aea868d2ffe57479ee7702f4e2dce2a387dfb8c',
  amount: 10,
  signature: '30440220241e8992965af63e43ef34e10c3c98d1d323e817698bc08364e4932668516ced0
2206c98ebdd4adac79f936d759e36d4f11ce439f9d61ccbbb34d712786c3d517b58'
},
```

Fig. 10. Transaction Signature.

We are now using a blockchain to perform 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. The example below can be used to demonstrate this. Suppose a sender has 10 bitcoin units and wants to simultaneously send them over 2 distinct blocks to 2 different recipients. The sender needs to have a total of 20 units on hand for both transactions to take place, but he only has 10, suggesting that he intends to reuse the money from the first transaction in the second transaction so that the 10 units are deducted simultaneously (and only 10 units are finally deducted from his balance).

```
Transaction {
  fromAddress: '0485c69fcadd380090078eb37b067371ded392b157cac8481796c9e3fc5e174fe658f440c04488bf3a2
aa4a97e740f6f34eb42e55ee261ac366e3a6d026ef55655',
  toAddress: '04651603030f5d80b64770ec9fb95738514f412d92816bb08d296ac483b03fe2f836bf91e724aa716b1d1
913a01aea868d2ffe57479ee7702f4e2dce2a387dfb8c',
  amount: 10,
  signature: '30440220241e8992965af63e43ef34e10c3c98d1d323e817698bc08364e4932668516ced02206c98ebdd4
adac79f936d759e36d4f11ce439f9d61ccbbb34d712786c3d517b58'
},
Transaction {
  fromAddress: '0485c69fcadd380090078eb37b067371ded392b157cac8481796c9e3fc5e174fe658f440c04488bf3a2
aa4a97e740f6f34eb42e55ee261ac366e3a6d026ef55655',
  toAddress: '04b788aeeffd88769e1d24fed7feb73b746459ec646ccf65b3013175f3dd989d039412ac8eafc958bf4f2
b67611c38f20cd2ee36e5cb34b08dc50bdb99d4626376',
  amount: 10,
  signature: '304402203e6f0c0edbd4e28fd5117717bd362dda28fc19da6b1100ef597a8694efcd541002201c95ddef1
1850979403994d6b4446eedc245c83546206fd987489175dc69c7ac'
},
```

Fig. 11. Double spending the same amount.

As can be seen above, two transactions with a total of ten digital currencies units each (underlined in blue) utilise the same sender hash address (highlighted in yellow), but they have separate receiver hash addresses. As a result, only 10 units will be taken out of his balance at once, despite the fact that his true deduction should be for 20 units, if these 2 transactions are carried out concurrently (i.e. at the same timestamp). Thus, by taking advantage of this problem, the sender can carry out numerous transactions of this kind while only paying half the total sum.

In a blockchain, a network observer will look for 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.

```
if(total>balance && num>1)
{
console.log("\nYour transaction has been aborted due to a suspected double-spending attack.");
console.log("\nPlease cancel your last transaction or try again later.");
}
```

Fig. 12. Checking number of pending transaction.

In the blockchain, a double spending attack takes place. The user is prompted to erase the most recent transaction or risk being temporarily suspended by the network observer, which throws an error. Following this, the peer alert mechanism will cut off connections between legitimate blocks and other blocks (while warning nearby blocks), as demonstrated below:

```
Number of pending transactions from address:
0485c69fcadd380090078eb37b067371ded392b157cac8481796c9e3fc5e174fe658f440c0448
8bf3a2aa4a97e740f6f34eb42e55ee261ac366e3a6d026ef55655 is:2

Total payment amount is: (10,10)

Your transaction has been aborted due to a suspected double-spending attack.

Please cancel your last transaction or try again later.
Disconnected block number  2 due to a suspected double spending attack.
Disconnected block number  3 due to a suspected double spending attack.

Initial balance was: 10
```

Fig. 13. Double spending attack.

The nearby blocks are informed in order to detach from the block where the fraudulent transaction or double spending attack occurred. Any upcoming transactions booked 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. The attack on double spending reduces the number of transactions from four to two as a result (the transactions implicated in the attack are halted). 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 replaced with a new genesis block that has a preceding hash of '0' to get around the problem of having a null preceding hash. Additionally, this will result in the creation of a new current hash that can be used to carry out the same transaction as previously (Change of transaction route).

Fig. 14. New genuine transaction.

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

```
Performing Transactions:

Initial balance was: 10
Current balance of address  04dee849035cee29de07ff8899eaaf86fcc7b5db3a7d6eaecbd1
ea75ceb7010f7e9a346b986752177bcacfceaa28dd5fca6f34398ff80920b7b567256fed2adae3 i
s: 7

Initial balance was: 10
Current balance of address  048283cc3178545c8967e58391ec39b75ca56256026a5b2202b9
fef7d71c305e9f9867e7f6b8396c1bc15c76bd2c7a624c15abe46f9a5c89e20c82e4d2f9a621c7 i
s: 5
```

Fig. 15. Performed genuine transaction.

IV. Conclusion

The double spending problem remains a critical challenge in blockchain technology. Blockchain is susceptible to double spending attacks because there is no central authority to authenticate transactions because of its decentralised structure. Many solutions, including Proof of Work (PoW), Proof of Stake (PoS), Byzantine Fault Tolerance (BFT), Directed Acyclic Graph (DAG), and other consensus mechanisms, have been put forth by researchers and developers to solve this issue. 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.

Acknowledgment

This research paper is based on research work conducted for “A Sybil-resistant Scalable Blockchain-Trust Chain.” This work would not be possible without all those people whose contributions cannot be ignored. We specially acknowledge Mr. Tushar Mehrotra for guiding us in Double Spending Problem research work and always supporting us. We are grateful to Sharda University for providing everything from faculty guides to resources for this work. We would like to thank all other people who have directly or indirectly helped me to complete this work.

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.