International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Blockchain-Based Security Model for Secure Data Transactions

Sowmya.G[1] , Mrs. C.Mohanapriya[2]

[1] Undergraduate Student [2] Associate Professor Department Of Computer Technology, Dr.N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India

https://doi.org/10.55041/ijsmt.v2i3.059

Cite this Article: Sowmya.G, (2026). Blockchain-Based Security Model for Secure Data Transactions. International Journal of Science, Strategic Management and Technology, *02*(03). https://doi.org/10.55041/ijsmt.v2i3.059

ABSTRACT

The frequency of online transaction between businesses and individuals is increasing every day, when it includes banking, data sharing and transaction record keeping. Many institutions today experience severe security issues such as ongoing data breaches and unauthorized access or modifications to their transaction records. These security issues show that there is very little to no secure and dependable way to manage digital transactions. A majority of people believe that blockchain technology can solve these issues because of its distinguishing features of being decentralized, allowing for the use of cryptographic techniques to secure data and providing a transparent public process for recording transactions.

This research proposes a new method for providing the security needed to conduct data transactions in a more trustworthy and efficient manner using blockchain technology. The proposed framework will provide additional integrity, transparency, reliability, and security to digital transaction systems by creating an alternative digital transaction system through blockchain network data storage and transaction validation without having a central authority. In addition to having the additional integrity, transparency, reliability and security provided to digital transaction systems, all transactions are also secured using cryptography and recorded in a series of blocks with secure links between blocks.

The proposed digital transaction model will ensure the integrity of individual transactions by supplying the means to prevent unauthorized modification and maintain the consistency of data generated by all transactions throughout the entire blockchain network. Therefore, the model will provide a secure and transparent platform for conducting digital transactions through the use of cryptographic hashes and consensus mechanisms. This research concludes that through the application of the proposed digital transaction model digital transactions will have a higher level of integrity and security through the implementation of integrated blockchain transactions.

Keywords — Blockchain, Data Security, Distributed Ledger, Cryptography, Secure Data Transactions, Consensus Mechanism, Smart Contracts.

INTRODUCTION

The technological growth of the past several years has created an exponential increase in the volume of data transactions between organizations and individuals using digital platforms (e.g., financial transactions, data sharing, cloud storage, and online services). These digital platforms have made transactions easier and faster, however they also pose major threats to transaction security. Centralized digital platforms are particularly vulnerable to cyber-attacks, data breaches, unauthorised access, and manipulation of transaction records. Because centralized platforms depend on one central authority to record and verify transactional information, centralized systems have a single point of failure and are often a target for malicious activity.

As such, many organizations and individuals are increasingly concerned about protecting the integrity, transparency, and reliability of digital transactions. A number of organizations have trouble ensuring that data remains intact and that sensitive data has not been modified without authorization. Traditional security solutions rely on centralized databases and encryption; however these traditional security solutions have the same risks as centralized systems: i.e., system failure, insider attacks, and data tampering. Accordingly, as the number of transactions continues to rapidly increase, organizations will have a growing need for a more secure, decentralised way to manage transaction data.

The potential of Blockchain to solve these issues seems very promising. The decentralized model relies on having many points where transaction records (the 'ledger') are created through a distributed network and stored on multiple servers around the world (also known as nodes). Each time a transaction is added to the ledger, it is bundled together into groups – known as 'blocks' – which are then linked back to previous blocks using cryptographic hashes to produce an unbiassed chain of record.

The lack of a central authority overseeing the integrity of these transaction records creates a considerable amount of transparency and traceability between all parties involved in a transaction, thus building trust among those participating in the network. Once recorded, transaction data is nearly impossible to alter, thereby providing both proof and transparency of each transaction.

The aforementioned security features of blockchain technology have spurred research and applications from various industries, including financial services, supply chain management, healthcare records, and secure data-sharing platforms, for example. Digital transaction-based platforms can benefit by having a much higher level of reliability and security than what traditional methods provide using cryptography and consensus algorithms.

This research aims to create a security model using blockchain technology to improve the integrity, transparency, and security of transaction data when transacting securely over the internet. We will also explore various decentralized validation systems and hashing techniques used in conjunction with the blockchain for ensuring accurate storage and protection of transactional data.

METHODOLOGY

A proposed Blockchain Based Security Model for the Secure Transaction of Data is to ensure security and transparency through the management of digital transactions through the use of the blockchain. The project will involve several stages, as indicated in the methodology, demonstrating how to verify, store, and secure transaction data in a distributed network.

Below are the main components of the methodology.

1. User Registration & Identification

The first step in using the system is to register and authenticate users. If a user wishes to perform a transaction on the blockchain, they must create a user account and then be verified as a legitimate user before having access to the system. This verification process will strictly limit transaction initiation to those users who have been approved.

2. Transaction Request

Once the user is authenticated, he/she can initiate a transaction request from the system's user interface. A transaction can take the form of a request to send data or to execute a secure digital transaction. Each transaction also contains other unique pieces of information (e.g., user ID, transaction description, request time, etc.) essential to the completion of the transaction request.

3. Transaction Verification

After the creation and distribution of the transaction request, it is sent back to the blockchain particularly to verify that the transaction has been validated by the nodes in the network through a series of predetermined criteria using cryptographic algorithms. The verification process will ensure that the transaction is a legitimate transaction.

4. Creation of a Block

After verification, the transactions get combined with other verified transactions to create a block. A Block is an array of transaction records and includes additional metadata about the transactions, for example; timestamps and identification data about the block.

5. Creation of the Hash

A unique hash value is generated for each block using a hashing algorithm (for example; SHA-256). This hash acts as a digital fingerprint for the block and helps maintain the integrity of the transaction data stored in that block. A change made within the data of the block will cause a different hash value to be generated, making it easy to detect any adjustment to the data in that block.

6. Adding the Block to the Blockchain

The new block is added to the blockchain by linking it to the previously created block in the blockchain, utilizing the hash that was created. This creates a continuous series of blocks that make up the blockchain. When this block is added to the blockchain network and subsequently becomes part of the distributed ledger, the block will never be changed.

7. Confirmation of the Transaction

Once the new block is added to the blockchain, the transactions included in the block are permanently and independently confirmed in the distributed ledger. Due to the fact that the blockchain is decentralized and unable to be altered, any data within the blockchain cannot be modified or removed from that point forward. Therefore, there is a level of security, transparency, and reliability with respect to the various digital data transactions.

LITERATURE REVIEW

The past few years have seen a great deal of attention focused on blockchain technology as a possible solution for secure, decentralized, and transparent systems that can manage data with ease. This concept of blockchain was originally introduced by Nakamoto [1] to serve as the foundation for Bitcoin, thus allowing peer-to-peer (P2P) electronic transactions to occur without a central authority governing them. In this way, a blockchain is essentially a distributively stored ledger containing all transaction information; each ledger consists of a number of blocks, all of which connect to each other using cryptographic hashes; thus, all blocks in the ledger are interconnected creating a very secure environment for data storage; all available time-stamped data entries cannot be altered or tampered with.

Crosby et. al. [2] explain that although blockchain technology is widely recognized for its association with cryptocurrencies, it has many other applications that can help to improve security in a variety of fields, i.e. financial systems security, healthcare records security, and digital identity management. Blockchain technology is able to offer these benefits due to its nature as a decentralized system, there is no longer a need to rely on a central database or authority; thus, helping to mitigate any risks associated with a reliance on a single central authority and establishing trust and transparency between parties to a transaction by establishing common rules for how and when to exchange information.

Zheng et al. [3] provided an overview of blockchain, including descriptions of what the platform is, consensus mechanisms used to develop it, and examples of how it has been used to create secure transaction records. They mentioned many characteristics of blockchain that contribute to its strong security, such as being unalterable, decentralized, and cryptographically secure, make it an ideal method for storing records of private transactions.

Li et al. [4] proposed a blockchain-based solution for secure transactions as part of their framework for exchanging and managing records across multiple entities. They showed that the combination of cryptographic hashing and distributed consensus mechanisms used by blockchain provides an effective means of preventing the tampering of transaction data. Additionally, they indicated that blockchain systems offer a more reliable and secure method for storing records of transaction.

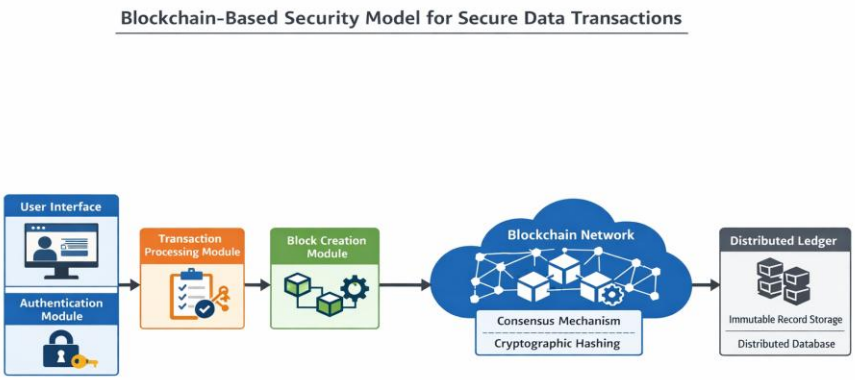
Xu et al. [5] researched the use of blockchain technology in order to improve data security in distributed systems. They illustrated how blockchain enables secure verification of transactions through the use of consensus algorithms and helps

prevent unauthorized manipulation of the data. The results of their research indicate that blockchain-based applications provide a greater level of security and trust for digital transaction systems.

Despite the strong security capabilities of blockchain technology, it currently faces challenges related to scalability, the computational complexity of running the system, and network performance associated with its use.

SYSTEM ARCHITECTURE

The blockchain-based Security Model for Secure Data Transactions provides a decentralized and secure transaction management solution. The architecture consists of interconnected modules, with various relationship types, which provide a secure and validated method for the processing, validating and storing of transaction data within the blockchain. By doing so, this model ensures that data integrity is maintained, transactions are credible and prevent against manipulation by the alteration of transaction data.



The first point of contact for a user is the User Interface Module, which provides the user the functionality to create a secure transaction request. In order for a user to be able to create a secure transaction, they must go through the process of registering as well as authenticating their identity to be identified by the system before they can submit a secure transaction request.

After a user authenticates their identity successfully, the transaction request is then transferred to the Transaction Processing Module. The Transaction Processing Module is responsible for processing the verification of the submitted transaction request and can be based on the user's identification, transaction data and other data related to their transaction (i.e. time stamps). The Transaction Processing Module is responsible for verifying or validating this information then sending the validated transaction to the blockchain network. The blockchain network is comprised of multiple nodes that are participated in transaction verification and rules validation.

After verifying a transaction, it is indicated in conjunction with other verified transactions into a block. Transactional information is formatted according to the Block Creation Module, and each block generated will have its own unique identifier in the form of a cryptographic hash using a hashing algorithm such as SHA-256. In addition to having a unique identifier, every block will store the hash of the block preceding it; this creates links between blocks that form a continuous chain, called the blockchain.

Once created, the new block will be added to the Distributed Ledger. The Distributed Ledger is used to share all blocks with every node on the blockchain network, which means that the Distributed Ledger maintains a permanent record of all transaction records in the blockchain and provides proof of record immutability. Thus, if someone were to alter one of the previously recorded transactions, then that person would also have to alter every subsequent block in order for the change to be valid; in other words, it is virtually impossible to accomplish this because of the amount of computational resources required to do so.

The proposed system provides a secure and transparent way to manage digital data transactions through the use of blockchain technology. By using blockchain, transaction data cannot be altered after it has been recorded, making it possible to verify and trace each transaction back to its source, and preventing any unauthorized access or alteration of the transaction data.

COMPONENTS OF THE SYSTEM ARCHITECTURE

1) Interface module that allows users to be able to initiate and monitor transactions.

2) Authentication module that ensures that persons are who they say they are (users).

3) Transaction process module that validates transaction details.

4) Distributed ledger technology (DLT) network of nodes that help ensure that transactions are verified.

5) Integration of an application development chain through Group transactions together into a block and calculate hash value for each.

6) Creation of a distributed database (or ledger) that will provide users with the ability to view transactions that were approved through blockchain.

ALGORITHMS

TRANSACTION VERIFICATION ALGORITHM

Initial Input: User Transaction Request

Final Output: Verified Transaction

Process for Verifying Transactions:

1. Transaction initiation process starts

2. User's request is received

3. Identify and validate user by using authentication Module.

4. Validate the transaction information (sender, receiver, transaction data)

5. Check if the transaction meets pre-determined criteria.

6. If the transaction is determined to be valid, transaction is broadcasted to the blockchain.

7. If the transaction is invalid, user requests are denied

8. End verification process

SHA-256 HASH GENERATION

The algorithm proceeds as follows:

1. All information about the current block is assembled, including transaction information and the hash value from the previous block.

2. The SHA-256 algorithm is applied to the block.

3. A 256-bit (32-byte) hash is created, which is a fixed-length value.

4. The new hash value is written into the block's header.

5. The block is linked to the previous block using the newly create hash.

6. If there are any changes made to the data contained within the block, a new hash will be generated.

7. These features ensure that the blockchain remains unchanged and secure.

CONSENSUS MECHANISM (proof of work)

The algorithm proceeds as follows:

1. The new block is published across all nodes in the network.
2. Each node will verify the validity of the new block by solving a cryptographic puzzle.
3. The first node to solve the puzzle will validate the new block (only one node can validate a block).
4. The first validating node will then publish the validated block to all other nodes.
5. All nodes will add the new block to their blockchain ledger.
6. The transactions that are included within the newly added block will become permanent and unchangeable.

RESULTS AND DISCUSSION

The proposed blockchain-based security model for secured data transactions aims to provide a secure and trustworthy environment for processing digital transactions. The security model will use blockchain technology to integrate it with cryptographic hashing and decentralized validation mechanisms to help safeguard transaction data's integrity and transparency. The implementation of the proposed model confirms that the use of blockchain technology to process digital transactions can greatly enhance digital transaction security in comparison to traditional and centralized transaction processing systems.

When processing transactions, verification of all user request data before processing by the system will be completed via an authentication mechanism. After the user request data has been verified, the verified transaction request is sent to the blockchain network, where it is validated by many separate nodes or computers in the blockchain network according to a predetermined set of rules. The decentralized method of transaction verification along the blockchain network ensures no single entity has control of the transaction data, thus eliminating the issues of centralized transaction processing systems.

The block creation and hashing methods involved in the blockchain create a secure transaction record. The blockchain network generates and links together the transaction records grouped into blocks to create the first block after verifying transactions. The SHA-256 algorithm calculates a unique cryptographic hash for each unique transaction and provides a link between each block and its previous block. If an entity attempted to modify the information or data stored in the transaction record, the transaction record would change.

Based on the findings, the proposed system provides increased levels of data integrity, transparency and trust in performing digital transactions. The implementation of a distributed ledger using blockchain technology provides the ability to avoid single points of failure due to transaction records being stored at several nodes throughout the blockchain network and therefore maintaining transactional integrity at all nodes throughout the network. The use of consensus algorithm methods ensures that only legitimate transactions can be performed and recorded into the blockchain ledger.

The security levels provided by the proposed blockchain model in comparison to traditional centralized transaction systems provide enhanced protection of transaction data due to less opportunity for fraudulent activity through improved traceability, as well as permanent documentation of all transactions on the distributed ledger. Such attributes make blockchain technology an ideal candidate for use in those applications that require high levels of security and reliability associated with transactional data.

In summary, the proposed model improves the security of digital transactions and provides a transparent method to facilitate the exchange of digital currency through the blockchain ledger as a result of the combination of cryptographic algorithms and blockchain technology used to secure transaction data and provide verification that transaction data has not been altered or modified without authorization.

CONCLUSION

As we all know digital transactions are becoming increasingly common but they present problems for both businesses and individual consumers because of the fact that data can be altered without any way to prove that it is accurate, users can gain access to confidential information without permission, and there is little to no visibility or documentation to rely on. Because of this, it is necessary for there to be a more secure means of facilitating digital transactions. One way that this can be achieved is through the implementation of a blockchain-based security model for secure data transactions.

The proposed solution uses a distributed network of decentralized nodes on the blockchain to create a permanent record of every transaction that happens on the network. Each time there is a transaction of any type it gets hashed using a cryptographic hashing algorithm, and then each transaction is collectively validated by a method referred to as 'consensus', on all nodes. This means that once a transaction gets recorded on the blockchain, there is a high degree of confidence that it will not be changed in any way (due to nature of the hashing algorithm) and therefore, the integrity of that transaction is guaranteed. Additionally, there is no longer a central authority (or point of failure) in order to validate a transaction, so individuals can trust each other to validate each other's transactions.

According to the results of this research, the newly proposed model will enhance safety, traceability and dependability of the electronic transaction systems through an environment that is tamper-proofed and decentralised. To protect sensitive transaction information from being altered and/or having access given without authorization to them, will greatly improve the level of protection afforded to those parties involved in making transactions, while continuing to provide transparency and traceability of all transactions to those parties that have access to such transaction records. The new model of using blockchain technology as a security mechanism provides the best opportunity available today for achieving greater safety for all digital data transactions.

The long-term goal for the new security system and model is to improve on existing security systems by integrating additional state of the art consensus models, improving scalability and merging blockchain technologies with other emerging technological advancements (i.e., artificial intelligence, Internet of Things (IoT), etc.) that will enable developers of digital applications to develop more efficient, safe and scalable electronic transaction systems.

REFERENCES

1. S. Nakamoto, "*Bitcoin: A Peer-to-Peer Electronic Cash System"*, 2008.

2. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, 2016.

3. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE International Congress on Big Data, 2017.

4. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A Survey on the Security of Blockchain Systems," Future Generation Computer Systems, 2019.

5. X. Xu et al., "A Taxonomy of Blockchain-Based Systems for Architecture Design," IEEE International Conference on Software Architecture, 2017.

6. D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology (NIST), 2018.