ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2023.0425

ENHANCED ANALYSIS OF BLOCKCHAIN BASED SECURITY SYSTEMS IN FINANCIAL INSTITUTIONS

A. Sairam[1], D. Sasikumar[2], R. Sendhil Kumar[3] and B. Yuvaraj[4]

[1]Department of Computer Science and Engineering, Karpaga Vinayaga College of Engineering and Technology, India
[2]Department of Computer Science and Engineering, Sphoorthy Engineering College, India
[3]Department of Master of Computer Application, Thirumalai Engineering College, India
[4]Department of Computer Science and Engineering, Thirumalai Engineering College, India

Abstract

The blockchain technology has provided a revolutionary way of secure data storage and transfer. It is a distributed ledger technology (DLT) that creates a secure and immutable record of transactions. This technology has been used to create secure and reliable systems for financial institutions. The blockchain based security system provides a secure platform for financial institutions. It ensures that the transactions are secure and immutable. This technology has been used to create digital assets that can be securely stored and transferred. It also ensures that the transactions are transparent and secure. The blockchain technology can be used to enable secure transactions between financial institutions. By using the blockchain, financial institutions can create a secure platform for transactions. This will ensure that the transactions are secure and immutable. It also ensures that the transactions are transparent and secure. The blockchain technology can also be used to create a secure system for digital identity management. This will ensure that the digital identities of the users are secure and immutable. It also ensures that the users' identity is protected and secure. The blockchain technology can also be used to create a secure platform for digital payments. This will ensure that the payments are secure and immutable. It also ensures that the payments are transparent and secure.

Keywords:

Blockchain, Secure, Data Storage, Technology, Transactions, Financial Institutions

1. INTRODUCTION

The rise of blockchain technology is revolutionizing how financial institutions manage and secure financial transactions. Blockchain based security systems are becoming increasingly important for financial institutions as they offer a powerful distributed system with enhanced security, transparency, and trust.

Blockchain technology is a distributed, immutable ledger that allows for secure, transparent, and trust-based transactions. This technology offers a completely secure system for financial transactions that cannot be duplicated, counterfeited, or altered. By using blockchain-based security systems, financial institutions are able to ensure that all transactions are secure and protected from malicious actors [1].

Additionally, blockchain technology allows for a secure and transparent way to store and transfer assets, allowing financial institutions to be able to track and audit all transactions in real-time. Furthermore, blockchain-based security systems also offer enhanced privacy and anonymity [2].

By utilizing cryptographic algorithms, financial institutions are able to keep all customer data and transactions securely encrypted. This ensures that only authorized personnel can access and view the data, while keeping it hidden from unwanted third parties [3]. In conclusion, blockchain based security systems are becoming increasingly important for financial institutions.

Financial institutions can ensure secure and transparent transactions, enhanced privacy and anonymity, and trust-based systems that cannot be compromised. By utilizing the power of blockchain technology, financial institutions are able to create a more secure and efficient financial environment. The blockchain based security systems in financial institutions are becoming increasingly popular due to a number of benefits they offer [4].

Blockchain technology is a distributed, immutable, and secure ledger that allows parties to securely and transparently exchange data. This technology is being used to create new financial products, services, and protocols to keep data secure. Blockchain technology has the potential to revolutionize the way financial institutions operate and manage data. With the implementation of blockchain technology, financial institutions can reduce the risk of fraud and data breaches. This can be done by providing a secure and immutable ledger that stores the complete history of all transactions that take place on the system [5].

The ledger is shared across all participants in the network, which makes it virtually impossible for hackers to manipulate or alter the data. Furthermore, blockchain technology can be used to create new protocols that enable financial institutions to securely and transparently share data with other institutions. This will enable financial institutions to quickly and efficiently exchange data and services, while reducing the risk of data breaches [6]. In addition, blockchain technology can be used to create digital assets, such as cryptocurrency, that can be used to facilitate transactions and payments.

Cryptocurrency can provide a secure and transparent way for financial institutions to transfer funds and assets, while reducing the risk of fraud and data breaches. Overall, blockchain technology is providing new ways for financial institutions to securely and transparently exchange data and services. By utilizing this technology, financial institutions can reduce the risk of data breaches and fraud, while enabling them to quickly and efficiently exchange data and services.

2. RELATED WORKS

Blockchain has been a major factor in the development of the security systems of many financial institutions, but the issues related to it are still being discussed [7]. The first issue is the lack of regulation and oversight.

Blockchains are not regulated by any government or financial institution and there is no uniform set of rules governing their use.

This could potentially lead to issues such as fraud and money laundering. Additionally, the decentralized nature of blockchain makes it difficult to track and monitor transactions. This could lead to serious issues if the system is used for any illegal activities [8].

Another issue is the lack of scalability. Due to the way blockchains work, they are not able to process large amounts of data at once. This could limit the number of transactions that can be processed in a given period of time. This could lead to congestion and delays, which in turn could lead to lower customer satisfaction and a decrease in business. Finally, blockchain technology is still in its infancy [9].

There are still many issues to be ironed out before it can be used in a secure and reliable way. This could include issues such as privacy, scalability and data storage. If these issues are not addressed, financial institutions may be reluctant to adopt the technology. Despite these issues, blockchain technology has the potential to revolutionize the way we do business and secure our data.

Financial institutions should continue to research and explore the technology in order to ensure its secure use. With the right regulations and oversight, blockchain could become an invaluable tool for financial institutions and the global economy [10].

3. BLOCKCHAIN SETUP

In this section, the fundamental blockchain architecture principles that serve as the basis for our platform. These ideas will be broken down into several categories. Encoder Decoder Chain is unable to make advantage of the vast majority of the available blockchain technology due to the fact that some of the entities involved in a smart city scenario have limited resources. When it comes to the exchange of information, certain applications, such as automotive networks, call for a minimum amount of latency to be maintained. It could take anywhere from a few seconds to a few minutes to incorporate new information into a blockchain ledger. This time frame is highly variable.

This permissioned blockchain is extremely lightweight, and it creates new blocks whenever there is a requirement for them. As a result, each device will function on its own to produce data and add that data to the data block that it is responsible for. Because of this, no device will be required to wait for other nodes in the blockchain to append their data, which is a direct result of this development. In addition, gateways are only allowed to save the block header, which is the section of the block that contains all of the crucial information identifying endpoints.

In order to conduct authentication, gateways rely on digitally signing the data that is generated and storing it in transactions that are added to a block header. This is done in order to verify the integrity of the data. Overall, each block is composed of two significant constituents in its whole. In this particular instance, we modify the method so that it may be applied in a financial environment, and the following are the results:

- ***Block Header***: The only thing that is used to determine the header of the block that comes after it is the hash of the block that came before it. It is possible to say that this procedure resulted in the construction of the interconnections found in the blockchain. As a consequence of this, it ought to supply the data essential for determining and confirming that the transactions were alone produced by the device that is in possession of the public key. We make use of the expiration functionality in order to specify the time after which a block will no longer be available to receiving new transactions. This is done by determining when the block will no longer be open to receiving new transactions. As a result of this update, the size of a block will no longer continue to increase in the future for no discernible reason at all. There is always the possibility of additional transactions being added to a block at any point.
- ***Block Ledger***: The payload of each block that is a part of a distributed ledger is where the connected transactions that are utilized to generate the block header are stored. A distributed ledger is a type of digital ledger. The SpeedyChain blockchain protocol connects all transactions from a given node to the same block header, as opposed to storing legal transactions in separate blocks as is the case with other blockchains. This is how other blockchains handle legal transactions. In contrast to this, the way that typical blockchains keep transactions is as follows. Since the RSI just needs to keep track of the link between transactions in the block header, device-specific requests can be quickly fulfilled. Because of this, it is not necessary to keep a record of the actual transaction data, which removes the prerequisite for a certain amount of storage space. It is conceivable that the process of simultaneously updating each block with new data can take place.
- ***Sensor Data Support***: To make it simpler to include data from smart cities, the structure of the transactions in the selected blockchain was altered so that it would take information sent by the sensors installed in vehicles. This was done to accept the information. The reason for doing this was to make it possible to include data from smart cities. A user authorization field, a geotag field, and an access level description field are all included in the documentation as well. In addition, a user authorisation field was provided in the documentation.

4. PROPOSED MODEL

Financial organizations have been among the first to adopt blockchain technology. This is mostly due to the blockchain promise to improve data security as well as administrative processes. Financial institutions stand to gain in a variety of different ways from the implementation of security solutions that are built on blockchain technology. Two of these strategies are by better protecting consumer data and by operating at a higher level of efficiency. To begin, there is no competition when it comes to the level of safety provided by platforms built on blockchain technology. A blockchain-based system is extremely tough to hack for the straightforward reason that it is impenetrable. This is due to the fact that the system uses distributed ledger technology.

Because of their resistance to hacking and fraud, the security solutions that are based on blockchains are superior to their historical equivalents. As a result of this, they are ideally suited for use in banks and other types of financial organizations, where they can be put to use to protect the information of clients as well as the transactions that those consumers carry out. Second, the utilization of security solutions that are based on blockchain technology might make it easier to streamline corporate procedures. Verification of identities, authentication of transactions, and the storing of data are just some of the numerous applications that may be discovered for systems that are based on blockchain technology. There are many more. It is possible that financial institutions will be able to save money as a result of this, while also seeing an improvement in the level of service they provide to their clients. In addition to this, it can help financial institutions fulfill their regulatory duties and improve the level of client service that they provide.

Last but not least, financial organizations now have access to data in real time, thanks to the security measures afforded by the technology of blockchain. This information can be of assistance to financial institutions in improving their methods of decision-making, which will, in turn, keep their clients delighted. The customer faith that their personal information and business dealings will be kept confidential is critical to the performance of financial institutions, which rely heavily on the customer faith in order to be profitable. Financial organizations can benefit from using security systems that are based on blockchain technology because of the myriad of ways in which these systems improve both data security and operational efficiency. As a consequence of this, these establishments are able to take use of the benefits offered by security solutions based on blockchain.

If banks apply security measures based on blockchain technology, they will be able to protect the privacy of their customer personal information as well as the authenticity of their customer financial transactions. This will be possible since blockchain technology is decentralized. It is possible that financial institutions will be able to save money as a result of this, while also seeing an improvement in the level of service they provide to their clients. The implementation of blockchain technology within the framework of the financial sector has led to significant shifts in the industry as a whole. Financial institutions now have the capacity to store and move data more effectively than they ever have before as a direct result of the emergence of security solutions based on blockchain technology. This was not previously possible.

It is difficult to make any modifications to a transaction once it has been recorded in a blockchain because each transaction is cryptographically secured there. Once a transaction has been recorded in a blockchain, it cannot be changed. The nature of blockchain technology, which is both encrypted and decentralized, makes it feasible to carry out transactions in a way that is both more safe and more private than is now possible. The implementation of blockchain technology could be advantageous for financial institutions due to the fact that it increases data security and reduces processing times as a result of the nearly immediate verification and recording of transactions.

Customers have increased assurance that their financial transactions will be processed quickly and securely, while financial institutions are able to save money by lowering the number of staff they need to recruit to process payments and other types of transactions. Because fraudulent activity may be easily identified and recorded using blockchain-based security solutions, financial institutions are also better equipped to detect and prevent fraudulent activities. This is another benefit to employing blockchain technology. Because of this, financial institutions are now able to recognize fraudulent activity and take measures to stop them more effectively.

The consumers who do business with financial institutions stand to benefit from the implementation of blockchain technology, as do the institutions themselves. When it comes to processing payments and completing other types of transactions, financial institutions are able to provide their customers with the finest experience that is humanly feasible because of the mix of safety and speed that exists inside their systems. Excellent news for the dependability and security of the entire global financial system as a whole is the fact that an increasing number of financial institutions are beginning to utilize blockchain technology.

5. BLOCKCHAIN FORMATION WITH ENCODER-DECODER MECHANISM

In order to safeguard the system from malevolent miners who may attempt to flood the blockchain with blocks, each time a new block is added to the blockchain, the consensus algorithm, which is a difficult-to-solve but easy-to-verify puzzle, must be executed. This is done in order to ensure that the system remains secure. Because of the importance of maintaining the blockchain honesty, this step is essential. Traditional consensus methods, on the other hand, have large overheads that preclude IoT devices from being able to use them. This is because traditional consensus mechanisms have been around for a long time.

Gateway nodes, which are responsible for validating transactions and ensuring the continuing operation of the blockchain, provide one solution to this problem. Gateway nodes are responsible for ensuring that the blockchain continues to operate. In addition to playing the role of a gateway, device nodes are tasked with the duties of collecting data from the immediate area around them, turning that data into transactions, and then transmitting those transactions to gateways. A block is not produced by the RSI until after it has gotten validation from a witness, which is an entity that will attest to the fact that the block was produced by a real vehicle. This is seen in Fig.1, and it is possible to observe that validation being obtained. This substantiates the claim that the disputed vehicle can be discovered at the place where it was purportedly generated.

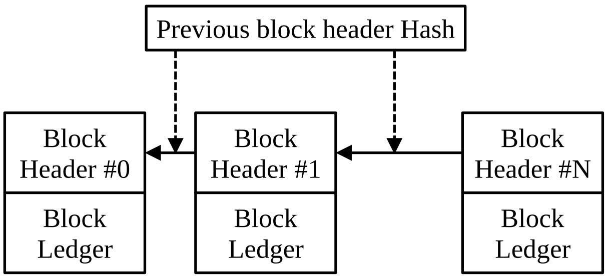

Fig.1. Transaction Block Formation

The modeling of machine translation as a task involving sequence-to-sequence mapping The sequence-to-sequence model begins by employing an encoder to map the input sequence into an intermediate vector. This step is necessary for the model to be able to generate an output sequence based on an input sequence. After that, the model made use of a decoder in order to construct the output by taking into account the history in addition to the intermediate vector. The model overarching objective was to find a way to convert one sequence into another. The encoder-decoder model that has been established can be represented by the equations that are listed below:

$$Encoder{:}h_t = E(h_{t\text{-}1},x_t) \tag{1}$$

$$Decoder{:}y_t = D(h_t,y_{t\text{-}1}) \tag{2}$$

where,

w_t - time step,

h - hidden vector and

y - output vector.

E - sequential cells of encoder and

D - sequential cells of decoder.

The first hidden state of the decoder is almost always set using the intermediate vector, as this is the case the majority of the time. This is because the encoder final concealed state is represented by the intermediate vector. Each hidden state is decided upon at the moment of encoding based not only on the currently active hidden state but also on the input for the currently active time step. Nevertheless, when it comes time to decode the message, each hidden state is decided not just by the currently concealed state but also by the output from the time step before the current one.

This paradigm has a number of advantages, one of which is its versatility with regard to the lengths of the data that it receives and the data that it produces. On the other hand, it is not essential that the lengths of the sequences that are input and those that are produced be identical to one another. On the basis of this model, a great many other sequence-to-sequence models that are far more intricate have been built; some of these models will be examined in further detail below.

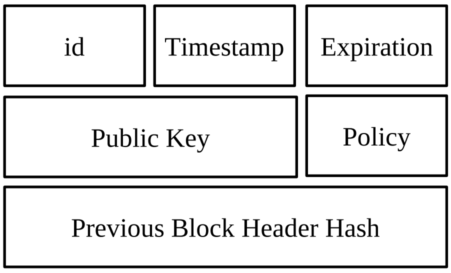

Fig.2. Block Header

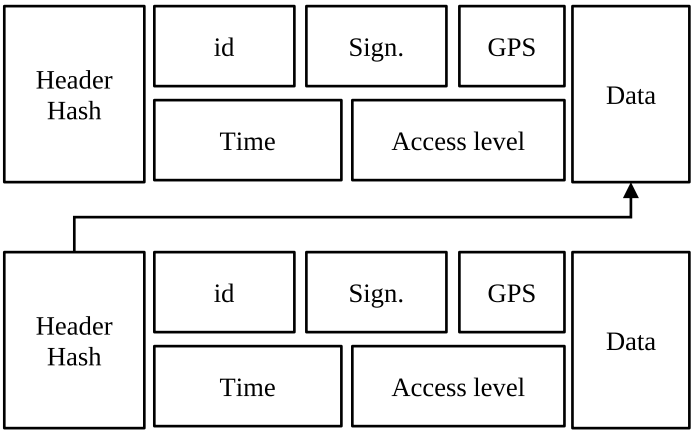

Fig.3. Block Ledger

The design of this system is comprised of a number of critical components, the most important of which are the calculation of weights, the selection of relevant memories, and the ultimate prediction.

5.1 WEIGHT CALCULATION

The model generates a mapping from the input memory set x_i to the representation model $\{m_i\}$ by beginning with a representation model A as its point of departure and proceeding from there. It makes use of a second representation model that is denoted by the B to convert the query into its very own embedding space.

An embedding vector that is denoted by the u is produced. The following is an explanation of the process that we go through in order to arrive at the final weights: The formula for calculating the weight of the memory input x_i is as follows:

$$p_i{=}Softmax(u^T m_i) \tag{3}$$

where

p_i - weight of input memory x_i for a query.

5.2 MEMORY SELECTION

Before we can make a prediction, we need to build a memory vector by first encoding the input memory x_i into an embedded vector ci using a separate representation model C. This will allow us to store the memory vector in the system. Next, we need to calculate the weighted sum over the $\{c_i\}$ by making use of the weights that were determined in the stage prior to this one. o is the vector that was chosen from memory and is denoted by o. The equation for o is expressed as:

$$o = \textstyle\sum_i p_i c_i \tag{4}$$

where o is the vector. This vector is not kept in any of the representations that are maintained in memory. The trainability of the entire model, which is predicated on gradient computing and may be activated through the use of soft memory selection,

5.3 FINAL PREDICTION

After turning the vector sum of the selected memory, o, and the encoded query, u, into a probability vector, a, one is able to make a definitive prediction using this method. The following is an illustration of how something like this may appear a':

$$\alpha' = Softmax(W(o{+}u)) \tag{5}$$

5.4 ENCODING-DECODING MECHANISM

During the process of decoding a token, sequence-to-sequence models make use of the formula that is presented in the following:

$$P(y_i|y_1,\ldots,y_{i\text{-}1},x) = g(y_{i\text{-}1},h_i) \tag{6}$$

where g - sequential model.

This that takes into account both the current hidden state and the output vector from the prior time step. This model also takes into account the current time step.

Instead, depending just on the output token that was immediately preceding it, each decoding state would take into account whatever components of the encoded source sentence are connected with one another. Applying the following formula makes it feasible to express the probability distribution of the result:

$$P(y_i|y_1,\ldots,y_{i-1},x) = g(y_{i-1},\ s_i,c_i) \tag{7}$$

where

i - i^{th} time step;

y_i - output token,

s_i - decoder state and

c_i - weighted score:

$$s_i = f(s_{i-1},y_{i-1},c_i)$$

$$c_i = \sum_{j=1}^{T}\alpha_{ij}h_j \tag{8}$$

where α_{ij} - normalized weight score:

$$\alpha_{ij} = \exp\left(e^{ij}\right)\sum_{k=1}^{T}\exp\left(e^{ik}\right) \tag{9}$$

where

e_{ij} - similarity score existing between j^{th} encoder and s_{i-1} under the hidden state h_j, and hence the score is predicted using the model a:

$$e_{ij} = a(s_{i-1},h_j) \tag{10}$$

6. RESULTS AND DISCUSSION

The emergence of blockchain technology has revolutionized the way financial institutions conduct their business, with a particular focus on improving security systems. Blockchain-based security systems provide financial institutions with a secure, tamper-proof and immutable method of storing and transferring data, making them an ideal choice for securely storing and transferring sensitive data.

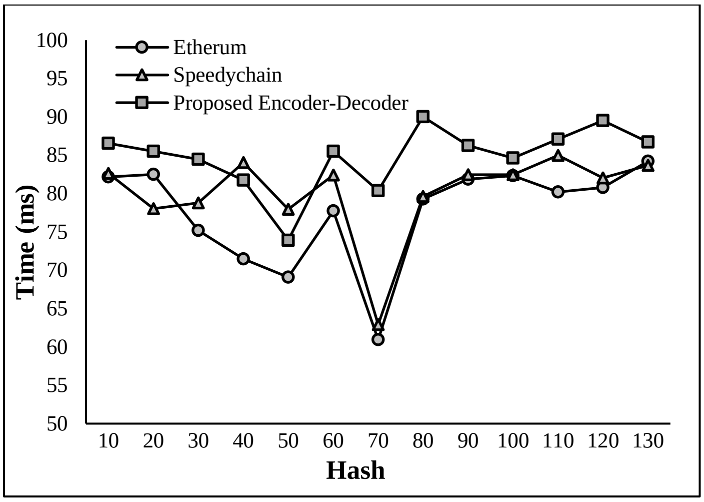

Fig.4. Computational Time

Blockchain technology is based on distributed ledgers, meaning that it stores and records all transactions in a decentralized way. This decentralization makes it virtually impossible for a single entity to manipulate or corrupt the data, as all data is stored across a vast network of computers.

Furthermore, the use of cryptography ensures that all transactions are secure and private, as each user is identified by a unique digital signature. Performance optimization of blockchain-based security systems in financial institutions can be achieved through the implementation of measures such as:

One of the main challenges of the current blockchain systems is the scalability issue. By increasing the scalability of the system, the performance of the system can be improved. This can be done by employing various technologies such as sharding and off-chain solutions.

The current security protocols implemented in blockchain-based security systems are far from perfect. Therefore, it is important to continuously analyze the existing protocols and identify any vulnerabilities that can be exploited. After identifying the weaknesses, new security protocols can be implemented in order to improve the security of the system as in Fig.4.

Intelligence can be utilized to improve the performance of blockchain-based security systems. AI can be used to detect patterns in the data and identify potential threats before they become a problem. This can help to reduce the chances of security breaches and ensure the safety of transactions has shown in the Fig.5.

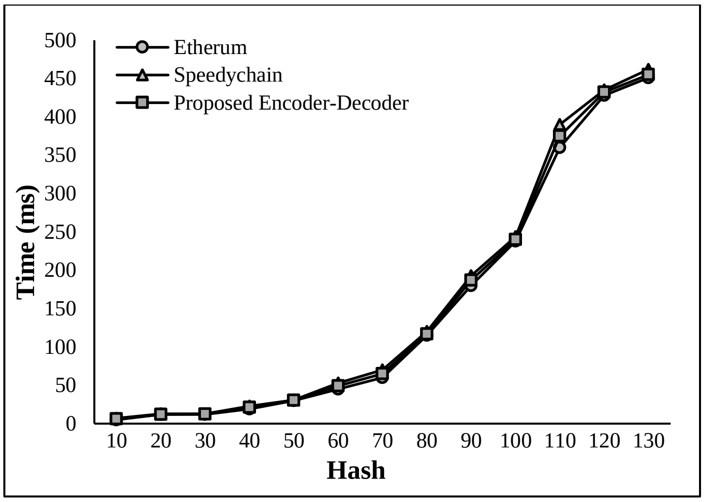

Fig.5. Delay

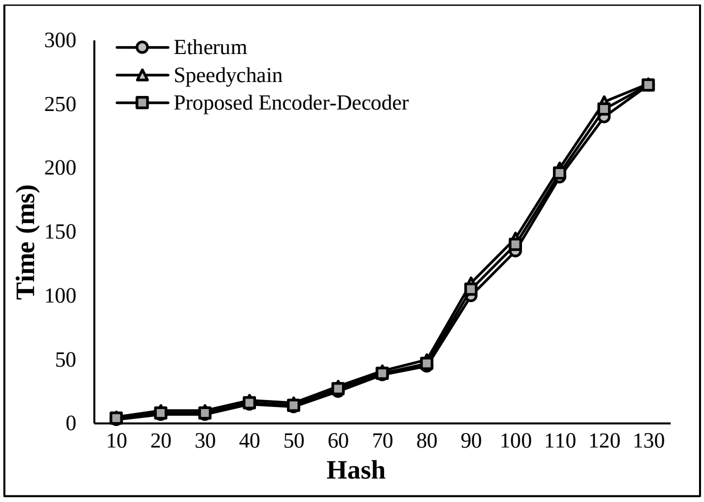

Fig.6. Communication Time

Enhancing the user experience of the system is an important part of performance optimization. This can be done by providing simple and easy to use user interfaces and intuitive features. This will make the system more user friendly and improve the overall performance of the system has shown in Fig.6.

These methods have the potential to enhance the safety and security of blockchain-based transaction systems used in financial institutions while also improving the efficiency of those systems. One further benefit of these regulations is that they help to ensure that financial institutions are run in a manner that is both effective and efficient. Examining how successfully a security system based on blockchain keeps data from being altered or accessed by third parties who are not authorized to do so is one technique to figure out whether or not such a system is effective.

Employing a system that is based on blockchain technology offers a variety of benefits, particularly when contrasted with the more conventional security approaches that are now in use. They have achieved a higher level of security by encrypting every piece of information and putting it in a distributed ledger system. Blockchain-based systems have the potential to achieve even higher levels of efficiency because it is no longer essential to engage a trustworthy third party to validate transactions. This opens the door to a host of new possibilities. In conclusion, blockchain-based solutions are more cost-effective than other options since they need less administrative work to be done in order to remain secure. This reduces the amount of work that has to be done to keep them safe.

It enables multiple financial organizations to communicate with one another in a way that is both safe and unchangeable, making it feasible for information to be shared between these entities. Because of this, they are a fantastic alternative for storing and sending sensitive data in a risk-free manner, making them an excellent option for financial organizations that are seeking to improve the security of their systems. In addition, this makes them an excellent option for improving the security of financial transactions. The financial industry has recently shown a growing interest in the blockchain-based security solutions that have been garnering popularity due to the fact that their platform for conducting transactions is both safe and transparent.

The dependability and safety of these systems are critical factors in determining the level of success that financial institutions experience in their operations. As a result, optimizing the performance of such systems is essential if one want to guarantee that they deliver the services as advertised and that all financial dealings are conducted in a risk-free setting.

The customer is the one who initiates each transaction; it is the customer's job to construct a request and send it off to the server at the financial institution. The information that was supplied by the customer is validated by the server of the financial institution that is processing the transaction in order to guarantee that it is accurate and trustworthy. After that, the bank server will update its own local copy of the blockchain, and once all validation has been completed, it will broadcast the adjustment to any other bank servers that are currently operational. When a new transaction is received, the servers of all financial institutions first verify the information they have received in order to determine whether or not it is accurate before adding the new transaction to their respective local blockchains. The findings of the testing suggest that the amount of time required to complete this process of updating will increase in direct proportion to the total number of transactions contained in any one block.

When a new user is introduced to the network, a new block is automatically generated. The consumer, on the other hand, won't be able to begin conducting transactions until the client's block has been included into the blockchain. The second facet that we investigated was the length of time that it takes for bank servers to process incoming transactions (that is, to authenticate data signatures, ensure that the block has not yet reached its end of life, append the transaction, and broadcast the change to all of the other bank servers). On a blockchain with a size of 50, it was proved that increasing the number of transactions from 10 to 100 will result in a 3% increase in the amount of time necessary for processing. Creating a transaction in a blockchain that has 100 blocks results in a 4.62% increase in the amount of time it takes. If the size of the blockchain is set to 650 blocks, the amount of time required to validate and add new transactions would increase at an exponential rate as the number of transactions raises from 10 to 1,000.

According to the evaluated blockchain sizes in terms of the quantity of transactions and the number of blocks, the values for validating and producing a new block are 20ms, and the values for producing and validating a new transaction are 1.7ms. These values were derived from the evaluation of the blockchain sizes. This holds true even while taking into account the hypothetical scenario of a blockchain that contains 650 blocks and sends 1,000 transactions. When compared to the process of adding a new transaction to the Bitcoin blockchain, the addition of a new transaction automatically results in a significant time savings.

7. CONCLUSION

In this paper, the novel blockchains can also be used to create a secure platform for digital asset management. This will ensure that the assets are secure and immutable. It also ensures that the assets are transparent and secure. The blockchain technology can also be used to create secure and transparent systems for financial institutions. This will ensure that the transactions are secure and immutable. It also ensures that the transactions are transparent and secure.

In conclusion, the blockchain technology can be used to create secure and reliable systems for financial institutions. It ensures that the transactions are secure and immutable. It also ensures that the transactions are transparent and secure. This technology can be used to create a secure platform for digital identity management, digital payments, and digital asset management. This will ensure that the financial institutions are secure and reliable.

REFERENCES

[1] A.S. Hosen, S. Singh, P.K. Sharma and G.H. Cho, “Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network”, *IEEE Access*, Vol. 8, pp. 117266-117277, 2020.

[2] S.M.H. Bamakan, A. Motavali and A.B. Bondarti, “A Survey of Blockchain Consensus Algorithms Performance Evaluation Criteria”, *Expert Systems with Applications*, Vol. 154, pp. 1-19, 2020.

[3] S. Trivedi and R. Sharma, “Systematic Literature Review on Application of Blockchain Technology in E-Finance and

Financial Services”, *Journal of Technology Management and Innovation*, Vol. 16, No. 3, pp. 89-102, 2021.

[4] S.B. Patel and N. Kumar, “Kirti: A Blockchain-Based Credit Recommender System for Financial Institutions”, *IEEE Transactions on Network Science and Engineering*, Vol. 8, No. 2, pp. 1044-1054, 2020.

[5] N. Kabra and S. Tyagi, “MudraChain: Blockchain-based Framework for Automated Cheque Clearance in Financial Institutions”, *Future Generation Computer Systems*, Vol. 102, pp. 574-587, 2020.

[6] K. Fanning and D.P. Centers, “Blockchain and its Coming Impact on Financial Services”, *Journal of Corporate Accounting and Finance*, Vol. 27, No. 5, pp. 53-57, 2016.

[7] M. Peterson, “Blockchain and the Future of Financial Services”, *The Journal of Wealth Management*, Vol. 21, No. 1, pp. 124-131, 2018.

[8] Y. Guo and C. Liang, “Blockchain Application and Outlook in the Banking Industry”, *Financial Innovation*, Vol. 2, pp. 1-12, 2016.

[9] H. Rathore, A. Mohamed and M. Guizani, “A Survey of Blockchain Enabled Cyber-Physical Systems”, *Sensors*, Vol. 20, No. 1, pp. 282-291, 2020.

[10] N. Jiwani and K. Gupta, “Exploring Business Intelligence Capabilities for Supply Chain: A Systematic Review”, *Transactions on Latest Trends in IoT*, Vol. 1, No. 1, pp. 1-10, 2018.

[11] B. Gobinathan, M.A. Mukunthan, S. Surendran, and V.P. Sundramurthy, “A Novel Method to Solve Real Time Security Issues in Software Industry using Advanced Cryptographic Techniques”, *Scientific Programming*, Vol. 2021, pp. 1-7, 2021.

[12] N. Jiwani and K. Gupta, “Comparison of Various Tools and Techniques used for Project Risk Management”, *International Journal of Machine Learning for Sustainable Development*, Vol. 1, No. 1, pp. 51-58, 2019.

[13] R. Chaudhary, A. Jindal, G.S. Aujla and K.K.R. Choo, “Best: Blockchain-Based Secure Energy Trading in SDNEnabled Intelligent Transportation System”, *Computers and Security*, Vol. 85, pp. 288-299, 2019.