Pakistan Journal of Scientific Research (Vol. 3 No. 2 December, 2023)

IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN THE BANKING SECTOR

H. Zaheer[1], F. Asrar[2], and M. M. A. Khan[5]

[1]Department of Computer Science, University of Engineering and TechnologyLahore, Pakistan
[2]Independant Researcher, Telecommunication Engineer.
[3]Assistant Professor, Department of Computer Science, University of Agriculture, Faisalabad
Corresponding author: Hira Zaheer (e-mail: hirazaheer97@hotmail.com)

ABSTRACT- Traditional Banking networks have been implemented worldwide. However, there are numerous security threats to these banking networks. Due to these threats, many banks have not been able to establish a sense of security among their customers. Every bank has different threats based on multiple factors such as network configuration, region, customer base, etc. Improving the security of banking networks worldwide is the need of the hour. For this purpose, the best solution to overcome all the existing security challenges of the banking networks worldwide is to upgrade them to blockchain networks. As of today, Blockchain is the best alternative to conventional banking networks. Despite its security challenges, it can be considered the best solution to overcome this global issue. This paper, first of all, highlights the significant issues in transactions in the banking sector. These issues include security and attack risks, and the involvement of multiple stakeholders. Then further, this paper proposes a new algorithm based on blockchain technology to overcome these issues. Additionally, the simulation results showing the transaction between 2 nodes are mentioned.

Keywords— Banking, Blockchain, Security, Smart Contracts, Transaction.

Received: 03/01/2024, Revised: 29/02/2024

INTRODUCTION

In this digital world, banks play vital roles in the world economy. One or more of these nodes of Banking networks, such as ATMs, Digital Banking apps, Digital Wallets, and POS systems, are directly or indirectly involved in every financial transaction. According to a survey, digital transactions worth billions of dollars are made annually. Traditional banking networks are based on client-server architectures and have fundamental and conventional security. Despite technological advancements in network and information security, orthodox banking networks are prone to attacks in many ways, such as fraudulent transactions, leaked sensitive data, and phishingscams [1].

Furthermore, delays are created in inter-bank funds transfers due to routing and the involvement of multiple banks or third parties in the transactions. These delays give further time to the attackers to do their illicit activities, suchas MITM and spoofing [2]. Overcoming the challenges is the most needed in the networks and information security setup of a bankingnetwork.

The best possible solution for these issues is interconnecting nodes of the banking sector, i.e., ATMs, Digital Banking apps, Digital Wallets, or POS systems using a decentralized peer-to-peer network, i.e., blockchain. In the blockchain, the link computers called nodes interconnect with each other to complete the network [3]. A Blockchain network has a shared unchangeable ledger duplicated and distributed across all the nodes in the network [4]. The way blockchain records and processes data, it is impossible to change, hack, or cheat the system. The generic structure of blockchain can be defined using the diagram shown in Figure 2 below.

In this paper, a new architecture and algorithm based on blockchain technology have been proposed. In the proposed system, the user arrives at any banking nodes mentioned earlier called Node-A. The user initiates a transaction using his private keys or the combination of private keys such as transaction pins, card credentials, etc., and the public credentials of the receiver. These transactions include funds transfers, vonline payments, or smart contracts [5]. After doing so, the Node-A transfers the data to the block chain net work of the bank. After passing through all the necessary steps of the block chain, the transaction reaches the receiving node. This is where the transaction is completed. The proposed system ensures all the characteristics of a blockchain network, thus making all the transactions highlysecure [6].

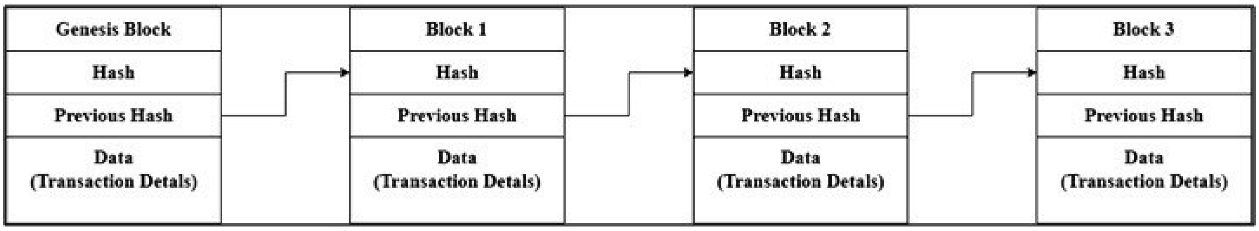


Figure 1. Generic Structure of Blockchain

Figure 2. Generic Structure of Blockchain

Section II of this paper covers the literature review, where the latest research workd one by the other researchers relevant to the domain of the papers is discussed precisely. Afterward, a side-by-side comparison of orthodox and decentralized block chain networks is mentioned in section III. in section IV, adetailed methodology of the proposed algorithm, mentioning every step in completing the transaction, is thoroughly explained. Following the methodology, section V contains a tests imulation based on the proposed algorithm. In section VI, the benefits of the proposed block chain-based algorithm are enlisted with brief details and a comparison with the orthodox banking network. The paper is concluded in section VII by providing a conclusive summary of all the work done in the paper. Finally, future work is mentioned in sectionVIII.

LITERATURE REVIEW

The term Block chain was first coined by Satoshi Nakamo to in a ground breaking paper entitled Bitcoin: A Peer-to-Peer Electronic Cash System [7]. The paper gave the concept to faunique P2 Pnetwork that eradicates trust issues in traditional networks. He further gave the basic concept of bitcoins that completely revamped the concept of digital currencies.

After this, rapid development started in blockchain technology. Many researchers worked on implementing, applying, and improving blockchain networks [8]. The latest research works are taken into account for this paper.

Amanda Castro, in her paper "Information Security in Banking and the Blockchain Connection" [1], has demonstrated the working of a blockchain network and its usefulness in organizations. The paper revolves around the network security of the banking sectors and highlights the challenges in the current network systems. Later, it provides the fundamentals that make blockchain a better choice for resolving internet security issues of the banking network.

Similarly, the paper "Measuring the perceived benefits of implementing blockchain technology in the banking sector," authored by Poonam Garg [9], analyses multiple aspects of blockchain technology through research and literature review and provides the results showing the benefits of using blockchain technology for secure and reliable business operations.

In their paper "Blockchain-based e-cheque clearing framework with trust-based consensus mechanism," Nikita Singh, Tarun Kumar, and Manu Vardhan proposed a blockchain-based e-cheque clearance system [10]. The proposed framework uses blockchain technology based on a consensus mechanism for processing online and physical cheques of the banks.

Comparing Existing System With Decentralized System: Decentralized systems are better than conventional systems in many ways. A comparison between Existing systems and Decentralized Systems is in Table ***1*** given below [10] [11]:

Table 1. Comparison between Existing systems and Decentralized Systems.

Feature	Existing System	Decentralized System
Ownership	Service Provider	All users
Architecture	Client/Server	Distributed[4]
Security	Basic	More Secure[3][12][13]
High Availability	No	Yes
Fault Tolerance	Single Point Failure	High Tolerant[14]
Collusion resistance	Basic because it's under the control of a groupor even a singleindividual	Highly resistant, as consensus algorithms ensure defense against adversaries
Application Architecture	Single Application	Application replicated across all nodes on the network.
Trust	Consumers have to trust the service provider	No Mutual Trust is Required.

Cost for consumer	Higher	Lower[15]

The attributes mentioned above are not the only reasons to adopt decentralized systems. There are many further advantages toit [16].

METHODOLOGY

The traditional banking transaction system uses a centralized system [17] [18] for the transaction and is full of security risks. On the contrary, an advanced and more secure blockchain system is recommended in this paper [19] [20]. After all verifications and authentications, the system establish esaprivate block chain network between the sending node and the beneficiary node [21][16]. The recommended transaction consists of multiple steps, i.e., (1) Initialization, (2) Broadcasting and Validation, (3) Mining and Block Formation, and (4) Appending a New Block (Completion of Transaction) [14].

Initialization: The sender first accesses a bank node and requests a transaction. This node can be an ATM, Digital Banking app, Digital Wallet, POS system, or any other digital means of the transaction directly or indirectly involved in every financial transaction. That node is hereafter referred to as Node-A. Once the user accesses Node-A, he provides his private key and requests a transaction. This private key can be the transaction password, ATM PIN, or other combination. The aforementioned transaction can be money transfers or smart contracts and consists of some values, rules, source and destination addresses,etc.

Broadcasting and Validation: As Node-A is triggered for a transaction, the request for a transaction is broadcasted to the P2P networks consisting of mining nodes or miners.These mining nodes are the trusted computers of the banking network connected to the P2P network. Once the P2 P network acknowledges the request, the next and most important step is verifying the user and the transaction. For this purpose, the nodes of the P2P network verify the user. This is done by the mining nodes of the P2P using pre-defined steps and asset of rules and criteria. Up on verification of the user, the P2P network validates the transaction initializedbytheuser.Thetransactionvalidationincludesthe validation of smart contracts, transaction records, and other necessarydata.

Initialization: After the verification, the transaction is executed. The process of inclusion of transactions into a block starts. The miners fulfill the consensus mechanism constituted in the given blockchain to form the block. The miners might get rewarded for the work they door the energy they use in this process. However, there is no hard and fast rule for reward systems, and this solely depends upon blockchain. For this purpose, there are multiple consensus mechanisms such as:

- Proof-of-Work
- Proof-of-Stake
- Delegated Proof-of-Stake
- Leased Proof-Of-Stake
- Proof of Elapsed Time
- Practical Byzantine Fault Tolerance
- Simplified Byzantine Fault Tolerance
- Delegated Byzantine Fault Tolerance
- Directed Acyclic Graphs
- Proof-of-Activity
- Proof-of-Importance
- Proof-of-Capacity
- Proof-of-Burn
- Proof-of-Weigh

- **Appending New Block:** The newly created block is validated, and the transaction embedded in the new block is executed. The new block is sharedwithotherpeersoftheP2Pnetworkoftheblockchain. Once shared, the block is added to the existing block chain (Ledger). The next block links it self cryptographically back to this block. This link is called a hash pointer.
- **Completion of Transaction:** Once a new block is appended, it means that the transaction is valid in every aspect. Therefore, the system will process the transaction, and the user request is completed at this last and final stage
- Figure 3 above, shows the complete flowchart of the proposed methodology
- **Implementation of The Methodology:** We used Remix IDE online to show basic transactions and created ademo account. After performing some steps, we got some Ethereum to perform successful transactions, as shown in Figure 4t

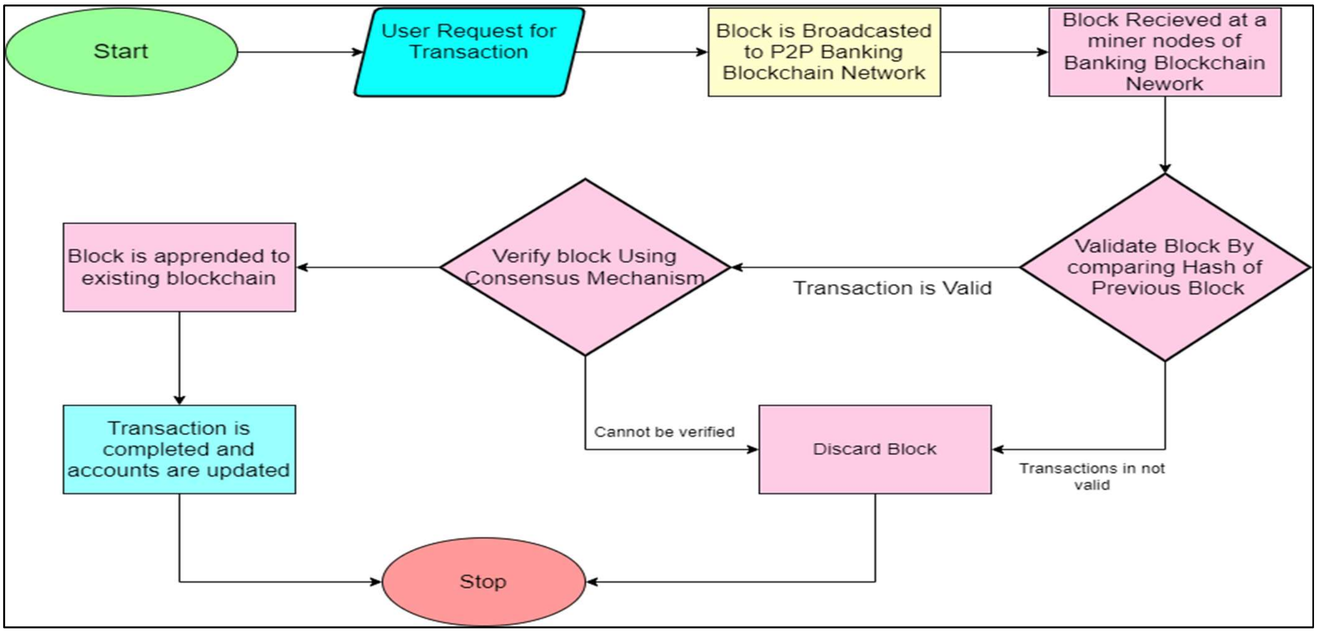
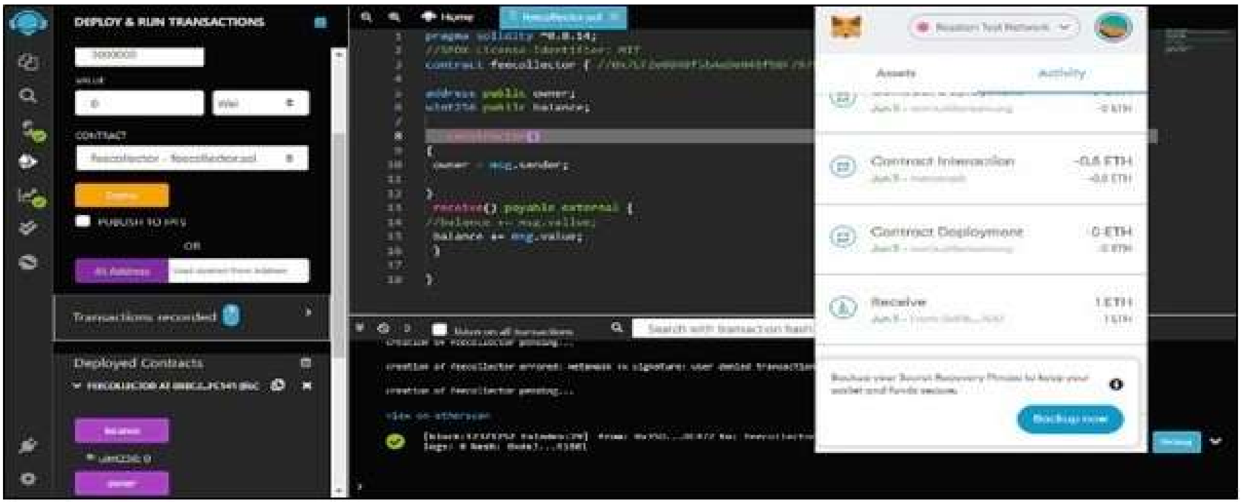

Start
User Request for Transaction
Block is Broadcasted to P2P Banking Blockchain Network
Block Recieved at a miner nodes of Banking Blockchain Nework
Validate Block By comparing Hash of Previous Block
Transaction is Valid
Verify block Using Consensus Mechanism
Block is apprended to existing blockchain
Transaction is completed and accounts are updated
Cannot be verified
Discard Block
Transactions in not valid
Stop

Figure 3. Flowchart of the proposed methodology

The criteria for choosing the best consensus mechanism purely depend upon the configuration of the network. However, the most commonly used consensus mechanisms are:

- Proof-of-Work
- Proof-of-Stake

Once the miners fulfill all the criteria set in block formation, the block is formed. Upon the formation of the block, the transaction is considered to be confirmed



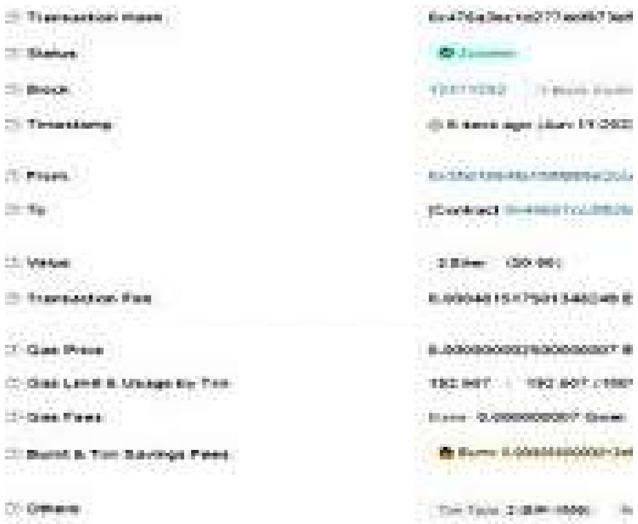
```
pragma solidity ^0.8.14;
//SPDX-License-Identifier: MIT
contract feecollector { [illegible]

address public owner;
uint256 public balance;

constructor()
{
 owner = msg.sender;

}
 receive() payable external {
//balance += msg.value;
 balance += msg.value;
 }

}
```

```
creation of feecollector pending...

creation of feecollector errored: MetaMask Tx Signature: User denied transaction [illegible]

creation of feecollector pending...

view on etherscan

[block:[illegible] txIndex:[illegible]] from: [illegible] to: feecollector[illegible]
logs: 0 hash: [illegible]
```

Figure 4. Example of Testing Transaction using IDE remix

Figure **5**below showsthe transaction details, e.g., sender account and receiver account ID, with the hash generated for a specific transaction.

The hash that has been generated in Fig. 6 for the transaction is not able to be decrypted. This is one of the benefits that it cannot be modified and is least prone to an MITM attack.



Transaction Hash: [illegible]

Status: Success

Block: [illegible]

Timestamp: [illegible]

From: [illegible]

To: [Contract [illegible]

Value: 0 Ether ($0.00)

Transaction Fee: 0.000481517501348249 E

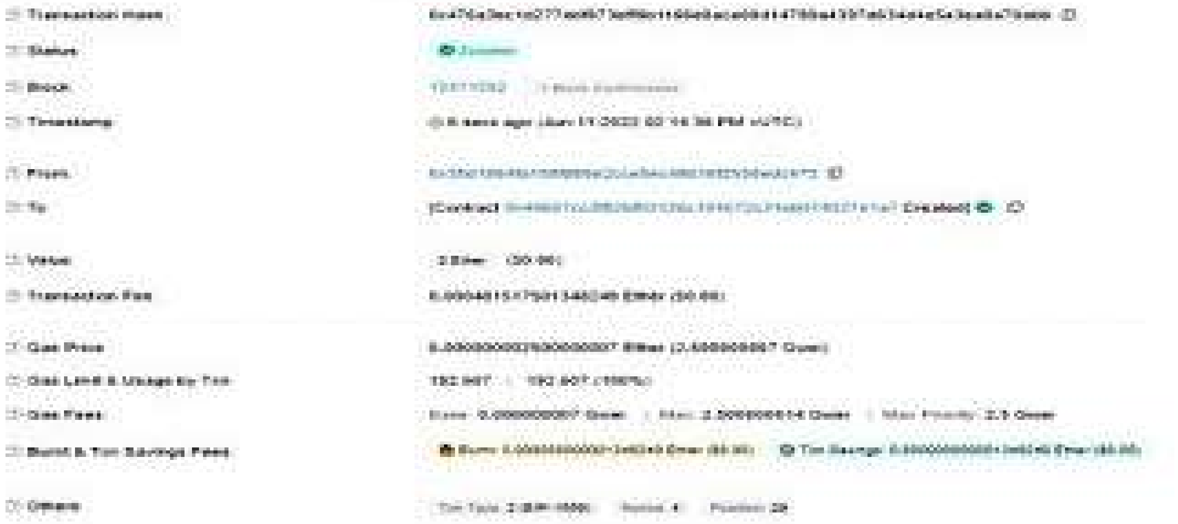
Gas Price: 0.000000002500000007 E

Gas Limit & Usage by Txn: 192,607 | 192,607 (100

Gas Fees: Base: 0.000000007 Gwei

Burnt & Txn Savings Fees: Burnt: [illegible]

Others: Txn Type: 2 (EIP-1559)



Transaction Hash: [illegible]

Status: Success

Block: [illegible] Block Confirmations

Timestamp: [illegible] (Jun-17-2023 [illegible] PM +UTC)

From: [illegible]

To: [Contract [illegible] Created]

Value: 0 Ether ($0.00)

Transaction Fee: 0.000481517501348249 Ether ($0.00)

Gas Price: 0.000000002500000007 Ether (2.500000007 Gwei)

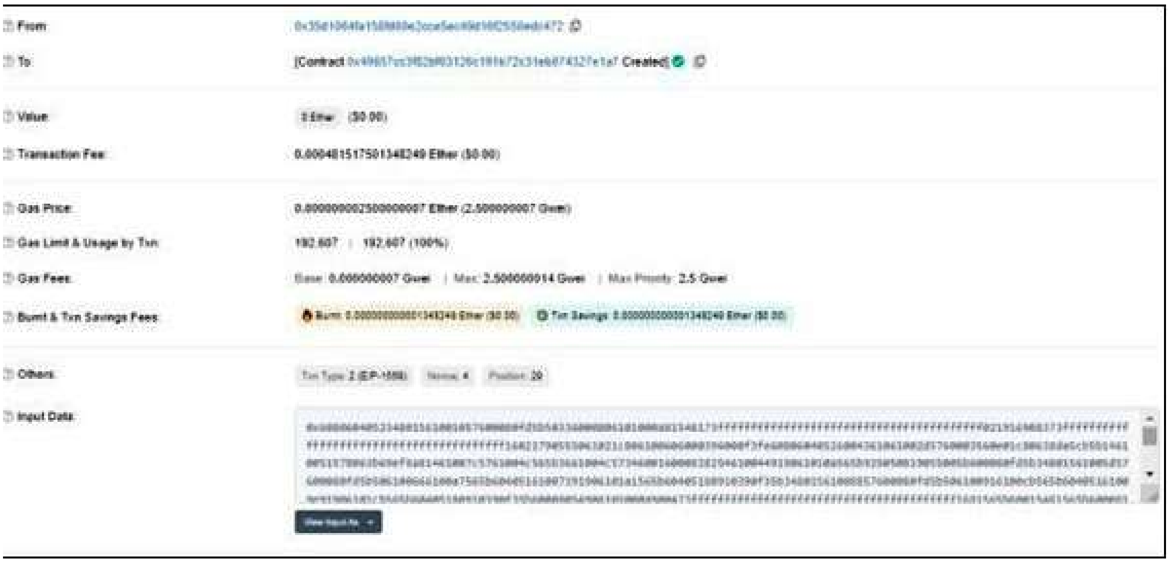
Gas Limit & Usage by Txn: 192,607 | 192,607 (100%)

Gas Fees: Base: 0.000000007 Gwei | Max: 2.500000014 Gwei | Max Priority: 2.5 Gwei

Burnt & Txn Savings Fees: Burnt: [illegible] Ether ($0.00) Txn Savings: [illegible] Ether ($0.00)

Others: Txn Type: 2 (EIP-1559) Nonce: 4 Position: 29

Figure 5. Transaction Details



From: [illegible]

To: [Contract [illegible] Created]

Value: 0 Ether ($0.00)

Transaction Fee: 0.000481517501348249 Ether ($0.00)

Gas Price: 0.000000002500000007 Ether (2.500000007 Gwei)

Gas Limit & Usage by Txn: 192,607 | 192,607 (100%)

Gas Fees: Base: 0.000000007 Gwei | Max: 2.500000014 Gwei | Max Priority: 2.5 Gwei

Burnt & Txn Savings Fees: Burnt: [illegible] Ether ($0.00) Txn Savings: [illegible] Ether ($0.00)

Others: Txn Type: 2 (EIP-1559) Nonce: 4 Position: 29

Input Data: [illegible]

Figure 6. Hash Generation

Benefits Of Using Blockchain In Financial Institutions: *Decentralization* Validation of transactions is mandatory; conventionally, a third party is used for validation purposes. Block chain makes the system independent of third-party validation. Instead, they use a consensus mechanism to validate transactions. Under this mechanism, all the nodes involved validate the transaction. Bydoingso, single-point failure is avoided [22].

Transparency andtrust: Trust is built on transparency of the system, and block chain provides complete transparency in all transactions. All block chain users can see what is on the block chain and the flow of transactions. This feature makes blockchain more trustable [22] [23] [24].

Immutability: Once the data has been written on the block chain, it becomes permanent; thus, it is impossible to amendorre move the data. This feature makes blockchain more reliable to use for transactions. As it maintains an immutable transactions ledger, all the transaction history can be checked and found [18].

High availability: The orthodox banking network becomes unavailable if the system gets an unusual load or some network components becomeunavailable.However,blockchainisacombinationof multiple nodes, and data always remain updated and synchronized.Ifanynodeisnotaccessibleforanyreason,the remaining system keeps working with updated data and availableresources.Thismakesthesystemhighlyavailableto all users all thetime [25].

Highly secure: Transactionsontheblockchainarehighlysecuredasthey are cryptographically secured and encrypted using a combination of private and public keys to maintain integrity [2]. Furthermore, All the transactions are first verifiedbasedonsomesetofrules,andafterverification,itis included in ablock [3] [12] [13].

Smart property: Blockchain can make properties secure in such a way that nobody can fake claim it or a person who owns the property cannot deny it. Every asset is inthe digital domain with full transparent ownership [26].

Digital Currency: With the help of Blockchain the concept of digital currency can be easily normalized which will not only reduce the printing cost of monetary notes but also will help banks to settle financial matters more efficiently and quickly [27]. Further digital currency can help in reducing black money

Limitation: Blockchain has many benefits, but it has some drawbacks too. Many researchers have explained the drawbacks and their solutions too. Some of the limitations of the blockchain are as follows:

Implementation Cost: Currently, the conventional banking network is implemented worldwide. A peer-to-peer network will be something very new for the current banking system. Hence a completely new P2P network shall be required to be implemented. Furthermore, there are very few developers that can implement blockchain keeping its integrity intact. These developers charge a huge amount because of the demand and supply gap [28]. Therefore, this upgrade will cost a huge amount to the banks.

Processing Speed: Depending upon the network size and consensus mechanism, the processing time of blockchain networks is very high. At times customers may require to wait for transaction completion more than the usual time.

Energy Consumption: The biggest drawback of the Blockchain is its energy consumption. Many researchers have worked on the energy efficiency of the blockchain. However, to date, no proposed methodology has been implemented at a commercial scale for this purpose. This high energy consumption makes the blockchain expensive in terms of operational costs. Additionally, it requires miners with very high processing powers.

Memory Consumption: Contrary to the conventional network where outdated data is deleted after a certain period, in blockchain, no previous data is deleted due to this the memory requirement of blockchain becomes higher and higher day by day. Due to this memory requirement, new storage systems are required to be added with every node at regular intervals

Legal Challenges: Due to the high security of the Blockchain, there is no third-party interference in any transaction on the blockchain. Therefore, at times, it becomes difficult for law enforcement agencies to intercept any illegal financial activity. Therefore, money laundering and Financing terrorism might become common. Thus, proper legal processing will be required to overcome such challenges

Conclusion: Traditional banking networks are vulnerable tomalicious attacks through which users' sensitive data can be compromised. As the current banking networks are based on client-server architecture, running on a single applicationhas thetendencyforsingle-pointfailure.Furthermore,inter-bank fund transfers become costly due to multiple stakeholders' involvement. To overcome these issues, blockchain-based network architecture and algorithms for a secure, decentralizedsystemwithalowoperationalcostareproposed for the financial transactions in this paper. The proposal has been supported by simulations that have been proven to be flawless. The newly proposed algorithm has numerous benefits, including decentralization, trust, transparency, availability,security,andoperationalcosts.Theproposedidea isnewandhasmuchroomforimprovement.Inthefuture,we will be working on implementing blockchain on ATMs. In addition to this, work will be done on how systems can be improvedfurther.

REFERENCES

1. Castro, "Information Security in Banking and the Blockchain Connection," 2022.
2. N. Sundareswaran, S. Sasirekha, T. Shanmugapriya, I. J. L. Paul and S. Sharma, "Secure banking transaction using Blockchain," in *AIP Conference Proceedings*, 2021. https://doi.org/10.1063/5.0045780
3. D. Boughaci and A. A. K. Alkhawaldeh, "Enhancing the security of financial transactions in Blockchain by using machine learning techniques: towards a sophisticated security tool for banking and finance," in *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, 2020.
4. V. Rajnak and T. Puschmann, "The impact of blockchain on business models in banking," *Information Systems and e-Business Management,* vol. 19, p. 809–861, April 2020.
5. R. Gupta, V. K. Shukla, S. S. Rao, S. Anwar, P. Sharma and R. Bathla, "Enhancing Privacy through “Smart Contract” using Blockchain-based Dynamic Access Control," in *2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, 2020. https://ieeexplore.ieee.org/document/9051521
6. M. Sumathi and S. Sangeetha, "Blockchain Based Sensitive Attribute Storage and Access Monitoring in Banking System," *International Journal of Cloud Applications and Computing,* vol. 10, p. 77–92, April 2020.
7. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review,* 2008.
8. O. Ali, M. Ally, Clutterbuck and Y. Dwivedi, "The state of play of blockchain technology in the financial services sector: A systematic literature review," *International Journal of Information Management,* vol. 54, p. 102199, October 2020.
9. P. Garg, B. Gupta, A. K. Chauhan, U. Sivarajah, S. Gupta and S. Modgil, "Measuring the perceived benefits of implementing blockchain technology in the banking sector," *Technological Forecasting and Social Change,* vol. 163, p. 120407, February 2021.
10. N. Singh, T. Kumar and M. Vardhan, "Blockchain-based e-cheque clearing framework with trust based consensus mechanism," *Cluster Computing,* vol. 24, p. 851–865, July 2020.
11. B. Wu and T. Duan, "The Advantages of Blockchain Technology in Commercial Bank Operation and Management," in *Proceedings of the 2019 4th International Conference on Machine Learning Technologies*, 2019.
12. S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *Journal of Management Analytics,* vol. 7, p. 189–208, February 2020.
13. Sultan, M. A. Mushtaq, and M. Abubakar, "IOT Security Issues Via Blockchain: A Review Paper," in *Proceedings of the 2019 International Conference on Blockchain Technology*, 2019.
14. Bashir, Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks, Packt Publishing Limited, 2017.
15. M. Osmani, R. El-Haddadeh, N. Hindi, M. Janssen, and V. Weerakkody, "Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis," *Journal of Enterprise Information Management,* vol. 34, p. 884–899, June 2020.
16. R. Arjun and K. R. Suprabha, "Innovation and Challenges of Blockchain in Banking: A Scientometric View," *International Journal of Interactive Multimedia and Artificial Intelligence,* vol. 6, p. 7, 2020.
17. S. Albeshr and H. Nobanee, "Blockchain applications in banking industry: A mini-review," *Available at SSRN 3539152,* 2020.
18. O. Hamza, "Smart Sukuk Structure from Sharia Perspective and Financing Benefits: Proposed Application of Smart Sukuk through Blockchain Technology in Islamic Banks within Turkey," *European Journal of Islamic Finance,* p. 2020: Second Special Issue for EJIF Workshop, 2020.
19. R. Wang, Z. Lin, and H. Luo, "Blockchain, bank credit, and SME financing," *Quality &amp; Quantity,* vol. 53, p. 1127–1140, August 2018.
20. S. Fernandez-Vazquez, R. Rosillo, D. De La Fuente and P. Priore, "Blockchain in FinTech: A Mapping Study," *Sustainability,* vol. 11, p. 6366, November 2019.
21. D. A. M. Younus and M. Abumandil, "Role of smart contract technology blockchain services in finance and banking systems: concept and core values," *Available at SSRN 4078566,* 2022.

22. M. U. Chowdhury, K. Suchana, S. M. E. Alam and M. M. Khan, "Blockchain Application in Banking System," *Journal of Software Engineering and Applications,* vol. 14, p. 298–311, 2021.

23. L. Madaan, A. Kumar and B. Bhushan, "Working principle, Application areas and Challenges for Blockchain Technology," in *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*, 2020.

24. Q. He, "Application of Blockchain Technology in Commercial Banks," *E3S Web of Conferences,* vol. 235, p. 03070, 2021.

25. W. Fan, S.-Y. Chang, S. Emery and X. Zhou, "Blockchain-based Distributed Banking for Permissioned and Accountable Financial Transaction Processing," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, 2020.

26. R. Xu, Z. Zhai, Y. Chen and J. K. Lum, "BIT: A Blockchain Integrated Time Banking System for Community Exchange Economy," in *2020 IEEE International Smart Cities Conference (ISC2)*, 2020.

27. S. Schuetz and V. Venkatesh, "Blockchain, adoption, and financial inclusion in India: Research opportunities," *International Journal of Information Management,* vol. 52, p. 101936, June 2020.

28. P. Martino, "Blockchain technology: challenges and opportunities for banks," *International Journal of Financial Innovation in Banking,* vol. 2, p. 314, 2019.