iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IX **Month of publication:** September 2024

DOI: https://doi.org/10.22214/ijraset.2024.64370

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IX Sep 2024- Available at www.ijraset.com

Proposing a Model to Enhance Security in Online Blockchain-Based Banking Transactions

Jaini Patel[1], Kiran R Dodiya[2]
[1]*MSc. (Digital Forensics and Information Security) NSIT-IFSCS (Affiliated to National Forensics Sciences University, Gandhinagar, Gujarat, INDIA)*
[2]*Assistant Professor (Cyber Security & Digital Forensics) NSIT-IFSCS (Affiliated to National Forensics Sciences University, Gandhinagar, Gujarat, INDIA)*

Abstract: ***In the banking industry, technologies are changing rapidly. The banking industry is the first target to implement the new technology to provide better customer services. In the past, banking systems used the manual ledger system, which has many drawbacks.***
To overcome this, the banking industry implemented the computerised mechanism to implement the centralised system, in which data is stored in one place, like a data warehouse. However, this centralised, automated system has also led to increased threats and cybercrimes.
There are various malicious software (ransomware, phishing) through which hackers can hack customers' private data and use it illegally.
The urgency to address these challenges has led to the adoption of blockchain, a leading technology based on decentralised, distributed behaviour and its public ledger system. Implementing blockchain in the banking sector is not just a choice, but a necessity.
It can increase security, immutability, faster transactions, a decentralised system, consensus manner, transparency, etc. We will be discussing blockchain and its functionality.
Furthermore, we will present a theoretical framework that uses consortium blockchain to reduce security threats in online transactions. Our model, IVSMOT, is a crucial step in this direction, as it divides the private key into two shares, thereby addressing the urgent need to enhance security in online banking transactions.
Keywords: Banking, Blockchain, consortium, security, decentralised, Shamir's Secret Sharing, Multiparty Computation (MPC), Private Key Separation.

I. INTRODUCTION

The traditional banking sectors often store the customer's data in the physical ledgers and books[1]. Although there are so many challenges like limited accessibility, lack of real-time updates, and risk of errors and frauds because it is a paper-based document, the maintenance and storing of these documents are very tough; also, we cannot correctly analyse the data because of its physical mode, etc. The banking sectors have adopted centralised data modules to overcome these challenges and make the banking system more convenient.

This centralised model stores data in a single central location and server [7]. This can be efficient for managing and accessing the data. A centralised system provides a combined and efficient way to manage vast banking data. This storage helps to maintain data consistency, and it enhances the overall security of sensitive financial information. It provides scalability and streamlined banking operations, including transaction processes, account management, and customer interactions [9]. This system has some core components, such as storing the entire database in one place and data warehousing, which can store and arrange large volumes of datasets.

Centralised systems implement backups and redundancy from which banks make copies of their data[10]. Over the past five decades, the banking sector has relied on computers to enhance its services and offer convenience to customers through centralised systems. However, this reliance has also led to challenges such as cybercrime, including hacking. Hackers can easily breach systems to steal customers' data and personally identifiable information (PII). Various malicious software like ransomware, phishing, and spoofing attacks are used to gain illegal access to bank databases. This software can potentially cause significant harm to the entire banking network[12]. It's essential to keep customer's information safe from illegal access.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IX Sep 2024- Available at www.ijraset.com

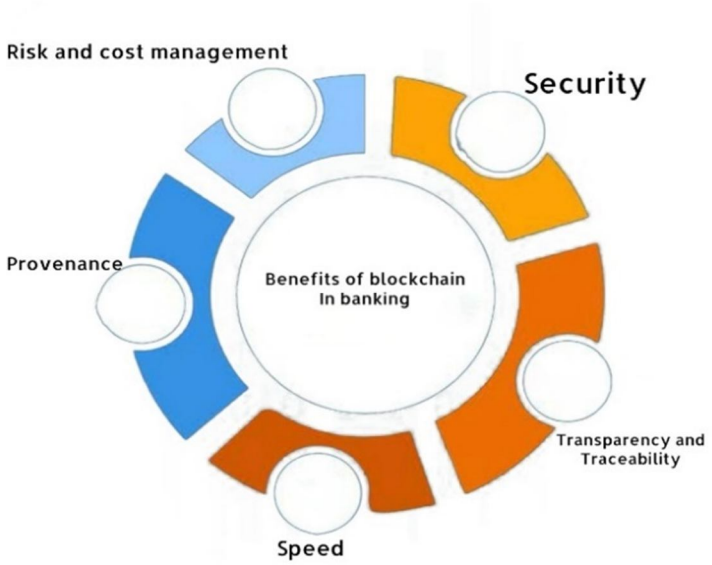


Figure 1 The benefits of blockchain in banking

Nowadays, blockchain is a highly renowned technology that provides enhanced security. The primary exposure to Blockchain started right after the submission of Bitcoin cryptocurrency [6]. The bitcoin uses this technology to track the records securely [5]. Blockchain is a technology that securely stores digital information in publicly shared databases. It is a decentralised and distributed ledger technology that secures records and verifies transactions across a network of computers.[2]. This technology is utilised in a peer-to-peer network, allowing participants to maintain shared and immutable data records. Blockchain is known as a reliable system because it acts as a transparent and temper-resistant system [22].

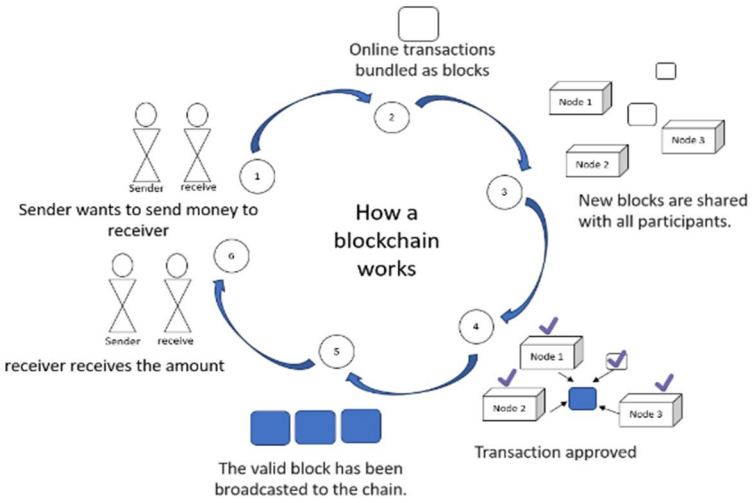


Figure 2Working of Blockchain

Blockchain, as its name refers, contains multiple blocks tied together. "Block" in Blockchain refers to a digital piece of information, while "Chain" refers to storing data in a public database. Each block in the network contains secured data connected through cryptographic principles. As mentioned earlier, cryptography ensures that transactions are conducted safely while securing all information.[14]. There are various types of blockchains, including public blockchain, consortium blockchain, private blockchain, and hybrid blockchain.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

There are two modes of blockchain: private mode and public mode. Blockchain is an emerging technology that applies to various public and private sectors, such as healthcare, supply chains, media, government, financial institutions, and banking. The banking sector has always prioritised regularly exploring, innovating, and upgrading technologies for better customer service. Today, the banking industry is implementing blockchain applications, which can completely transform and reshape banking services by providing high security, transaction transparency, a decentralised system, and more efficient transaction archiving. India's banking industry is a crucial component of the world's fastest-growing economy, contributing 7.7% to India's GDP. The "Indian Banks Blockchain Infrastructure Co PVT Ltd (IBBIC)" is a consortium of 15 banks, comprising ten private banks, four public sector banks, and one foreign bank. They are joining forces to address the significant challenges in traditional banking [2]. This paper is focused on exploring how blockchain architecture can improve technology and provide better security for customer data, which is the most critical information in the banking industry. We have proposed an Improved Version of the Secure Model for Online Transactions (IVSMOT) to ensure secure online transactions. The private key in this model is split into two shares: one stored on the user's device and the other given to the bank's server.

II. LITERATURE REVIEW

Saripalli et al. worked on [4]. They found current issues, such as slower payment transactions between the government and central bank, and tried to provide a solution using blockchain distributed ledger technology. Albeshr et al. reviewed [5] and found knowledge about blockchain technology regarding Bitcoin and some of its applications. Finally, they examined how blockchain is used in banking with its high security, transaction transparency, decentralised system, etc. Kalemis et al. study [6] and introduce the blockchain and its modern functionalities like payments, KYC, FX trading, etc. This paper discusses the use of blockchain technology in the banking sector and its potential to enhance banking operations. Chowdhury et al. worked on [7] and found how implementing blockchain technology can improve security and speed up transactions in the banking industry. The main goal is to show how blockchain functions and its potential usefulness in securing the banking sector. Chellaian et al. studied [9] and found the development of information security guidelines for the distributed system of the banking sector. They show concerns about the security of data collected by the banks, which can be easily attacked. They aim to utilise blockchain technology to enhance data security in the banking sector.

Bhatti et al. reviewed [12] and found a technique called Multi-Factor Authentication (MFA) by Blockchain technology, which is used to find authorised users by asking them for multiple identification information. The main motto of the authors is to prevent data breaches in the banking sector by using this new authentication method, which can't be hacked so easily. Ko et al. work [13] and propose a secure and appropriate online payment solution through a web application. They provide solutions for challenges faced by non-face-to-face transactions like voice phishing, identity verification, transactional security, etc. They use the key management module to store private keys securely in critical store files and databases. Thanapal et al. study [14] proposing a secured online payment system.

The current gateways are easily attacked and tempered by attackers. So, the authors introduced a system that provides peer-to-peer transactions without involving any third party using blockchain technology, enhancing payment security. They also use a digital signature to ensure data integrity in the blockchain. Wankhade et al. reviewed [16], and they found an outline of blockchain technology, its fundamental workings, and how it can be used in the finance industry. This study investigates the applications of blockchain technology in the banking sector.

They also discovered various challenges (e.g., scalability, data privacy, and security) in implementing blockchain technology in the banking sector. Weerawarna et al. review [22], and they discuss blockchain meaning, its steps, its types, and various applications used in the banking industry.

They also address the success of blockchain in the banking industry and numerous challenges (Initial setup, Efficient Infrastructure, Legal issues, Security, etc.) faced by the banking sector while adopting blockchain technology. Further, they mentioned how to implement a blockchain in the Indian Banking Sector. Khare et al. [23] found the implementation of this phenomenal technology. The authors introduce blockchain technology's use and benefits (cost-effective, paperless, faster transaction) in this paper. The main focus is on explaining how this technology works and how the implementation of this technology can also make it easier for banking employees.

Khan et al. studies [25] and introduce a theoretical model based on consortium blockchain to resolve data storage, privacy, and transparency issues. This model provides three primary services: registration, the transaction between parties, and the transaction to the customer from the bank.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Types of Blockchain

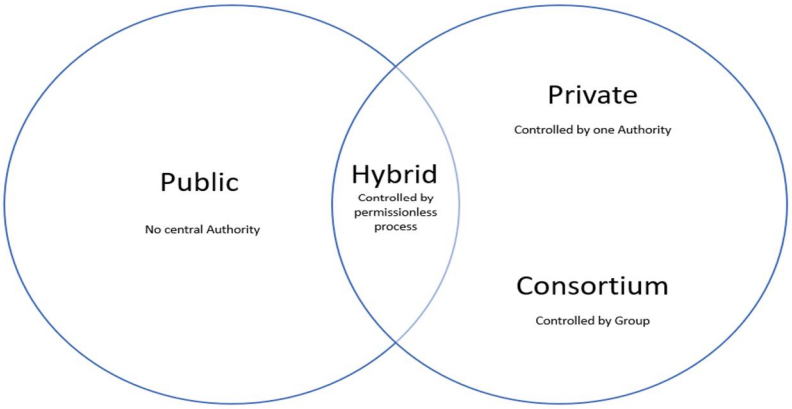


Figure 3.Types of Blockchain [14]

Public Blockchain: Anyone can join and participate in the network on a public blockchain. This means anyone can read, write, and verify the transactions on the blockchain [16]. Transactions on a public blockchain are transparent and immutable, which means records of this network can't be altered. Nowadays, Bitcoin, Ethereum, and many other cryptocurrencies use the network of public blockchains.

Private Blockchain: Private blockchains are also known as permission networks, which means only authorised persons have permission to join and participate. Organisations using this network gain more control over who can access and use the blockchain [17]. Many companies, such as HSBC, VISA, Barclays, and Intesa San Paolo, use private networks. Banks are using them for interbranch transactions.

Consortium Blockchain: A consortium blockchain is a hybrid approach that merges the characteristics of public and private blockchains [7]. A consortium network is also known as a semi-decentralized network. Multiple organisations are allowed to join and participate, but they must be approved by other members of the consortium blockchain[16]. Consortium blockchains are used to share data securely and effectively in industries like healthcare and finance.

Hybrid Blockchain: Blockchains bridge the gap between public and private networks, providing transparency and privacy features [7]. They get the benefits of both public and private networks. Organisations use public chains for transactions that need to be verifiable and private chains for transactions that need to be kept sensitive [17].

III. VARIOUS EFFECTS ON THE BANKING SECTOR AFTER IMPLEMENTING BLOCKCHAIN TECHNOLOGY

1) *Increased Efficiency and Transparency:* Blockchain can improve efficiency and streamline processes by creating a shared, secured transaction ledger, eliminating the need for third-party dependency. In Blockchain technology, every person on the network can see the same data, and information disorganisation is reduced [4]. This builds trust and allows better decision-making by all parties.
2) *Improve Security and Data Integrity:* Blockchain implements cryptography algorithms to create tamper-proof records. Every transaction in the network is encrypted and linked to the previous block by using hashing techniques to form an unbreakable chain. Once the data is recorded, any unauthorised person cannot alter it, and the integrity and security of data can be increased [15]. Implementing blockchain technology in banking can reduce fraudulent activities, data breaches, and unauthorised access and provide more protection for sensitive data.
3) *Cost Reduction:* Implementing blockchain can eliminate the involvement of third parties and reduce transaction costs [4]. It can also decrease the requirement of manual operations for banking transactions, which is time-saving and cost-effective.
4) *Decentralised Finance:* Blockchain uses decentralised finance, giving individuals more control over their financial data and reducing their dependency on traditional banks.

©IJRASET: All Rights are Reserved

5) *Cross-Border Payments:* Blockchain could significantly improve the speed and cost of cross-border transactions. It offers speed, cost-effectiveness, transparency, accessibility, security, etc [20]. The traditional method of cross-border payments requires intermediates, different banks, and currencies, which can delay the transaction and increase the transaction fees.
6) *Smart Contract:* A contract executes itself when the condition is satisfied and encoded into the code. It initiates a specific action when a condition is satisfied [15]. Applying intelligent contracts in the banking sector is very beneficial for automating various activities like loan approval, trade settlement, etc.

IV. OBSTACLES TO BLOCKCHAIN ADOPTION IN BANKING

Implementing blockchain technology in banking has several challenges that must be overcome before a project can succeed.

1) *Scalability Concerns:* Scalability is one of the most crucial challenges that must be overcome. Public blockchains like Bitcoin and Ethereum rely on proof-of-work (PoW) technology for consensus. This process is slow and more energy-consuming [16]. It can handle limited network transactions per second, leading to more extended processing and high transaction costs. Some faster consensus mechanisms are available called Proof-of-Stake and Byzantine Fault Tolerance (BFT), which provide speedier validation times but are unsuitable for all the use cases.
2) *Regulatory Uncertainty:* Blockchain's decentralised nature makes it unsuitable for the existing regulations designed for a centralised system. Regulations built for centralised systems make it challenging to adopt a decentralised network like Blockchain [15]. Some systems, like Know Your Customer (KYC) and Anti-Money Laundering (AML), are designed for centralised systems, which need to accommodate blockchain.
3) *Data Privacy and Security:* Blockchain technology is known for its storage security and data privacy characteristics, but there is still a concern over the privacy and security of sensitive data. Some techniques are zero-knowledge proofs and homomorphic encryption, which can help identify sensitive data with confidentiality [16]. GDRP (General Data Protection Regulation) is a data privacy regulation that requires banks to ensure user control over personal information.
4) *High Implementing Cost:* Implementing Blockchain technology with a traditional banking infrastructure requires complex system modifications. Further, an entirely new system called smart contracts has to be developed. However, implementing smart contracts can lead to high implementation costs [20].
5) *Lack of Interoperability:* Different blockchain platforms often use their communication protocol and may lack interoperability. This can make it difficult for different banks to exchange data seamlessly. Hyperledger Fabric and Interledger Protocol (ILP) provide a standardised platform.

V. SWOT ANALYSIS



Figure 4 SWOT analysis of Blockchain

A. *Strength*

1) *Enhanced Security:* Blockchain's distributed ledger nature makes it more tamperproof, reducing fraud and the risk of cybercrimes. Its transactions are encrypted using hashing and verified by all the participants, eliminating the single point of failure.
2) *Increased Transparency:* Blockchain enables immutability because all network participants can access transaction records, fostering trust and accountability.
3) *Improve Efficiency:* Blockchain technology can streamline banking operations by providing a transparent, tamper-proof, automated system. It can reduce transaction times and costs, improve record-keeping, and increase efficiency.

B. *Weakness*

1) *Limited Scalability:* Despite its early stages, blockchain technology is constrained by scalability issues. Its current transaction throughput may hinder its application in large-scale banking operations.

2) *Regulatory Challenges:* Regulatory challenges pose obstacles to blockchain adoption in the banking industry, as regulators may need to develop new frameworks to address this emerging technology's unique aspects.
3) *Standardisation Issues:* The absence of standardisation protocols across the different blockchain platforms can hinder interoperability and information exchange between banks.

C. Opportunities

1) *New Business Models:* Blockchain technology has the potential to revolutionise the banking sector by creating new business models and revenue streams, such as smart contracts, cross-border payments, and digital identity verification.
2) *Cost Saving:* Blockchain technology can help banks reduce costs by eliminating intermediaries, reducing transaction times, and automating processes.
3) *Enhanced Customer Experience:* Blockchain provides faster transaction processing and improved data security, leading to a more efficient and secure banking experience for customers.

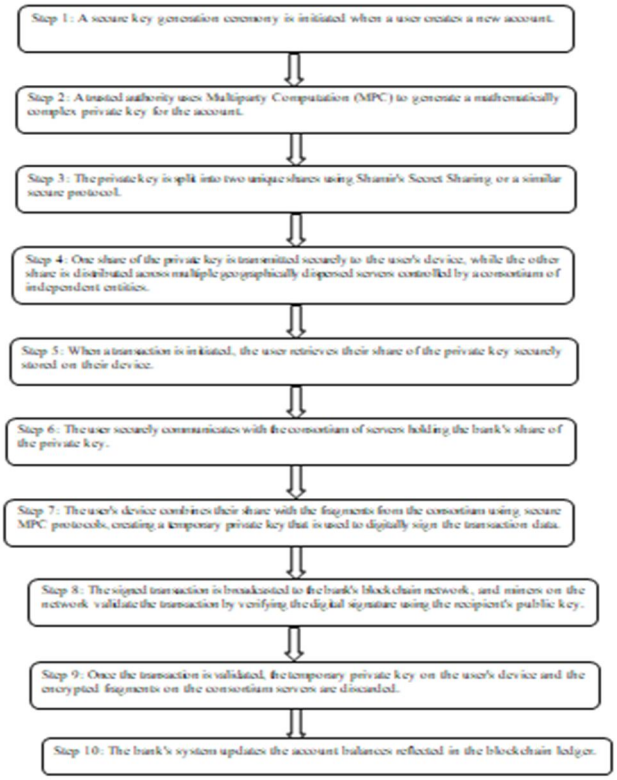
D. Threats

1) *Cybersecurity Risks:* Despite increased security, blockchain is not impervious to cyber threats. Banks adopting blockchain technology must implement rigorous security protocols to mitigate risks.
2) *Evolving Regulatory Landscape:* Frequent regulation changes can create uncertainty and hinder the development and implementation of blockchain.

VI. PROPOSED WORK

The current banking sector needs to adopt blockchain technology due to its high level of security for online transactions. Researchers like Mausumi Das Nath [24] have explored blockchain implementation to protect e-banking transactions. Nath proposed using the sender's public and private keys for authentication and security while utilising the SHA algorithm for the sender's signature. One primary security concern is phishing attacks, where malicious individuals trick others into giving away their passwords, installing harmful software on their devices, and stealing their private keys and secret phrases [26]. An Improved Version of the Secure Model for Online Transactions (IVSMOT) has been proposed to address this vulnerability, which is explained below.

A. Algorithm: Secure Key Distribution with IVSMOT



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IX Sep 2024- Available at www.ijraset.com

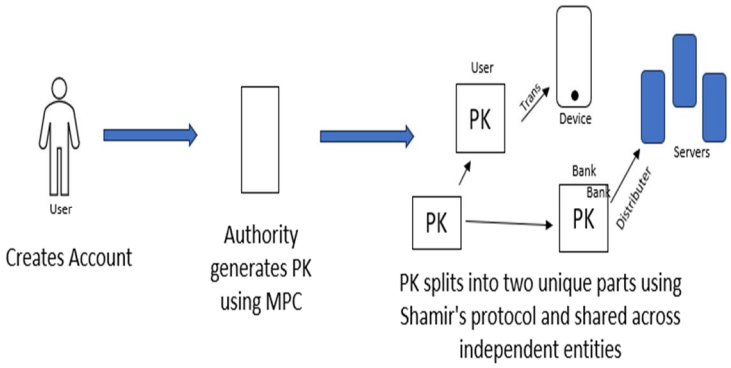


Figure 5 Splitting of Private key using Shamir's Secret Sharing

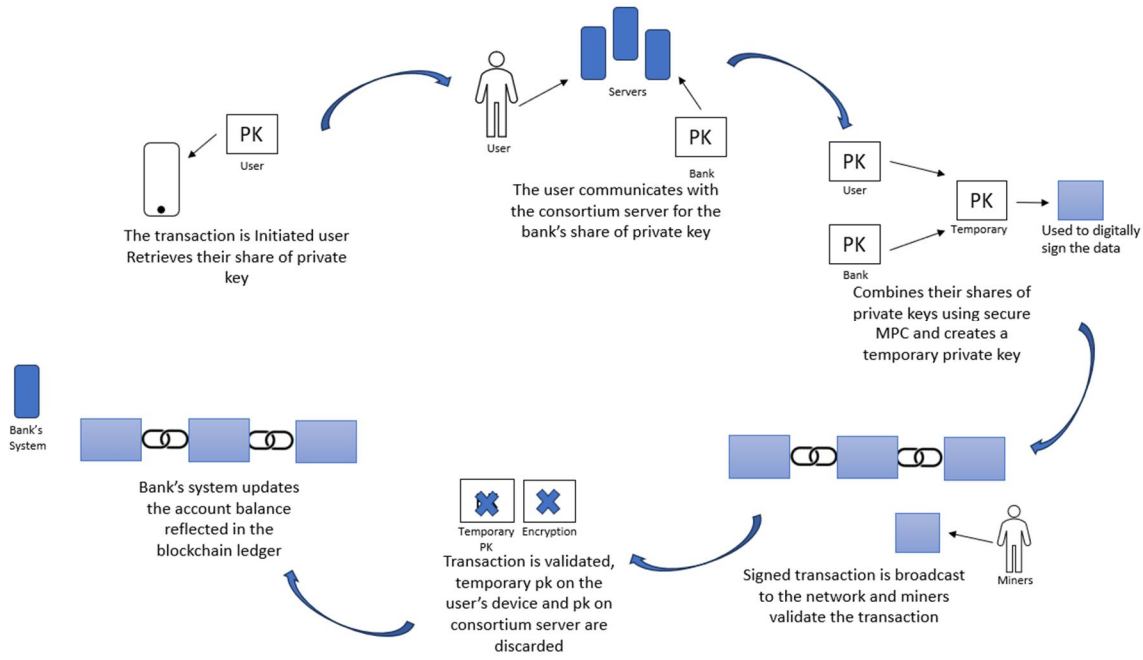


Figure 6 Improved Version of Secure Model for Online Transactions (IVSMOT)

VII. CONCLUSION AND FUTURE WORK

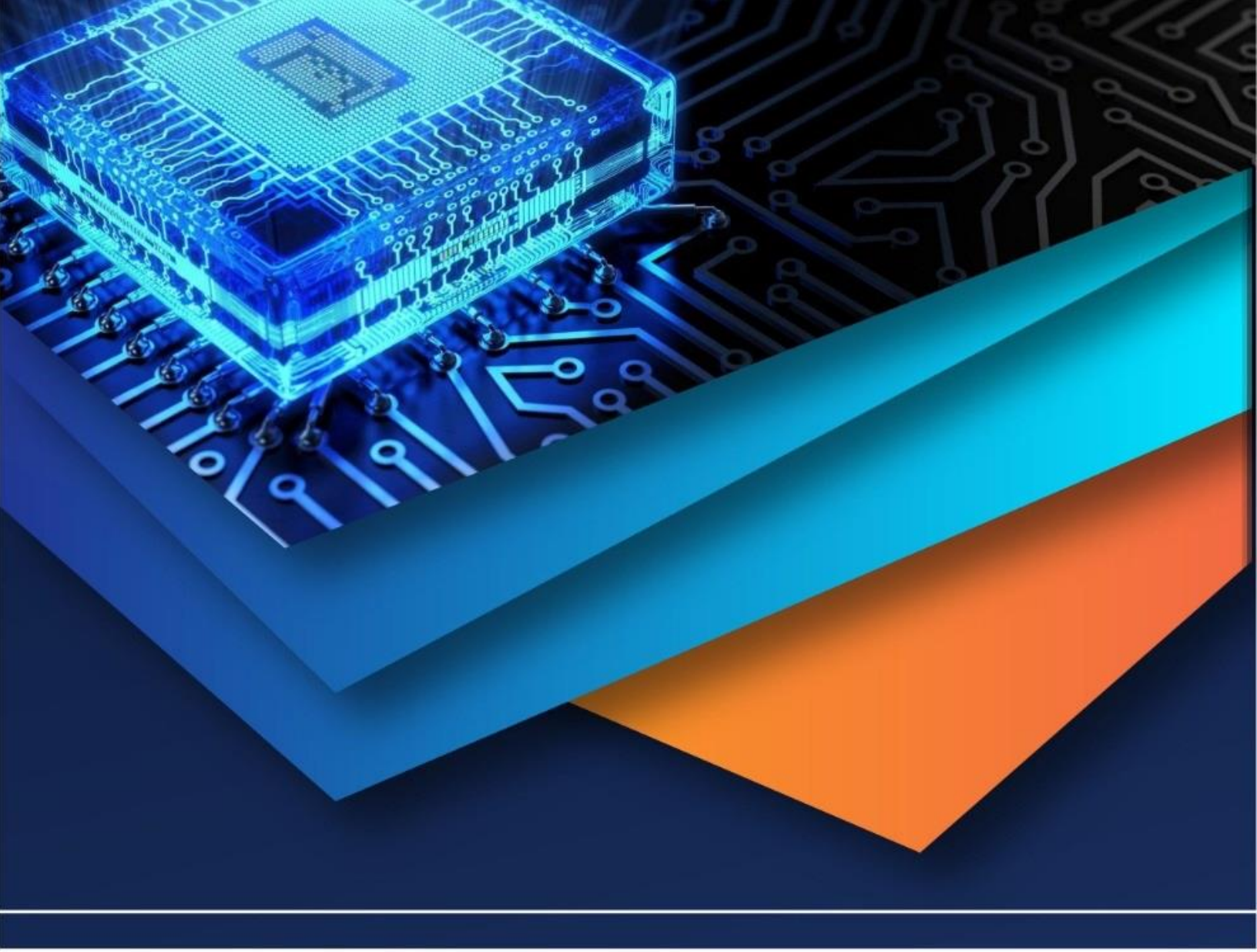
Blockchain technology is primarily recognised for its ability to provide security. Implementing blockchain technology in the banking sector is essential due to the increasing frequency of cyber-attacks that result in the theft of sensitive customer information. Many efforts have been made to enhance blockchain security, but unfortunately, there are still some vulnerabilities, such as phishing attacks, where attackers try to steal private keys. To address this issue, we have proposed a model called the Improved Version of Secure Model for Online Transactions (IVSMOT), which aims to prevent such thefts. The private key is divided into two shares, which prevents the risk of a single point of failure. Also, Miners are not involved in key management, maintaining decentralisation and security. A limitation of our proposed model is that secure key generation ceremonies and multi-party computation protocols add complexity that needs to be addressed.

©IJRASET: All Rights are Reserved

REFERENCES

[1] Shah, Tejal, and Shalilak Jani. "Applications of blockchain technology in banking & finance." Parul CUniversity, Vadodara, India (2018).
[2] Garg, Poonam, Bhumika Gupta, Kanwal Nayan Kapil, Uthayasankar Sivarajah, and Shivam Gupta. "Examining the relationship between blockchain capabilities and organisational performance in the Indian banking sector." Annals of Operations Research (2023): 1-34.
[3] Chen, Hungyi, Yuan-Chia Chu, and Feipei Lai. "Mobile time banking on blockchain system development for community elderly care." Journal of Ambient Intelligence and Humanized Computing 14, no. 10 (2023): 13223-13235.
[4] Saripalli, Sri Harsha. "Transforming Government banking by leveraging the potential of blockchain technology." Journal of Banking and Financial Technology 5.2 (2021): 135-142.
[5] Albeshr, Salah, and Haitham Nobanee. "Blockchain applications in the banking industry: A mini-review." Available at SSRN 3539152 (2020).
[6] Kalemis, Ilias. (2022). How blockchain can be adapted in the banking sector. 1. 10.
[7] Chowdhury, Minhaj Uddin, et al. "Blockchain application in the banking system." Journal of Software Engineering and Applications 14.7 (2021): 298-311.
[8] Chellaian, Geetha. (2022). Blockchain Technology to Protect Banking Transactions. Xi'an Dianzi Keji Daxue Xuebao/Journal of Xidian University. 14. 649. 10.37896/jxu14.6/073.
[9] Hakke, H., Bharati, A., Ranit, A., & Khonde, S. R. (2022). Blockchain-based payment method for secure transactions. International Journal for Research in Applied Science and Engineering Technology, 10(12), 835–840. https://doi.org/10.22214/ijraset.2022.48008
[10] Bhatti, Muhammad Ghazanfar, Rizwan Ali Shah, and Muhammad Asif Chaudhry. "Impact of Blockchain Technology in Modern Banking Sector to Exterminate the Financial Scams." Sukkur IBA Journal of Computing and Mathematical Sciences 6.2 (2022): 27-38.
[11] Ko, H.-J.; Han, S.-S.; Jeong, C.-S. Non-Face-to-Face P2P (Peer-to-Peer) Real-Time Token Payment Blockchain System. Appl. Sci. **2023**, 13, 7364. https://doi.org/10.3390/app13137364
[12] Thanapal, Karthikeya & Mehta, Dhiraj & Mudaliar, Karthik & Shaikh, Bushra. (2020). Online Payment Using Blockchain. ITM Web of Conferences. 32. 03007. 10.1051/itmconf/20203203007.
[13] Hasan, Ikram. (2022). Modern Blockchain Technology: Security Opportunities in Traditional Banking Supply Chain.
[14] Wankhade, Mahesh &. S, Balakrishnan & Chaudhari, Madhuri & Agarwal, Dr & Bahadur, Dr. (2023). Challenges in Implementing Blockchain Technology in the Banking Sector. Harbin Gongcheng Daxue Xuebao/Journal of Harbin Engineering University. 44. 1459-1471.
[15] Kalemis, Ilias. (2022). How blockchain can be adapted in the banking sector. 1. 10.
[16] Albeshr, Salah & Nobanee, Haitham. (2020). Blockchain Application in Banking Industry: A Mini-Review. SSRN Electronic Journal. 10.2139/ssrn.3539152.
[17] Irawan, B. (2021). Blockchain technology is an alternative method of payment transaction proof. International Journal of Science, Technology & Management, 2(5), 1769–1774. https://doi.org/10.46729/ijstm.v2i5.309
[18] Rella, L. (2019). Blockchain Technologies and remittances: From financial inclusion to correspondent banking. Frontiers in Blockchain, 2. https://doi.org/10.3389/fbloc.2019.00014
[19] Weerawarna, R., Miah, S.J. & Shao, X. Emerging advances of blockchain technology in finance: a content analysis. Pers Ubiquit Comput 27, 1495–1508 (2023). https://doi.org/10.1007/s00779-023-01712-5
[20] Verma, Amit, and Veena Prasad Vemuri. "BLOCKCHAIN TECHNOLOGY–A BOON FOR THE BANKING SECTOR TO ENSURE SECURE TRANSACTION."
[21] Khare, Jyoti & Singh, Dr Jaikaran. (2019). Innovative Socio-Economic Trends in BFM Blockchain in India: A Tool for Reshaping the Banking Sector.
[22] Das Nath, Mausumi & Bhattasali, Tapalina. (2019). Impact of Blockchain to Secure E-Banking Transactions.
[23] Khan, M. K., Nisar, K., Farooq, Y., Habib, S., Danish, M., & Hyder, I. (2021). An Improved Banking Application Model Using Blockchain.
[24] Halim, N. S. B. A., Rahman, A., Azad, S., & Kabir, M. N. (2017). Blockchain security hole: issues and solutions. Lecture notes on data engineering and communications technologies (pp. 739–746). https://doi.org/10.1007/978-3-319-59427-9_76
[25] Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain-based efficient fraud detection mechanism. Sensors, 22(19), 7162. https://doi.org/10.3390/s22197162
[26] https://www.techtarget.com/searchsecurity/tip/Top-blockchain-security-attacks-hacks-and-issues

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)