Enhanced UPI Technology for Secured Banking Transactions in Blockchain Platform

[1]Neethu Tressa, [2]Dr. C. Priya

[1]*Research Scholar*
Department of Computer Science
Dr.M.G.R. Educational and Research Institute, Chennai, TamilNadu
neethutressa89@gmail.com

[2]*Professor and Research Supervisor*
Department of Computer Applications
Dr.M.G.R. Educational and Research Institute, Chennai, TamilNadu
drcpriya.research@gmail.com

KEYWORDS

Device Binding, Two-factor MPIN Authentication, Signed QR/Intent, UPI 123Pay, Smart Contracts, Consensus Algorithms, Payment Service Providers, Merkle Tree, Sidechain, Consortium Blockchain.

ABSTRACT

The dependency on Unified Payments Interface (UPI) technology has increased a lot with all sorts of banking transactions. UPI provides high level of simplicity and privacy in financial transactions, which made it the most popular and highly demanded technology in India. So many researches are going on in terms of the methods for improving the security as well as interoperability features employed in UPI. The security of financial transactions should be ensured from transaction request till confirmation of transaction. In these levels, Blockchain platform can provide efficient contributions as compared with other existing network platforms. Immutability and distributed networking are the key features that help Blockchain platform in meeting with this criterion with the power of smart contracts. Blockchain provides tamper proof data storage with the help of encryption and consensus mechanisms. This paper describes the required features for a Blockchain based secured UPI technology.

1 Introduction

The real world has been moved a lot from the traditional physical cash concept to digital payments by the emergence of e-commerce activities. Once the financial organizations introduced the digital payment schemes, everyone learnt the convenience of going cashless. Among all the digital payments services available, now the entire world is looking at Unified Payments Interface (UPI) and its continuously improving features. As Reserve Bank of India (RBI) launched the UPI facility for feature phones as well called UPI 123Pay, there may not be the need for a look back. A person with a mobile phone in hand can freely live his life without the physical money, which was a concept that cannot be even imagined about a few years before. Even though UPI transactions are enabled with secured technologies, still they lack with the privacy and security assurance. In such a situation, we can definitely think of Blockchain Technology which is having the most security features in terms of financial transactions. If the existing UPI architecture can be enhanced with Blockchain Technology features, we can create a much more efficient and secured digital payment system. The following parts of the chapter will be describing the overview of UPI and Blockchain Technology. Also, we will show how we can merge these technologies together. Still, we can assume the chances of privacy and security issues in the new system. So, through

this chapter we can illustrate those key features that may be introduced in the system to assure better privacy and security for the transactions.

2 Related Works

A. Unified Payment Interface (UPI) – Transaction Flow and Architecture

National Payments Corporation of India (NPCI) launched the UPI architecture framework for real-time digital payments in 2016. UPI interface is helping the people with great user-friendliness along with fast and safe inter-bank transactions. Just by simplifying the customer experience in online payments, UPI crossed per month transactions to be more than a billion in India. With UPI, all the fund transfers and payments can be scheduled and done easily from multiple bank accounts through a single application. This is called UPI Autopay feature for recurring payments. Now, the UPI feature is also launched with feature phones as well via Unstructured Supplementary Services Data (USSD) channel which enables offline money transfer [1].

The following picture represents the Market Share of leading UPI apps in India as of July 2024 [2]:

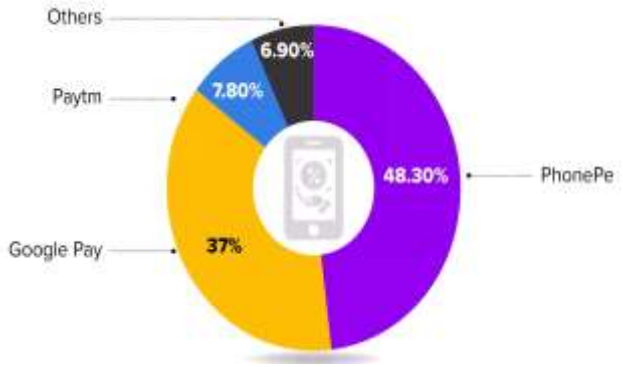

Fig. 1. Global Market Share of Leading UPI Apps in India

We can see that among the total Market Share, PhonePe and Google Pay occupy the highest score, with Paytm as the second highest. The increase in the number of users of these applications were responsible for such a hike in their Market Rate. It's not always the comfortability and ease of use, but it's the security factors that amplified the user count. From the stage of configuration, till the end of each transaction, what the user looks for is nothing but the security features imposed on the UPI application. UPI provides the following security features from user perspectives [3]:

1. Device Binding
2. Two-factor MPIN Authentication
3. Aadhaar based Verification
4. Signed QR/Intent
5. Invoice in the Inbox

Device binding becomes the initial security level which is ensured during registration. In this level, the mobile number gets bound with the UPI application. It requires identity verification upon each device or mobile number change, provided the number should have been linked with the corresponding bank account. During any device related threats, this device binding will ensure safety. The second level security is ensured using an MPIN (Mobile PIN). MPIN is a 4- or 6-digit number created during registration itself which is used for transaction authenticity. Using the debit card details of the linked bank account, this MPIN can be set up easily. We can reset this MPIN as and when required. If debit card credentials are not available, an Indian citizen can make use of Aadhaar card details also for registration and can create Aadhaar based UPI pin for authenticated transactions following simple steps. These features will help to verify the authenticity of payees as well. For a further level of transaction security, Signed QR/Intent is used. During Scan and Pay option with QR (Quick Response) Code, this feature will help to verify the authenticity of the merchant. Using signed intent, we don't need to use the application passcode as well. This can eliminate the risk for QR code tampering also. Invoice in the

Inbox is a feature in which we can view and verify the invoice before payment. Also, this invoice is a valid document wherever applicable.

The Reserve Bank of India launched UPI for feature phone users under the name UPI 123Pay which uses Server-Side Common Library system. This facilitates UPI transactions for the users without internet. UPI 123Pay service is available in multiple Indian Languages too. The debit card credentials are needed to do UPI transactions. The Payer can use the mobile number of the verified payee to start the transaction, provided the payer's bank account should have been linked with his/her mobile number. The payment can be done as application based, or through a missed call or via audio-based facility.

UPI enables us to easily facilitate interbank, peer-to-peer and peer-to-merchant transactions. Each UPI transaction involves multiple entities each of which is having its own roles and responsibilities. The major parties that take part in each UPI transaction are as follows [4]:

1. Payer and Payee
2. UPI Application
3. Payment Service Providers (PSP's)
4. The Remitter and Beneficiary Bank
5. NPCI

The Payer pays to the Payee using the UPI application in his/her device. The UPI application acts as the user interface for both payee and payer. The sender and receiver are associated with Payment Service Providers (PSPs). Payment Service Providers are third-party companies like Amazon Pay and PayPal, that help businesses to accept online payment methods. In a UPI transaction, the PSPs are used for authorization purposes and also for routing the requests. The UPI application should be linked with a bank account for debit and credit in each transaction. A UPI application can also be linked with multiple bank accounts. The remitter bank will be placing the debit request and the beneficiary bank will be placing the credit request.

The following figure shows the relationship between these entities and how these entities are connected to each other:

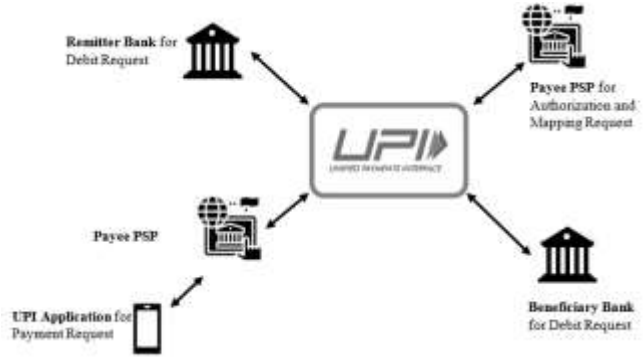

Fig. 2. Major entities involved in UPI Transaction

The basic building block of every UPI transaction is the payment address, which is used to uniquely identify the account details of the person. This transaction address takes the format similar to a mail id, like account@providers. For enhancing security, the transaction uses authentication as well as authorization. Usually, authentication is pin-based or OTP-based. UPI transactions use pin-based authentication. The pin can be different for different bank accounts. The authorization mechanism used by UPI transaction is via a third party authentication tool which provides a token less payment scheme. This makes the account management to be in control.

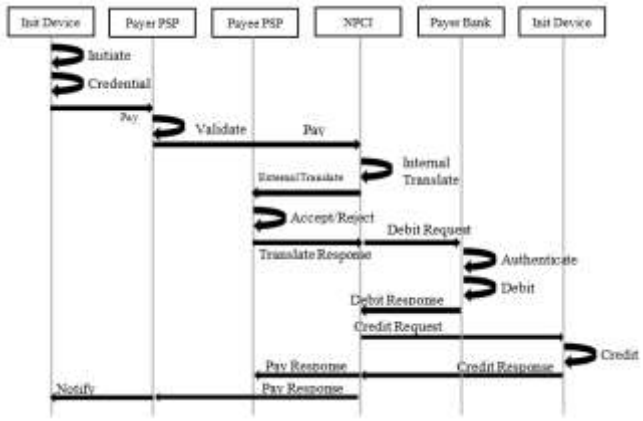

Fig. 3. UPI Transaction Flow

As in the above shown figure, the typical flow of a UPI transaction through a smart phone can be seen as follows. The payer can initiate the transaction by accessing the receiver's virtual payment address via the PSP application. The credentials for the transaction can also be a global identifier like mobile number linked to the PSP bank account, bank account number itself or even the Aadhaar number. After that, the sender can enter the amount to be transferred followed by selecting the bank account from the list of accounts which are linked using the UPI application. As the sender use the send button, the UPI network will place a request for the bank details for authorization, which will be provided by the associated Payment Service Provider (PSP). With the global identifier, the validation of payee address will be done by the NPCI central mapper. If virtual address is used, NPCI will place the pay request for address translation to the payee's PSP. Now, the NPCI will send the debit request to the remitter bank. Post authentication, the debit will reflect in sender's bank account with a notification. The receiver will also receive the credit notification after reflecting the credit in beneficiary bank account.
UPI is having a layered architecture which comprises of three layers. These layers can be represented as follows:

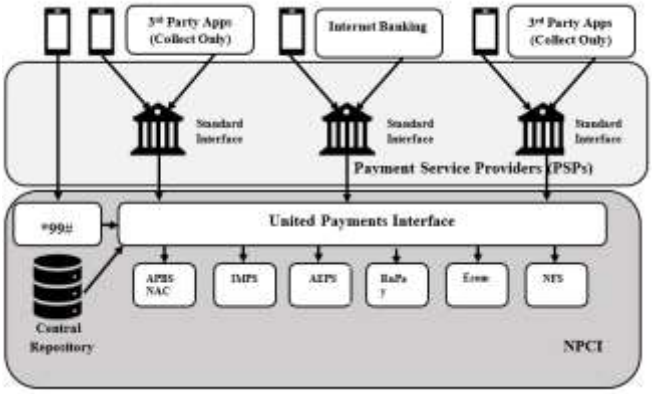

Fig. 4. UPI Architecture

As shown in the picture, the top layer in the architecture forms the mobile applications, internet banking and third-party applications like Paytm, Google Pay etc. These applications are connected to the bank accounts by entering the account details which are validated through the corresponding bank. These are the Payment Service Providers which include Standard Interfaces for Banks or other regulated providers like PPI/MM/Wallet providers. The PSPs are then connected to the UPI. Feature phones use USSD channels through National Unified USSD Platform (NUUP) also called *99# to get connected to the UPI. The UPI is having its own central repository which is used to store all the payment credentials like UID and bank account details which are used each time to validate and verify the users involved in the transaction. Now this UPI can also be used for different types of payments through APBS (Aadhaar

Payment Bridge System), National Automated Clearing House (NACH), Immediate Payment Service (IMPS), Aadhaar Enabled Payment System (AEPS), RuPay Cards, Ecommerce payments, National Financial Switch (NFS) etc. These different payment applications are integrated with UPI using stateless Application Programming Interfaces (API).

B. Blockchain Technology – Implementation in Financial Sector

As in [5], Blockchain is a revolutionary technology which can be now seen as the redefined internet. This technology is been said to have introduced by a pseudonym Satoshi Nakamoto under whose name, the initial studies on Bitcoins and blockchain were happened. In the beginning, blockchain was considered to be a safe and secure means for cryptocurrency transactions where there will be no presence of third-party intermediaries and hence transactions can be done with reduced cost [6]. This was under the principle of No Cash or No Plastic/Paper Money for financial transactions. It got designed as a self-growing public ledger where all the parties involved in the transaction will be able to view the entire transaction history thereby providing transparency. Later on, it started to get a distributed database like architecture where all the information is stored in the entire network of nodes which will help the data to be available always which makes it reliable [7]. Since the underlying architecture helps the information to be immutable, data loss can be prevented and also will be very difficult to modify the data stored in the network.

Blockchain provides the following security features during different levels of transaction [8]:

1. Encryption
2. Smart Contracts
3. Consensus Algorithms

The blockchain can be simply viewed as a chain of blocks, where each block contains the data. It is actually a collection of decentralized nodes where each node contains multiple blocks. The data in the blockchain is made secured by applying cryptographic encryption before creating the block. Also, the usage of smart contracts helps the network in effectively identifying the sender and receiver during any transaction which will ensure the authenticity of the data. Another security feature of Blockchain Technology is the use of Consensus Algorithms where the information is validated and verified by multiple users of the blockchain before permanently stored in the network. Due to these features, Blockchain technology became the key technology in the industrial revolution from IT, Business, Education etc. towards Supply Chain and even Governance.

The following chart [9] represents the global market size of Blockchain Technology which clearly shows the adoption statistics of the technology worldwide throughout the below mentioned years:

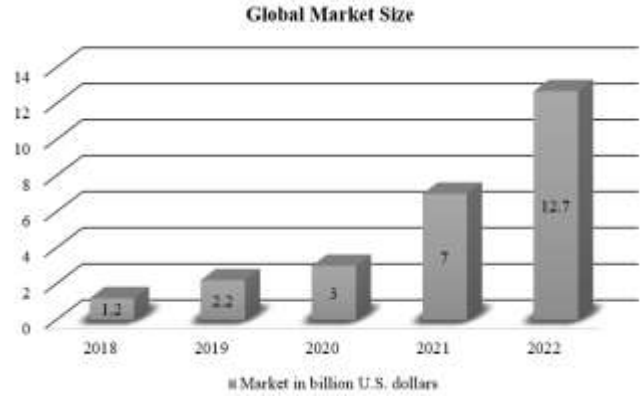

Fig. 5. Global Market Size of Blockchain Technology

According to the forecast, it is concluded that in the coming years Blockchain Technology revenues will be increased and reach 39.7 billion U.S. dollars by 2025.

Merkle Tree which is a form of Binary Hash Tree is the storage structure implemented for a blockchain, where each non-leaf node stores the hash values of the corresponding child node [10]. A usual Cryptocurrency transaction in a blockchain follows the below given steps [11]:

i. Request for a new transaction
ii. Create a block for the transaction

iii. Distribute the block to all nodes in the network
iv. Validate the transaction based on the type of blockchain implementation
v. Reward the nodes for the corresponding consensus algorithm they have applied
vi. Add the block to the existing blockchain
vii. Distribute the update across the entire network
viii. Finish the transaction

Identifying the type of Blockchain used will help in recognizing the risk factors in the implementation. Based on the implementation requirements, Blockchain is divided into five categories [12]:

1. Public Blockchain
2. Private Blockchain
3. Consortium Blockchain
4. Hybrid Blockchain
5. Sidechain

Public Blockchain can be viewed as an open network where without constraints, nodes can be added and participated in validation mechanisms. In a Private Blockchain, nodes will be added and managed by a single authority with certain restrictions. Consortium Blockchain and Hybrid Blockchain are combination of Private and Public Blockchains. The difference is that, in Consortium Blockchain, a group of authorities will act together as a central authority to manage the nodes, whereas in Hybrid Blockchain, single authority will be managing all participating nodes with lesser constraints than a Consortium Blockchain. Based on these characteristics, Blockchains are again classified in a more general way as follows [13]:

1. Permissionless Blockchain
2. Permissioned Blockchain

These are shown with the help of the following figure [14]:

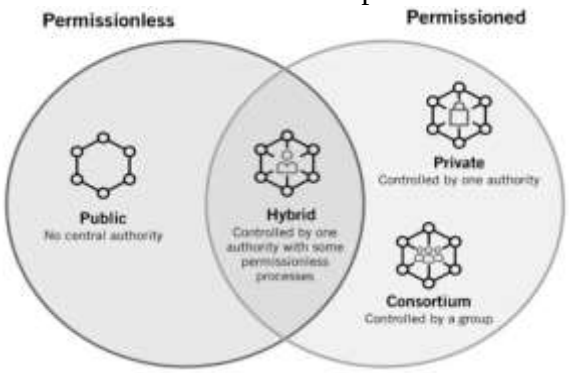

Fig. 6. Categories of Blockchain

Public blockchain is meant for individual usage whereas Private, Consortium and Hybrid Blockchains are used by large as well as Government organizations. Today, Sidechains are also developed to be used by everyone without considering the size or activities.

Blockchain is now the best option for data storage which eliminates the need for a central authority and also processing and service charges that the usual banking system demands [15]. When a user in need of a distributed transaction mechanism for improving the trust factor along with an interest in cryptocurrency transactions, Blockchain is suitable. As the size of the organizations grow exponentially, the financial transaction should also be considered with utmost focus to get rid of risks. In financial sector only, many tools and methods are available with blockchain [16]. Tools like Geth and parity are the enabled with security, whereas TIERION and remix provides transparency. INFURA and METAMASK are been widely used by bigger organizations due to its ability to track Real-time transactions and also Web 3.js and TRUFFLE are best known for their cost-effectiveness with respect to implementation.

3 Proposed Work

In this paper a blockchain-based UPI platform is been proposed which can improvise the major security aspects of the UPI transactions. The following sections point out the mainly reported challenges with UPI transactions in India and the features of Blockchain that can mitigate the chances of the risks associated with UPI. Further, the paper illustrates how blockchain can be integrated with UPI technology.

A. Major Challenges with UPI usage

UPI technology, just like any new technology launching in the market and with the usage afterwards, faces so many challenges in terms of adoption, customer-base, security and threats [17]. As an online payment mechanism, this paper focuses on the critical challenges which are reported many-a-number of times in India solely related with UPI transactions. These challenges are shown below [18-20]:

Fig. 7. UPI Related Challenges

One of the notable security concerns raised was Phishing Attacks in which the cybercriminals will be sharing fake UPI payment links through any online communication mechanisms where the receivers will be directed to fill the confidential information including account details. Yet another risk was SIM swapping, where the attacker can get the SIM with the same mobile number of victim and do unauthorized payments by getting control over his mobile number. As with any online applications, there is still a chance for unauthorized access through hacking and malware attacks. Nowadays social engineering attacks are heavily reported by the victims who have been tricked by attackers prompting for the UPI payments credentials.

B. Integrating UPI with Blockchain for Risk Reduction

As a distributed networking mechanism with high level of encryption scenarios, UPI can be very well integrated with blockchain technology which can effectively reduce the above raised concerns. The following figure illustrates the features of Blockchain technology, that can mitigate the challenges associated with UPI transactions:

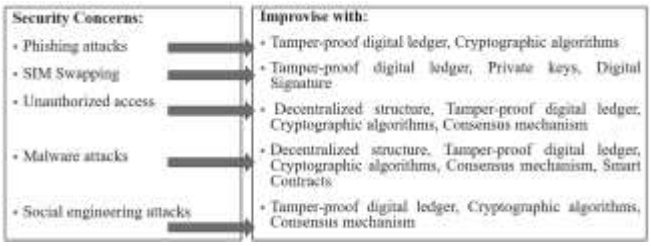

Fig. 8. Blockchain Features to Support UPI

By employing Smart Contracts in UPI transactions and also using cryptocurrencies Blockchain integration is possible with UPI [21]. As Blockchain keeps the digital ledger as tamper-proof, it is very easy to identify the attack where all the transactions are transparent to all nodes in the network. Also, the use of Cryptographic algorithms with Private Keys and Digital Signature will do efficient encryption and

decryption for maximum security in data storage making the attacker difficult to retrieve the actual data from the network. The decentralized structure of blockchain is actually making it strong against attackers while trying to destroy the nodes in the network, as the disturbed information can still be recovered from the rest of the nodes in the network [22].

Unauthorised access will be difficult for the attackers with the implementation of Consensus Algorithms, because until and unless all the nodes in the network validates the request, no transaction will happen in the blockchain. Apart from that the Smart Contracts between the parties taking part in the transaction will be automatically executed using predefined rules and regulations which will be tough to violate by the attackers [23].

4 Conclusion

Unified Payment Interface (UPI) is a successful online payment mechanism in India which is implemented with high security features in storage and in transit of the data. But still, UPI is also facing some of those risks that online applications also face. The study involved thorough research on the major challenges reported in India with respect to UPI transactions. It involves Phishing Attacks, SIM Swapping, Unauthorized Access, Malware Attacks and Social Engineering attacks. And, during the work, it was found that the blockchain features like Tamper-Proof Digital Ledger, Cryptographic Algorithms, Private-Public Keys, Digital Signatures, Decentralized Structure, Consensus Mechanism and Smart Contracts can improvise the existing security aspects of the UPI to a greater level.

References

[1] MC, A., & Shanmugam, K. (2023). Unified Payment Interface—Taking India to the next generation in payments. Journal of Information Technology Teaching Cases, 20438869231178843.

[2] NPCI, “Status quo on UPI market share cap; P2P lenders in focus,” The Economic Times, https://img.etimg.com/photo/msid-112638789 /UPI%20market%20share%20gfx..jpg (accessed Nov. 06, 2024)

[3] A., Mahesh & S., Ganesh. (2022). A Systematic Review and Research Agenda of Digital Payment System with reference to Unified Payment Interface. International Journal of Management, Technology, and Social Sciences. 679-709. 10.47992/IJMTS.2581.6012.0245.

[4] Vadlamudi, S., & Sam, J. (2022, October). Unified payments interface–Preserving the data privacy of consumers. In 2022 International Conference on Cyber Resilience (ICCR) (pp. 1-6). IEEE.

[5] Singh, S., & Chakraborty, A. (2023). Demystifying blockchain adoption in financial sector—A critical analysis. In Distributed Computing to Blockchain (pp. 367-375). Academic Press.

[6] Durga, H. K., & Sarvani, K. (2023). A Study on Fintech Start-Ups in India Special Refernce to Payments and Blockchain. European Economic Letters (EEL), 13(3), 887-891.

[7] Guntara, R. G., & Nurfirmansyah, M. N. (2023). Blockchain Implementation in E-Commerce to Improve the Security Online Transactions. Journal of Scientific Research, Education, and Technology (JSRET), 2(1), 328-338.

[8] Nirolia, M. (2023). A Study on the Application of Blockchain Technology in the Banking and Financial Sector in India. In Revolutionizing Financial Services and Markets Through FinTech and Blockchain (pp. 251-268). IGI Global.

[9] Taylor, P. (2022) Global market for Blockchain Technology 2018-2025, Statista. Available at: https://www.statista.com/statistics/647231/ worldwide-blockchain- technology-market-size/ (Accessed: 22 August 2023).

[10] Ravichandran, M. R., & Laxmi, K. V. N. (2023). BLOCK CHAIN TECHNOLOGIES AND FINANCIAL DATA PROTECTION–AN APPLICATION APPROACH TO FINANCIAL AND OPERATIONAL DATA–AN INDIAN PERSPECTIVE.

[11] Kawsalya, M., AV, S. K., Akash, V., Lolit, M. V., Masadeh, S. R., & Rawat, A. (2023). Blockchain-Based Secure Transactions. In Handbook of Research on Blockchain Technology and the Digitalization of the Supply Chain (pp. 86-112). IGI Global.

[12] Manda, V. K., & Nihar, K. L. Recent Trends in Blockchain Adoption in India.

[13] Sonekar, S. V., Bejjaniwar, S., Dandekar, S., Pal, S., & Karwade, P. (2023, April). Review Based on Blockchain and Financial Transactions Related to Cryptocurrencies Across Globe. In 2023 11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP) (pp. 1-6). IEEE.

[14] Jain, R., Prajapati, D., & Dangi, A. (2023). Transforming the Financial Sector: A Review of Recent Advancements in FinTech. Available at SSRN 4380348.

[15] Liu, H., Yang, B., Xiong, X., Zhu, S., Chen, B., Tolba, A., & Zhang, X. (2023). A financial management platform based on the integration of blockchain and supply chain. Sensors, 23(3), 1497.

[16] Kaushik, K. (2023). Blockchain Technology for the Financial Market. In Contemporary Studies of Risks in Emerging Technology, Part A (pp. 305-320). Emerald Publishing Limited.

[17] Kumar, S. P., Guhan, M., Kishorekumar, S., & Akshay, A. L. (2023, May). Investigation of failure in UPI transactions using cause & effect diagram and fault-tree analysis. In AIP Conference Proceedings (Vol. 2773, No. 1). AIP Publishing.

[18] George, A. S., George, A. H., Baskar, T., & Martin, A. G. (2023). An Overview of India's Unified Payments Interface (UPI): Benefits, Challenges, and Opportunities. Partners Universal International Research Journal, 2(1), 16-23.

[19] Virdi, A. S., & Mer, A. (2023). Fintech and Banking: An Indian Perspective. In Green Finance Instruments, FinTech, and Investment Strategies: Sustainable Portfolio Management in the Post-COVID Era (pp. 261-281). Cham: Springer International Publishing.

[20] Mothukuri, N. P. H. K., Rakesh, A., Babu, P. Y., Kiran, U., Bindu, G., & Hazarika, B. B. (2023, February). A Comprehensive Study of Different Security Features in eBanking. In 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS) (pp. 1177-1181). IEEE.

[21] Wan, H., Li, K., Huang, Y., & Zhang, L. (2023). Blockchain and Financial E-services. In Springer Handbook of Automation (pp. 1371-1383). Cham: Springer International Publishing.

[22] Kshetri, N., Miller, K., Banerjee, G., & Upreti, B. R. (2023). FinChain: Adaptation of Blockchain Technology in Finance and Business-An Ethical Analysis of Applications, Challenges, Issues and Solutions. International Journal of Emerging and Disruptive Innovation in Education: VISIONARIUM, 1(1), 4.

[23] Chand, M., Ahmad, V., Kathuria, S., Negi, P., Singh, T., & Chhabra, G. (2023, March). Digital Currency Security with the Intervention of Blockchain. In 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) (pp. 1356-1362). IEEE.