



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: <https://doi.org/10.22214/ijraset.2026.81301>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Secure Pay-Blockchain based UPI Payment System

Mr. VSSPLN Balaji Lanka¹, G. Jhansi², M. Dheeraj Kumar³, Shaik Lutfiyah⁴, K. Uday Kiran⁵

¹Assistant Professor, ^{2,3,4,5}UG Student, Department of CSE, Vignan Institute of Technology and Science, Deshmukhi, Hyderabad

Abstract- Due to the popularity of the digital payment system, there has been an increase in the need to adopt frameworks of secure and reliable transaction systems, especially in Unified Payments Interface (UPI) systems. This paper will overcome the issue of security, transparency, and trust by offering a Blockchain-Based UPI Payment System, a decentralized system that will provide security to financial transactions and user data. The proposed system provides blockchain technology which guarantees integrity of the data and prevents unauthorised modifications because it stores the UPI transactions in a decentralized form in an immutable way. Smart contracts are also used to automate the procedure of validating and processing transactions and reduce the required number of intermediaries. In the proposed system, cryptography techniques are merged to enhance authenticity, confidentiality and security of the system against fraud. The system that is proposed will enable the real-time tracking of transactions without the impact of user privacy. The transactions can also be traced with the system and this will assist in detection of suspicious transactions at an early stage. Overall, the UPI system based on blockchain is a safe, open, and reliable digital payment system that may be applied in the modern financial landscape.

Index terms—Blockchain, Smart contracts, secure payment

I. INTRODUCTION

The online payment services have become popular in the current digital economy, due to the convenience it offers to the users. One such widely used online payment service is UPI and it is utilized in financial transactions. However, due to the growing usage of online payment services, the risks of fraud, data breach, and unauthorized access are also growing, especially when the services are stored on a centralized control. The weaknesses of the system give way to cyber attackers who may interfere with the data of transactions or exploit the user credentials or loss of money or loss of confidence among the users.

In order to resolve these concerns, this paper will present a proposal of a Blockchain-Based UPI Payment System that will harness the strength of decentralized ledger technology to improve the security and authenticity of UPI transactions. The proposed system, based on blockchain technology, cryptographic security, and use of smart contracts, however, stands in contrast with traditional payment systems, which require a single entity to accomplish their work successfully. This makes the transaction details tamper-proof, transparent, and viewable by all the parties that have the authority to do so and therefore any form of fraud or alterations is avoided.

The greatest advantage of the suggested system is the opportunity to guarantee the integrity of transactions and make real-time payments. It can track the operations of the transactions among the distributed nodes and as such, it can identify any kind of suspicious activity that can be the signifier of fraud. The blockchain also follows the principle of making sure that once the records are stored in the system they cannot be changed.

The paper explains how and what the blockchain-based UPI payment system looks like and how it works alongside the major elements of the system such as smart contracts and cryptographic validation procedures. It also provides the importance of incorporating transaction details, user identification details and network validation processes to augment the security of the payment system. The results of the given research allow stating that the offered system can help to reduce the threat of fraud, increase the level of transparency, and address the changing risks of digital payments.

II. EASE OF USE

The UPI payment system is easy to use in blockchain since the payment system follows the same easy procedure just like other UPI applications allowing any user to make payment by scanning the QR code or typing the UPI ID without any understanding of the blockchain technology. The entire complicated procedures such as encryption, verification and secure storage take place in the background thus making transactions run smoothly with a couple of clicks. The system is usable since it is familiar, prompt confirmation of payments, and the history of transactions can be easily obtained, and blockchain technology enhances the level of security and transparency of the system without the user making any additional effort.

A. Existing System

In the existing system, a transaction of UPI is processed without blockchain technology. The transaction relies on centralized servers, and rules and authentication procedures that are provided by banks to ensure the security of the transaction. In spite of the fact that this system is effective in terms of payment and familiar frauds, it is lacking transparency and flexibility to address emerging security threats.

B. Proposed System

The proposed UPI payment system based on the blockchain and designed on the Ethereum platform with the help of Ganache will allow creating a controlled and safe testing environment. The transactions will be processed using the smart contracts and automatically verified and stored in the blockchain.

III. LITERATURE SURVEY

A number of researchers have tried to improve the safety and confidence that comes with digital payment systems like UPI using the blockchain technology. Li et al. (2020) created a decentralized system of storing transactions with a secure payment system through blockchain and smart contracts. Their study showed that fraud resistant records and distributed consensus could be used to increase trust. Their solution was however generic to digital payments and not specific to the needs of real-time and high volume payment systems like UPI.

Singh and Sharma (2021) have explored how blockchain technology can be used to ensure online transactions are secure since there is no central authority involved. The researchers came to a conclusion that blockchain technology contributes to a significant increase in transparency and prevents the risk of central control. The study has shown the advantages of the blockchain technology use, but still, made no comments on the necessity to protect privacy of the users and quick processing of the transactions needed in the UPI transactions.

The authors use the review of the application of blockchain in financial technology to examine how blockchain is used to enhance security, traceability, and reliability (Movva and Dasaraju, 2024). Although they mentioned the utility of decentralized systems in payment, their research was theoretical and it did not include any models and experiments of the working UPI integration.

Tyagi and Beri (2025) came up with a proposal of digital payment systems that were integrated with blockchain to promote trust and transparency. It was a research on how distributed ledgers can be used to eliminate centralized servers to secure payments. Nevertheless, the paper did not dwell on the functionality analysis and practical evaluation of the suggested model, which would have contributed to the evaluation of its capability to replicate real UPI traffic.

Lastly, Lin et al. (2025) developed a payment processing system that was based on blockchain technology, which combined decentralized technology and a secure verification system. In terms of security, the research indicated improved security and reduced chances of manipulation of transactions. Nonetheless, the interoperability challenges of compatibility between the current banking structure and regulatory provisions of UPI systems were not discussed in the study.

Collectively, these studies indicate that despite the potential of blockchain to offer the digital payment security, there is hardly any literature that specifically covers the needs of the UPI systems i.e. the real-time processing, scalability, privacy, and easy integration with existing banking infrastructure. This shows that the UPI payment systems require tailored blockchain solutions.

The importance of smart contracts to blockchain payment systems has also been mentioned recently. Smart contracts can be used to enable transactions validation to be automated, transaction rules enforced, including transaction limits, and disputes resolved without human intervention.

Such contracts that are optimized are of great significance in the UPI network setting where the transactions occur in real time, and that they involve a huge number of users. Unless such contracts are optimized, there are possibilities of performance problems or errors.

The other specific focus of recent research is the decision on the type of blockchain. Public blockchains are extremely transparent and, however, they may be slower in processing as they have to reach consensus, whereas permissioned or hybrid blockchains are faster in processing and also provide more control on who is able to access the data. Hybrid blockchains tend to be more acceptable in the UPI transactions.

By filling these gaps, future research can come up with secure, fast, scalable, and compliant blockchain-based UPI systems to present a reliable solution to the existing digital payment system and nullify the threats posed by the centralized one.

IV. ARCHITECTURE AND METHODOLOGY

The UPI payment system architecture design based on blockchain is designed to provide secure, transparent, and real-time transactions, including banks and users. The design is a modular type, where each unit is concerned with a specific task.

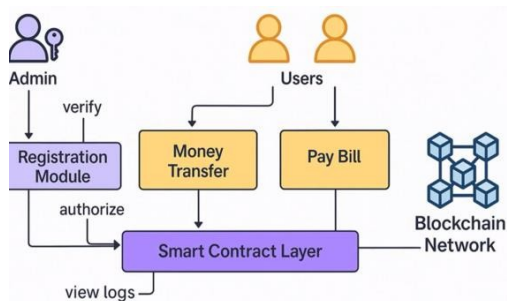


Fig1: System Architecture

A. User Interface Layer

This layer will provide a web interface that is interactive where users are able to register, log in and in the process carry out payment transactions. The interface is designed with the help of standard web technologies which also offer a smooth means of interaction with the blockchain network.

B. Application Layer

Application layer provides an interface between the blockchain network and the user interface. It is based on Web3 libraries to interact with the deployed smart contracts on the network. Application layer is also to handle the request of transactions, get account details and display status of transactions to the user in real time.

C. Smart Contract Layer

The Smart contracts written in Solidity programming language are the implementation of the business logic of the system. The smart contract is what takes care of user account management, validation of transactions and automatic transfer of funds. Once deployed, the smart contract is executed on blockchain environment

D. Blockchain Network Layer

The Ethereum platform forms the basis of the blockchain layer. All the transactions are cryptographically signed and time-stamped, and stored in the distributed ledger. This gives mutability, transparency and fault tolerance. The development and testing is done in a local Ethereum test environment (Ganache).

V. METHODOLOGY

The system of the proposed system is developed in a systematic methodology to guarantee that it is right, secure and scalable.

1) Step 1: Requirement Analysis

The Identification of the system requirements has been carried out through the analysis of the flaws of the traditional centralized UPI payment system, including the use of third-party servers and vulnerability to single points of failure. The primary objective will be to provide a safe payment service.

2) Step 2: Smart Contract Development

Smart contracts were also meant to establish the guidelines on how to address user registration, balances and fund transfers. Validation checks are also added to prevent transactions of unauthorized people and to have a enough balance to make the transaction.

3) Step 3: Blockchain Environment Setup

The development was done on a local Ethereum blockchain environment (Ganache) that was configured as a private network using local testing tools. A blockchain development framework was used to compile and deploy smart contracts and frontend interfaces were developed.

4) *Step4:FrontendandBlockchainIntegration*

Web3.js were used to connect the web application to the blockchain network. The user must log in and authenticate transaction using a digital wallet that will enable the user to sign a transaction in a secure way without exposing his / her private keys.

5) *Step5:TransactionProcessing*

Upon a user paying, a payment is handled to receive validation via the smart contract. After validation, the transfer is made and the transaction is stored in the blockchain. The transaction status is then updated in user interface.

6) *Step6:TestingandPerformanceEvaluation*

The system was put towards functional accuracy, transaction integrity, and security. Different transaction situations were performed to test the immutability and transparency of payment system based on blockchain.

VI. IMPLEMENTATION

A. *BlockchainbasedUPIOverview:*

Blockchain-based UPI Payment System: It is a decentralized digital payment system which is based on blockchain technology to support peer-to-peer transactions without having centralized banking servers. The proposed system uses smart contracts on a blockchain network to automatically validate and process transactions.

Unlike the traditional system where the UPI payment system requires the intermediaries of the banks to validate and process transaction.

The proposed system is secure, transparent and immutable in its transactions. The system will join UPI-like handles with blockchain wallet addresses so that, the users can send and receive payments in a manner similar to the UPI apps but with the added benefit of decentralization.

1) *LocalBlockchainSetup*

The initial stage of the UPI system based on blockchain implementation is the configuration of the local blockchain with the help of Ganache. Ganache is a simulator that is a local blockchain, and it allows development and testing to be done in a controlled environment. When an installation is made a new workspace is created to configure the project. Ganache will automatically create a test ten accounts, with each account loaded with 100 Ether in it, together with a private key. These are the accounts that are used to simulate users and carry out blockchain transactions in the process of development and testing.

2) *MetamaskIntegration*

The MetaMask browser extension is then set and linked to the Ganache local blockchain network. In MetaMask, a custom network is added with the network name of Ganache, the RPC URL of `http:127.0.0.1:7545` and the relevant chain ID (1337 or 5777). The Ganache generated test accounts are then imported into the MetaMask with their individual private keys. This can be integrated to allow the user wallet interface to interact and test the transactions on the local blockchain environment in a seamless manner.

3) *SmartContractImplementation*

Smart contracts are executable computer programs which have predefined rules and conditions to perform transactions like user registration, balance checking, fund transfer activities etc. The logic specified in such contracts automatically makes sure that the specified logic is enforced without the need of any manual intervention, which means that the transactions are executed securely and reliably.

4) *TransactionValidationLogic*

The smart contract authenticates a transaction before a payment is made depending on some conditions.

Let: B_s = Sender Balance B_r = Receiver Balance A = Transfer Amount

A transaction is valid if: $B_s \geq A \wedge A > 0 \wedge S! = R$

In case the requirements are satisfied, the transaction will be valid and will be automatically processed.

5) *PaymentExecutionandLedgerUpdate*

Once analyzed, the balances of the two users will be updated by the smart contract as follows:

$$B_s^{new} = B_s - A \quad B_r^{new} = B_r + A$$

This is then permanently written in the blockchain ledger.

6) *SmartContractDeployment*

Once the smart contract logic and rules of transaction are defined, the contract is implemented to the blockchain network.

Deployment The smart contract source code is compiled and sent to blockchain as a transaction.

After an deployment, thecontractreceives a different address on the blockchain that is used as a permanent identifier to address its functions.

The blockchain authenticates the code of the contract and logs it in a block during deployment, which imposes an immutable and tamper-resistant contract. This makes sure that the rules that have been set up, which govern user registration, balance inquiry and transfer of funds can not be changed once they are deployed. The implemented smart contract is then a trusted backend that performs several transactions automatically under the given conditions.

B. WebApplicationandUserInteractionModel

The web application is a significant element that interacts with the blockchain network with the users. The network of blockchain carries out the transactions and security, whereas the web application carries out the ease of use by hiding the complexities of technicalities. The web application is coded in a modular manner in which each user action is synthesized into a blockchain operation through engaging with smart contracts.

1) PaymentRequestFormation

The web application constructs a request of payment when the user makes a transaction that comprises ofthe sender address, receiver address, the value being transferred and the transaction details. The request is structured in the interface requirements of the smart contract. At this stage, the web application only processes non sensitive data and the private keys are held safe.

The payment request is an input to the smart contract and this is not executed until the user approves it.

2) SmartContractInteraction

After the payment request is created, the web application makes an invocation of the transferfunction of the deployed smart contract. This is achieved by having a secure blockchaincommunication layer which sends the details of the transaction to the blockchain network.

The smart contract independentlyvalidates therequest checking account balances, sender address, receiver address and amount of transaction. This is to makesure that the application will not modify the rules ofthe transaction because all the rules are imposed in the blockchain.

3) TransactionAuthorizationandExecution

After the transaction request has been sent to the blockchain, authorization is performed using cryptographicsignatures.Thesignedtransaction issent to the network in which it is decentrally verified. The transaction is validated by a number of blockchain nodes before being passed.

After the validation is successfully completed, the smart contract carries out the transfer of funds and leaves the required entries in the ledger.

4) Real-TimeTransactionStatusMonitoring

The web application waits to have the blockchain transaction confirmed. Once the transaction is part of a validated block it is responded to with a confirmation message by the web application.

The feedback mechanism can be used to help the user track the transaction status on a real-time basis as was the case with traditional UPI payments.

5) TransactionLoggingandAuditability

Every transaction gets registered on the blockchain automatically having a transaction hash. With the help of thetransactionhash,theapplicationretrievesthedetailsof the transaction and presents it to a user.

The transaction logs are immutable due to theimmutability of the blockchain records, and hence they cannot be altered or deleted. The latter allows having complete auditability and gives increased confidence tothe payment system.

6) HandlingTransactionFailures

The smart contract will also not accept the transaction in case of a failed transaction because of lack of balance, incorrect address or any network problems. The cause of the failure will be re-sent back to the application and displayed to the user.

This simple failure management system will allow theuser to know about the issue and rectify it respectively.

7) ScalabilityandUserLoadHandling

The web application is designed in such a way that it supports several users and concurrent requests of transactions. The transactions are processed asynchronously by the system to maintain the responsiveness of the interface during the peak network traffic.

The system can be scaled up easily and does not impact the user experience.

8) *CompatibilitywithExistingUPIWorkflow*

The backend is blockchain-based but user flow is nearly equivalent to the conventional UPI system. Similar functions such as typing in the details of the recipient, choosing the amount, and authorizing the payment are performed by users.

9) *PrivacyPreservation*

The system keeps the privacy of the user who does not keep any personal or banking details. The system merely captures wallet addresses and transaction data on the blockchain. No sensitive identity information is disclosed or shared.

CODESNIPPET

```

contract MoneyTransferBank {
    /**
     * @dev Transfer money to a recipient.
     */
    function sendMoney(address payable _to) public payable {
        require(s_isRegistered[msg.sender], "MoneyTransferBank: Sender is not a registered user.");
        require(s_isRegistered[_to], "MoneyTransferBank: Recipient is not a registered user.");
        require(msg.value > 0, "MoneyTransferBank: Amount must be greater than zero.");
        require(s_balances[msg.sender] >= msg.value, "MoneyTransferBank: Insufficient balance.");

        s_balances[msg.sender] -= msg.value;
        s_balances[_to] += msg.value;

        // Record transaction
        s_allTransactions.push(Transaction(msg.sender, _to, msg.value, block.timestamp));
        uint transactionId = s_allTransactions.length - 1; // Get the index of the newly added transaction
        s_userTransactionIds[msg.sender].push(transactionId);
        s_userTransactionIds[_to].push(transactionId);

        emit Transfer(msg.sender, _to, msg.value);
    }
}

```

Fig2:Samplesmartcontractfunction

VII. RESULTS AND OUTPUT

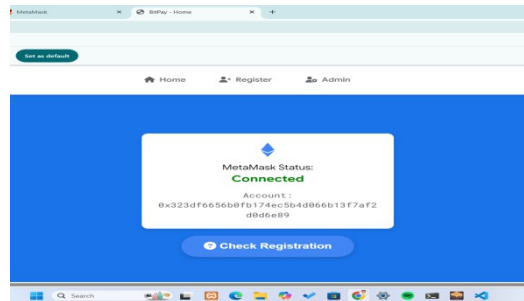


Fig3:MetamaskWalletConnection

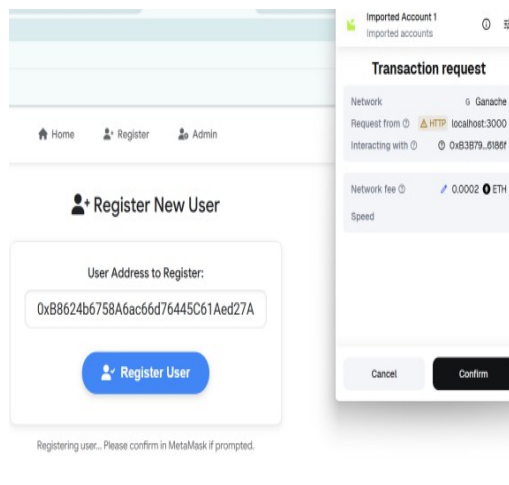


Fig4:RegisternewuserandConfirmation

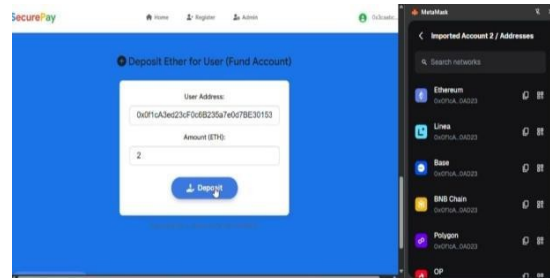


Fig5:FunddepositInterface

From	To	Amount (ETH)	Timestamp	Type
0x3CAAbC...	0x01cA3...	2 ETH	12/01/2026, 22:57:56	Deposit

From: 0x3CAAbC61EFB2928c68926FFE24D124db13a93A7b
 To: 0x01cA3ed23cF0c6B235a7e0d7BE301538990AD23
 Amount: 2 ETH
 Timestamp: 12/01/2026, 22:57:56
 Type: Deposit

Fig6:Blockchaintransactionrecord

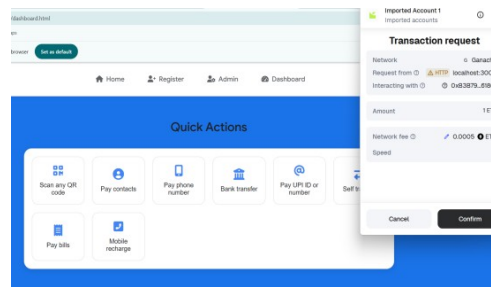


Fig7: QuickactionstouseSecurePay

Registered Users	
Address	Balance (ETH)
0x78b4A3Cb4D9cfc7219c159cCe37Dd50f09582	1 ETH

All Transactions

From	To	Amount (ETH)	Timestamp	Type
0xEa351E...	0x78b4A3...	1 ETH	1/26/2026, 10:53:33 AM	Deposit

Fig8:UpdatedUser Balance

VIII. CONCLUSION

The suggested UPI payment system based on blockchain has shown that blockchain technology can be used successfully to enhance the security, transparency, and dependability of blockchain-based payments. The suggested system is developed based on blockchain technology and smart contracts to manage transactions and is entirely independent of central servers, which guarantees the secure transactions, proper balance update, and immutable records of transactions. The test outcomes confirm that the suggested system can handle payments effectively and stop unauthorized and invalid transactions, as well as an experience that a user can experience due to the current UPI apps. As this paper establishes, the blockchain technology has the potential to be a dependable substitute in the next generation UPI payment systems.

IX. FUTURE SCOPE

To enhance the UPI payment system based on the SecurePay blockchain computing, one may introduce the deployment of the system on a real blockchain instead of on a local test system. Users can be enabled to pay by use of a simple identifier like mobile numbers or UPI IDs linked to their blockchain wallets in the future. The system can also be made easier with the help of QR code payments and mobile app support. Basic security verification and the user authentication can also be used to make the system more credible. Scalable blockchain networks or layer 2 scale solutions can be used to exploit more users and transactions, ensuring cost and latency is minimized. These changes can be used to make SecurePay a more practical digital payment system.

The other possible future development of SecurePay would be the integration of advanced monitoring and control capability to the advantage of the users and the administrators. To increase the security of the system and educate users, it is possible to introduce live transaction notifications, expense reports, and simple fraud filters. The transaction restrictions and self recovery can also be developed into the smart contracts in order to reduce abuse. SecurePay can be incorporated to operate alongside the existing digital payment systems with sufficient testing and incremental improvements thus becoming a potential solution to reliable digital transactions in future.

REFERENCES

- [1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008
- [2] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.
- [3] A. Antonopoulos, *Mastering Ethereum*, O'Reilly Media, 2018
- [4] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [5] M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, 2015.
- [6] D. Tapscott and A. Tapscott, *Blockchain Revolution*, Penguin Random House, 2016.
- [7] G. Wood, "Ethereum: Secure Decentralized Generalized Transaction Ledger," *Ethereum Yellow Paper*, 2014.
- [8] Y. Yuan and F. Wang, "Blockchain: The State of the Art and Future Trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.
- [9] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "Blockchain – The Gateway to Trust-Free Cryptographic Transactions," *European Conference on Information Systems*, 2016.
- [10] A. Gervais et al., "On the Security and Performance of Proof of Work Blockchains," *ACM CCS*, pp. 3–16, 2016.
- [11] S. Haber and W. S. Stornetta, "How to Time-Stamp a Digital Document," *Journal of Cryptology*, vol. 3, no. 2, pp. 99–111, 1991.
- [12] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, no. 2, pp. 6–19, 2016.
- [13] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.
- [14] K. Kshetri, "Blockchain's Roles in Meeting Key Supply Chain Management Objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.
- [15] R. Wattenhofer, *The Science of the Blockchain*, Inverted Forest Publishing, 2017.
- [16] National Payments Corporation of India (NPCI), "Unified Payments Interface (UPI) – Procedural Guidelines," *NPCI White Paper*, 2020.
- [17] A. Banafa, "Blockchain and Secure Digital Payments," *IEEE Technology and Engineering Management Society*, 2017.
- [18] P. Vasin, "BlackCoin's Proof-of-Stake Protocol," *White Paper*, 2014.
- [19] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1997.
- [20] D. Chaum, "Blind Signatures for Untraceable Payments," *Advances in Cryptology*, pp. 199–203, 1983.
- [21] S. Underwood, "Blockchain Beyond Bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.
- [22] World Economic Forum, "The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services," 2016.
- [23] Reserve Bank of India (RBI), "Digital Payments in India: Evolution and Challenges," *RBI Bulletin*, 2021.
- [24] A. Tapscott and D. Tapscott, "How Blockchain Is Changing Finance," *Harvard Business Review*, 2017.
- [25] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?," *PLOS ONE*, vol. 11, no. 10, 2016.
- [26] S. Singh and N. Singh, "Blockchain: Future of Financial and Cyber Security," *International Conference on Computing, Communication and Automation*, 2016.
- [27] V. Pilkington, "Blockchain Technology: Principles and Applications," *Research Handbook on Digital Transformations*, 2016.
- [28] Deloitte, "Blockchain Technology and Its Potential in Digital Payments," *Deloitte Insights*, 2017.
- [29] IBM, "Blockchain for Secure Digital Payments," *IBM White Paper*, 2018.
- [30] Accenture, "Transforming Digital Payments Using Blockchain," *Accenture Research Report*, 2019.



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)