International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-13, Issue-4, July 2025
DOI: https:/doi.org/10.55524/ijircst.2025.13.4.3
Article ID IRP-1655, Pages 33-40
www.ijircst.org

BlockPay: A Blockchain-Based Framework for Secure and Scalable Digital Payments

Prasad S R [1], Deepali [2], Samarth Jain [3], Samyakth Kumar [4], and Sudeep D Gowda [5]

[1] Assistant Professor, Department of Computer Science and Engineering, Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire, Karnataka, India
[2, 3, 4 & 5] Graduates, Department of Computer Science and Engineering, Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire, Karnataka, India

Correspondence should be addressed to Prasad S R; prasad.gowda029@sdmit.in

Received 26 May 2025; Revised 9 June 2025; Accepted 25 June 2025

Copyright © 2025 Made Prasad S R et al. This is an open-access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT- In recent years, blockchain has gained serious traction as a promising tool for fixing long-standing issues in how digital payments work—especially around trust, data security, and transaction delays. This paper shares our experience developing BlockPay, a blockchain-based payment system designed to improve on traditional methods. Many current platforms struggle with things like limited transaction sizes and poor international support. BlockPay addresses these by using a distributed ledger that makes it hard to tamper with records. We also built smart contracts to handle payments automatically, which helps to reduce mistakes or fraud. To keep everything reliable, we rely on a consensus model so that all the network's nodes agree before a transaction goes through. We have added strong encryption and user authentication which is based on the private keys to make sure users' data stays safe. The system works smoothly across devices and is built to be user-friendly for individuals or for running a business. One highlight is its real-time payment processing and built-in currency conversion. All in all, we see BlockPay as a practical step forward in making financial systems more open, faster, and secure.

KEYWORDS- Blockchain Architecture, Consensus Mechanism, Smart Contract Automation, Cryptographic Protocols, Decentralised Payment Systems, and Real-Time Transaction Processing.

I. INTRODUCTION

Digital payment systems have come a long way in recent years, but this progress has brought new challenges, especially in the case of security, transparency, and the ability to handle large, fast-moving transactions. Blockchain has entered the picture as a technology that could potentially solve many of these issues, offering a decentralized and tamper-proof way to manage financial exchanges. In this paper, we introduce BlockPay application, a payment platform built on blockchain technology that we developed to deal with common issues in today's financial systems. These issues include over-dependence on middlemen, exposure to cyberattacks, limited transaction volume, and slow cross-border payments [1].

BlockPay is built with decentralization, transparency, and immutability at its core—qualities that help establish trust and keep records tamper-free. We have applied strong encryption and used decentralized data storage to protect the user data. We also rely on smart contracts to run transactions automatically and apply rules without needing someone to intervene, which helps reduce errors and fraud [2].

The transaction data is spread by the platform across many nodes in the network. This setup not only improves resilience by avoiding a single point of failure but also helps to speed up transaction times and reduce costs. That makes it a practical fit for industries like online retail, financial services, and digital commerce [3]. We've also made sure BlockPay is easy to use across devices, with a clean interface for individuals and businesses alike. It's especially built to handle real-world problems like low transaction limits and slow international payments—issues that continue to hold back global financial systems [4].

In this work, we walk through how BlockPay was developed and how it solves some of the problems found in standard payment systems. We believe that systems like this can support larger transaction volumes, smoother international payments, and better security. In the long run, they could help accelerate the shift toward decentralized digital finance [1].

II. RELATED WORK

In recent years, blockchain has grown rapidly, which has caught the attention of many researchers in the process. It is due to the potential of blockchain systems to make payments both safer and efficient. Scholars have done a lot of research on different technical aspects, including how blockchain networks are built, how consensus is formed across nodes, and how encryption helps protect the data. This growing body of work has created a strong base for developing decentralised platforms in the financial sector.

One review by An et al. [5] traces how blockchain has developed over time, touching on system design and different use cases—including how it's being linked with technologies like federated learning. They highlight the importance of decentralization and immutability in maintaining trust and keeping transactions secure, both in finance and in IoT applications.

A deeper dive into how blockchain works internally was done by Ahmed et al. [6], who explored the technical layout of blocks—like genesis and transaction blocks—and their cryptographic roles. Their analysis sheds light on how secure transaction records are created and retrieved.

Anascavage and Davis [7] provided a comparative assessment of transaction speed, scalability, and security protocols in blockchain-based payment systems. Their review delineates the practical constraints and advantages of various consensus algorithms and encryption strategies, informing the design of secure, real-time transaction infrastructures.

When it comes to smart contracts, Virani and Kyada [8] reviewed how they function and the risks they carry. They looked at the programming environments used to build them and gave examples from industries like supply chains, healthcare, and finance. Importantly, they also called out security vulnerabilities and how those can be managed.

Monrat et al. [9] in this paper, the authors have reviewed the implementation of blockchain concepts in different sectors, including supply chain operations, healthcare systems, and decentralized finance. In their review, they also highlighted the key challenges, such as interoperability issues, scalability, and ongoing regulatory uncertainty that still hinder broader adoption. Authors also identified the future scope, where blockchain is integrated with emerging technologies like artificial intelligence (AI), the Internet of Things (IoT), and 5G.

Nakamoto [10] the authors introduced Bitcoin as a peer-to-peer digital cash system. This landmark paper laid out the core ideas behind decentralized currency and the proof-of-work consensus model, setting the stage for the blockchain systems that followed.

Zheng et al. [11] contributed further to the discussion on blockchain adoption with a detailed survey on both the benifits and its challenges. Their study highlighted challenges like security risks, limitations of scalability, and the need for a unified regulatory framework. Meanwhile, authors have also highlited the potential of blockchain to reshape not only financial services, but also governance systems.

When it comes to scalability, Bhosale and Waghmare [12] compared different solutions—both Layer 1 and Layer 2 approaches like Plasma and Rollups. Their work looks at the trade-offs between speed, security, and decentralization, and gives helpful guidance on what options might suit different needs.

To understand where research is headed, Dubey [13] analyzed over 1,500 papers on blockchain-based payment systems. His bibliometric study mapped out research trends, major contributors, and key topics emerging in the field.

In financial settings, Weerawarna et al. [14] explored how blockchain could change services like identity checks and remittance transfers. They found that blockchain can improve how transparent and fast these services are, but they also mentioned ongoing problems like high transaction fees and slower verification processes.

These studies all point to what makes a blockchain payment system functional and secure—from encryption and consensus models to smart contracts. Using what we've learned from this literature, our work focuses on building three main components: the transaction validation algorithm, the consensus mechanism, and the SHA-256 hashing algorithm. Together, these form the core of the secure payment system we propose.

III. PROBLEM STATEMENT

Nowadays, Digital payment systems are facing several practical challenges, like low transaction limits and poor support for cross-border payments. These challenges are the barriers for the both individuals and businesses, which limit financial flexibility and make it harder to scale operations smoothly. When users can't carry out huge transactions or when international transfers take time and come with high costs, it will naturally lead to inefficiencies and delays. This, in turn, will affect the global financial flow and trade connectivity. For a globally integrated economy, such issues become major obstacles. A truly effective payment system should make transactions across countries in real-time, without any restrictions. This kind of setup will boost the economic activity and also make the financial services more inclusive and accessible, especially for those currently underserved. It would also encourage foreign investments, improve trade operations, and strengthen international cooperation [15]. To achieve this, there is a need for a system to build the next generation of payment infrastructure that is scalable, interoperable, secure, and regulatory-compliant. Only then can we make a move towards a smoother, borderless financial ecosystem that will work well for individuals, small businesses, or large enterprises.

The Current challenges of digital payment systems are addressed by a new and smarter system of Blockchain technology, which utilises its key features, like decentralization, cryptographic security, and immutability, to offer a secure, transparent, and tamper-resistant transaction environment. Integration of blockchain with the payment system can enable instant transactions, eliminate the need for intermediaries, and minimise the additional cost. Additionally, advanced security measures and consensus methods ensure that the transactions are trustworthy and confidential. Blockchain utilises tools like smart contracts and shared digital records to improve automation, simplify payment tracking, and support through auditing. Collectively, these qualities highlight the blockchain's ability to transform digital payments by making them more secure, faster and more reliable [16].

A. *Objectives of the Proposed System*

The following are the Objectives of the proposed project, each of which is aimed at addressing the current challenges and the existing gaps in the digital payment system through blockchain integration:

- **To increase Transaction Limits for Greater Financial Flexibility:** To overcome the limitations of the current financial systems, the proposed solution targets to support high-value transactions. This enhancement will enable both individual users and institutions to function more efficiently, supporting high-volume transactions and reducing dependency on traditional banking limitations.
- **To Enable Seamless Cross-Border Transactions:** Designing a globally interoperable infrastructure, the system will simplify cross-border transactions. The system adheres to both local and international financial

regulations while ensuring that it reduces transaction fees and delays, consequently making cross-border payments faster, cheaper, and more reliable.

- **To improve transaction speed and Network scalability:** The system will adopt optimized mechanisms and parallel processing techniques to boost processing speed and handle the high transaction volumes. This will ensure that even under heavy usage, the payment network remains efficient and scalable.
- **To Strengthen Security and Safeguard Data Integrity:** To secure the user access to different sections of the system, and protect the transaction data, advanced cryptographic techniques and multi-factor authentication are used. These measures are used to resist fraud, cyberattacks and to ensure that all financial transactions remain confidential and tamper-proof.
- **To promote Eco-Friendly Blockchain Practices:** To design a system which is energy-efficient, eco-friendly, has less environmental impact and is sustainable over time, blockchain technologies like BNB Chain and Ethereum 2.0 are used.

IV. METHODOLOGY

The BlockPay application development follows the streamlined and technically robust framework to facilitate secured and efficient blockchine based payment system. Following are the different methodological steps used to implement the objectives of the BlockPay.

A. Requirements and Platform Selection:

Objectives or Goals of the Project are defined, with support for high scalability, focusing on high security and cross-border transactions. Based on these requirements, a supportable blockchain platform is selected (e.g., Ethereum or BNB Chain).

B. Architecture and Smart Contracts:

The architectural design ensures the fulfilment of all the targeted objectives, and smart contracts are developed to automate transactions using Solidity and impose different payment rules.

C. Security Integration:

Advanced cryptographic methods are used, and digital signatures are applied. For the protection of data and ensuring privacy, Secure key management, multi-signature wallets, and ZKPs are incorporated.

D. Wallet and Authentication Development:

Digital wallets' security is enhanced with biometric and two-factor authentication. To secure the System, interaction is enabled with the enforcement of Role-based access controls.

E. Payment Gateway Integration:

API connections are secured with fiat gateways, which also enable the smooth crypto-to-fiat conversions, while enhancing the interoperability with traditional financial systems.

F. UI/UX and Compliance:

The application is built to be simple and easy for anyone to use, with a smooth and user-friendly interface, while it ensures verification of user identity (KYC), prevents financial crimes (AML), and ensures personal data is protected (GDPR).

G. Testing and Validation:

Different contexts are used to test the performance of the proposed system, integration, and security testing is performed, which also includes penetration testing and performance benchmarking under different load conditions.

H. Deployment and Monitoring:

A secure platform is selected to host the application, which ensures the availability and security of user data. The system is continuously monitored for real-time issues and is fixed quickly. Required updates and improvements are implemented smoothly using automated tools (CI/CD), without disrupting the user experience.

I. User Training:

Users are provided with clear guides and learning materials to understand how BlockPay can be used safely, which encourages active participation of users with boosted user confidence.

V. SYSTEM DESIGN

Figure 1 presents the system architecture of the proposed blockchain-enabled payment model. It consists of key components, like user wallets, API interfaces, middleware services, and a distributed ledger. Supporting smooth integration and Tamper-proof information across the network [17].

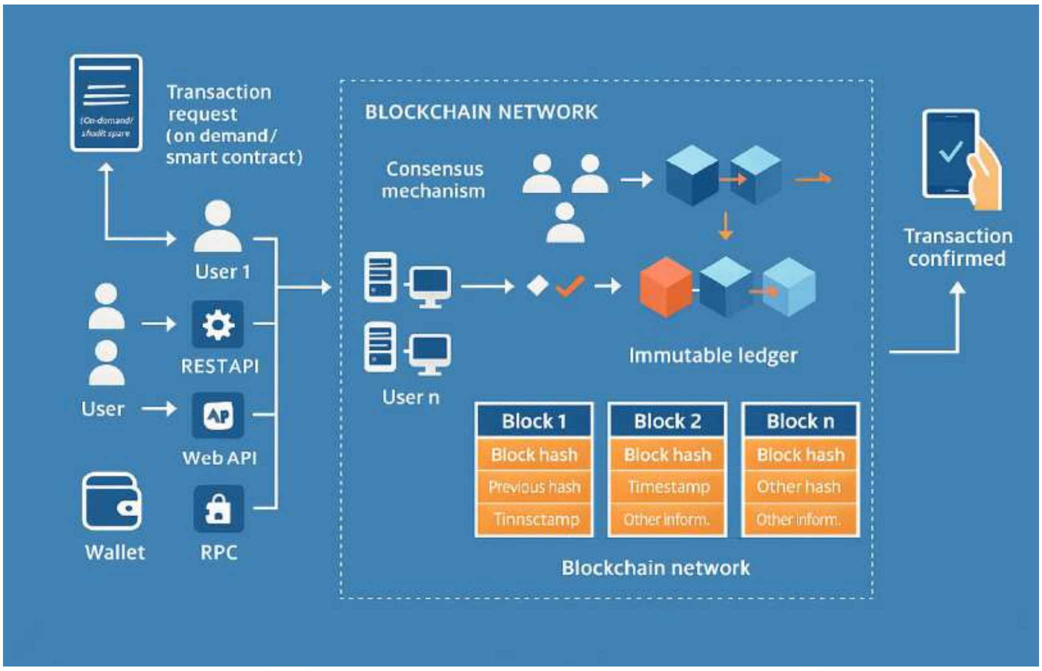

Figure 1: System Architecture of the Blockchain-based Payment Network

- **User Layer (Initiators and Recipients):** Web or mobile interfaces are used by the end users to interact with the system. This layer includes entities that initiate or receive transactions, like merchants, customers, and other entities. Each user is authenticated and linked to a secure digital wallet. Users initiate payment transactions, which are encapsulated and forwarded to the application layer via APIs.
- **Wallet Management System:** The wallet subsystem handles private key generation, secure storage, and cryptographic signing of transactions. Each wallet supports secure identification of users and ensures data integrity through public-private key mechanisms. Wallets interact with smart contracts to authorize fund transfers.
- **API Gateway Layer (REST/Web APIs):** This layer exposes endpoints for system integration. REST APIs support application-level transaction processing, while Web APIs facilitate user-side access, transaction initiation, and real-time data retrieval. Also, ensure security, scalability and abstraction.
- **Application and Integration Layer:** This layer is responsible for managing the orchestration logic between the user layer and the blockchain network. It includes the middlewares which connect the External systems, such as accounting platforms, and enable synchronization of financial records. Also, includes the logic of verifying the transaction, handling the user requests and smart contract invocation.
- **Blockchain Interaction Layer (RPC & Smart Contracts):** The Remote Procedure Call interface is used to enable the communication between the back-end application and the blockchain nodes. This layer supports transaction submission, contract interaction, and ledger queries. Blockchain environment integrated with Smart contracts enforces payment rules, escrow conditions, and automatic settlement.
- **Blockchain Network Core:** This core includes two aspects, one is validator nodes and the other is the distributed ledger. Consensus mechanisms such as Proof of Work or Proof of Stake are used to validate the transactions. Cryptographically linked groups of verified transactions are used to form blocks and added to the tamper-proof blockchain system. Transaction hashes, timestamps, and the hash of the previous block are maintained in each block, which ensures integrity and non-repudiation.
- **Ledger and Audit Layer:** A secured ledger structure is used to store the transaction histories. Each node maintains a synchronized copy of the ledger. Transparent auditing, traceability, and compliance reporting are supported by this laye. Auditing tools are integrated to ensure the real-time integrity checks and facilitate regulatory compliance.

A. Algorithms Used

- **Transaction Validation Algorithm:** The transaction validation process ensures the authenticity and correctness of submitted transactions. It begins with syntax and format verification, followed by cryptographic signature checks to confirm user identity. Double-spending prevention is enforced through balance verification, while consensus rules validate compliance with protocol logic. State transition checks ensure smart contract execution accuracy. Transactions must include gas fees to prevent network misuse. Valid transactions are broadcast to the network and queued for inclusion in a block by miners or validators [18].
- **Consensus Algorithm:** Consensus algorithms enable distributed agreement across network nodes. Nodes initialize and propose values, broadcasting them for validation. On receiving the proposal, they undergo verification based on a set of rules. Decisions are reached through repeated discussions and typically require the approval of a large majority. Finalized values are disseminated and applied for block formation or state updates. This mechanism ensures data consistency, fault tolerance, and resilience in decentralized networks [19].

- **Secure Hash Algorithm:** Blockchain systems employ the SHA-256 hash algorithm to maintain data integrity within the systems. Input messages are padded, segmented into 512-bit blocks, and processed through iterative compression functions. The output is a 256-bit hash that uniquely represents the input data. In blockchain, SHA-256 secures transaction records and block headers, ensuring immutability and non-repudiation by detecting any alteration in the data [18].

VI. SYSTEM IMPLEMENTATION SNAPSHOTS

The following section provides snapshots (Figure 2 to Figure 6) of the developed blockchain-based BlockPay system prototype, which demonstrates the critical functional modules, including transaction validation, RESTful API-based interaction, and the progressive formation of blockchain data blocks. Specifically, Figure 2 displays the transaction validation interface, incorporating real-time balance computation and associated transaction metadata. Figure 3 visualizes the dynamic account balance in USD, reflecting user-specific wallet status. Figure 4 illustrates the identity configuration mechanism via a username setup prompt. Figures 5 and 6 capture the transaction initiation and confirmation stages, wherein users specify payment details such as crypto-currency amount, source address, and supplementary message fields, followed by confirmation dialogues. Collectively, these interfaces affirm the operational feasibility, system usability, and practical realization of the proposed architectural model.

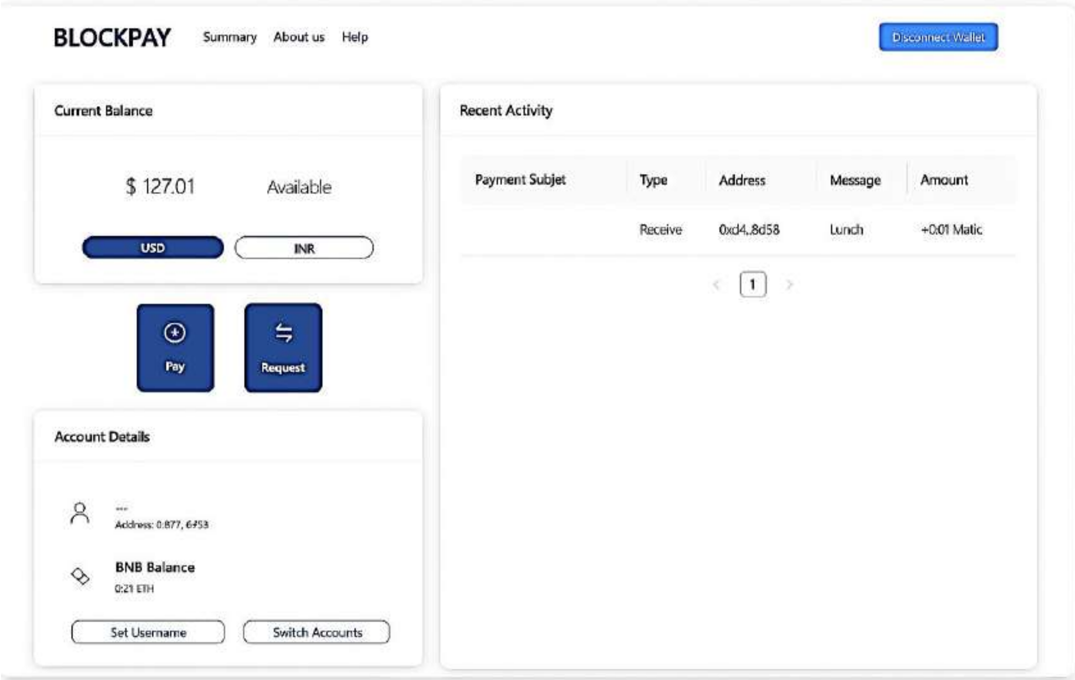

Figure 2: Current Balance in USD

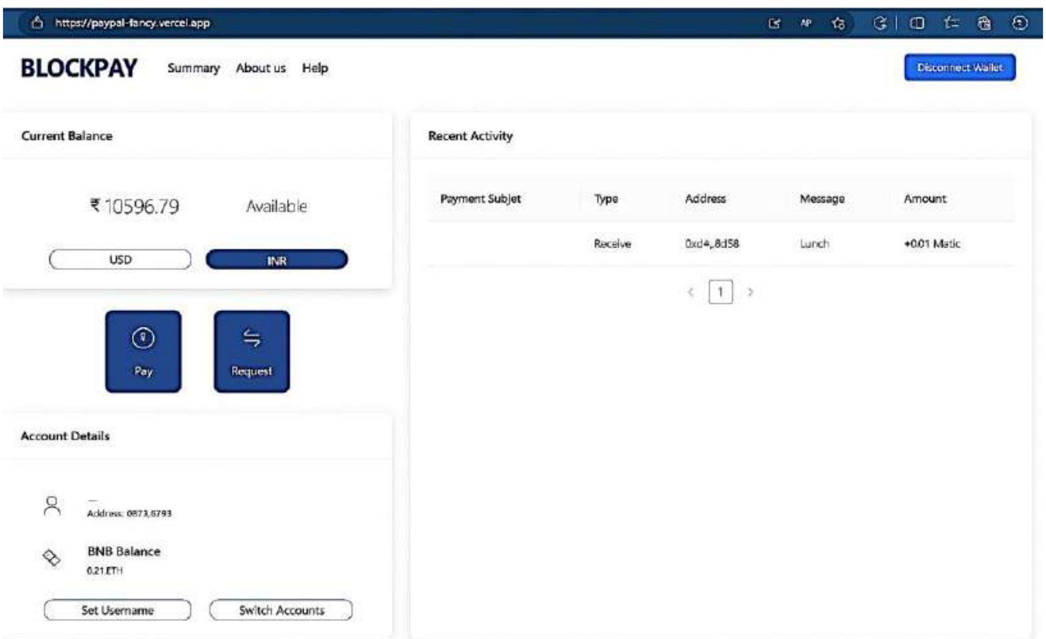

Figure 3: Native Balance indicator in INR

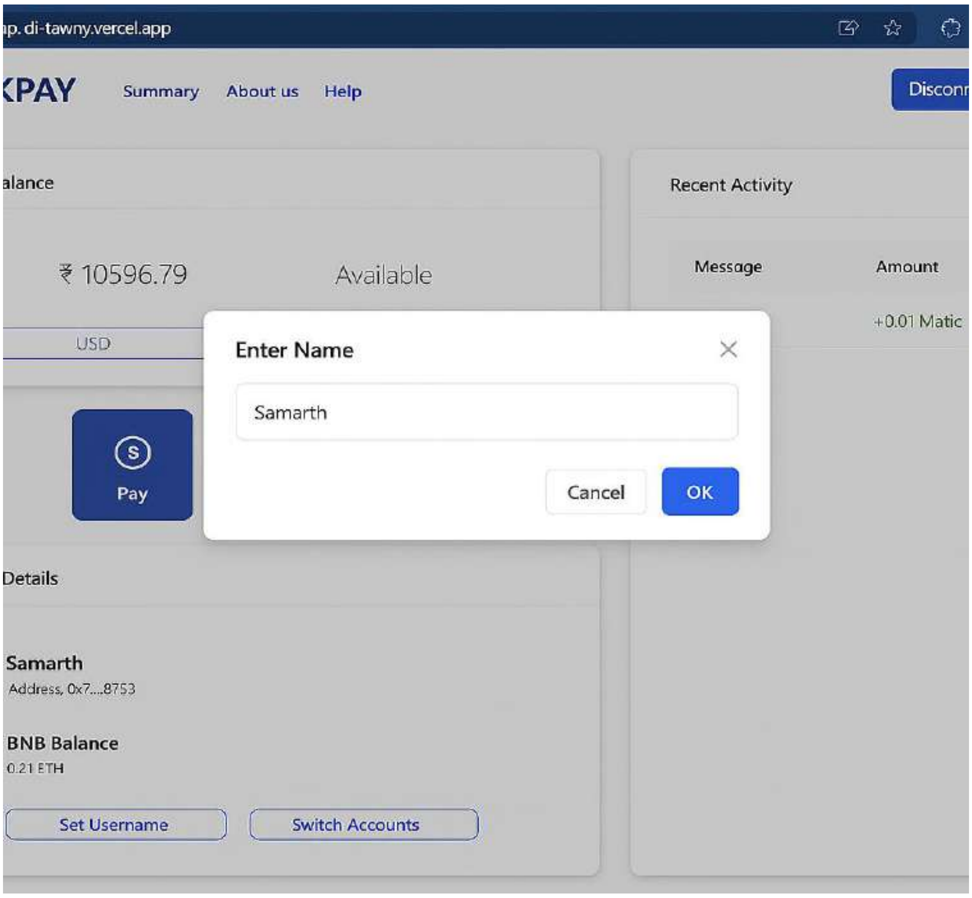

Figure 4: Set Username

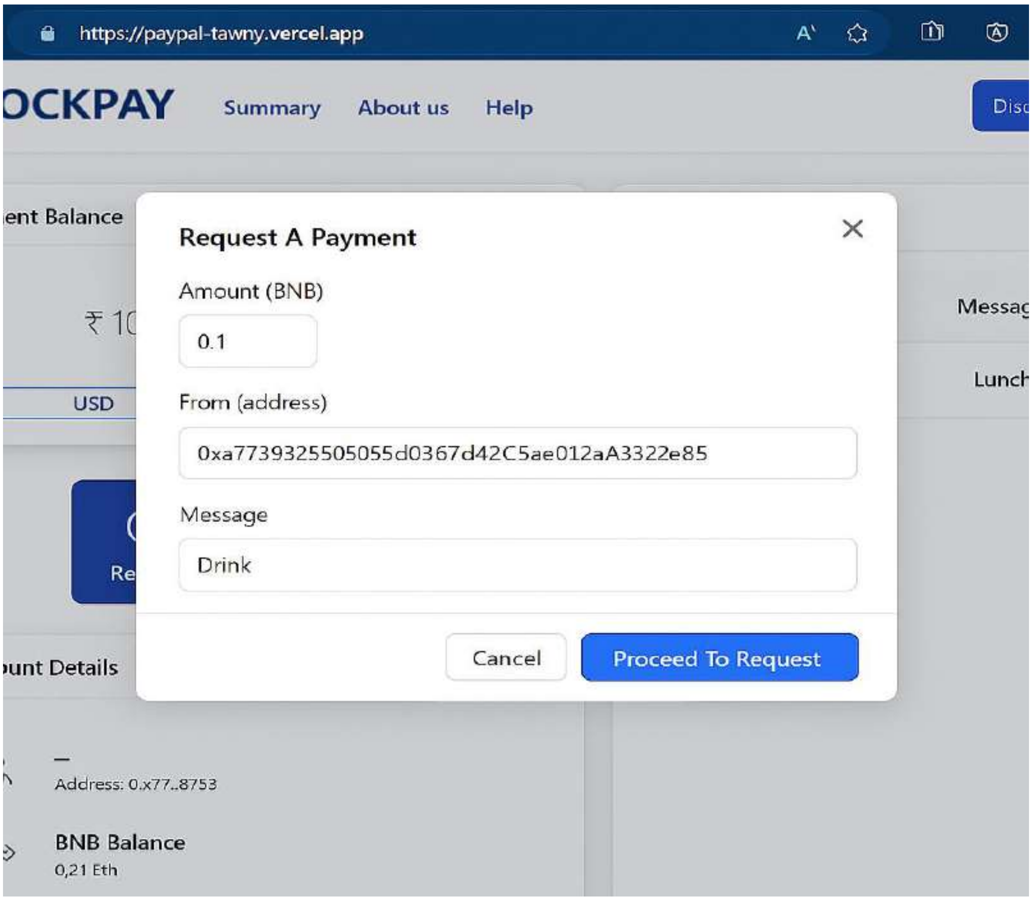

Figure 5: Request a payment from another user

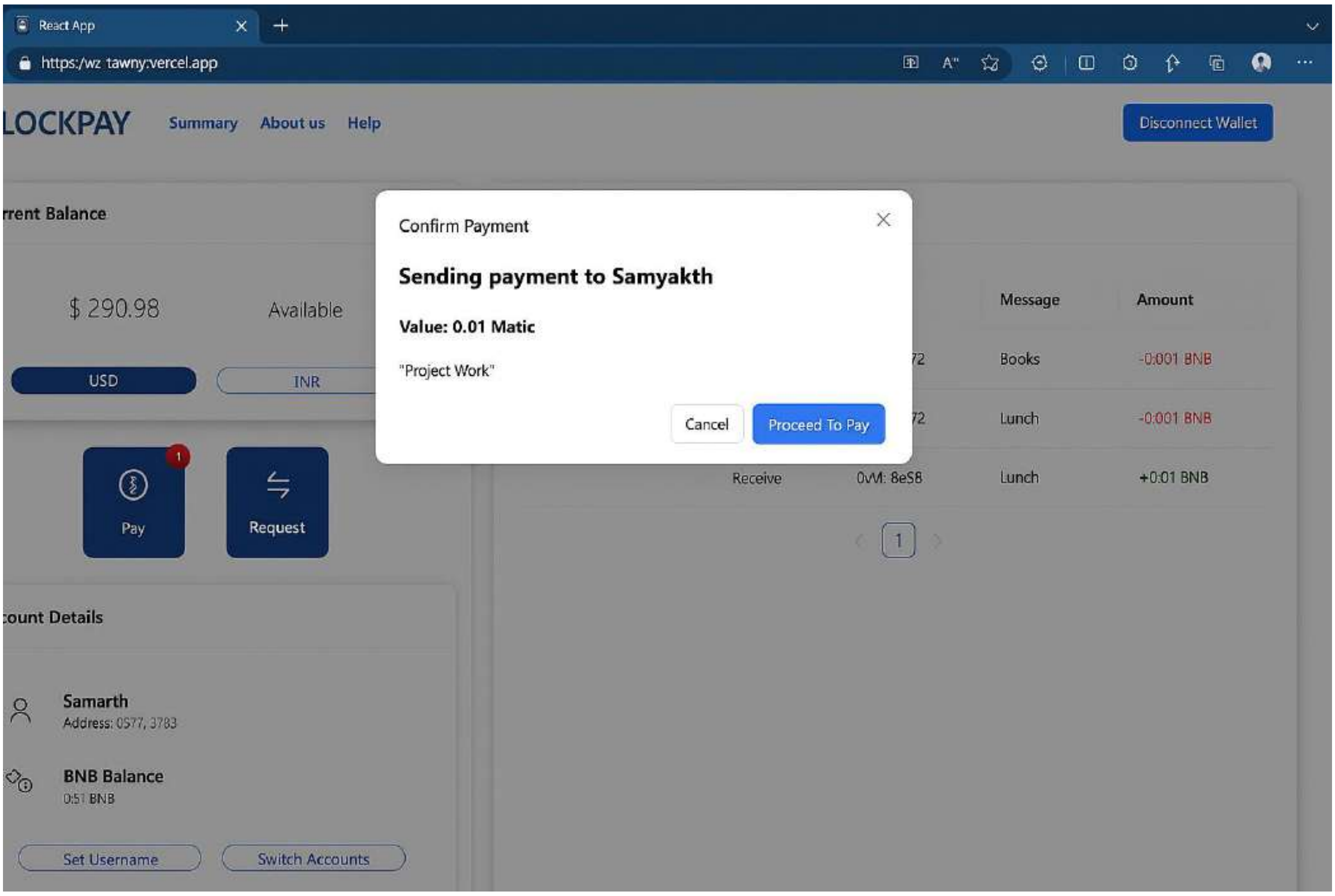

Figure 6: Paying the request made by the other user

VII. CONCLUSION

BlockPay presents a decentralized payment framework designed for smooth and secured cryptocurrency transactions. The system integrates the core blockchain functionalities, like verifiable transaction tracking, real-time balance computation, and metric visualization, within a responsive and user-centric interface developed using the React framework. Native integration with MetaMask facilitates secure authentication and direct access to users' digital assets, which eliminates the intermediary dependencies. This architecture makes the cross-border payments easier by integrating the automated conversion of cryptocurrency values into USD in real-time, which enhances the transactional transparency and eliminating the computation of manual exchange rates. The platform also maintains and displays the transaction history, which supports enhancing the traceability and user-centric analytics.BlockPay thus exemplifies a scalable and accessible solution for global digital payments, aligning blockchain principles with practical financial utility.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] S. Aumbur, N. Eyo-Udo, M. Agho, and C. Azubuike, "Implementing Blockchain for Secure and Efficient Cross-Border Payment Systems," International Journal of Research and Innovation in Applied Science, vol. IX, pp. 508-535, 2025. Available from: https://doi.org/10.51584/IJRIAS.2024.912047

[2] N. L. Eyo-Udo, M. O. Agho, E. C. Onukwulu, A. K. Sule, and C. Azubuike, "Advances in blockchain solutions for secure and efficient cross-border payment systems," International Journal of Research and Innovation in Applied Science, vol. 9, no. 12, pp. 536-563, Dec. 2024. Available from: https://doi.org/10.51584/ijrias.2024.912048.

[3] Y. Jiao, "The Impact of Blockchain Technology: Cross-Border Payments, Digital Currencies, and Financial Risks," Advances in Economics, Management and Political Sciences, 2024. Available from: https://doi.org/10.54254/2754-1169/85/20240828.

[4] S. Lin et al., "Automated Execution Algorithm for Smart Contracts in Payment Systems Based on Blockchain and Big Data," 2025. Available from: https://doi.org/10.1117/12.3055863.

[5] M. An, Q. Fan, H. Yu, and H. Zhao, "Blockchain Technology Research and Application: A Systematic Literature Review and Future Trends," Journal of Data Science and Intelligent Systems, 2023. Available from: https://doi.org/10.47852/bonviewJDSIS32021403.

[6] I. Ahmed, A. Ibrar, S. Shilpi, and M. Amjad, "Blockchain Technology: A Literature Survey," International Research Journal of Engineering and Technology, vol. 5, no. 10, pp. 1493-1498, 2020. Available from: https://www.irjet.net/archives/V5/i10/IRJET-V5I10284.pdf

[7] R. Anascavage and N. Davis, "Blockchain Technology: A Literature Review," SSRN Electronic Journal, May 3, 2018. Available from: https://doi.org/10.2139/ssrn.3173406.

[8] H. Virani and M. Kyada, "A Systematic Literature Review on Smart Contracts Security," arXiv, Dec. 9, 2022. Available from: https://doi.org/10.48550/arXiv.2212.05099.

[9] A. A. Monrat, O. Schelén, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications,

Challenges, and Opportunities," IEEE Access, vol. 7, pp. 117134-117151, 2019. Available from: https://doi.org/10.1109/ACCESS.2019.2936094.

[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. Available from: https://bitcoin.org/bitcoin.pdf

[11] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352-375, 2018. Available from: https://doi.org/10.1504/IJWGS.2018.095647.

[12] K. Bhosale and M. Waghmare, "Enhancing Blockchain Scalability Through Layer 1 and Layer 2 Solutions: A Comparative Analysis," International Journal for Science Technology and Engineering, 2025. Available from: https://doi.org/10.22214/ijraset.2025.66647.

[13] S. Dubey, "Blockchain-based Payment Systems: A Bibliometric & Network Analysis," arXiv preprint, Dec. 4, 2022. Available from: https://doi.org/10.48550/arXiv.2212.03790.

[14] R. Weerawarna, S. J. Miah, and X. Shao, "Emerging Advances of Blockchain Technology in Finance: A Content Analysis," Personal and Ubiquitous Computing, vol. 27, no. 4, pp. 1495-1508, 2023. Available from: https://doi.org/10.1007/s00779-023-01712-5.

[15] N. L. Eyo-Udo, M. O. Agho, E. C. Onukwulu, A. K. Sule, and C. Azubuike, "Advances in Blockchain Solutions for Secure and Efficient Cross-Border Payment Systems," International Journal of Research and Innovation in Applied Science, vol. 9, no. 12, pp. 536-563, 2024. Available from: https://doi.org/10.51584/ijrias.2024.912048.

[16] N. Gafarov, "The Role of Blockchain in Securing Financial Transactions," 2024. Available from: https://doi.org/10.62802/2ad9q749.

[17] M. Wohrer, U. Zdun, and S. Rinderle-Ma, "Architecture Design of Blockchain-Based Applications," in 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2021. Available from: https://doi.org/10.1109/BRAINS52497.2021.9569813.

[18] S. Bhatnagar et al., "Block-Hash Signature (BHS) for Transaction Validation in Smart Contracts for Security and Privacy Using Blockchain," Journal of Mobile Multimedia, vol. 19, no. 4, 2023. Available from: https://doi.org/10.13052/jmm1550-4646.1941.

[19] A. Imteaj, M. H. Amini, and P. M. Pardalos, "Toward Smart Contract and Consensus Mechanisms of Blockchain," in Blockchain for Distributed Systems Security, pp. 13-31, Springer, 2021. Available from: https://doi.org/10.1007/978-3-030-75025-1_2

ABOUT THE AUTHORS

Mr. Prasad S. R. received his B.E. degree in Computer Science and Engineering from Visvesvaraya Technological University (VTU), Belagavi, in 2011, and his M.Tech. degree from Jawaharlal Nehru Technological University (JNTU), Hyderabad, in 2015. He is currently serving as an Assistant Professor in the Department of Computer Science and Engineering at SDM Institute of Technology, Ujire. His research interests include Deep Learning, the Internet of Things (IoT), and Artificial Intelligence (AI).

Ms. Deepali received her B.E. degree in Computer Science and Engineering from Visvesvaraya Technological University (VTU), Belagavi. Her areas of interest include Deep Learning, the Internet of Things (IoT), and Artificial Intelligence (AI). She was a student in the Department of Computer Science and Engineering at SDM Institute of Technology, Ujire.

Mr. Samarth Jain received his B.E. degree in Computer Science and Engineering from Visvesvaraya Technological University (VTU), Belagavi. His areas of interest include Deep Learning, the Internet of Things (IoT), and Artificial Intelligence (AI). He was a student in the Department of Computer Science and Engineering at SDM Institute of Technology, Ujire.

Mr. Samyakth Kumar received his B.E. degree in Computer Science and Engineering from Visvesvaraya Technological University (VTU), Belagavi. His areas of interest include Deep Learning, the Internet of Things (IoT), and Artificial Intelligence (AI). He was a student in the Department of Computer Science and Engineering at SDM Institute of Technology, Ujire.

Mr. Sudeep D Gowda received his B.E. degree in Computer Science and Engineering from Visvesvaraya Technological University (VTU), Belagavi. His areas of interest include Deep Learning, the Internet of Things (IoT), and Artificial Intelligence (AI). He was a student in the Department of Computer Science and Engineering at SDM Institute of Technology, Ujire.