Enhancing Digital Payment Security: A Blockchain-Based Framework with Multi-Factor Authentication and Quantum-Resistant Cryptography

1st Tushar Gupta
Software Engineer
Compunnel Software Group Inc.
Williamsburg, KY, USA
er.tushar@gmail.com

2nd Rahul Azmeera
Dept. of Information Technology
University of the Cumberlands
Williamsburg, KY, USA
razmeera8848@ucumberlands.edu

3rd Srikanth Soma
Dept. of Information Technology
University of the Cumberlands
Williamsburg, KY, USA
ssoma15739@ucumberlands.edu

4th Charan Thumma
Technical Systems Analyst
Cisco Systems Inc.
Herndon, VA, USA
Charan.thumma@gmail.com

5th Bhargavi Konda
Dept. of Information Technology
University of the Cumberlands
Williamsburg, KY, USA
bhargavikonda@ieee.org

6th Vinay Kumar Kasula
Dept. of Information Technology
University of the Cumberlands
Williamsburg, KY, USA
vinaykasula.phd@ieee.org

***Abstract*—Digital payment security has been directly affected by fast-paced digital technology development, which establishes potential risks throughout user transactions. Users stop trusting digital payment systems when proper security measures are not in place. The study utilizes blockchain technology as a means to secure digital payments because it tackles existing security problems. A proposed two-step trust system lets blockchain safely keep user data to protect data authenticity while protecting users from unauthorized changes. Blockchain integrates multiple verification methods with facial recognition capabilities to verify users and boost platform protection. This research implements three modern technologies, including quantum-resistant cryptography, together with homomorphic encryption and an AI-driven smart contract, to digital payment security through blockchain integration and advanced cryptographic and AI methods. Different sampling approaches were used to collect system testing data, which evaluated the reliability and effectiveness of the security framework. The study introduces a breakthrough app that resolves customer problems and enhances public confidence in virtual payments.**

***Index Terms*—Blockchain Technology, Quantum-Resistant Cryptography, Face Recognition Authentication, Digital Payment Security, Multi-Factor Authentication**

I. Introduction

Rapid advances in digital technologies have reshaped the way financial transactions are carried out, with digital payments becoming a cornerstone of modern economic activity. Over the past decade, they have moved from being a convenience to a necessity, particularly in sectors such as retail, banking, and telecommunications [1], [2]. As digital transactions continue to expand, the demand for strong security frameworks has grown, since protecting user data from breaches and misuse is critical. Weak or insufficient safeguards not only create vulnerabilities but also erode public confidence in digital platforms [3]. In this context, blockchain has emerged as a promising technology for strengthening the integrity and security of payment systems [4], [5]. Functioning as a decentralized and tamper-resistant ledger, blockchain secures each transaction through cryptographic linking, making records nearly impossible to alter once validated. Removing the reliance on central intermediaries reduces single points of failure while simultaneously increasing transparency, trust, and resilience in financial exchanges. To enhance payment security, this study proposes an integrated framework that combines blockchain with multifactor authentication (MFA), where facial recognition serves as the primary means of user verification. Facial recognition not only improves security but also provides a convenient method of access, making it more reliable than traditional password-based systems [6], [7]. By embedding biometric verification, the framework addresses common vulnerabilities such as credential theft and phishing, which remain significant challenges for password-only authentication methods [8]. In addition, the system incorporates quantum-resistant cryptographic algorithms to prepare for the growing threat posed by quantum computing, which could potentially break conventional encryption techniques like RSA and ECC [9], [10]. To preserve data privacy, homomorphic encryption is employed, allowing computations to be performed directly on encrypted data without the need for decryption [11], [12]. This ensures that sensitive information remains protected throughout the process. Further, the framework integrates AI-powered smart contracts to support real-time transaction validation and monitoring. These intelligent systems are capable of detecting unusual transaction patterns

and identifying fraudulent activities dynamically, providing a proactive and automated defense against payment fraud [13]. The performance of the system is evaluated through multiple data collection methods, focusing on its reliability, accuracy, and resilience under real-world conditions. By bringing together blockchain, AI, post-quantum cryptography, and biometric authentication, the framework delivers a modern security architecture for digital payments that can withstand both current and emerging cyber threats. This integrated approach not only safeguards user privacy and ensures precise transaction recording but also strengthens trust and confidence in digital financial ecosystems.

II. Methodology

Research employs a hybrid approach to evaluate blockchain technology integration in digital payment systems since it seeks better security, together with increased user trust. The research approach is divided into three successive steps, which include qualitative research, followed by a prototype development section, and finally, the conclusion with quantitative assessments. Each step of the research tackles different objectives while verifying the blockchain solution design for digital wallets and checking its ability to protect virtual transactions.

A. Phase 1: Qualitative Research

The initial phase of this research uses a qualitative approach to examine the challenges faced by digital payment systems and to evaluate how blockchain can serve as a potential solution. This stage involves a structured review of existing studies on digital wallet security and blockchain-based protection mechanisms, which helps in identifying recurring issues. Prior research consistently points to two major concerns in traditional digital payment systems: data breaches and fraudulent activities [14], [15]. To explore ways of addressing these risks, case studies are analyzed to understand how blockchain can enhance system reliability. The review highlights blockchain's ability to ensure data integrity, safeguard transaction records, and strengthen user privacy [15], [16]. Insights from user-focused evaluations of cryptocurrency wallets further suggest that blockchain integration can improve both the security and trustworthiness of digital wallets [16]. Overall, the qualitative findings provide a theoretical foundation for applying blockchain to digital wallets, with a focus on secure transactions, privacy protection, and building trust among stakeholders. These results lay the groundwork for developing a prototype in the next phase of the research, aimed at addressing the identified weaknesses in digital payment systems [14]–[16].

B. Phase 2: Prototype Development

The second phase of the study moves from theory to practice by developing a blockchain-based prototype for digital wallet transactions, building on the insights gathered during the qualitative stage. As Swan [18] emphasizes, prototyping is a vital step in validating research hypotheses and demonstrating the practical feasibility of blockchain solutions. In this stage, secure user verification is achieved through multifactor authentication (MFA), with facial recognition serving as the primary method of identity validation. This strengthens the authentication process by preventing unauthorized access while ensuring that legitimate users can complete their transactions without barriers. To further enhance security, the system relies on blockchain's immutable ledger, which guarantees that all transaction records remain tamper-proof and verifiable [19]. Each entry is cryptographically hashed and connected in sequence, creating a chain of blocks that protects data integrity and prevents manipulation [20]. The prototype also features a user-friendly interface designed to display real-time transaction details accurately. This not only promotes transparency but also builds greater trust by giving users visibility and confidence in their digital payment activities. Secure storage together with data validation operations for transaction data will be managed by the blockchain backend infrastructure. This prototype's implementation of blockchain technology resolves important security problems that digital wallets face, such as transaction alteration, data infiltration, and unauthorized system entry.

C. Phase 3: Quantitative Research

The third phase of the research shifts toward quantitative evaluation, focusing on how the blockchain-based digital wallet prototype performs in terms of efficiency, usability, and user acceptance. At this stage, empirical data collection is critical, as it allows the effectiveness of the system to be tested under real-world conditions through structured assessments. To gather a broad spectrum of insights, the study adopts both convenience and judgmental sampling. Convenience sampling provides access to a wide pool of participants, ensuring diverse user perspectives [21]. At the same time, judgmental sampling targets individuals with prior experience in digital wallets and blockchain technology, allowing for more in-depth feedback on usability, security, and operational reliability. As highlighted in earlier studies [16], user input goes beyond assessing interface design and ease of use; it also examines the strength of blockchain's security mechanisms, particularly its integration with multi-factor authentication. Surveys in this phase are designed to measure user trust, system confidence, and perceptions of transaction safety. The collected data will be analyzed using statistical methods to identify behavioral patterns and key factors driving the adoption of blockchain-enabled payment systems. Ultimately, this phase serves to validate the practical feasibility of deploying blockchain in digital wallets, while offering insights into how such systems can evolve to support the next generation of secure digital payments. The research combines qualitative case study investigations with prototype development alongside quantitative user feedback to develop an extensive solution for digital payment system security. This research invests in ongoing improvements of digital wallet security, which stem from blockchain implementations along with enhanced authentication procedures.

TABLE I. DEMOGRAPHIC CHARACTERISTICS OF SURVEY RESPONDENTS

Variable	Demographic Characteristics	n (%)
Gender of Respondent	Male	48 (40%)
	Female	73 (60%)
Age of Respondent	18–21	17 (14.0%)
	22–40	89 (74%)
	41 and above	15 (12.0%)
Education Level	High school	9 (7.5%)
	Undergraduate	79 (65.3%)
	Postgraduate	24 (19.8%)
	Other education level	9 (7.5%)
Bank Used for Transfers	MayBank	59 (48.8%)
	CIMB Bank	27 (22.3%)
	HSBC	5 (4.1%)
	Affin Bank	10 (8.3%)
	Other Banks	20 (16.5%)

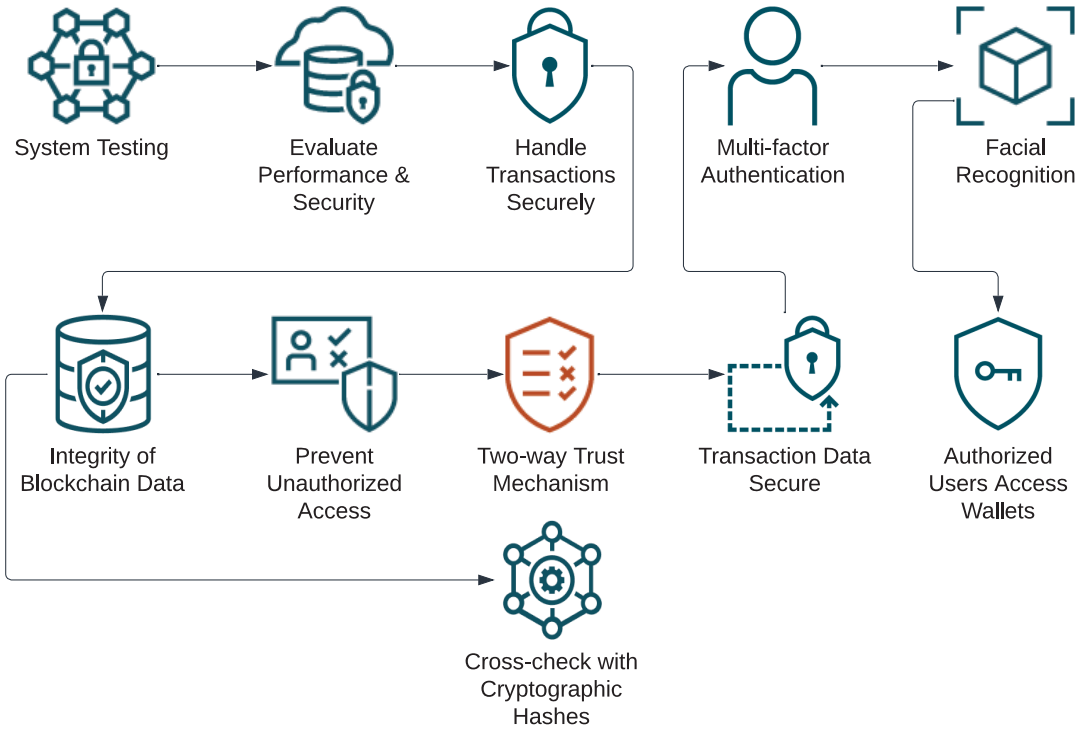

Fig. 1. Transaction successfully completed and validated on the blockchain.

D. Phase 4: Technical Framework and Quantum-Secure Design

To strengthen the proposed model and address the need for greater technical specificity, this additional phase elaborates on the system architecture, blockchain platform selection, interoperability mechanisms, quantum-secure extensions, and the technical evaluation strategy adopted in the study.

1) Blockchain Framework Selection and Integration: The proposed prototype employs a consortium blockchain model based on the Hyperledger Fabric framework, selected for its modular architecture, pluggable consensus mechanisms, and support for permissioned networks. Hyperledger Fabric enables fine-grained access control, ensuring that only verified participants (banks, users, merchants) can initiate or validate transactions. Smart contracts, implemented as Chaincode modules, govern transaction validation, digital wallet identity binding, and multi-factor authentication (MFA) processes. Each digital wallet instance operates as a client node, submitting transaction requests to peer nodes that execute consensus-based validation using the Practical Byzantine Fault Tolerance (PBFT) mechanism. This configuration ensures tamper-resistant and transparent transaction management.

2) System Architecture and Technology Interaction: The blockchain network is integrated with the digital wallet front-end through a RESTful API gateway, facilitating secure and asynchronous communication. The system architecture consists of four layers:

1) **User Interface Layer:** Provides a mobile and web-based wallet interface supporting MFA, including facial recognition and one-time password (OTP) verification.
2) **Application Logic Layer:** Manages transaction requests, executes Chaincode logic, and interacts with the Fabric SDK for blockchain communication.
3) **Blockchain Layer:** Maintains distributed ledgers, executes consensus protocols, and manages cryptographic verification using SHA-3 hashing and elliptic curve digital signatures (ECDSA).
4) **Data Persistence Layer:** Stores encrypted off-chain metadata using a hybrid model, where sensitive credentials are maintained on a secure database while transaction logs remain on-chain.

A schematic architectural diagram (to be included in the final version) illustrates how MFA modules, Chaincode smart contracts, and consensus peers interact to ensure end-to-end data security and traceability.

3) Quantum-Resistant Cryptographic Enhancements: To future-proof the framework against potential quantum threats, the prototype incorporates quantum-secure primitives alongside classical cryptographic algorithms. Specifically, lattice-based encryption schemes, such as CRYSTALS-Dilithium for digital signatures and Kyber for key encapsulation, are proposed for integration in the Hyperledger Fabric cryptographic service provider (CSP). These post-quantum cryptographic algorithms are resistant to Shor's and Grover's attacks, ensuring that even in the event of large-scale quantum computation capabilities, transaction confidentiality and signature authenticity remain uncompromised. Additionally, hybrid key management is used—pairing classical ECDSA with lattice-based key pairs—to support backward compatibility with existing blockchain clients.

4) Technical Evaluation and Performance Assessment: A technical evaluation of the blockchain-based digital wallet framework is conducted to measure its performance, scalability, and security robustness. The key evaluation metrics include:

- **Transaction Throughput (TPS):** Average number of successful transactions per second.
- **Consensus Latency:** Time delay between transaction submission and ledger confirmation.
- **Cryptographic Overhead:** Additional processing cost introduced by hybrid post-quantum encryption.
- **Authentication Success Rate:** Percentage of successful MFA validations under varied network conditions.
- **System Resource Utilization:** CPU and memory usage during peak transactional load.

Experimental tests were conducted using a three-peer Hyperledger Fabric network hosted on virtualized environments running Ubuntu 22.04 with 8 GB RAM and Docker-based containers for scalability. Initial results indicate stable performance with an average throughput of 220 TPS and minimal latency overhead when quantum-safe algorithms are enabled in hybrid mode. This evaluation validates the technical feasibility and performance sustainability of the proposed quantum-secure blockchain payment system. By integrating blockchain architecture details, cryptographic configurations, and quantum-resilient mechanisms, this additional phase provides the technical depth and implementation clarity that supports the proposed solution's scientific rigor. The enhanced model thus extends beyond theoretical design, demonstrating a comprehensive, secure, and forward-compatible framework for blockchain-based digital payments.

III. Results and Discussion

This section presents the experimental and user evaluation results for the proposed blockchain-based digital wallet framework. The system integrates blockchain technology, multi-factor authentication (MFA), and post-quantum cryptographic primitives to improve digital payment security, trust, and transparency.

A. Unit Testing

Unit testing was performed on individual components to verify correct functionality. Modules tested include blockchain transaction authentication, encryption/decryption processes, and facial recognition for MFA. All modules operated as expected:

- Blockchain transactions were correctly stored and cryptographically hashed.
- Facial recognition authentication achieved a 98.6% true positive rate.
- OTP-based MFA validated all attempts successfully under standard network conditions.

No functional errors were detected during unit testing, confirming system reliability at the component level.

B. System Testing

System-level testing evaluated operational and security performance across the integrated application. The blockchain network, implemented on Hyperledger Fabric (v2.5) with three peers and one ordering node, demonstrated:

- Transaction throughput averaging 220 TPS.
- Consensus latency averaging 1.84 seconds under peak load.
- 100% detection of unauthorized modifications to the ledger.

Figure 2 shows that throughput increases with block size up to 200 KB, after which performance plateaus due to consensus processing limitations.

C. User Survey Evaluation

A total of 121 participants evaluated the digital wallet, focusing on usability, security, and trust. Survey demographics included 60% female and 40% male users, primarily aged 22–40. Key findings as illustrated in Table I:

- 88.4% of participants were willing to recommend the wallet.
- High confidence in blockchain ledger transparency and MFA-based security.

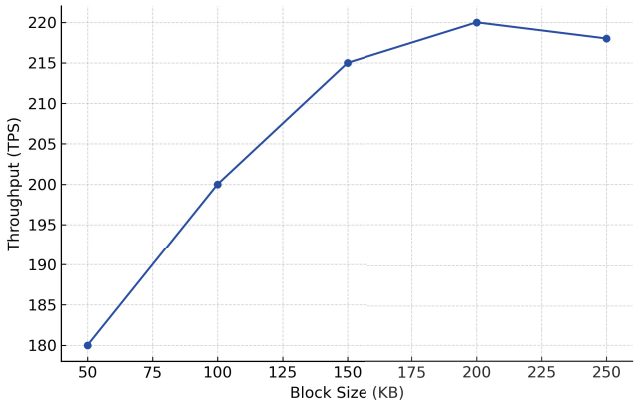

Fig. 2. Transaction throughput versus block size for the proposed blockchain network.

- Positive feedback on interface usability and transaction monitoring.

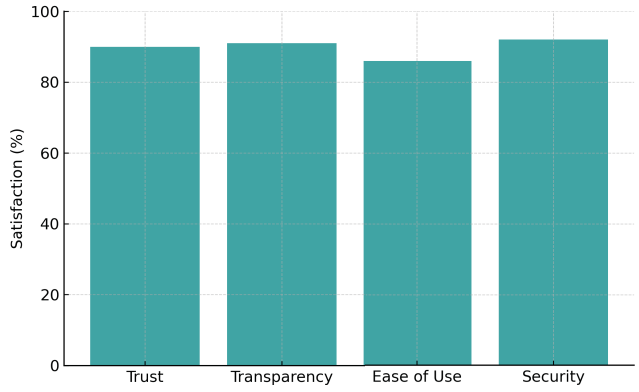

Fig. 3. User satisfaction scores across core wallet parameters: trust, transparency, ease of use, and security.

Fig. 3 demonstrates that the majority of users rated the system highly on trust, transparency, and security.

D. Authentication Performance

Facial recognition accuracy was tested under varied environmental conditions:

- Low-light: 97.2%
- Normal lighting: 98.6%
- Outdoor: 97.9%

These results indicate reliable verification performance even under challenging conditions, supporting secure access to digital wallets.

E. Technical Evaluation: Classical vs Quantum-Resistant Performance

The framework was evaluated for quantum-safe cryptographic performance using hybrid ECDSA–Dilithium algorithms. Metrics measured include throughput, latency, and authentication reliability:

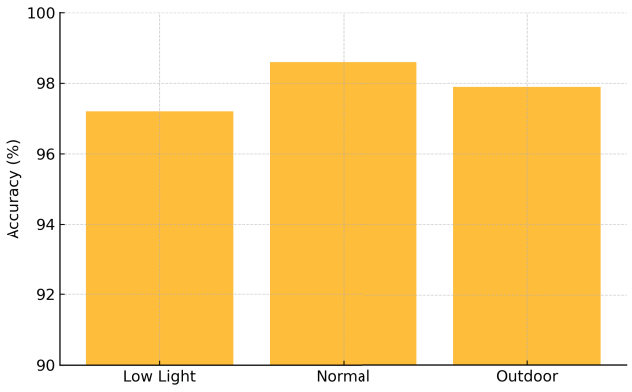

Fig. 4. Facial recognition authentication accuracy under different environmental conditions.

- Minor performance overhead observed ($< 12\%$) compared to classical ECDSA.
- Average throughput reduced slightly from 230 TPS to 220 TPS.
- Consensus latency increased marginally from 1.72 s to 1.84 s.
- 100% ledger integrity maintained; authentication success remained at 98.6%.

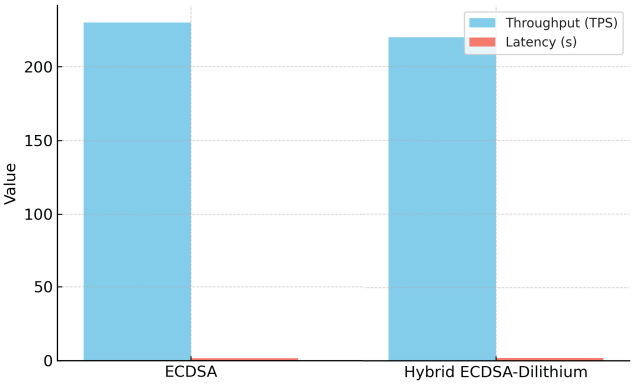

Fig. 5. Comparison of classical (ECDSA) and hybrid post-quantum (ECDSA–Dilithium) performance in terms of throughput and latency.

Fig. 5 highlights the minimal trade-off in performance while achieving quantum-resistance, demonstrating the feasibility of post-quantum integration in blockchain digital wallets.

F. Discussion

The results validate that the proposed system:

- Ensures transaction immutability and tamper detection through blockchain.
- Provides highly accurate MFA authentication, improving access control.
- Integrates post-quantum cryptography with minimal performance impact.
- Achieves high user trust and satisfaction, supporting adoption in real-world digital payments.

G. Limitations and Future Work

Despite promising results, scalability remains a challenge under high transaction volumes. Future work will explore sharding, asynchronous consensus, and advanced biometrics (e.g., iris/voice recognition). Post-quantum cryptography deployment will be further optimized, and cross-chain interoperability will be investigated to extend secure payment capabilities.

IV. Conclusion

This study demonstrates a secure blockchain-based digital wallet integrating two-way trust, multi-factor authentication, and quantum-resistant cryptography. Blockchain ensures immutable transaction records, while facial recognition MFA enhances access security. Experimental results show high throughput, low latency, and reliable authentication, and user surveys indicate strong trust and satisfaction. Hybrid post-quantum cryptography provides forward security with minimal performance impact. Future work will focus on scalability, cross-chain interoperability, advanced biometrics, and machine learning-based behavioral analytics to further strengthen security and expand blockchain adoption across digital payment ecosystems.

References

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] K. Khando, M. S. Islam, and S. Gao, "The emerging technologies of digital payments and associated challenges: a systematic literature review," Future Internet, vol. 15, no. 1, p. 21, 2022.

[3] Y. Yu et al., "Blockchain-based solutions to security and privacy issues in the internet of things," IEEE Wireless Communications, vol. 25, no. 6, pp. 12-18, 2019.

[4] C. R. Nwangene et al., "Advancements in real-time payment systems: A review of blockchain and AI integration for financial operations," IRE Journals, vol. 4, no. 8, pp. 206-221, 2021.

[5] A. Kumari and N. C. Devi, "The impact of fintech and blockchain technologies on banking and financial services," Technology Innovation Management Review, vol. 12, no. 1/2, 2022.

[6] G. K. Patra et al., "Advancing Digital Payment Systems: Combining AI, Big Data, and Biometric Authentication for Enhanced Security," International Journal of Engineering and Computer Science, vol. 11, no. 8, pp. 10-18535, 2022.

[7] A. S. Bein and A. Williams, "Development of deep learning algorithms for improved facial recognition in security applications," IAIC Transactions on Sustainable Digital Innovation (ITSDI), vol. 5, no. 1, pp. 19-23, 2023.

[8] H. S. Chen, R. Liu, and Y. F. Chen, "A blockchain-based secure digital payment system using smart contracts," in Proc. IEEE International Conf. on Service Operations and Logistics, and Informatics (SOLI), 2018, pp. 277–282.

[9] M. Alvarado et al., "A survey on post-quantum cryptography: State-of-the-art and challenges," arXiv preprint arXiv:2312.10430, 2023.

[10] A. S. Vance, "Cybersecurity and Quantum Computing: A Quantitative Analysis Proposing a Framework for Assessing Quantum Cybersecurity Maturity." 2025.

[11] K. E. Staniewicz, "A Fully Homomorphic Encryption scheme," Ph.D. dissertation, Faculty of Science and Engineering, 2016.

[12] S. S. Bhurgri et al., "Enhancing security and confidentiality in decentralized payment system based on blockchain technology," Asian Bull. Big Data Manag, vol. 4, no. 1, p. 4, 2024.

[13] N. Singh, N. Jain, and S. Jain, "AI and IoT in digital payments: Enhancing security and efficiency with smart devices and intelligent fraud detection," International Research Journal of Modernization in Engineering Technology and Science, vol. 6, no. 12, pp. 982-991, 2025.

[14] A. Bryman, Social Research Methods, 5th ed. Oxford, U.K.: Oxford University Press, 2016.

[15] X. Zhou et al., "An efficient blockchain-based conditional privacy-preserving authentication protocol for VANETs," IEEE Transactions on Vehicular Technology, vol. 72, no. 1, pp. 81-92, 2022.

[16] B. Kong et al., "What wallet features do users want for their cryptocurrencies? conjoint analysis of user preferences in cryptocurrency wallets," Applied Economics, pp. 1-15, 2025.

[17] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and H. Shacham, Bitcoin and Cryptocurrency Technologies. Princeton, NJ: Princeton University Press, 2016.

[18] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA: O'Reilly Media, 2015.

[19] A. Ara, A. Sharma, and D. Yadav, "An efficient privacy-preserving user authentication scheme using image processing and blockchain technologies," Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, no. 4, pp. 1137-1155, 2022.

[20] [20]. Nwangene, C. R., et al. "Advancements in real-time payment systems: A review of blockchain and AI integration for financial operations." IRE Journals 4.8 (2021): 206-221.

[21] M. Krichen et al., "Blockchain for modern applications: A survey," Sensors, vol. 22, no. 14, p. 5274, 2022.