2026 Volume: 02 Issue: 05 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-12

A COMPREHENSIVE SURVEY OF BLOCKCHAIN-DRIVEN DIGITAL ASSET EXCHANGE PLATFORM

Dr. Ramya B. N.*[1], Prajwal R.[2], Pranav V. Bajikar[3], Prasad R.[4], Rajeshwar S.[5]

[1]Associate Professor, Department of CSE, Jyothy Institute of Technology Bangalore, India.

[2,3,4,5]BE, CSE Department of CSE, Jyothy Institute of Technology Bangalore, India.

Article Received: 08 April 2026
Article Revised: 28 April 2026
Published on: 18 May 2026

***Corresponding Author: Dr. Ramya B. N.**
Associate Professor, Department of CSE, Jyothy Institute of Technology Bangalore, India.

DOI: https://doi-doi.org/101555/ijrpa.2716

ABSTRACT

Digital asset management and secure transaction handling have become critical challenges in the growing field of blockchain and decentralized finance. Existing systems such as crypto wallets, transaction platforms, and monitoring tools operate independently, forcing users to rely on multiple solutions without unified security or intelligent decision-making support. This project proposes an AI Smart Vault system that integrates blockchain-based asset management, multi-signature authentication, and AI-driven risk analysis into a single platform. The system evaluates transaction patterns such as amount, frequency, and user behavior to dynamically adjust approval requirements and detect suspicious activities. By combining decentralized security with intelligent analysis, the proposed system enhances transaction reliability, improves user control, and provides a scalable and secure solution for modern digital asset management.

KEYWORDS: Blockchain, Smart Contracts, Multi-Signature Authentication, AI Risk Analysis, Digital Asset Management, Ethereum, Decentralized Security, Transaction Monitoring, Cryptographic Authentication, Fraud Detection

1 INTRODUCTION

The rapid expansion of blockchain technology and the increasing adoption of digital assets have significantly transformed the way individuals and organizations manage and transfer financial resources. However, with this growth comes major challenges related to security, unauthorized access, and lack of intelligent monitoring. Users often rely on traditional cryptocurrency wallets and transaction platforms that provide basic functionality but fail to

offer advanced security mechanisms or adaptive decision-making capabilities.

Currently, digital asset management solutions are highly fragmented. Wallets handle transactions, separate platforms monitor suspicious activities, and multi-signature systems provide enhanced security, but these components operate independently. As a result, users are forced to interact with multiple systems to achieve complete control over their assets, leading to inefficiency and increased risk. This lack of integration limits the effectiveness of each component and creates gaps in security and usability.

Another critical issue is the absence of intelligent systems that can analyze transaction behavior in real time. Existing solutions do not adapt based on transaction patterns such as frequency, amount, or user behavior. This makes it difficult to detect potentially risky transactions before execution. Additionally, traditional multi-signature wallets enforce static approval rules without considering the dynamic risk level of transactions, which reduces their overall effectiveness.

To address these challenges, this project proposes an AI Smart Vault system that integrates blockchain-based asset management, multi-signature authentication, and AI-driven risk analysis into a unified platform. The system dynamically evaluates transaction risk and adjusts approval requirements accordingly, ensuring higher security and better control. By combining decentralized security with intelligent analysis, the proposed solution enhances reliability, reduces fraud risk, and provides a scalable and efficient approach to digital asset management.

This project studies 11 recent research works and surveys that collectively address various aspects of blockchain-based asset management, multi-signature security, and AI-driven monitoring systems. It analyzes their methodologies, evaluates their contributions, and identifies critical limitations that remain unresolved in current solutions. The study is organized as follows: Section 2 discusses the evolution of digital asset management systems through blockchain technology; Section 3 describes the core components of the proposed AI Smart Vault system; Section 4 focuses on safety features and AI-based monitoring; Section 5 presents a comparative analysis of existing systems; Section 6 identifies research gaps; Section 7 outlines future enhancements and scope; and Section 8 concludes the project.

2 Evolution of Systems

2.1 Traditional Approaches

Early digital asset management systems relied heavily on centralized financial institutions and custodial services to store and manage assets. Users depended on banks or centralized exchanges to perform transactions, maintain records, and enforce security. While these systems provided convenience, they introduced significant risks such as single points of failure, lack of transparency, and vulnerability to cyberattacks.

With the introduction of cryptocurrencies, basic digital wallets emerged to allow users to store and transfer assets independently. However, these wallets offered limited security features, typically relying on private keys without additional safeguards. If a key was lost or compromised, the assets became irrecoverable. Furthermore, traditional transaction systems lacked mechanisms for monitoring suspicious activities or preventing fraudulent transfers.

2.2 Blockchain-Based Systems

The adoption of blockchain technology marked a major shift toward decentralized asset management. Blockchain introduced immutable ledgers, ensuring that transactions are transparent, verifiable, and tamper-resistant. Platforms like Ethereum enabled the use of smart contracts, which automate transaction execution based on predefined rules.

Multi-signature wallets were developed to enhance security by requiring multiple approvals before executing a transaction. This reduced the risk of unauthorized access and provided shared control over assets. However, these systems still relied on static rules, where the number of approvals remained fixed regardless of transaction context. They lacked the ability to adapt based on risk levels or user behavior.

2.3 Smart Contract-Based Systems

The Smart contracts enabled programmable asset management, allowing developers to define custom rules for transaction execution, ownership, and access control. These systems improved automation and reduced the need for intermediaries, making transactions faster and more efficient.

Despite these advancements, smart contract-based systems often focused only on execution logic and did not incorporate intelligent monitoring or decision-making. Security depended entirely on predefined conditions, and any vulnerability in the contract code could lead to

significant losses. Additionally, these systems did not analyze transaction patterns or detect anomalies in real time.

2.4 AI Integrated Monitoring Systems

The integration of artificial intelligence introduced a new layer of intelligence in financial and asset management systems. AI-based models began to analyze transaction patterns, detect anomalies, and identify potential fraud using techniques such as machine learning and behavioral analysis.

Modern systems utilize features like transaction frequency, amount patterns, and user activity history to evaluate risk. However, most AI-based monitoring systems operate separately from blockchain execution systems. While they can detect suspicious activity, they often cannot directly influence or prevent transactions, limiting their effectiveness in real-time security enforcement.

2.5 Towards Intelligent Integrated Systems

Recent advancements focus on combining blockchain security with AI-driven decision-making to create more adaptive and intelligent systems. The goal is to move beyond static security mechanisms and introduce dynamic controls that adjust based on transaction risk.

This evolution highlights the need for an integrated approach where decentralized asset management, multi-signature authentication, and AI-based risk analysis work together. Such systems can provide enhanced security, real-time monitoring, and improved usability, forming the foundation for next-generation digital asset management solutions like the proposed AI Smart Vault.

3 System Components

3.1 Authentication and Access Control Module

Authentication in blockchain-based systems relies on cryptographic techniques rather than traditional password-based mechanisms. Digital signature-based authentication ensures secure identity verification without storing sensitive credentials centrally, thereby reducing risks such as data breaches and unauthorized access [3], [7]. This decentralized approach aligns with secure system design principles and enhances trust in distributed environments.

In addition, role-based access control mechanisms are implemented to regulate system

interaction among different users such as vault owners and authorized signers. Research highlights that secure authentication combined with controlled access policies is essential for maintaining integrity in blockchain systems [3]. This ensures that only authorized users can initiate or approve transactions, strengthening overall system security.
Resume Builder Module.

3.2 Vault Management Module

Digital asset management systems have evolved to support structured storage through secure vault mechanisms. Blockchain-based frameworks emphasize controlled environments where ownership, permissions, and governance policies are clearly defined [2], [4]. These vaults enable collaborative asset management while maintaining transparency and accountability.

Furthermore, vault configurations allow dynamic modification of participants and approval thresholds. This prevents centralized control and improves security by distributing authority among multiple users. Such approaches align with modern decentralized asset management systems and enhance reliability and control.

3.3 Transaction Management Module

Transaction management ensures secure and valid transfer of digital assets across the blockchain network. Blockchain systems validate transactions using cryptographic verification and consensus mechanisms to maintain data integrity and prevent tampering [1], [5]. Each transaction undergoes strict validation before execution.

Additionally, maintaining transaction logs and history is essential for transparency and auditing. Research highlights the importance of traceability and monitoring for analyzing system behavior and detecting inconsistencies [1], [8]. This enables users to track transaction status and ensures accountability within the system.

3.4 AI-Based Risk Analysis Module

Artificial intelligence enhances transaction monitoring by analyzing behavioral patterns such as transaction frequency, value, and user activity. AI-based systems can detect anomalies and identify fraudulent activities with higher accuracy compared to traditional rule-based approaches [9]. This significantly improves system security.

Moreover, AI-driven models assign risk scores to transactions, enabling adaptive security

mechanisms. Based on the risk level, the system can dynamically enforce stricter controls. Studies in fraud detection using machine learning demonstrate improved efficiency and reduced false positives [9]. This ensures proactive protection against malicious activities.

3.5 Approval and Multi-Signature Module

Multi-signature authentication is widely used in blockchain systems to enhance transaction security. It requires multiple approvals before executing a transaction, reducing the risk of unauthorized access and single-point failure [6]. This ensures shared control over assets.

In addition, integrating multi-signature mechanisms with AI enables dynamic approval thresholds. High-risk transactions may require additional approvals, improving both flexibility and security. This combination creates a robust and adaptive authorization framework.

3.6 Smart Contract Execution Module

Smart contracts automate transaction execution based on predefined rules, eliminating the need for intermediaries. They ensure transparency, efficiency, and immutability in blockchain systems [10], [11]. Once deployed, smart contracts execute operations reliably without manual intervention.

However, research indicates that vulnerabilities in smart contracts can lead to significant risks [10]. Therefore, secure design, testing, and validation are essential. By leveraging well-designed contracts, the system ensures safe and tamper-proof execution.

3.7 Database and Monitoring Module

While blockchain stores immutable transaction data, off-chain databases are used to manage metadata such as logs, approvals, and system states. Hybrid storage approaches improve system scalability and performance [2]. These databases enable efficient querying and faster data access.

Additionally, monitoring systems provide real-time insights into system activity. They enable anomaly detection, alert generation, and transaction tracking. This enhances transparency, improves user experience, and supports informed decision-making.

4 Safety features and AI-Based Monitoring

Blockchain-based systems ensure security primarily through cryptographic mechanisms such as public-key encryption and digital signatures, which authenticate users and protect

transaction integrity. These techniques eliminate the need for centralized credential storage and significantly reduce risks such as unauthorized access and data breaches. Additionally, hashing ensures that transaction data remains immutable, forming a secure and tamper-proof system foundation.

To further enhance security, multi-signature mechanisms are implemented, requiring multiple approvals before executing transactions. This prevents single-point control and ensures collaborative decision-making among authorized users. Smart contracts automate execution based on predefined rules, improving transparency and eliminating intermediaries, although proper validation is essential to avoid vulnerabilities.

Artificial intelligence introduces an advanced layer of security by enabling real-time transaction monitoring and anomaly detection. AI models analyze transaction patterns such as amount, frequency, and user behavior to identify suspicious activities. Compared to traditional rule-based systems, AI-driven approaches provide higher accuracy in fraud detection and enable proactive security measures.

Moreover, adaptive security mechanisms use AI-generated risk scores to dynamically adjust system controls. High-risk transactions may require additional approvals or verification, while low-risk transactions follow standard procedures. Combined with real-time monitoring and alert systems, this approach enhances user awareness, improves system reliability, and ensures secure and efficient digital asset management.

5 Comparative Analysis of Existing Studies

Table 1 presents a structured comparison of the nine systems reviewed in this survey. The comparison covers the system type, primary technique, key features, and identified limitations for each work.

Table 1: Comparison of AI-Based Career Systems.

No.	Author(s)	System	Technique	Key Features	Limitations
1	Zheng et al. [1]	Blockchain Architecture Overview	Distributed Ledger, Consensus Algorithms	Secure, decentralized, transparent transactions	No intelligent monitoring or adaptive security
2	Zakhary et al. [2]	Blockchain Asset Management System	Distributed Systems, Blockchain Storage	Global asset management, scalable architecture	Limited real-time monitoring and AI integration

3	McCabe et al. [3]	Blockchain Authentication System	Cryptographic Authentication, Digital Signatures	Secure identity verification, decentralized access	No transaction-level intelligence or risk analysis
4	Yusandika et al. [4]	Onchain Analysis System	Blockchain Analytics, Data Analysis	Insight into transaction behavior, DEX analysis	No direct transaction control or security enforcement
5	Blockchain Fundamentals [5]	Basic Blockchain System	Consensus, Cryptography	Secure transaction validation, immutability	Lacks advanced features like AI or multi-signature
6	Tan et al. [6]	Multi-Signature Authentication System	Multi-signature Cryptography	Enhanced security, shared control over transactions	Static approval rules, no adaptive mechanism
7	Kokoris-Kogias et al. [7]	OmniLedger	Sharding, Distributed Consensus	High scalability, secure decentralized ledger	Complex implementation, no AI-based monitoring
8	Bünz et al. [8]	Confidential Transactions (Bulletproofs)	Zero-Knowledge Proofs	Privacy-preserving transactions, efficiency	Focus only on privacy, not overall system control
9	Weber et al. [9]	Fraud Detection in Blockchain	Machine Learning, Graph Neural Networks	Detects suspicious transactions, high accuracy	Not integrated with execution systems
10	Alharby et al. [10]	Smart Contract Systems	Smart Contracts, Blockchain	Automated execution, transparency	Vulnerabilities possible, no dynamic risk control
11	Hewa et al. [11]	Smart Contract Survey	Blockchain + Smart Contracts	Comprehensive analysis, scalability insights	Lacks real-time monitoring and AI integration

Several observations emerge from this comparison. First, there is a clear progression from basic blockchain systems toward more advanced and secure architectures. Early systems primarily focused on decentralization, cryptographic validation, and transaction integrity [1], [5], whereas later works introduced improvements such as multi-signature authentication [6], scalable architectures like sharding [7], and enhanced asset management frameworks [2]. This evolution highlights a shift from foundational blockchain design to more secure and scalable systems.

Second, the role of intelligent monitoring and security mechanisms has significantly increased in recent research. Traditional blockchain systems lacked the ability to detect suspicious activities, while newer approaches incorporate machine learning and graph-based techniques for fraud detection and transaction analysis [9]. Additionally, advancements in

authentication and smart contract security [3], [10], [11] reflect a growing emphasis on strengthening system reliability and protecting against vulnerabilities.

Third, and most importantly, existing systems remain highly fragmented, with each solution focusing on a specific component such as authentication, transaction processing, asset management, or fraud detection. None of the reviewed works provide a fully integrated system that combines blockchain security, multi-signature authorization, and AI-based risk analysis into a single unified platform. This limitation highlights a critical research gap and justifies the need for the proposed AI Smart Vault system, which aims to integrate these components into a comprehensive and intelligent solution.

6 Research Gaps

The survey reveals several significant gaps in the current state of Blockchain based asset management research:

- Lack of Integrated Systems: Existing solutions focus on individual components such as authentication, transaction processing, or fraud detection, but do not provide a unified platform. This forces users to depend on multiple systems, reducing efficiency and increasing complexity.
- Absence of Adaptive Security: Most multi-signature mechanisms use fixed approval thresholds that do not change based on transaction context. They fail to consider dynamic factors like transaction value or behavior patterns, limiting real-world effectiveness.
- Limited Real-Time Fraud Prevention: AI-based systems can detect suspicious activities but are not directly integrated with transaction execution. They cannot actively prevent or modify transactions in real time, reducing their practical security impact.
- Smart Contract Vulnerabilities: Smart contracts automate processes but are prone to coding errors and security flaws. Many systems lack proper auditing and validation mechanisms, leading to potential exploitation and financial risks.
- Scalability and Security Trade-off: Advanced techniques such as sharding improve scalability but introduce complexity in maintaining security. Existing systems struggle to balance high performance with strong and consistent protection.
- Lack of User-Centric Monitoring: Most platforms do not provide intuitive dashboards or real-time alerts for users. This limits visibility into transaction activities and delays response to potential threats.

7 Future Research Directions

Based on the identified gaps, several promising directions for future research emerge:

- Integration of AI with Blockchain Execution: Future systems should tightly integrate AI-based risk analysis with blockchain transaction execution. This would enable real-time decision-making where suspicious transactions can be automatically blocked or modified before completion.
- Dynamic Multi-Signature Mechanisms: Research can focus on adaptive multi-signature models where approval thresholds change based on transaction risk. This would improve flexibility and enhance security compared to static approval systems.
- Advanced AI Models for Fraud Detection: Future work can explore deep learning and graph neural networks for more accurate fraud detection. These models can better capture complex transaction relationships and evolving attack patterns.
- Secure Smart Contract Development: There is a need for automated tools and frameworks for detecting vulnerabilities in smart contracts. Future research can focus on formal verification and AI-assisted auditing to improve contract reliability.
- Scalable and Secure Architectures: Developing systems that balance scalability and security remains a key challenge. Future solutions can explore hybrid models combining sharding, layer-2 solutions, and secure consensus mechanisms.
- User-Centric Security Interfaces: Future systems should focus on improving usability by providing intuitive dashboards, real-time alerts, and clear risk visualization. This will enhance user awareness and enable better decision-making.
- Cross-Platform and Interoperability Solutions: Research can explore interoperability between different blockchain networks and financial systems. This would allow seamless asset management across multiple platforms while maintaining security and efficiency.

8 CONCLUSION

The study of existing blockchain-based systems highlights the rapid evolution of digital asset management from basic decentralized transaction platforms to more advanced and secure architectures. Early systems focused primarily on cryptographic validation, transparency, and immutability, ensuring reliable transaction processing [1], [5]. Over time, enhancements such as multi-signature authentication and scalable frameworks have significantly improved system security and performance [6], [7]. However, these systems still operate with limited adaptability and lack intelligent decision-making capabilities.

The integration of artificial intelligence has introduced new possibilities for improving security through real-time monitoring and fraud detection. AI-based techniques enable systems to analyze transaction behavior, identify anomalies, and enhance overall reliability [9]. Additionally, smart contracts have automated transaction execution, reducing dependency on intermediaries and improving efficiency [10], [11]. Despite these advancements, most existing solutions remain fragmented, addressing only specific aspects such as authentication, monitoring, or execution without providing a unified approach.

To address these limitations, the proposed AI Smart Vault system combines blockchain security, multi-signature authentication, and AI-driven risk analysis into a single integrated framework. This approach enhances security through adaptive mechanisms, improves usability with real-time monitoring, and ensures efficient asset management. By bridging the gap between decentralized execution and intelligent analysis, the system provides a scalable and comprehensive solution for modern digital asset management challenges.

REFERENCES

1. Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H., “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” IEEE 6th International Congress on Big Data, 2017.
2. Zakhary, V., Amiri, M. J., Maiyya, S., Agrawal, D., and El Abbadi, A., “Towards Global Asset Management in Blockchain Systems,” arXiv preprint arXiv:1905.09359, 2019.
3. McCabe, C., Mohideen, A. I. C., and Singh, R., “A Blockchain-Based Authentication Mechanism for Enhanced Security,” Sensors, vol. 24, no. 17, p. 5830, 2024.
4. Yusandika, A. D., Bhuiyan, A. H., and Laskar, P. S., “Onchain Analysis: A Comparative Study of Decentralized Exchange (DEX) Activities on Ethereum, Solana, and Binance Smart Chain (BSC),” Blockchain, Artificial Intelligence, and Future Research, vol. 1, no. 1, pp. 23–34, 2025.
5. Zakhary, V., Amiri, M. J., Maiyya, S., Agrawal, D., and El Abbadi, A., “Towards Global Asset Management in Blockchain Systems,” arXiv preprint arXiv:1905.09359, 2019.
6. Tan, Y., Cheng, Y., Ding, L., and Zhao, Y., “Multi-signature Authentication and Simulation Extractability Security Optimization for Account-Based Blockchain Anonymous Systems,” Proc. SPIE 13562, International Conference on Computer Application and Information Security (ICCAIS), 2024.
7. Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., and Ford, B.,

"OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding," IEEE Symposium on Security and Privacy (SP), 2018.

8. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., and Maxwell, G., "Bulletproofs: Short Proofs for Confidential Transactions and More," IEEE Symposium on Security and Privacy (SP), 2018.
9. Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., and Leiserson, C. E., "Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics," KDD '19 Workshop on Anomaly Detection in Finance, 2019.
10. Alharby, M., and van Moorsel, A., "Blockchain-Based Smart Contracts: A Systematic Mapping Study," Computer Science & Information Technology (CS & IT), pp. 125–140, 2017.
11. Hewa, T. M., Hu, Y., Liyanage, M., Kanhare, S. S., and Ylianttila, M., "Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research," IEEE Access, vol. 9, pp. 87643–87662, 202.