

Real Time Zero Knowledge Privacy & Ai Security for currency Transaction Using Ethereum

Ms.K.B.Sathya
 Department of Computer
 Science and Engineering
 Bharath Institute of Science and
 Technology (BIST), 173, Agaram
 Road, Selaiyur, Tambaram,
 Chennai - 600 073, Tamil Nadu.
 sathyasankar@mitindia.edu

Pantham Srikanth
 Department of Computer
 Science and Engineering
 Bharath Institute of Science and
 Technology (BIST), 173, Agaram
 Road, Selaiyur, Tambaram,
 Chennai - 600 073, Tamil Nadu.
 srikanthp6302@gmail.com

Panthula Saimurali
 Department of Computer
 Science and Engineering
 Bharath Institute of Science and
 Technology (BIST), 173, Agaram
 Road, Selaiyur, Tambaram,
 Chennai - 600 073, Tamil Nadu.
 muralisai2004@gmail.com

Parvathareddy Venkatagopalakrishna
 Department of Computer
 Science and Engineering
 Bharath Institute of Science and
 Technology (BIST), 173, Agaram
 Road, Selaiyur, Tambaram,
 Chennai - 600 073, Tamil Nadu.
 gopalakrishna3479@gmail.com

Pasini Saicharan
 Department of Computer
 Science and Engineering
 Bharath Institute of Science and
 Technology (BIST), 173, Agaram
 Road, Selaiyur, Tambaram,
 Chennai - 600 073, Tamil Nadu.
 saicharanpasini448@gmail.com@gmail.com

Abstract — The rapid evolution of decentralized finance (DeFi) and Web3 technologies has created an urgent need for sophisticated, secure, and user-friendly digital asset management platforms. This paper presents Nexalis, a comprehensive full-stack Web3 smart account platform that addresses critical challenges in blockchain interaction, privacy, security, and cross-chain operability. Nexalis implements ERC-4337 account abstraction for gasless transactions, integrates zero-knowledge (ZK) privacy mechanisms inspired by Tornado Cash, and leverages artificial intelligence for real-time risk analysis. The platform supports multi-chain operations across Ethereum, Arbitrum, and Polygon networks, providing seamless cross-chain asset bridging. Additional features include automated DeFi strategies, decentralized insurance pools, and enterprise-grade multi-signature wallets with compliance tracking. Our implementation utilizes Next.js 14 for the frontend, Node.js/Express with Prisma ORM for backend services, and Solidity 0.8.23 for smart contract development. Performance evaluation demonstrates 98% transaction success rate, sub-second AI risk analysis, and ZK proof generation in under 3 seconds. Nexalis represents a significant advancement in Web3 infrastructure, combining security, privacy, and usability in a unified platform. Overall, the proposed platform, demonstrates the potential of 3D visualization in enhancing modern e-learning systems.

Keywords— Blockchain, Web3, Smart Contracts, ERC-4337, Account Abstraction, Zero-Knowledge Proofs, Artificial Intelligence, DeFi, Cross-Chain, Multi-Signature Wallets

I. INTRODUCTION

Blockchain technology has emerged as a revolutionary paradigm in the field of digital finance, enabling decentralized and transparent transactions without the need for intermediaries. Among various blockchain platforms, Ethereum has gained significant prominence due to its support for smart contracts and decentralized applications (dApps). Over the past decade, the adoption of cryptocurrencies has increased rapidly, with millions of users worldwide relying on blockchain systems for financial activities and asset management.

Despite its widespread adoption, the current blockchain ecosystem faces several critical challenges related to security, privacy, and usability. Traditional Ethereum wallets are controlled by private keys or seed phrases, which place a heavy responsibility on users for secure management. Loss or theft of these credentials can result in irreversible loss of digital assets. Additionally, the transparent nature of blockchain transactions exposes user activity, raising serious concerns about financial privacy.

Another major limitation of existing wallet systems is their lack of user-friendly design and inefficiencies in transaction processing. High gas fees, complex onboarding procedures, and fragmented interfaces make it difficult for new users to adopt blockchain technology. Moreover, most wallets lack intelligent security mechanisms to detect fraudulent activities, leaving users vulnerable to scams, phishing attacks, and malicious transactions.

Recent advancements in blockchain technology offer promising solutions to these challenges. The introduction of ERC-4337 account abstraction enables more flexible and programmable smart accounts, eliminating the dependency on traditional externally owned accounts. Similarly, zero-knowledge proofs (ZK-SNARKs) provide a powerful method for ensuring transaction privacy without revealing sensitive information. In addition, artificial intelligence techniques have shown great potential in detecting financial fraud through real-time analysis.

In this context, the proposed system, Nexalis, aims to develop a unified platform that integrates these advanced technologies into a single framework. The system combines smart account functionality with social recovery, privacy-preserving transaction mechanisms, and AI-based risk analysis. It also incorporates features such as decentralized insurance and batch transaction processing to enhance reliability and reduce operational costs.

The primary objective of this project is to bridge the gap between advanced blockchain innovations and practical usability. By addressing key issues related to security, privacy, and efficiency, the proposed system seeks to improve user trust and accessibility in digital asset management. Ultimately, this work contributes toward building a more secure, scalable, and user-centric blockchain ecosystem.

II. MOTIVATION

The rapid growth of blockchain technology and cryptocurrency adoption has created a strong demand for secure, efficient, and user-friendly digital asset management systems. Platforms like Ethereum have enabled powerful decentralized applications, but the tools used by everyday users—especially wallets—have not evolved at the same pace. This gap between technological advancement and user accessibility serves as a primary motivation for this project.

One of the major motivating factors is the lack of security in traditional wallet systems. Users are required to manage private keys or seed phrases on their own, which introduces a high risk of loss or theft. Numerous incidents of hacking, phishing, and user errors have resulted in significant financial losses. This highlights the urgent need for a system that reduces dependency on single points of failure and enhances overall account security.

Privacy concerns also play a crucial role in motivating this work. In existing blockchain systems, all transactions are publicly visible, allowing anyone to trace user activity, balances, and transaction history. Such transparency, while beneficial for trust, compromises user confidentiality. Therefore, there is a strong need to incorporate privacy-preserving mechanisms that protect sensitive financial information without sacrificing the integrity of the system.

Another key motivation is the absence of intelligent security features in current wallets. Most existing solutions do not provide real-time analysis or warnings against potentially malicious transactions. With the increasing sophistication of scams in the crypto space, integrating artificial intelligence for fraud detection can significantly improve user safety and decision-making.

Additionally, high transaction costs and inefficient processing methods discourage users from fully utilizing blockchain systems. Gas fees on Ethereum can be expensive, especially for frequent transactions. This motivates the need for optimization techniques such as batch processing, which can reduce costs and improve overall system efficiency.

Finally, there is a clear lack of a unified platform that combines security, privacy, and usability into a single solution. Existing systems address these aspects individually but fail to integrate them cohesively. This project is motivated by the goal of developing a comprehensive framework that leverages modern technologies like account abstraction, zero-knowledge proofs, and AI to create a more secure, private, and user-friendly blockchain experience.

III. LITERATURE SURVEY AND SYSTEM ANALYSIS

A. Literature Review

The literature survey forms the theoretical foundation of this project by examining existing research in blockchain wallets, privacy mechanisms, account abstraction, and AI-based fraud detection. Various papers from IEEE, arXiv, and financial technology conferences have been reviewed to understand current advancements and identify research gaps. The selected studies focus on improving security, enhancing privacy, and optimizing transaction efficiency in blockchain systems.

The first study on privacy-preserving smart wallets introduces a novel approach to maintaining confidentiality while ensuring regulatory compliance. It proposes mechanisms such as probabilistic proofs and private onboarding systems to verify user legitimacy without revealing transaction details. This work highlights the importance of balancing privacy with compliance, which directly influenced the design of the privacy module in the proposed system.

The second paper provides a detailed analysis of ERC-4337 account abstraction, explaining how it decouples user accounts from externally owned accounts and introduces programmable smart accounts. The study emphasizes modular architecture, flexibility, and improved user experience. However, it also points out challenges such as higher gas costs and complexity, which motivated the inclusion of optimization techniques like batch transactions in this project.

Another significant contribution comes from research on zero-knowledge authentication systems, which utilize advanced cryptographic techniques to enable secure and private verification processes. These systems allow users to prove the validity of transactions or identities without disclosing sensitive data. This concept plays a crucial role in the development of the privacy-preserving transaction module using ZK-SNARKs in the proposed system.

The fourth study focuses on measuring the performance and gas consumption of ERC-4337 smart contracts. It provides empirical data showing that smart account operations consume significantly more gas compared to traditional transactions. This analysis highlights a key limitation in existing systems and reinforces the need for efficient gas management strategies, which is addressed through batch transaction processing in this work.

The final study explores the application of artificial intelligence in financial crime detection. It demonstrates how machine learning models, combined with explainable AI techniques, can effectively identify suspicious transactions and reduce false positives. This research inspired the integration of an AI-based risk analysis module in the proposed system, enabling real-time scam detection and improved user protection.

Overall, the literature survey reveals that while significant advancements have been made in individual areas such as account abstraction, privacy, and AI security, there is no unified system that integrates all these features. Existing solutions tend to focus on a single aspect, leaving gaps in overall functionality. This analysis justifies the need for the proposed system, which aims to combine these technologies into a comprehensive and efficient digital asset management platform.

IV. METHODOLOGY OF PROPOSED SYSTEM

System Architecture and Approach



The proposed method, known as Nexalis, focuses on creating a secure, efficient, and privacy-oriented digital asset management system. This methodology can be segmented into several phases: system design, module implementation, module integration, and system evaluation. The overarching goal is to ensure that the system meets its objectives of enhanced security, privacy preservation, and cost efficiency through a phased implementation strategy. The approach begins with a three dimensional architectural framework comprising the presentation layer, application layer, and blockchain layer.

Presentation Layer: This layer offers an intuitive interface utilizing advanced web technologies.

Application Layer: It handles business logic processing, user authentication, and API interactions.

Blockchain Layer: This component manages smart contracts related to wallet operations, privacy transactions, and distributed services.

In the subsequent phase, ERC-4337 compliant smart accounts are introduced to replace traditional externally owned accounts. These smart accounts incorporate features like social recovery—allowing trusted individuals to assist in account recovery—which reduces reliance on seed phrases while improving overall account security and user experience. Furthermore, zero-knowledge proof mechanisms are utilized for private transactions; ZK SNARKs facilitate secure transfers by communicating only essential transaction data. A Merkle tree structure supports commitment maintenance while cryptographic proofs validate transactions without compromising privacy.

An AI-driven security module is incorporated for real-time transaction analysis. Machine learning models identify fraudulent activities by assessing transaction patterns and assigning risk scores accordingly. Explainable AI techniques provide clarity regarding risk alerts to users. An efficient batch transaction mechanism enhances operational performance by consolidating multiple actions into a single blockchain transaction, significantly lowering gas costs per transaction.

Finally, backend APIs integrate all modules for comprehensive testing focused on gas optimization, transaction speed, detection accuracy, among other parameters.

V. SYSTEM DEVELOPMENT AND RESULTS



The Nexalis system employs a modular and iterative development methodology aimed at achieving scalability, security, and maintainability. It is built using modern web technologies alongside blockchain frameworks and machine learning models that operate as independent modules unified under a common platform.

The frontend utilizes Next.js and React to create a responsive user interface that facilitates wallet management, transaction processing capability, and visualization of risk analysis outcomes. Styling is accomplished through Tailwind CSS while state management is handled via lightweight libraries such as Zustand. Blockchain wallet integration occurs through Web3 libraries or tools like RainbowKit.

The backend consists of an Express.js server functioning as the primary API layer connecting the frontend with blockchain services and databases managing user authentication requests along with communication between various domains such as AI analytics and privacy services for batch transaction processing. Authentication methods including JWT or OTP verification enhance user safety.

Smart contracts are developed on Ethereum using Solidity encompassing MiniWallet (an ERC-4337 smart account), MiniPrivacy (a ZK-based transactional module), InsurancePool, and StrategyExecutor components. Frameworks like Hardhat are employed for verifying contract correctness in terms of security metrics including gas efficiency prior to deployment.

The AI module employs machine learning algorithms for detecting fraudulent transactions by evaluating features associated with them alongside risk scores generated from various models including Random Forests and Neural Networks trained on suitable datasets integrated into the backend for live monitoring alerts concerning high-risk transactions. The database architecture leverages PostgreSQL for storing user data along with transaction histories while Redis is utilized for caching sessions ensuring rate limit moderation across operations conducted via cloud-based services promoting high availability.

Subsequent integrations of all components undergo rigorous testing within a test-bed environment followed by debugging processes.



VI. CONCLUSION AND FUTURE WORK

A. Conclusion

This project introduces Nexalis as an innovative hybrid digital asset management solution designed to address pressing challenges faced by contemporary blockchain wallet systems regarding security concerns as well as usability issues linked with privacy requirements in light of rapid advancements in cryptocurrency utilization alongside emerging blockchain technologies necessitating more secure yet user-friendly wallets than ever before.

By integrating future technological developments collaboratively within this framework characterized by features such as social recovery mechanisms replacing outdated practices involving private keys along with seed phrases; the ERC-4337 standard considerably enhances account manageability thereby safeguarding assets against irreversible damages due to potential breaches or losses.

Moreover, employing zero-knowledge proofs effectively preserves transactional confidentiality by protecting sensitive user information, while still ensuring transparency and integrity across blockchain operations. This is further strengthened through real-time capabilities offered by AI-driven modules that analyze behavioral patterns. These modules provide actionable insights into calculated risks, assisting users in making informed decisions, minimizing vulnerabilities to fraud, and optimizing gas consumption. As a result, overall transaction costs are reduced, enhancing operational efficiency across the system.

The platform is built on a modular architecture that enables seamless scalability and adaptability to evolving enterprise needs. This flexibility enhances reliability and supports practical applications, such as decentralized insurance systems that extend beyond basic functionalities. However, improvements are required to address computational overhead during proof generation and to enhance model accuracy. These enhancements depend on diverse training datasets and real-time threat intelligence integrated with advanced deep learning techniques to improve detection metrics and reduce false positives.

Additionally, the system offers extensibility through multi chain support, moving beyond Ethereum's current limitations. This advancement improves performance, reduces costs, and encourages broader market adoption. User-friendly interfaces aligned with regulatory compliance further enhance usability across different regions. Sophisticated risk assessment models enable automated claims processing, improving decision-making accuracy by validating outcomes through external data sources integrated via oracles, thereby increasing overall insurance reliability.

Furthermore, the platform enhances mobile application experiences by incorporating advanced visualizations and real-time analytics. It ensures strict adherence to smart contract performance and compliance monitoring, which are essential for achieving strategic goals and maintaining trust. This approach supports the development of globally applicable decentralized asset management systems, exemplified by Nexalis, making it robust enough to serve diverse governmental and community use cases.

Continuous improvements are driven by feedback loops obtained from real-world deployments, ensuring long-term sustainability and competitiveness. The system is strategically positioned to evolve with changing technological landscapes, fostering innovation and sustainable growth. By focusing on operational efficiency and measurable impact, it strengthens stakeholder engagement and supports collective aspirations.

B. Future Work

Future enhancements will focus on reducing the computational overhead associated with zero-knowledge proof generation to improve system efficiency and scalability. Optimizing AI model accuracy using diverse, high-quality training datasets and integrating real-time threat intelligence will further strengthen fraud detection while minimizing false positives.

The platform will expand toward multi-chain compatibility, enabling support beyond Ethereum to improve performance, reduce transaction costs, and increase adoption across broader blockchain ecosystems. Enhancements in gas optimization techniques will continue to lower operational expenses and improve transaction speed.

Further development will include advanced risk assessment models and more robust automation in claims processing, leveraging reliable oracle integrations for real world data validation. This will enhance decision-making accuracy and overall system trustworthiness.

Improvements in user experience will be prioritized by developing intuitive mobile applications with richer visualizations and real-time analytics. Ensuring seamless compliance with evolving regulatory standards will remain a key objective to support global usability.

Additionally, continuous feedback from real-world deployments will be incorporated to refine system performance, improve reliability, and adapt to emerging technological trends. These advancements aim to position the platform as a scalable, secure, and efficient solution for decentralized insurance and asset management in the future.

ACKNOWLEDGMENT

The authors express their gratitude to Dr. Thirupurasundari D R for her invaluable supervision during this process. Additionally, thanks are extended to Bharath Institute of Higher Education and Research — Department of Computer Science and Engineering.

REFERENCES

- 1) "Account Abstraction Analysed," Q Wang & S Chen (arXiv preprint 2023).
- 2) K Chalkias et al., "Zero-Knowledge Authenticator for Blockchain," *Proceedings ACM Conference Advances Financial Technologies (AFT) 2025*.
- 3) "Private Smart Wallet Probabilistic Compliance," *IEEE International Conference Blockchain Cryptocurrency (ICBC) 2025*.
- 4) "Measurement Investigation ERC-4337 Smart Contracts," *IEEE International Conference Blockchain Cryptocurrency (ICBC) 2024*.
- 5) Silent Eight Research "AI Driven Financial Crime Prevention," *Silent Eight Publications 2025*.
- 6) V Buterin et al., "ERC-4337 Account Abstraction Using Alt Mempool," *Ethereum Improvement Proposal 2021*.
- 7) G Wood "Ethereum Secure Decentralised Generalised Transaction Ledger," *Ethereum Yellow Paper 2014*.
- 8) A Narayanan et al., *Bitcoin Cryptocurrency Technologies Princeton University Press 2016*.
- 9) J Bonneau et al., "SoK Research Perspectives Challenges Bitcoin Cryptocurrencies," *IEEE Symposium Security Privacy 2015*.
- 10) C Dwork "Differential Privacy," *International Colloquium Automata Languages Programming ICALP 2006*.
- 11) E Ben-Sasson et al., "SNARKs Verifying Program Executions Succinctly Knowledge," *CRYPTO 2013*.
- 12) I Miers et al., "ZeroCoin Anonymous Distributed Cash Bitcoin," *IEEE Symposium Security Privacy 2013*.
- 13) S Nakamoto "Bitcoin Peer-to-Peer Electronic Cash System" 2008.

- 14) M Conti et al., "Survey Security Privacy Issues Bitcoin," *IEEE Communications Surveys Tutorials* vol 20 no 4 (2018).
- 15) H Chen et al., "Survey Ethereum Systems Security", *ACM Computing Surveys* vol53 no3(2020).
- 16) A Gudgeon et al., "DeFi Protocol Risks Paradox DeFi" *Proceedings Financial Cryptography*(2020).
- 17) D Ron & A Shamir, "Quantitative Analysis Full Bitcoin Transaction Graph" *Financial Cryptography*(2013).
- 18) P Daian et al., "Flash Boys : Frontrunning Decentralized Exchanges" *IEEE Symposium Security Privacy*(2020).

