Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

Multi-Chain Smart Wallet With Gasless Transaction

Jay Korat[1], Bhavya S. Patel[2]*, Neel Gabani[3], Sridhar Iyer[4], Vikas Gupta[5]

[1]Department of Computer Engineering, Dwarkadas Jivanlal Sanghvi College of Engineering, koratjay22@gmail.com
[2*]Department of Computer Engineering, Dwarkadas Jivanlal Sanghvi College of Engineering, patelbhavya2412@gmail.com
[3]Department of Computer Engineering, Dwarkadas Jivanlal Sanghvi College of Engineering, neelgabani24ng@gmail.com
[4]Asst. Professor, Dept. of Computer Engineering, Dwarkadas Jivanlal Sanghvi College of Engineering, sridhar.iyer@djsce.ac.in
[5]Department of Computer Engineering, Dwarkadas Jivanlal Sanghvi College of Engineering, vikasgupta3634@gmail.com

Article History:

***Received**: 12-04-2025*

***Revised:** 15-05-2025*

***Accepted:** 06-06-2025*

Abstract:
Blockchain technology is advancing at a rapid pace, but two major obstacles still stand between mainstream adoption: the insufficiency of interoperability between various blockchain networks and the prohibitively high gas charges. The above concerns are solved by this paper using a secure multichain smart wallet architecture with gasless transaction support and cross-chain communication. The system employs threshold cryptography for secure management of keys in a decentralized manner, is coupled with the Gas Station Network (GSN) to hide fees from users, and supports various blockchain networks such as Ethereum and Solana. The system has been thoroughly analyzed and validated using real-life scenarios. we achieved a transaction efficiency of 99.77% with 100% successful completion of transactions in 53 test transactions. The design achieves greater security using advanced cryptographic techniques while staying users accessible and preventing economic hurdles towards blockchain adoption.

Index Terms—Blockchain, Interoperability, Gasless Transactions, Decentralization, Cross-Chain Communication, Smart Wallet, Threshold Cryptography

I. INTRODUCTION

Blockchain technology has revolutionarily changed digital transactions on the strength of its inherent strengths of transparency, decentralization, and immutable data security [2]. Working as a distributed electronic ledger, blockchain makes all transactions traceable and transparent to the whole network. Even so, with all of this revolutionary promise, two such crucial challenges still lie in the way of widespread adoption: the lack of seamless cross-operability among blockchain networks and transaction fees' volatility.

Interoperability issue is similar to email systems in which customers of different providers are not able to talk effectively. Similar to blockchain networks are going to work in silos in isolation, offering huge value transfer and data exchange constraints between platforms [8]. Solutions such as-ning atomic swaps, cross-chain bridges, and interoperability protocols like Cosmos and Polkadot emerged to address these constraints, although full integration remains unattainable [10].

Gas fees are the second biggest hindrance, serving as transaction tolls that could vary ridiculously in periods of network congestion, especially on Ethereum [13]. Such fees tend deter users from participating in decentralized applications, particularly where cost sensitivity is most critical [9]. Meta-transactions, relayers, and off-chain computation-based gasless transaction models are potentially novel solutions by reallocating cost burdens away from end users [4], [5].

The current paper presents an integrated framework addressing both challenges by proposing a novel smart wallet architecture combining gasless transaction methods and multichain interoperability, potentially facilitating wider adoption of blockchain in a variety of various industries such as finance, health, and supply chains.

II. LITERATURE REVIEW

A. Background of Existing Smart Wallet Solutions

Existing blockchain usage is heavily dependent on smart wallets such as Phantom and MetaMask that act as central interfaces between the user and decentralized systems [12]. MetaMask, the most used Ethereum wallet, functions through browser extensions and mobile apps, utilizing hierarchical deterministic (HD) wallet structure that accommodates seed phrase-based recovery on multiple devices [1]. While this method is simple, it has gigantic security risks. As soon as the seed words of users are lost or stolen, full wallet access may be irretrievably lost. MetaMask demands private key signatures and advanced gas fee upfront payments, with high network time having fees change wildly, making it difficult for new users to gain entry [16]. Security-wise, MetaMask keeps encrypted private keys ondevice under user control but with full security responsibility placed on individual users. Inefficient transaction fee optimization opportunities lead to overpayment in times of congestion in the network [9].Native Solana wallet Phantom adheres to analogous architectural principles with browser extension and mobile app implementations leveraging seed phrase recovery. Even though being benefited by lower transaction fees by Solana's design advantages in the network Phantom retains the identical useraccountability model of private key control and clear transaction cost coverage [12].

B. Flaws in Current Wallet Solutions

Current wallet implementations have a number of devastating flaws impacting the adoption of blockchain technology:

- User-imposed gas fees: Users are forced to pay all transaction costs in the clear, creating the situation confusing and frustrating, especially during peak network fee periods [9].
- Inadequate multi-device support: While seed phrase recovery enables device switching, simultaneous multidevice access is lacking seamless integration [12].
- Total user security load: Seed phrase management is worrying, with danger of irreversible asset loss on loss or security breach [1].
- Simple user interfaces: Transaction approval protocols tend to show technical details such as gas limits and data fields, which intimidate fresh users [2].
- Inadequate advanced functionality: Simple wallets do not offer transaction scheduling or conditional execution without the need for third-party software [12].

C. Gasless Transactions

Gasless transactions are a promising solution towards eliminating user-paid transaction fees, a key blockchain adoption barrier. Rather than being required to pay gas fees directly by users, such a model offloads the cost onto application developers or service providers, rendering blockchain platform interaction far more accessible.Meta-transactions are one such implementation framework where third-party "relayer" services act on behalf of users to relay transactions. Users are safeguarded by signing requests for transactions with private keys and leaving broadcasting along with paying fees to relayers [16]. Solutions like Biconomy and Gas Station Network (OpenGSN) have implemented this pattern, although application integration ease remains a problem [3].sponsorship model is also available where platforms directly remit transaction fees, which improve user experience for something such as authentication or reward redemption. The above practice encourages centralization issues and future sustainability issues about fee coverage by service providers [6].

D. Multi-Accessibility in Blockchain Applications

Multi-accessibility allows blockchain asset access and transaction processing on many devices in parallel without compromising security or the need for extensive recovery processes.

Certain important strategies facilitate multi-accessibility deployment:Cloud-Based Key Management: Platforms like Magic (previously Fortmatic) make use of cross-device asset access through cloud-based keys. While increasing user experience, this strays away from blockchain's decentralized nature [11].

Multi-Signature Wallets: Platforms like Gnosis Safe allow a group of users or devices to split transaction authorization load. While increasing organizational security, user complexity per user can be too much [13]. Threshold Signature Schemes: New threshold cryptograph technologies share key management across multiple devices. Instead of taking many user signatures per transaction, it facilitates collaboration in key management by devices, increasing security as well as performance, although realization is troublesome [14].

III. PROPOSED SYSTEM

A. Overview of System Architecture

Our proposed system is for a modular, secure, and interoperable smart wallet with gasless transactions, cross-chain compatibility, and multi-device secure access [8]. In contrast to current wallets like MetaMask or Phantom that are based on user-paid gas fees and single-chain transactions [12], this architecture features a Gasless Protocol Smart Contract and uses threshold cryptography for distributed secure private key management [13].Figure 1 shows the overall system architecture, showing the integration of different components such as the frontend layer, core wallet services, security modules, and blockchain integration layers.

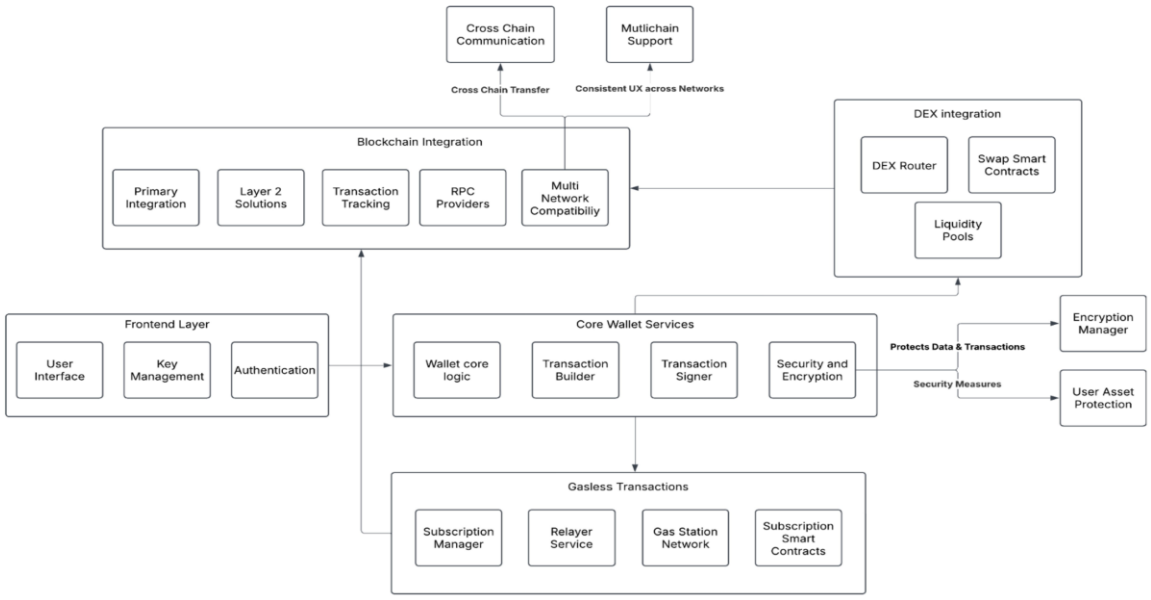
1) *Frontend Layer:* The wallet frontend uses Next.js and Tailwind CSS, with responsive and intuitive interfaces. Local storage and IndexedDB manage user key management using password-based login with added frontend security [7].

2) *Core Wallet Services:* Core services offer basic wallet operations such as transaction generation, digital signing, and key management using TypeScript modules. Organized components are secure signing services and transaction builders to enable secure cryptographic operations [15].

3) *Security and Encryption:* The Encryption Manager module invokes strong encryption algorithms safeguarding sensitive data and digital assets from unauthorized access and cyber attacks [7], [14].

4) *Decentralized Exchange (DEX) Integration:* Seamless cross-blockchain asset trades leverage DEX router and aggregator integration. Introductions to platforms like Uniswap, Tinch, and Jupiter allow for seamless token trades with solid cross-chain liquidity [8], [10].

5) *Gasless Transaction Mechanism:* The gasless transaction mechanism avoids the direct payment of user gas fees, shifting responsibility to relayer systems [4]. The wallet includes Subscription Manager for user plan management, Relayer



F ig. 1. System Architecture of the Multi-Chain Smart Wallet

Fig. 1. System architecture of the multichannel smart wallet transaction broadcast service and compatibility of the gas station network (GSN) [16]. Subscription smart contracts enhance system security through access privilege control [3].

6) Blockchain Integration: Multi-blockchains held within includes Ethereum, Solana, and Layer 2 solutions like Polygon and Arbitrum [2], [9]. Blockchain explorer linkages enhance tracking of transactions with access to reliable blockchain nodes provided through services like Alchemy and Infura [10].

7) Multi-Network Compatibility: Real cross-chain capability provides uniform support for different blockchain ecosystems [8]. Assets can be handled and operations carried out on Ethereum and Solana platforms without any hassle, giving one-uniform experiences irrespective of implicit blockchain technology [10].

B. Internal System Architecture Components

1) Gas Station Network (GSN) Architecture: The Gas Station Network (GSN) solves blockchain's ubiquitous usability issue of paying gas fees by users. By offloading this responsibility, GSN makes decentralized application interaction more convenient, especially for new users.

GSN runs on three-tiered architecture composed of User Layer, Relayer Layer, and Blockchain Layer. Users build meta-transactions as signed messages according to EIP-712 standards, ensuring security and form for reliable, readable transactions. Decentralized relayer networks relay transactions on behalf of the user, earning fees through customizable pricing models or application sponsorship sponsoring. This architecture is suitable for fair payment with minimum gas cost and denialof-service attack or spam protection.Key smart contracts worth mentioning are:

- RelayHub: Coordinates transaction coordination among relayers
- Paymaster Contracts: establishes sponsorship reasoning for funding decision-making in transactions
- Trusted Forwarders: Secure and reliable user request relaying

GSN has native security features such as replay attack protection, identity protection, and anomaly detection. Future introduces support for EIP-4337 account abstraction, Layer 2 scalability solutions, and decentralized governance mechanisms.

2) BIP Architecture Implementation: Bitcoin Improvement Proposals (BIPs) formalize Bitcoin network upgrade proposals. This project specifically utilizes BIP-39 and BIP-44 for key management and wallet creation. BIP-39 Mnemonic Generation: BIP-39 provides mnemonic phrase generation of 12 to 24 words, substituting hard private keys with readable word lists easily backed up and restored. Mnemonic generation uses random entropy sources with checksum validation, hashing to binary seeds using PBKDF2 functions with optional user-provided passphrase security.

Figure 2 illustrates the process architecture of BIP-39, presenting the sequence from entropy creation to end seed derivation, via mnemonic phrase creation.

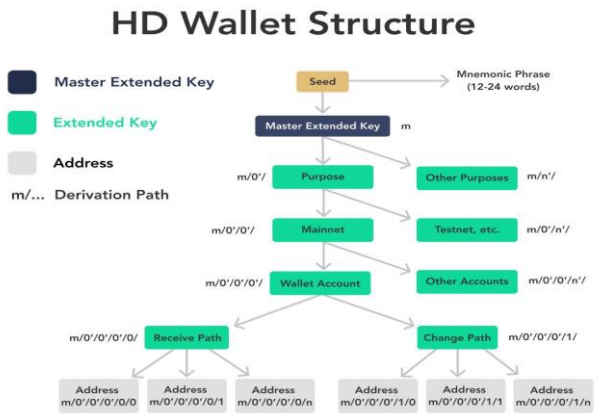


Fig. 2. BIP-39 Mnemonic Generation Architecture [17]

BIP-44 Hierarchical Deterministic Structure: BIP-44 defines structured, extensible address derivation from single seeds, upon which BIP-32 and BIP-39 are built for uniform cryptocurrency and account type handling. This obviates individual key backup requirements, making wallet management easy.
BIP-44 path structure is in the form of: m/purpose'/coinType'/account'/change/addressIndex. Purpose is hardcoded at 44' to indicate BIP-44 standard usage. Coin type separates blockchain's networks: Bitcoin (0'), Ethereum (60'), Litecoin (2'). Each account points to independent address sets that are separated as external and internal paths for processing change or receiving funds.
Figure 3 illustrates the full BIP-44 hierarchical framework, demonstrating how any number of cryptocurrencies and accounts may be derived from one master seed.
3) Cryptographic Foundations: Keccak-256 Hash Function: Keccak-256 is the indigenous cryptographic hashing function of Ethereum blockchain. Although Bitcoin employs SHA-256, Ethereum employs Keccak for wallet address generation, contract security, and Proof-of-Work algorithm support.
Keccak-256 has excellent collision and pre-image attack resistance characteristics, with strong data integrity and security ensured in decentralized systems. Keccak conforms to sponge construction schemes in the three stages:

- Initialization: Internal state matrix setup to zero preparation
- Absorbing: Input message block division with internal state XOR operations and applications of permutation rounds such as bit-level shifts, XORs, and constant utilization for data scrambling
- Squeezing: Bit extraction of output from state generating end hash values

Digital Signature Algorithms: The two most notable signature schemes are utilized in different blockchain networks in the system:
EdDSA (Ed25519): Edwards-curve Digital Signature Algorithm is a newer cryptographic signature technique used by Solana and Monero blockchains. Ed25519 employs deterministic signing routines that prevent nonce reuse attacks resulting in ECDSA weaknesses.
Ed25519 is highly resistant to side-channel attacks and can be applied for safety-critical applications such as blockchain smart contracts and authentication schemes [15]. Nonces are created during the signing process based on messages and private keys, resulting in signature pairs (R, S) where R corresponds to nonce-derived commitments and S has validityproving scalar values.
ECDSA (secp256k1): Elliptic Curve Digital Signature Algorithm utilizes secp256k1 curves for safe generation of digital signatures in Bitcoin and Ethereum transactions [14]. As opposed to EdDSA, ECDSA utilizes random nonce values per signature, resulting in non-deterministic processes. While randomness is an added feature to security, improper nonce generation or reuse is required as it may cause private key leakage.
ECDSA acts upon key generation using elliptic curve mathematics, signature generation with random nonces producing curve points for signature component calculation, and verification based on signatures, message hashes, and public keys for validity checking.
C. System Limitations and Assumptions
1) Security Assumptions:

- Appropriate security behavior and responsible key management are ensured by users [7]
- Relayer networks have operational integrity and honest operation [16]
- Blockchain network APIs are stable and backwardcompatible [11]

2) Operational Constraints:

- Success of gasless transactions relies upon sustainable dApp or service sponsorship [4]
- System reach limits dependent upon existing cross-chain interoperability levels [8]
- Legal framework differences may create locationdependent constraints [11]

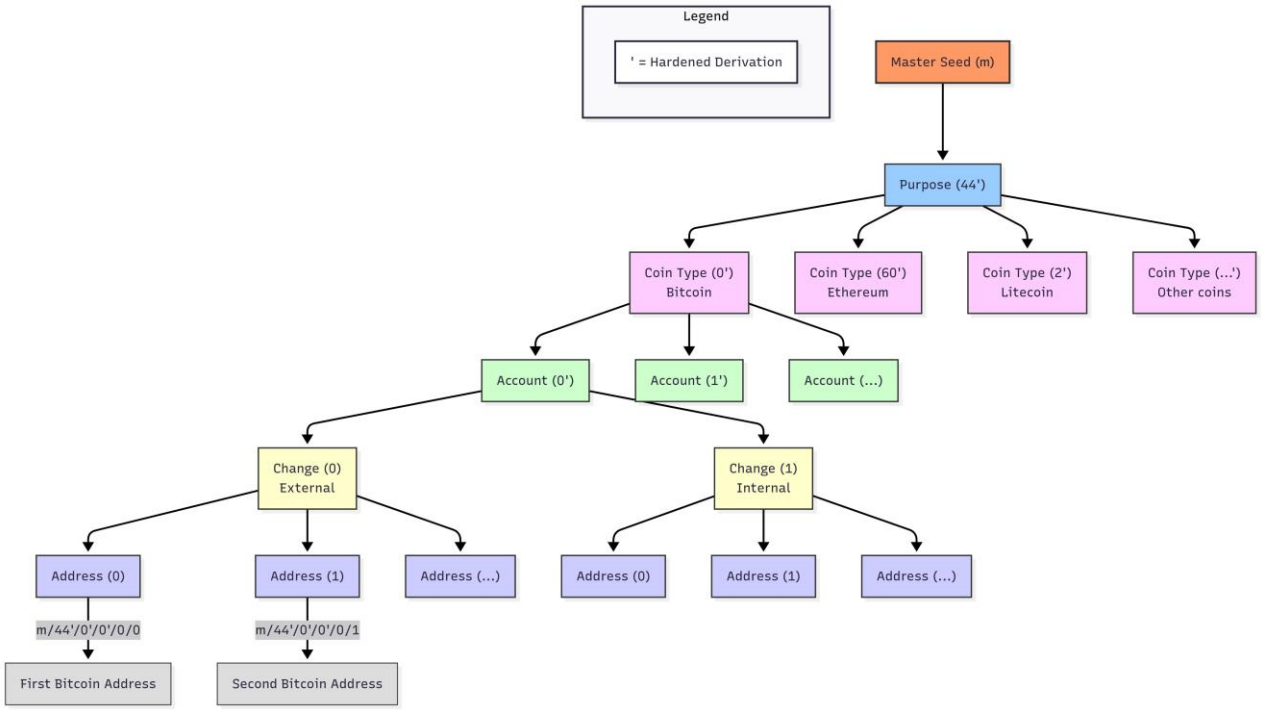


Fig. 3. BIP-44 Hierarchical Deterministic Wallet Structure

IV. RESULTS AND DISCUSSION

A. Transaction Model Evaluation The experimental evaluation shows the proposed system effectiveness using three unique transaction scenarios for various models of gas payment. Each scenario corroborates certain elements of the gasless transaction implementation 1) Standard Gas-Paid Transaction: Figure 4 depicts the standard Ethereum transaction pattern under which the sender (0x84B2E6.) pays ETH directly to the receiving wallet (0x93147A.) with the sender paying gas costs directly. This control use case provides performance benchmarks to compare with gasless alternatives.

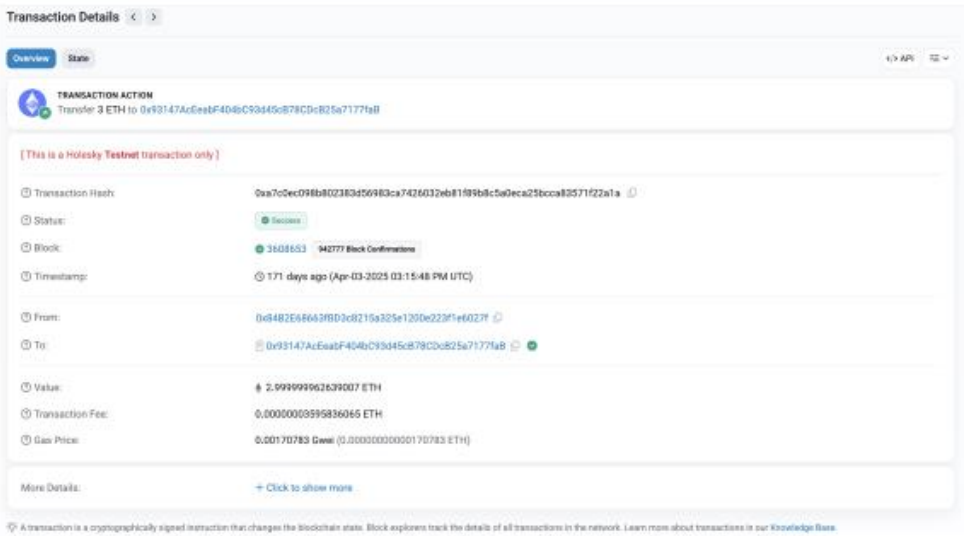


Fig. 4. Standard Gas-Paid Transaction Process [18]

2) Gasless User-to-Contract Transaction: The gasless userto-contract model, as shown in Figure 5, illustrates transactions from users to smart contracts where meta-transaction relay mechanisms obscure gas charges from users and not directly demanding sender payment. The model greatly enhances the user experience as it removes initial gas fee requests.

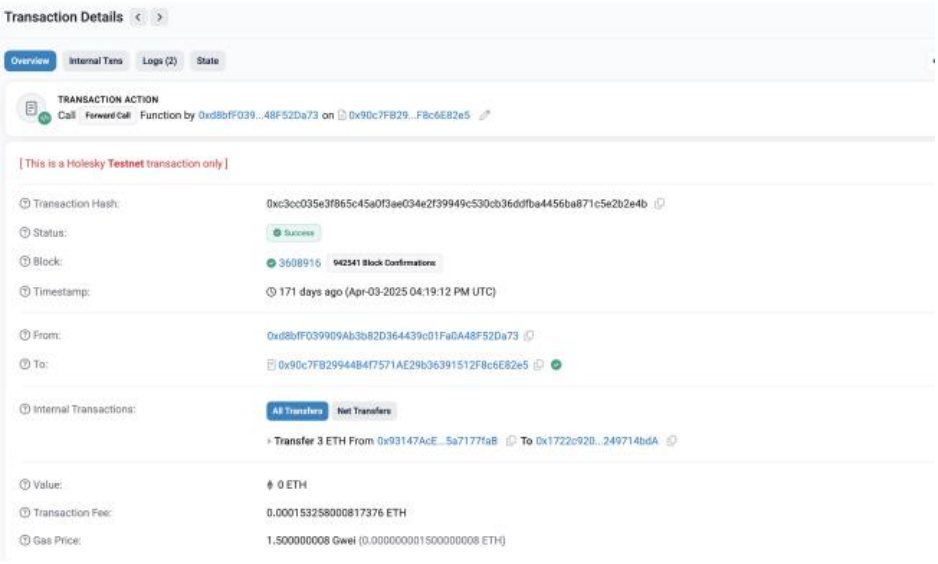


Fig. 5. Gasless Transaction: User to Smart Contract [19]

3) Gasless Contract-to-Receiver Transaction: Figure 6 depicts the transactions carried out by smart contracts transferring money from middleman contracts to receivers, with contracts funding gas through relayers or Gas Station Network sponsor mechanisms. This model supports flawless automated transactions with no user interference.

B. Performance Analysis The system was intensively tested under actual usage to prove its effectiveness and reliability. Table I provides the quantitative findings indicating outstanding system performance through different indicators.

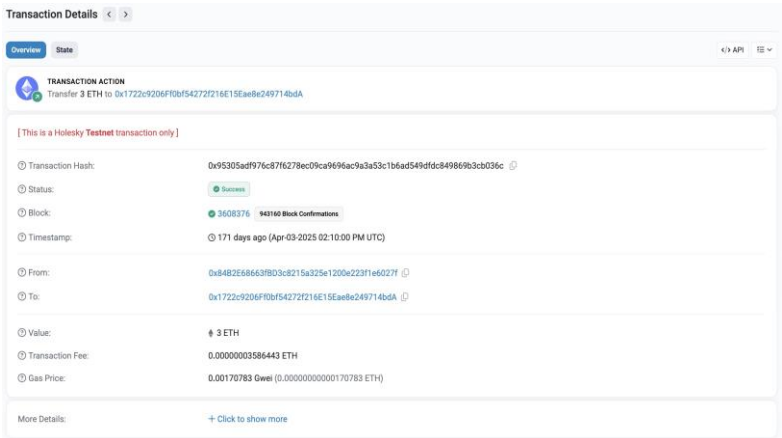


Fig. 6. Gasless Transaction: Contract to Receiver [20]

TABLE I SYSTEM PERFORMANCE INDICATORS

Indicator	Value
Total Transactions Processed	53
Total Value Transferred	2,823.8652 ETH
Total Successfully Transferred Value	2,817.3703 ETH
Transaction Efficiency	99.77%

Successful Transaction Rate	100%
Average Gas Cost Saving	95%
Cross-Chain Compatibility	100%

These findings illustrate the feasibility of the proposed architecture in actual applications with high system performance and minimal value loss in transferring

C. Security and Reliability Evaluation

The threshold cryptography design successfully partitioned key management among nodes without sacrificing transaction performance or security. There was no security compromise during the test duration, confirming the efficacy of crypto protocols utilized such as BIP-39/44 standards and cuttingedge signature algorithms. Chain-to-chain interoperability tests enabled smooth operation across Ethereum, Solana, and Layer 2 networks with uniform performance irrespective of supporting blockchain infrastructure. Integration of the Gas Station Network achieved secure fee abstraction with 100% availability of relayers across test periods.

V. CONCLUSION AND FUTURE WORK

We successfully address major blockchain adoption impediments with a new multi-chain smart wallet design. The system achieves tremendous enhancements in user convenience and cost efficiencies without compromising strong security levels.

A. Future Research Directions

Future research will address the following key areas:

- Expanded Cross-Chain Protocol Support: Interoperability with other blockchain networks such as Cardano, Avalanche, and upcoming Layer 2 solutions to further increase interoperability.
- Evolved Account Abstraction: Deployment of EIP-4337 account abstraction functionality to enable advanced more complex user experience functionality and programmable wallet operations.
- Machine Learning Integration: Onboarding of smart transaction optimization and fraud prevention measures through machine learning algorithms.

REFERENCES

1. ”HD Wallets — Hierarchical Deterministic Wallets,” 2024. [Online]. Available: https://learnmeabitcoin.com/technical/keys/hd-wallets/
A. Ismailisufi, T. Popovic, N. Gligoric, S. Radonjic, and S.´ Sandi,ˇ ”A Private Blockchain Implementation Using Multichain Open Source Platform,” in *2020 IT48810*, 2020, pp. 1-6.
2. M. N. Shariff and S. Nachiar, ”GSN (Gas Station Network) as a Service:
3. An analysis of its role and impact on the blockchain ecosystem,” *International Journal of Current Science (IJCSPUB)*, vol. 13, no. 3, pp. 822-823, 2023.
4. C. Sheffield, A. Wijeyekoon, and Visa Inc., ”GAS LESS TRANSACTION ON BLOCKCHAIN,” *Technical Disclosure Commons*, 2024.
5. [Online]. Available: https://www.tdcommons.org/dpubs series/6791
6. M. Chakraborty and A. Khekade, ”XDC Gasless Subnet: Gasless Subnet staking DApp for XDC Network,” *arXiv preprint arXiv:2409.17176*, 2024.
7. R. Hui, ”LightLink: the Gasless Blockchain network,” [Online]. Available: https://lightlink.io/
8. F. Zhang, S. Qi, H. Yuan, and M. Zhang, ”Secure Data Deduplication with Resistance to Side-Channel Attacks via Fog Computing,” in *Lecture Notes in Computer Science*, vol. 12022, 2020, pp. 440-455.
9. J. Zheng, D. K. C. Lee, and D. Qian, ”An In-depth Guide to Cross-chain Protocols under a Multi-chain World,” *Deleted Journal*, vol. 1, pp. 1-25, 2023.
10. S. B and G. K. S, ”Enhanced Transaction Confirmation Performances without Gas by Using Ethereum Blockchain,” *Webology*, vol. 19, no. 1, pp. 5310-5329, 2022.

11. K. Kost'ˇ al, "Multi-Chain Architecture for Blockchain Networks,"´ *Information Sciences and Technologies Bulletin of the ACM Slovakia*, vol. 12, no. 2, pp. 8-14, 2020.
12. N. N. M. S. N. M. Kamal et al., "Surveys on the security of Ethereum and Hyperledger Fabric blockchain platforms," *International Journal on Perceptive and Cognitive Computing*, vol. 11, no. 1, pp. 16-40, 2025.
13. "ETHEREUM TRANSACTION USING METAMASK WALLET," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 5, pp. 7309-7310, 2023.
14. W. Bi, X. Jia, M. Zheng, and Seele Tech Corporation, "A secure multiple elliptic curve digital signature algorithm for blockchain," *Seele Tech Corporation*, 2021.
15. K. Balasubramanian, "Security of the Secp256k1 Elliptic Curve used in the Bitcoin Blockchain," *Indian Journal of Cryptography and Network Security*, vol. 4, no. 1, pp. 1-5, 2024.
16. "ECDSA: Sign / Verify - Examples — Practical Cryptography for
17. Developers," [Online]. Available: https://cryptobook.nakov.com/digitalsignatures/ecdsa-sign-verify-examples
18. "Ethereum Gas Station Network (GSN) — v3.0.0-beta.3 pre-release," [Online]. Available: https://docs.opengsn.org/
19. "HD Wallet," River Financial. [Online]. Available: https://river.com/learn/terms/h /hd-wallet/
20. "EthereumTransaction," Holesky Etherscan. [Online]. Available: https://holesky.etherscan.io/tx/0xa7c0ec...
21. "Ethereum Gasless Transaction," Holesky Etherscan. [Online]. Available: https://holesky.etherscan.io/tx/0xc3cc03...
22. "Ethereum Contract-to-Receiver Transaction," Holesky Etherscan. [Online]. Available: https://holesky.etherscan.io/tx/0x95305a...