Cypher Zer0x: A Compliant L2 Solution for Private Transactions

Thomas Hussenet, FinTech Engineer
Member of KRYPTOSPHERE®

Adam Dahmoul, Data Scientist / Engineer
Board Member of KRYPTOSPHERE®

Maxime Dienger, FinTech & Software Engineer
Head of KRYPTOSPHERE®

Nathan Hervier, FinTech Engineer
Member of KRYPTOSPHERE®

February 29, 2024

Abstract

The proliferation of blockchain technology has ushered in an era of unprecedented transparency. However, this transparency often comes at the cost of privacy, leaving a critical gap in the market for compliant, private transactions. Cypher Zer0x aims to bridge this gap by introducing the first cross-chain, compliant Layer 2 (L2) solution specifically designed for private transactions. Leveraging cutting-edge zero-knowledge (ZK) technology and ring signatures, Cypher Zer0x offers a secure, confidential, and modular platform for private transactions without compromising on compliance.

1 Introduction

Blockchain technology has transformed the landscape of digital transactions, offering unparalleled security and transparency. However, this transparency poses significant privacy concerns, hindering the adoption of blockchain in sectors where confidentiality is paramount. The absence of a compliant mechanism for private transactions stifles innovation and limits blockchain's potential applications.

2 Layer ZER0X: Bridging the Privacy Gap

Cypher Zer0x introduces Layer ZER0X, a revolutionary cross-chain L2 solution designed to facilitate private transactions while adhering to regulatory compliance. Layer ZER0X characteristics include:

- **High Transaction Output:** Capable of handling a vast number of transactions efficiently.
- **Confidential:** Ensures the privacy of transaction details through ZK technology and ring signatures.
- **Plasma Based:** Utilizes Plasma technology for scalable and secure off-chain transactions.
- **UTXO Based Model:** Employs an Unspent Transaction Output (UTXO) model for enhanced privacy and efficiency.
- **Secured by ZK:** Incorporates zero-knowledge proofs to ensure transaction validity without revealing sensitive information.
- **Modular:** Designed with a modular architecture to support diverse applications and scalability.

3 Practical Use Cases

Cypher Zer0x addresses a wide array of applications where privacy and compliance are critical:

- Banking secret for inner transactions.
- Confidential transactions across various sectors.
- Private payments and bridges for secure, anonymous transfers.
- Privacy for commercial transactions to protect trade secrets and customer data.

4 Compliance and Security

At the heart of Cypher Zer0x lies a strong commitment to compliance and security:

- **Daily Transfer Limits:** Imposes limits based on user type to prevent illicit activities.
- **KYC Processes:** Mandatory KYC through PolygonID or ZKPass before deposits and withdrawals.

- **Address Monitoring and Blacklisting:** Utilizes Harpi to monitor addresses and build blacklists.
- **Geo Restrictions:** Enforces geographical limitations to mitigate risks associated with illicit activities.

5 Technical Overview

Cypher Zer0x introduces a cutting-edge architecture designed to integrate seamlessly with blockchain ecosystems, ensuring privacy and compliance in transactions. The framework is structured around four key components: Client, Compliance Stack, Wallet, and Blockchain. Each component plays a crucial role in Cypher Zer0x's operations, delivering a comprehensive solution for private and secure transactions.

5.1 Client

The client-side of Cypher Zer0x is built with Rust for its core logic and TypeScript for its cryptographic operations. The platform utilizes LMDB (Lightning Memory-Mapped Database) for a high-performance, synchronous key-value store, facilitating efficient data management.

The platform's state management and integrity verification leverage Rust for the creation of snapshots, generation of Merkle roots, and verification processes. These operations ensure the accuracy and security of state transitions within the system. Upon verifying the state, Cypher Zer0x employs RiscZER0 to generate a zero-knowledge proof, confirming the authenticity of the state verification without exposing sensitive information. This meticulous process underscores Cypher Zer0x's commitment to privacy and security.

TypeScript is utilized for the cryptographic components of the platform, specifically for generating ring signatures that sign transactions. This approach enhances the privacy of transactions by enabling users to prove transaction authenticity without revealing the signer's identity.

5.2 Compliance Stack

The compliance framework within Cypher Zer0x is bolstered by integrating Polygon ID and Harpie for KYC and background checks. This ensures that all users comply with regulatory requirements before participating in transactions. Future enhancements include the potential integration of Harpie on-chain or dynamically with Polygon ID to streamline and secure the compliance process further.

5.3 Wallet Integration

Cypher Zer0x leverages Metamask SNAP for wallet integration, allowing for efficient and secure on-chain wallet interactions. This integration simplifies the management of digital assets on the platform, emphasizing user convenience and security.

5.4 Blockchain Compatibility

Designed for cross-chain functionality, Cypher Zer0x supports a variety of blockchain networks, including Ethereum, XDC Network, Zircuit, Hedera Hashgraph, Near Protocol, Moonbeam, Oasis Network, Inco, Injective Protocol, Linea, and Polygon. This extensive compatibility facilitates deposits, withdrawals, and L2 state maintenance across these diverse ecosystems, positioning Cypher Zer0x as a versatile platform for conducting private, compliant transactions.

5.5 Data Availability and Resilience

To ensure system resilience and data availability, Cypher Zer0x integrates with the NEAR Protocol, especially for maintaining access to funds even when the primary blockchain is down. Following state verification, the platform commits the UTXO set to NEAR, effectively duplicating the chain's state on this blockchain. This strategy guarantees that information necessary for fund recovery is always accessible, enhancing the platform's reliability and user trust.

6 The Team

Cypher Zer0x is spearheaded by a team of experts in FinTech and blockchain technology:

- Thomas Hussenet, FinTech Engineer, Member of KRYPTOSPHERE®.
- Adam Dahmoul, Data Scientist / Engineer, Board Member of KRYPTOSPHERE®.
- Maxime Dienger, FinTech & Software Engineer, Head of KRYPTOSPHERE®.
- Nathan Hervier, FinTech Engineer, Member of KRYPTOSPHERE®.

7 Conclusion

Cypher Zer0x's innovative technical architecture, emphasizing privacy, compliance, and cross-chain interoperability, establishes a new standard in the field of private blockchain transactions. By leveraging advanced technologies and ensuring robust data availability through NEAR Protocol, Cypher Zer0x delivers a secure, efficient, and user-friendly platform for digital asset management. Its dedication to maintaining a compliant and resilient infrastructure makes it an exemplary solution for users seeking privacy in their blockchain interactions.