Kaviar: A Regulatory-Compliant and Privacy-Preserving Cross-Chain Protocol

Version 0.1

Abstract

Blockchain technology heralds a new era of decentralization, yet it struggles with the dual challenges of privacy and regulatory compliance. Existing cross-chain solutions either lack privacy preservation or support for regulation. Kaviar emerges as a revolutionary solution, striking a delicate balance between these two imperatives. This white paper outlines KAVIAR's innovative approach to secure, private, and compliant cross-chain transactions by utilizing zero-knowledge proofs and privacy pool techniques. With advanced regulatory-compliant privacy-preserving techniques, Kaviar is also capable of enabling interchain decentralized finance (DeFi) applications for real-world assets (RWAs) from the traditional financial sector.

1 Introduction

In the transformative wave of blockchain technology, the promise of decentralization has been a driving force for innovation and growth. The immutable and transparent nature of blockchain has redefined the concept of trust in digital transactions, laying the groundwork for a future where decentralized finance (DeFi) and real-world assets (RWAs) can interact seamlessly within the digital ecosystem. However, as the technology matures, it faces significant challenges that threaten to stifle its potential: the need for privacy and the imperative of regulatory compliance.

The privacy of individuals and entities on the blockchain is often compromised by the very features that make the technology secure: the public ledger and the traceability of transactions. While these aspects are crucial for transparency and fraud prevention, they leave little room for confidentiality, exposing users to risks and deterring the participation of traditional financial sectors that operate under strict privacy requirements.

At the same time, the evolving regulatory landscape presents another layer of complexity. As governments and financial authorities strive to implement regulations to safeguard against illicit activities, blockchain platforms and applications must navigate a maze of compliance standards. This is particularly challenging for cross-chain transactions, where assets and information traverse multiple blockchains, each with its own protocols and security measures.

Existing cross-chain solutions seldom target the challenges of privacy and regulatory compliance simultaneously. Some solutions, such as Multichain and LayerZero, focus on blockchain interoperability but do not address privacy preservation. Others, like the Webb Protocol and Zecrey Protocol, concentrate on private cross-chain transactions but overlook compliance concerns. Mystiko is a privacy-preserving cross-chain protocol that supports regulatory compliance; however, it relies on third parties called auditors to audit the cross-chain transactions, which does not fully adhere to decentralization principles.

Multichain [5]: is a cross-chain protocol that employs a committee of validators to verify transactions across multiple blockchains. It is a semi-decentralized solution that does not support privacy preservation. The cross-chain transactions are verified and signed by a committee of validators using a multi-signature technique.

LayerZero[3]: This cross-chain protocol is comprised of a Relayer and Oracle. The Relayer is used to deliver cross-chain transactions and proofs across different blockchains, while the Oracle is used for updating the light client data and verifying the cross-chain transactions and proofs. This protocol is fully decentralized but does not support privacy preservation.

Webb protocol[6]: This is a cross-chain protocol designed to enable private applications across various blockchain systems. It aims to create a shared anonymity set across bridged blockchains, facilitating private and secure transactions. The protocol utilizes Merkle trees for state verification and zero-knowledge proofs to maintain privacy. However, it does not support regulatory compliance.

Zecrey Protocol[2]: This cross-chain protocol is dedicated to privacy preservation, employing ZK-Rollup technology to facilitate confidential and anonymous transactions across multiple blockchains. It is tailored to work with blockchains that support smart contracts, providing a second-level general cross-chain bridge for asset transfers. Zecrey ensures transaction privacy and offers functionality for private cross-chain swaps, serving users and entities that prioritize confidentiality in their blockchain interactions. While it emphasizes privacy, the protocol does not inherently address regulatory compliance, setting it apart from solutions that strive for a balance between privacy and regulatory adherence.

Mystiko Netwrok[1]: This is a cross-chain protocol that upholds regulatory compliance and privacy preservation. It operates as a private cross-chain bridge with support for auditing by a set of auditors. Each transaction has an auditing key (public key, private key), with the private key securely shared among all the auditors through threshold secret sharing. A significant portion of auditors can audit a private transaction by identifying the source transaction address. To reduce the cost of updating the Merkle tree of the deposit commitment on smart contract, the protocol uses zk-rollup to update the Merkle root along with a zk-proof.

To address the challenges of privacy and regulatory compliance, Kaviar has developed a cross-chain protocol that leverages zero-knowledge proofs and privacy pool techniques. The protocol is designed to support the transfer of assets and information across multiple

blockchains, while preserving the privacy of users and entities and adhering to regulatory standards. Kaviar's solution is based on the following principles:

- **Privacy preserving:** Kaviar's cross-chain protocol is crafted to safeguard the privacy of users and entities, ensuring that sensitive data is not disclosed to unauthorized parties. The protocol employs zero-knowledge proofs, enabling cross-chain transactions without revealing the connection between the source and destination transactions.
- **Regulatory compliant:** Kaviar's cross-chain protocol is built to conform to regulatory standards, guaranteeing that transactions comply with pertinent regulations. The protocol uses a privacy pool technique that supports the transfer of assets and information across multiple blockchains while adhering to regulatory demands.
- **Fully decentralized:** Kaviar's cross-chain protocol is architected to operate in a completely decentralized manner, ensuring that the protocol functions within a permissionless environment. It leverages smart contracts and zero-knowledge proofs to validate transactions, thereby obviating the necessity for a centralized overseer.

2 Background

2.1 Zero-Knowledge Proof

Zero-Knowledge Proofs (ZKPs) are a cryptographic innovation that allows a party, known as the prover, to validate the truth of a claim to another party, the verifier, without revealing any information beyond the verification of the statement itself. These proofs are characterized by two primary attributes:

- **Zero-Knowledge**: This property ensures that no private data is revealed, other than the fact that the claim being proven is true.
- **Succinctness**: This attribute ensures that the proof is concise and can be quickly verified, regardless of the complexity of the claim.

In blockchain technology, ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) are used to enhance privacy in transactions, allowing the anonymity set of each transaction to potentially encompass all previous transactions.

2.2 Merkle Tree Membership Proof

Merkle Trees are pivotal data structures in blockchain technology, used for secure and efficient verification of large data sets. In privacy protocols, these trees manage coin IDs and nullifiers, enabling proofs of membership or non-membership. This system allows verification of transactions while maintaining the confidentiality of detailed transaction information.

2.3 Privacy Pool

Privacy Pools are novel protocols designed to improve privacy in blockchain transactions. They utilize ZKPs to enable users to prove specific properties about their transactions, such as their inclusion in or exclusion from certain sets of transactions, known as association sets from Vitalik's paper [4]. This functionality is crucial in striking a balance between privacy preservation and regulatory compliance, enabling users to demonstrate compliance without revealing their entire transaction history.

3 Kaivar Protocol

The Kaviar Protocol represents a groundbreaking advancement in the realm of blockchain technology, specifically addressing the critical need for privacy preservation and regulatory compliance in cross-chain transactions. This overview provides a high-level understanding of how the Kaviar Protocol functions, its unique features, and the benefits it brings to the blockchain ecosystem.

3.1 Core Principles

The Kaviar Protocol is built upon three foundational principles:

1. **Privacy Preservation:** Ensuring the confidentiality of user transactions and data across multiple blockchain networks.
2. **Regulatory Compliance:** Adhering to the diverse and evolving regulatory standards across jurisdictions.
3. **Decentralization:** Maintaining a fully decentralized system that operates without reliance on centralized control or intermediaries.

3.2 Operational Flow

The Kaviar Protocol operates through a series of meticulously designed steps to ensure secure, private, and compliant cross-chain transactions:

- **Step 1: Asset Deposit and Commit Hash Generation**
  - **User Action:** The user utilizes their address (referred to as address1) on the sending chain to deposit the asset.
  - **Commit Hash Creation:** Concurrently, a commit hash is generated by the user, incorporating private commit information, which includes a secret and a nullifier. This hash serves as a cryptographic commitment to the transaction, ensuring privacy and security.

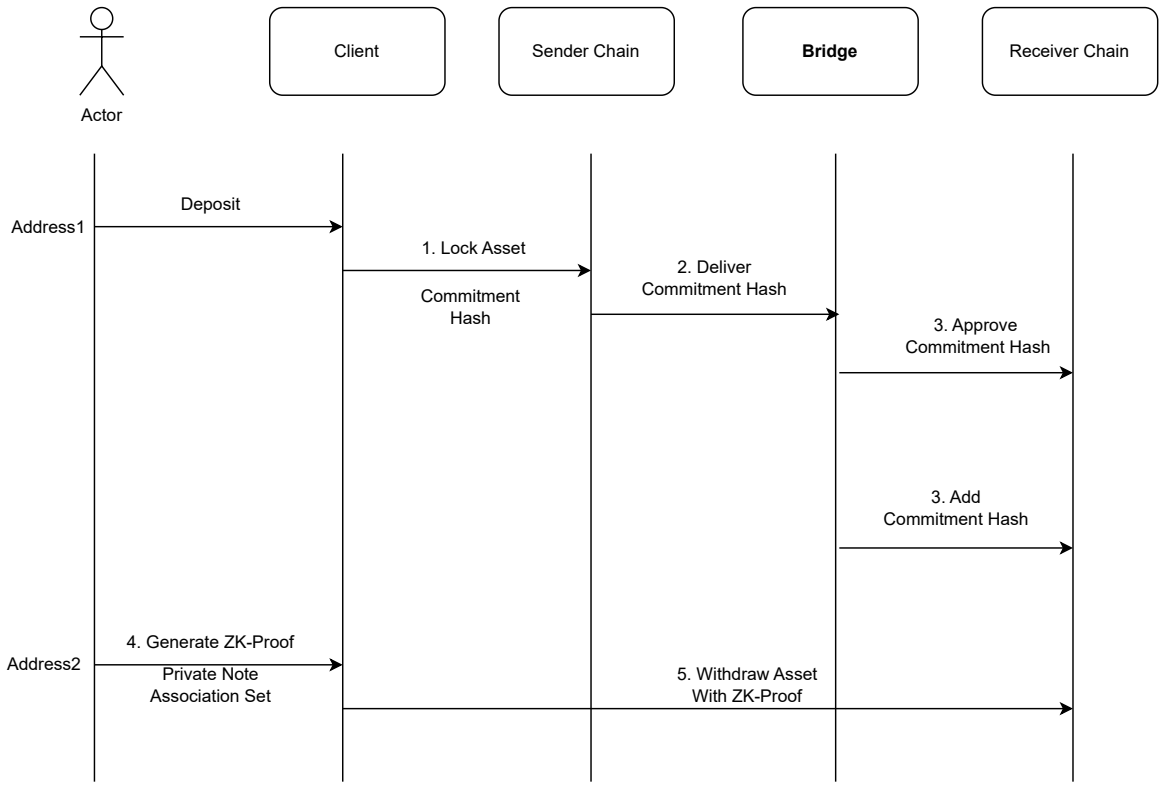

Figure 1: Kaviar Cross-chain asset transfer workflow

- **Step 2: Cross-Chain Message Passing**
  - **Protocol Functionality:** The Cross-Chain Message Passing Protocol comes into play, tasked with the secure and efficient delivery of the commit hash data to the receiver chain.
  - **Data Transmission:** This step involves the transfer of the commit hash, encapsulating the transaction details, from the send chain to the receiver chain, maintaining the integrity and confidentiality of the data.
- **Step 3: Zero-Knowledge Proof Generation and Transaction Finalization**
  - **User Action on Receiver Chain:** The user, now operating with a different address (address2) on the receiver chain, generates a Zero-Knowledge proof (ZK-proof). This proof is constructed using their private note, which again includes the secret and nullifier, along with Association Set information.
  - **ZK-Proof Utilization:** The ZK-proof, a cornerstone of privacy preservation, validates the transaction without revealing the underlying private information, thereby maintaining the confidentiality of the user's data and adhering to privacy norms.

- **Step 4: Smart Contract Verification and Asset Withdrawal**
  - **Smart Contract Involvement:** Upon receiving the ZK-proof, the smart contract on the receiver chain initiates a verification process.
  - **Verification and Withdrawal:** The smart contract meticulously verifies the validity of the ZK-proof. Once verified, it facilitates the withdrawal of assets on the receiver chain. This step is crucial as it ensures that the transaction is not only private but also complies with the integrity and security standards of the protocol.

3.3 Multi-chain Anonymous Set

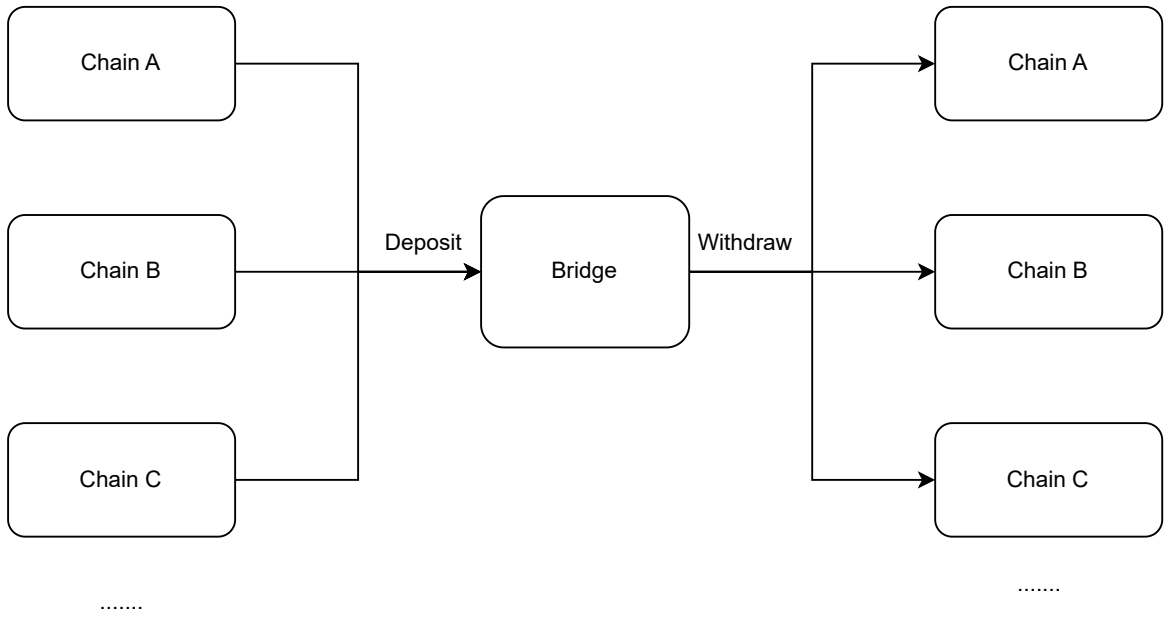

Figure 2: Kaviar multi-chain anonymous set

The Kaviar Protocol introduces an innovative concept in the realm of blockchain privacy and security - the Multi-chain Anonymous Set. This feature significantly enhances the privacy-preserving capabilities of the protocol, surpassing the traditional single-chain mixers like Tornado Cash in terms of anonymity and flexibility.

- **Enhanced Anonymity Set Size:** The anonymous set in Kaviar is inherently larger than that of typical single-chain mixers. By aggregating users across multiple chains, Kaviar creates a more extensive and diverse pool of participants. This increased size of the anonymity set substantially improves privacy, as it becomes more challenging to trace individual transactions within a larger group.

- **Cross-Chain Flexibility:** A distinctive feature of the Kaviar Protocol is its ability to allow users to join the anonymous set from any send chain and to mix and withdraw assets across different chains, including the option to return to the original chain. This flexibility not only enhances user convenience but also adds an additional layer of privacy. Users are not restricted to mixing and withdrawing assets within the same blockchain, thereby broadening the scope of anonymity.

- **Implementation of Inter-Chain Mixer:** Kaviar implements an inter-chain mixer, a pioneering approach in the field of blockchain privacy. This mixer is designed to operate seamlessly across multiple blockchains, providing a robust privacy-preserving mechanism. By enabling asset mixing and withdrawal across different chains, Kaviar's inter-chain mixer offers a level of privacy and security that is a significant advancement over traditional single-chain solutions.

The Multi-chain Anonymous Set is a cornerstone of Kaviar's approach to privacy and security in the blockchain space. By leveraging the power of cross-chain interactions and a larger anonymity set, Kaviar sets a new standard for privacy-preserving protocols in decentralized finance.

3.4 Association Sets Construction

The Kaviar Protocol introduces a sophisticated mechanism known as Association Sets Construction, which plays a pivotal role in enhancing both privacy and regulatory compliance. This mechanism comprises three distinct types of sets: whitelist sets, blacklist sets, and semi-blacklist sets, each serving a unique purpose in the protocol's ecosystem.

- **Whitelist Sets:** These sets are user-defined and allow any participant to create their own whitelist by adding trusted users from a community source. The effectiveness of a whitelist set in preserving privacy is directly proportional to its size; larger whitelist sets provide better privacy. This is because they increase the number of potential transaction partners, thereby diluting the probability of linking transactions to specific individuals.

- **Blacklist Sets:** Blacklist sets are crucial for maintaining the integrity and security of the network. They are composed of addresses associated with known blockchain attacks or sanctioned by governments, derived from public data sources. The update and maintenance of blacklist sets require a consensus from the community, ensuring that the process is democratic and transparent. This feature helps in safeguarding the network against malicious entities and complying with global regulatory standards.

- **Semi-Blacklist Sets:** These sets are generated through big data analysis, utilizing AI technologies such as large language models. Semi-blacklist sets are designed to enhance

the regulatory compliance aspect of the protocol, particularly for users with specific regulatory needs. They help in identifying potentially risky transactions or entities by analyzing patterns and behaviors that may not be explicitly listed in traditional blacklist sets. This proactive approach aids in maintaining a high standard of regulatory compliance while preserving the decentralized nature of the blockchain.

The Association Sets Construction feature of the Kaviar Protocol represents a balanced approach to privacy and regulatory compliance. By allowing users to define their own trusted networks while also protecting against known risks and potential regulatory issues, Kaviar sets a new benchmark in the realm of cross-chain protocols.

4 Future Directions

As the Kaviar Protocol continues to evolve, there are several exciting avenues for future development that can further enhance its capabilities and applications in the blockchain ecosystem. These directions not only aim to expand the protocol's functionality but also to integrate it more deeply into the broader landscape of decentralized finance (DeFi) and real-world asset (RWA) management. The following are key areas of focus for future development:

4.1 Privacy-Preserving Cross-Chain Decentralized Exchange (DEX)

- The Kaviar Protocol aims to extend its privacy-preserving features beyond asset transfers to include a fully functional cross-chain decentralized exchange (DEX). This development will enable users to engage in secure, private trading activities across different blockchain networks.
- By leveraging the protocol's privacy and security mechanisms, the cross-chain DEX will offer a platform where users can trade a variety of assets without compromising their transactional privacy. This initiative will mark a significant step forward in the realm of DeFi, combining the benefits of decentralization with enhanced privacy.

4.2 On-Chain KYC Service

- Utilizing the rich dataset from Kaviar's association sets, the protocol plans to offer an on-chain KYC (Know Your Customer) service. This service will be designed to provide DeFi projects with reliable and secure identity verification tools.
- The on-chain KYC service will leverage Kaviar's privacy-preserving technology to ensure that user identity verification is conducted in a manner that respects user privacy while adhering to regulatory requirements. This service will be instrumental in bridging the gap between the need for regulatory compliance and the ethos of user privacy in DeFi.

4.3 Real World Asset (RWA) Integration

- The Kaviar Protocol is uniquely positioned to drive the integration of real-world assets (RWAs) into the blockchain space. With its strong focus on privacy and regulatory compliance, Kaviar can facilitate the tokenization and management of RWAs, opening up new use cases and opportunities.
- This integration will enable the seamless and secure representation of physical assets on the blockchain, enhancing the utility and reach of DeFi. It will allow for innovative applications such as fractional ownership, asset-backed lending, and more, all within a privacy-preserving and compliant framework.

These future directions represent a strategic expansion of the Kaviar Protocol's capabilities, aiming to solidify its position as a leading solution in the intersection of privacy, compliance, and innovation in the blockchain domain.

5 Conclusion

The Kaviar Protocol represents a pivotal advancement in the blockchain sphere, skillfully addressing the dual challenges of maintaining privacy and ensuring regulatory compliance in cross-chain transactions. Its cornerstone is the innovative use of zero-knowledge proofs, which enables the protocol to offer a high level of privacy while upholding decentralization and compliance standards. The introduction of Multi-chain Anonymous Sets and Association Sets Construction enhances transaction privacy and flexibility, setting Kaviar apart from existing solutions. Looking ahead, the protocol aims to broaden its impact by integrating privacy-preserving Cross-Chain Decentralized Exchanges (DEX), on-chain KYC services, and Real World Asset (RWA) management. These future directions underscore Kaviar's commitment to innovation, positioning it as a key player in reshaping the landscape of decentralized finance and blockchain technology.

6 References

[1] Mystiko whitepaper. https://mystiko.network/whitepaper.pdf. (Accessed on 11/26/2023).

[2] Zecrey whitepaper. https://docsend.com/view/ntcsmt7meu84gcqk. (Accessed on 11/26/2023).

[3] Layerzero whitepaper. https://archive.ph/LONdd, 2021.

[4] V. Buterin, J. Illum, M. Nadler, F. Schär, and A. Soleimani. Blockchain privacy and regulatory compliance: Towards a practical equilibrium. *Available at SSRN*, 2023.

[5] Multichain. Cross-chain bridge. https://archive.ph/wip/9yvRZ, 2023.

[6] D. Stone. Webb protocol: A cross-chain private application and governance protocol. *Cryptology ePrint Archive*, 2023.