# CHAI

## Part I — A Chain Aggregation Identity Layer

Shlok Dharmesh Mange
shlok@0xrivendell.xyz

*as of* May 31, 2024

***Abstract.*** The Chain Aggregate Identity (CHAI) protocol is designed to serve as the unified identity layer for all of internet applications, integrating both on-chain and off-chain identities into a single, secure layer. Leveraging on-chain data such as decentralized finance (DeFi) activity, recency bias, active transactions, and NFTs/tokens held, alongside off-chain data such as Emirates ID, Social Security Numbers (SSN) (& other country-specific documents), CHAI provides a comprehensive on-chain KYC system. This system is fortified by zero-knowledge proofs (ZKPs) submitted onchain via an Eigenlayer Active Validated Services (AVS), ensuring privacy, security, and compliance across all applications.

# 1. Introduction

The evolution of blockchain technology has brought about a myriad of decentralized applications (dApps) and financial services that require robust identity verification mechanisms. However, the lack of a unified identity layer has led to fragmented identity verification processes, posing significant challenges in terms of compliance, security, and user experience.
CHAI aims to address these challenges by providing a unified identity protocol that aggregates on-chain and off-chain identity data. By doing so, CHAI simplifies the identity verification process, enhances security through zero-knowledge proofs, and ensures compliance with global regulatory standards. With aggregating onchain & offchain identities, this has implications beyond web3 and can be used as api level replacements in various compliance centric apps using centralised kyc api services.

# 2. Problem Statement

Current identity verification systems in the Web3 ecosystem suffer from fragmentation and inefficiencies. Users often need to undergo multiple wallet connection processes for different chains, multiple user owned wallets & app-specific smart wallets leading to redundancy and increased risk of data breaches. Additionally, existing systems do not fully leverage the potential of on-chain data, which can provide a more comprehensive view of a user's identity and activity.
The lack of a unified identity protocol also hampers interoperability among dApps and financial services, limiting the seamless user experience that Web3 promises. Furthermore, ensuring compliance with diverse regulatory requirements while maintaining user privacy remains a significant challenge.

## 3. The Need for Unified Identity in Web3

In the decentralized world of Web3, identity verification is crucial for ensuring security, trust, and compliance. Traditional KYC processes are not only cumbersome but also fail to utilize the rich data available on-chain. By aggregating both on-chain and off-chain identities, including but not limited to: farcaster activity, defi transaction history, multiple wallet ownership, erc721 ownership, activities in governance forums etc. CHAI provides a holistic solution that streamlines verification processes and enhances security.

## 4. Onchain Data Utilization

On-chain data, including but not limited to: farcaster activity, defi transaction history, multiple wallet ownership, erc721 ownership, activities in governance forums etc offers a dynamic and transparent view of a user's behavior and trustworthiness. CHAI leverages this data to provide real-time, verifiable identity proofs that can be used across various platforms.

## 5. Offchain Data Integration

Off-chain data such as twitter activity (deign score), GitHub commit history(extremely useful incase of developer centric airdrops) & physical resident proofs i.e national IDs, SSNs, and other country-specific documents which are essential for compliance with regulatory standards. CHAI seamlessly integrates this data, ensuring that users meet the necessary compliance requirements without compromising on privacy.

## 6. Zero-Knowledge Proofs and Eigenlayer AVS

Zero-knowledge proofs (ZKPs) are a cornerstone of CHAI's security architecture. ZKPs allow the verification of identity data without revealing the actual data, preserving user privacy. Eigenlayer's Actively Validated Services (AVS) enables this by allowing the users to connect multiple wallets & prove their ownership, this ownership signatures are then aggregated as a merkle root with a keystore tied to the users activity score. This score is dynamically updated based on the user activity (onchain & offchain), ensuring that the identity data remains current and accurate.

## 7. Security and Compliance

CHAI's integration of on-chain and off-chain data, secured by ZKPs, offers a robust solution for identity verification. This approach not only ensures compliance with global regulatory standards but also protects against identity fraud and data breaches.

## 8. Interoperability

By providing a unified identity layer, CHAI enhances interoperability among dApps and financial services. Users can seamlessly access multiple platforms with a single, verifiable identity, improving the overall user experience and fostering greater adoption of Web3 technologies.

# 9. Implementation of CHAI

For developers and businesses looking to integrate CHAI, the protocol provides comprehensive APIs and SDKs that facilitate easy integration. The use of ZKPs ensures that identity data remains private and secure, while the Eigenlayer AVS provides ongoing verification and updates.

# 10. Adoption Strategies

To drive adoption, CHAI will engage with key stakeholders in the Web3 ecosystem, including dApp developers, financial services, and regulatory bodies. By demonstrating the benefits of a unified identity layer, CHAI aims to become the standard for identity verification in the decentralized world.

### *Future Developments*

CHAI will continue to evolve, incorporating advancements in blockchain technology and expanding its data sources. Future developments may include enhanced biometric integrations and partnerships with global identity verification providers.

# 11. Conclusion

CHAI represents a significant advancement in the realm of identity verification for Web3. By aggregating on-chain and off-chain identities into a single, secure layer, CHAI addresses the key challenges of fragmentation, security, and compliance. Through the use of zero-knowledge proofs and the Eigenlayer AVS, CHAI ensures that user identities are verifiable, private, and continuously updated. As the unified identity layer for Web3, CHAI is poised to drive greater adoption and trust in decentralized applications and financial services.

# 12. References

Polygon ID: Zero Knowledge Identity for Web3
**https://polygon.technology/blog/introducing-polygon-id-zero-knowledge-own-your-identity-for-web3**

Web3: A decentralized societal infrastructure for Identity, Trust, Money, Data
**https://ar5iv.labs.arxiv.org/html/2203.00398**

Digital Identity: Assessing Web3's Building Blocks by JP Morgan
**https://www.jpmorgan.com/onyx/digital-identity-web3-building-blocks**

Mastering Decentralized Identity: A Pillar of Web3
**https://blockworks.co/news/what-is-decentralized-identity**

Using Aggregation To Solve Identity
**https://workweek.com/2022/08/22/using-aggregation-in-web3-to-solve-identity/**