Identity Bridge Litepaper

Michael Kerr, Jason Child

November 2024 v0.4

Abstract. Identity Bridge transforms digital identity and key management by combining zero-knowledge proofs (ZKPs) with seamless interoperability across Web3 and Web2. Its innovative ZK authentication framework eliminates static seed phrases and centralized systems, enabling users to securely create and recover cryptographic keys while protecting sensitive data. With Wrapped Identity Tokens (WITs), the platform empowers users to assert identity privately and efficiently across decentralized and traditional platforms. Designed with a user-first approach, Identity Bridge sets a new benchmark for privacy-preserving identity solutions in a connected digital era.

Keywords—Zero-Knowledge Proofs, Identity Verification, Key Management, Interoperability, Decentralized Identity

1 INTRODUCTION

1.1 Key Management Challenges - Traditional crypto key management systems rely on insecure and cumbersome methods like seed phrases. Users who lose their phrases risk permanent asset loss, while exposed phrases can lead to security breaches and account takeover. Centralized authentication systems shift custodial control to third parties, introducing risks and discouraging self-sovereignty. These systems also lack practical recovery processes, further complicating their adoption.

1.2 Identity Verification Challenges - Existing identity verification methods require users to share sensitive personal information, leading to privacy concerns and risks, regulatory complications, and fragmentation/limited use across platforms. Current solutions fail to support flexible verification levels or interoperability, making them impractical for both Web3 and Web2 ecosystems.

2 CONCEPT OVERVIEW

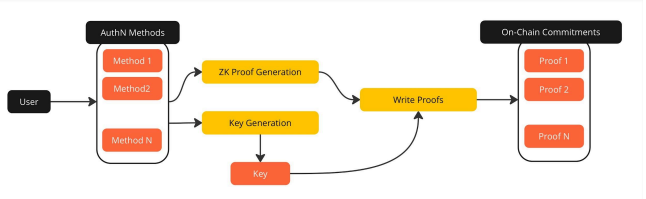
2.1 Zero-Knowledge Authentication Framework - Identity Bridge implements a zero-knowledge (ZK) authentication framework that eliminates reliance on only static secrets or centralized storage for key management and identity verification. Users can generate cryptographic keys deterministically and authenticate their identity using ZK proofs, ensuring security, flexibility, and privacy.

Key Features:

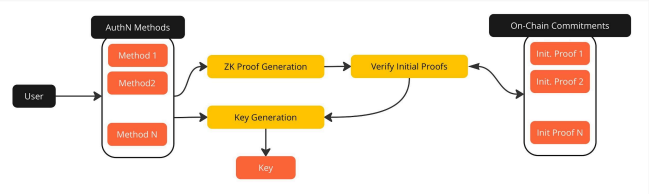
- ***ZKP-Driven Key Management:*** Users provide cryptographic proofs to register, verify, and recover their keys or identities without exposing sensitive details.
- ***Factor Attribute-Based Threshold System:*** A modular, multi-factor structure allows users to register multiple identity factors (such as biometrics, passwords, or attestations) and recover their keys using only a subset of these.
- ***On-Chain Privacy Preservation:*** Zero knowledge commitments, as proofs stored on-chain, ensuring tamper-proof recovery while protecting user data.

Implementation Details:

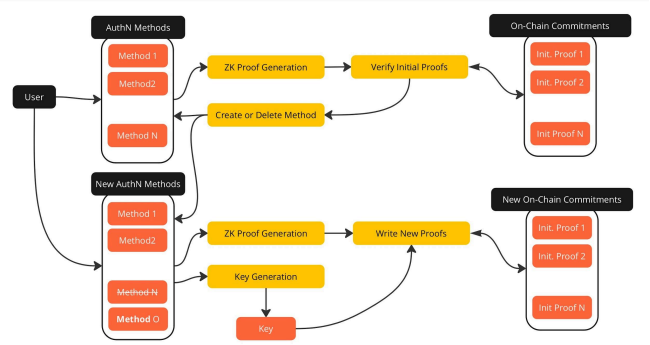
2.1.1 Key Creation: Users register their identity locally via authentication (AuthN) methods (including attributes and metadata) which are hashed and stored on-chain as a ZKP.



2.1.2 Key Recovery: Users generate a ZKP proving knowledge of a subset of AuthNs, which are validated against the original commitments.



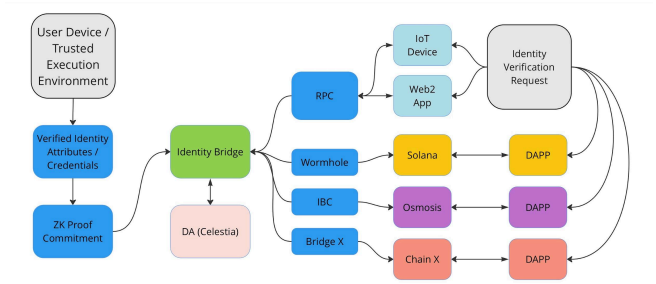
2.1.3 Factor Update: AuthN factors can then be updated (added or removed) based on an ZKP proving knowledge of a subset of AuthNs with new proof being updated to the chain.



2.1.4 Interoperability: The framework supports cross-chain compatibility, letting users recover and use keys across various blockchains.

This framework provides decentralized and secure key recovery - eliminating the risks of seed phrases while offering users the flexibility to customize their authentication.

2.2 Identity Bridge - Building on the ZK authentication framework, Identity Bridge acts as a hub for identity brokering and federation, enabling secure, privacy-preserving identity sharing across Web3 and Web2 ecosystems.



Key Features:

- ***Wrapped Identity Tokens (WITs):*** Non-Transferrable tokens that represent verified credentials (similar to soulbound tokens) ensuring non-transferability and secure identity portability.
- ***ZKP-Based Identity Proofs:*** The bridge uses ZKPs to verify user attributes or credentials without exposing sensitive details.
- ***Cross-Platform Compatibility:*** Identity proofs are verifiable on multiple blockchains and off-chain systems, enabling seamless interoperability.
- ***Customizable Proof Levels:*** Users can choose the scope and detail of their proofs to meet specific security or compliance requirements.

The Identity Bridge combines ZK authentication with a robust interoperability layer, supporting secure key management and privacy-centric identity brokering and federation across decentralized and traditional systems.

Implementation Details:

2.2.1 Onboarding identity Sources

User Attribute Input: Users register various identity attributes from traditional and decentralized sources (e.g., government IDs, biometric data, decentralized credentials).

Hashing and Commitment Creation: Attributes are hashed locally, and the resulting cryptographic commitment is used to generate a ZKP.

ZKP Submission: A ZK circuit generates a proof that the attributes meet verification conditions (e.g., age, residency, KYC compliance). This proof is submitted on-chain for validation.

2.2.2 Creating Wrapped Identities:

Proof Validation: The bridge validates the submitted ZKP against on-chain commitments.

Wrapped Identity Token Issuance: Upon successful validation, the Identity Bridge issues a soulbound WIT representing the user's verified credentials.

Metadata Linking: Minimal metadata associated with the WIT is stored on-chain to enable verification without revealing user attributes.

2.2.3 Assertion and Verification:

Identity Assertions via ZKPs: The user presents their WIT to a dApp or external system.

Proof Validation: The Identity Bridge validates the proof and issues an attestation to the requesting system, confirming that the identity meets the required conditions (e.g., age verification or KYC compliance).

Dynamic Proof Levels: The bridge supports configurable levels of identity proofs, enabling users to tailor assertions to meet specific use case requirements.

3 BENEFITS AND USE CASES

3.1 Benefits

Flexible Key Recovery: Users can register multiple authentication factors and recover their keys using a subset of these factors, validated via ZKPs.

Privacy by Design: Utilize zero-knowledge proofs (ZKPs) to verify user identities and manage keys without exposing sensitive personal information.

Dynamic Factor Management: Users can easily add or remove authentication methods, (such as biometrics, hardware keys, or attestations) without affecting their cryptographic keys.

Cross-Chain Compatibility: Identity proofs and key management processes work seamlessly across blockchain ecosystems, enabling users to interact with multiple networks.

Interoperability with Web2 Systems: Bridges Web3 and Web2 by Enabling privacy-preserving identity verification for traditional platforms like SaaS applications or financial institutions.

Customizable Proof Levels: Supports tailored identity assertions to meet compliance requirements, ranging from basic identity checks to full KYC/AML verification.

3.2 Use Cases

Improved Self-Custody Wallets: Secure key recovery for wallets without relying on seed phrases or centralized storage.

Compliance: Privacy-preserving KYC/AML compliance for DeFi platforms during lending, borrowing, or trading.

Future: Gaming and NFTs Age Verification, Web2 Brokering and Federation, Decentralized Identity for DAOs, E-Commerce and Payments, Cross-Border Compliance, Secure AI Agent Authentication, and more.

4 GOVERNANCE

4.1 Stakeholder Governance with Weighted Voting. The Identity Bridge uses a stakeholder governance model based on weighted voting to ensure fair and balanced decision-making. Different stakeholder groups—such as users, developers, identity providers, and partner projects—are assigned voting rights based on their contributions, engagement, or token holdings.

Weighted Voting Mechanism: Votes are weighted to reflect each stakeholder's role or level of involvement, promoting fairness and preventing over-concentration of power.

Empowering the Community: Decisions are influenced by those with a vested interest in the platform's success, ensuring that the community's voice drives development.

Sustainable Growth: This model ensures informed and representative decision-making, supporting the platform's long-term adaptability and growth.

4.2 Security and Maintenance - Identity Bridge will conduct regular security audits and create incentivized bug bounty programs to play a crucial role in maintaining the

platform's integrity and trustworthiness. Stakeholders can propose and approve budgets for audits and bounty programs through the weighted voting system, promoting transparency and proactive risk management. Security and privacy issues can be fast tracked for faster fixes.

5 TOKEN MECHANICS

5.1 Token Details

Ticker: $IDBR

Primary Utility: Transaction fees, validator rewards, cross-chain fees, and staking, with multi-currency fee to support to increase accessibility.

Fee Splits and Validator Incentives: Validators earn rewards based on participation in zk-STARK verification and cross-chain interactions, with additional rewards for high PoIV scores.

Governance and Treasury: IDBR holders participate in governance, influencing key parameters and treasury allocation, with the treasury supporting buybacks and grants.

Cross-Chain Identity and IBC Utility: IDBR enables cross-chain identity verification, with fees supporting validators handling IBC-based requests, enhancing interoperability.

5.2 Token Utility and Core Functions

Transaction Fees: IDBR tokens are used to pay transaction fees on the Identity Bridge chain. These fees cover costs for identity verification, proof submission, and cross-chain verification requests.

Multi-Currency Support: Users and dApps may also pay fees in other tokens (e.g., stablecoins or the chain's native token, such as $ATOM or $OSMOS).

Discounts for IDBR Payments: Users who pay fees with IDBR receive a discount to fees to incentivize token use.

Validator Incentives: Validators earn IDBR for securing the network, verifying zk-STARK proofs, managing data availability with Celestia, and handling cross-chain IBC requests.

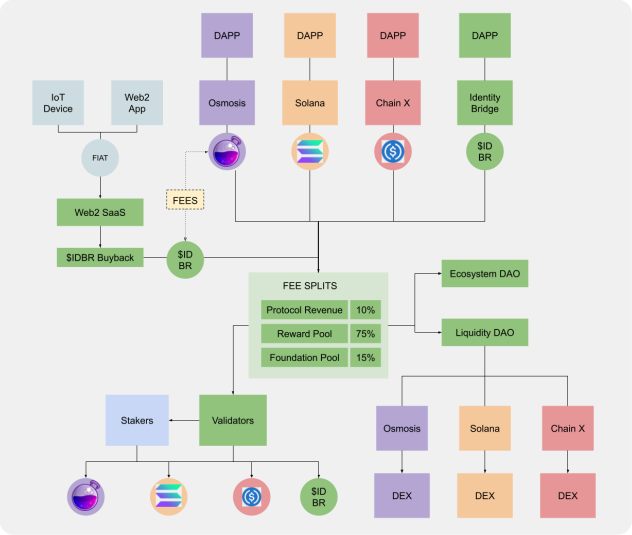
Proof-of-Identity Verification (PoIV) Score: Validators are ranked by a PoIV score based on their engagement with identity tasks, zk-STARK verifications, and cross-chain requests. A higher PoIV score provides higher rewards.

Batch Verification Rewards: Validators earn additional rewards for performing batch verifications of zk-STARK proofs, reducing network costs and improving efficiency.

Cross-Chain Identity Fees: IDBR or native tokens may be used as a payment mechanism for cross-chain identity assertions for interoperability with other blockchains.

Wrapped Identity Tokens: When users need cross-chain identity verification, a small fee (in IDBR or other tokens) is required and via Fee Splits used as validator compensation for handling cross-chain proof verification.

Fee Splits



Fee Allocation: Collected fees (whether paid in IDBR, stablecoins, or native chain tokens) are allocated as follows:

Reward Pool: A portion of all transaction fees goes to the Identity Task Reward Pool, which funds validator rewards for proof verification, cross-chain requests, and zk-STARK batch processing.

Foundation Pool: A portion of non-IDBR fees is allocated to a Liquidity DAO and Ecosystem DAO treasuries. These treasuries periodically buy back IDBR on the open market, bootstrap and balance liquidity in DEXs or fund ecosystem initiatives such as bounties and integrations.

Fee Burning Mechanism: A small portion of IDBR fees may be burned.

Multi-Currency Fee Conversion: Fees paid in non-IDBR tokens (such as stablecoins or ATOM) may be partially converted into IDBR.

Validator and Developer Incentives

Identity Task Rewards: Validators earn rewards for verifying zk-STARK proofs and handling IBC requests. Validators with higher PoIV scores earn a larger share of rewards.

Developer Grants and Bug Bounties: A portion of the Ecosystem DAO treasury is allocated for grants and bounties to encourage development and improvements.

Innovation Challenges: Developers and dApps that introduce innovative uses of zk-STARKs or cross-chain identity verifications can earn rewards.

6 CONCLUSION

Identity Bridge transforms how we manage digital identity and cryptographic keys by using zero-knowledge proofs (ZKPs) to deliver privacy, security, and decentralized control. By removing the need for static seed phrases and centralized systems, the platform enables users to recover their keys securely without exposing sensitive data. Its Wrapped Identity Tokens (WITs) make it possible to verify identities privately and seamlessly across Web3 and Web2 environments.

Built with a focus on users and privacy, Identity Bridge offers customizable proof levels to meet diverse needs, supported by a robust governance model that ensures trust and transparency. Its scalable and flexible architecture empowers individuals and organizations to navigate the complexities of digital identity with confidence. By combining innovative technology with a commitment to decentralization, Identity Bridge sets a new benchmark for privacy-preserving identity and key management in a connected, decentralized world.