Tunnel ID Network

A Decentralized, Privacy-Preserving Proof of Personhood Protocol
Empowering Humanity in the Age of AI

WHITE PAPER DRAFT VERSION 0.2
February 3, 2025

Executive Summary

In a world where bots and AI impersonators threaten digital trust, **Tunnel ID Network** offers a groundbreaking solution: **decentralized, biometric-based Proof of Personhood (PoH)**. Unlike traditional systems that store sensitive data, Tunnel ID never retains biometric information—not even in encrypted form. By combining lattice-based cryptography, Zero-Knowledge Proofs (ZKPs), and multi-modal biometrics, Tunnel ID enables users to:

- Prove they're human **without revealing their identity**.
- Securely authenticate across platforms (DeFi, DAOs, social media, IoT).
- Recover credentials seamlessly using privacy-preserving biometric backups.
- Stay resilient against quantum computing threats.

This white paper explains how Tunnel ID redefines digital identity for the AI era.

1 Introduction

1.1 The Crisis of Digital Identity

As AI tools like deepfakes and chatbots blur the line between humans and machines, trust in online interactions has eroded. **Bots dominate social media**, **Sybil attacks plague DeFi**, and **fraudsters exploit anonymous systems**. Traditional solutions—passwords, centralized KYC, or error-prone biometric databases—fail to balance privacy, security, and usability.

1.2 The Tunnel ID Solution

Tunnel ID Network is a **decentralized identity protocol** that lets users prove they're unique humans using biometrics (fingerprints, facial scans, etc.) while preserving absolute privacy. Here's how it works:

- **Biometric Keys**: Convert biometric data into cryptographic keys *without storing the raw data.*
- **Zero-Knowledge Proofs (ZKPs)**: Prove you're human without revealing *who* you are.
- **Quantum Resistance**: Leverage lattice-based cryptography for post-quantum security.

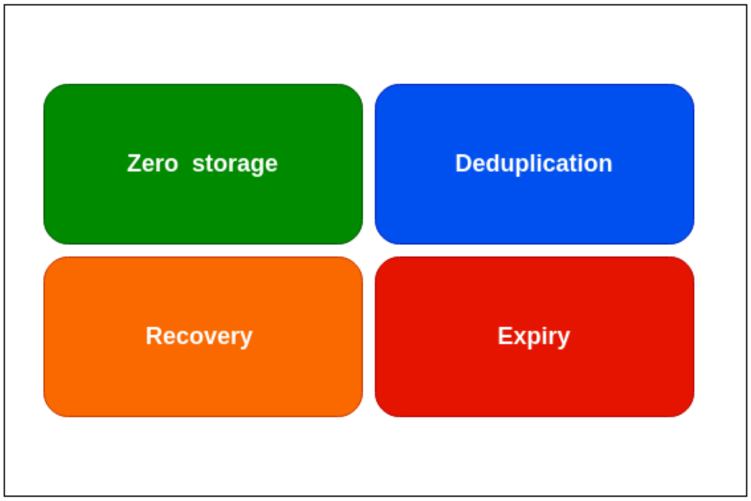

Figure 1: Fundamental Pillars of Tunnel ID Network

- **Deduplication**: Ensure one human = one ID using multi-modal biometric checks.

Example: A DAO uses Tunnel ID to ensure only verified humans vote, eliminating Sybil attacks.

2 Applications

2.1 1. DeFi & Crypto: Privacy-Preserving Compliance

- **Problem**: KYC processes expose personal data; bots manipulate markets.
- **Solution**: Tunnel ID verifies users' humanity and geographic eligibility *without exposing identities.*
- **Use Case**: A lending platform approves under-collateralized loans to verified humans, reducing defaults.

2.2 Sybil-Resistant Governance

- **Problem**: Bots sway decentralized voting.
- **Solution**: 1 human = 1 vote, tied to a Tunnel ID.
- **Use Case**: A decentralized city uses Tunnel ID for fair resident voting.

2.3 Eliminating Fake Accounts

- **Problem**: Bots spread misinformation on Twitter/Reddit.
- **Solution**: Users prove humanness via biometrics.
- **Use Case**: Twitter integrates Tunnel ID to flag unverified accounts.

2.4 Fraud-Proof Distribution

- **Problem**: Duplicate identities exploit UBI systems.

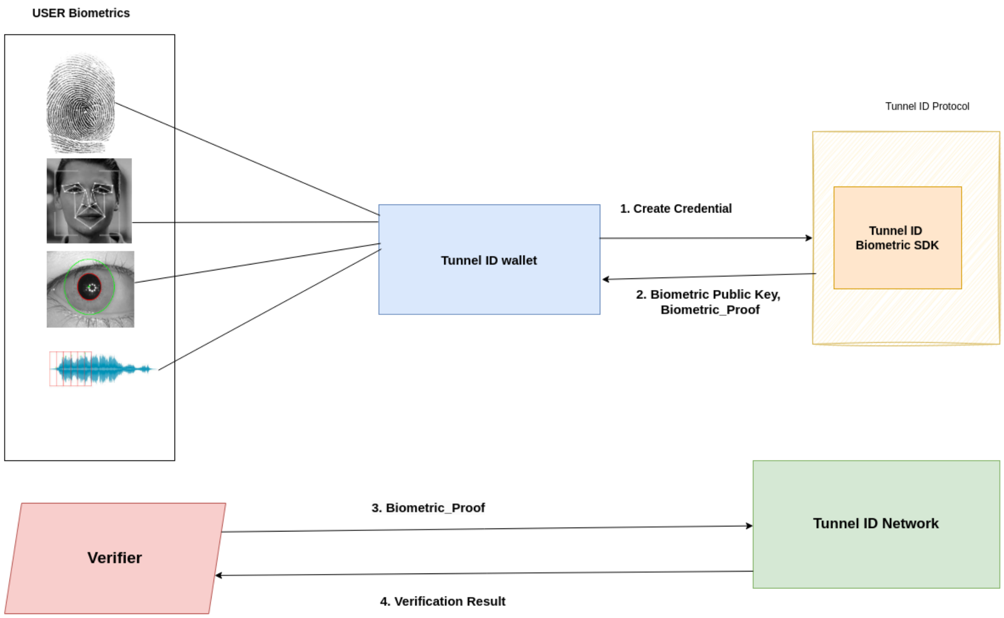

Figure 2: Bird's eye view of Tunnel ID ecosystem

- **Solution**: Biometric deduplication ensures 1 person = 1 UBI wallet.

2.5 Secure Access

- **Problem**: Weak passwords compromise smart devices.
- **Solution**: Biometric-based authentication for homes, cars, and public services.
- **Use Case**: A smart lock opens only for verified Tunnel ID holders.

3 How Tunnel ID Works

The sequence diagram illustrates the end-to-end workflow for verifying a user's biometric-based decentralized identity using the Tunnel ID system. It integrates Layer 2 off-chain processing, zk-SNARK proof generation, and Layer 1 anchoring and validation. Here's a detailed breakdown of the flow:

1. **User Provides Biometric Input** The user initiates the identity verification process by submitting their biometric data (e.g., fingerprint or facial scan) to the Tunnel ID system.
2. **Compute Biometric Sketch and Proxy Key** The Tunnel ID Layer 2 system processes the biometric data to generate:
   - A **biometric sketch** that represents the user's input.
   - A **proxy key** (c, a) that cryptographically represents the biometric features.
3. **Generate zk-SNARK Proof of Uniqueness (zkPoU)** Using the biometric sketch and proxy key, the system generates a **Zero-Knowledge Proof of Uniqueness (zkPoU)**. This proof ensures that the user is unique and valid without revealing their biometric data.

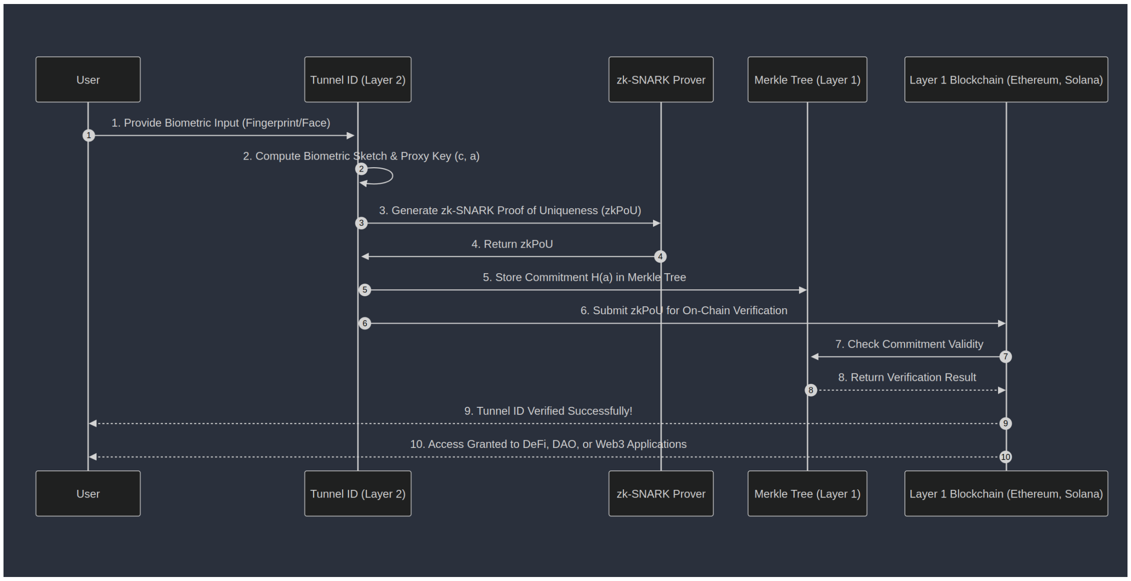
User
Tunnel ID (Layer 2)
zk-SNARK Prover
Merkle Tree (Layer 1)
Layer 1 Blockchain (Ethereum, Solana)
1. Provide Biometric Input (Fingerprint/Face)
2. Compute Biometric Sketch & Proxy Key (c, a)
3. Generate zk-SNARK Proof of Uniqueness (zkPoU)
4. Return zkPoU
5. Store Commitment H(a) in Merkle Tree
6. Submit zkPoU for On-Chain Verification
7. Check Commitment Validity
8. Return Verification Result
9. Tunnel ID Verified Successfully!
10. Access Granted to DeFi, DAO, or Web3 Applications
1
2
3
4
5
6
7
8
9
10
User
Tunnel ID (Layer 2)
zk-SNARK Prover
Merkle Tree (Layer 1)
Layer 1 Blockchain (Ethereum, Solana)

Figure 3: Caption

4. **Return zk-SNARK Proof** The zk-SNARK proof is returned to the Tunnel ID system for storage and further validation.

5. **Store Commitment in Merkle Tree (Layer 1)** A cryptographic commitment $H(a)$ derived from the proxy key is securely stored in a **Merkle Tree** on the Layer 1 blockchain (e.g., Ethereum or Solana). This ensures immutability and provides a decentralized mechanism for future identity verification.

6. **Submit zkPoU for On-Chain Verification** The zk-SNARK proof is submitted to the Layer 1 blockchain for validation. The system ensures the proof meets all requirements for privacy-preserving uniqueness.

7. **Check Commitment Validity** The Layer 1 smart contract interacts with the Merkle Tree to validate the user's identity commitment against existing commitments. This step ensures the user hasn't registered multiple times.

8. **Return Verification Result** The result of the verification (valid or invalid) is returned to the Tunnel ID system.

9. **Identity Verified Successfully** If the verification succeeds, the system confirms that the user's Tunnel ID is valid and unique.

10. **Access Granted to Applications** Upon successful verification, the user gains access to **Web3 applications, DeFi platforms, or DAO governance systems** that are integrated with Tunnel ID.

Why It's Secure:

- **No Storage**: Biometric data isn't stored, encrypted, or sharded.
- **Correctness**: Keys regenerate even with minor biometric changes (e.g., a cut finger).
- **Security**: No leakage of biometric data from public key because the security is based on

discrete logarithm assumption.

3.1 2. Deduplication: Ensuring Uniqueness

To prevent duplicate IDs:

- Users must register **two biometric modalities** (e.g., fingerprint + face).
- The protocol checks new registrations against existing sketches using **Zero-Knowledge Proof of Uniqueness (ZkPoU)**.
- If a duplicate is detected (e.g., someone tries to register with a second fingerprint), registration is blocked *without revealing existing users' data*.

3.2 3. Privacy by Design

- **Unlinkable Transactions**: Each transaction uses a new, transient identifier derived from biometric sketches.
- **ZKPs for Everything**: Users prove ownership of biometric keys without exposing them.

3.3 4. Recovery & Expiry

- **Lost Your Device?** Recover access via secondary biometrics (e.g., facial scan).
- **Auto-Expiry**: Credentials refresh periodically, forcing users to re-verify. This prevents long-term biometric theft.

4 Tunnel ID vs Existing Biometric Proof of Humanity Protocols

Tunnel ID represents a significant advancement over existing Proof of Humanity (PoH) protocols such as Worldcoin and Holonym, addressing key limitations while introducing unique features that prioritize privacy, inclusivity, and scalability. Unlike Worldcoin, which relies on specialized hardware (e.g., the Orb) to scan users' irises and create a centralized biometric database, Tunnel ID utilizes a decentralized approach based on Fuzzy Schnorr Signatures. This enables biometric key generation from fingerprints or facial scans without storing sensitive data, ensuring that the system is inherently privacy-preserving. Tunnel ID avoids the risk of centralized data breaches by storing cryptographic commitments (not raw biometrics) in a Merkle Tree on-chain.

In comparison to Holonym, which uses biometric key generation techniques but leans heavily on traditional decentralized identity frameworks like Verifiable Credentials (VCs), Tunnel ID enhances deduplication with DiffRec, a cryptographic algorithm that checks biometric uniqueness without requiring access to a centralized database. This approach eliminates the reliance on trusted third parties and enables dynamic scalability for billions of users, leveraging zk-SNARKs for efficient, privacy-preserving verification. Furthermore, Tunnel ID's system is designed to be person-bound, meaning that credentials cannot be transferred, traded, or coerced, a critical weakness in many current identity systems.

By combining these innovations with a privacy-first, decentralized architecture, Tunnel ID offers an identity layer that is more inclusive, fraud-resistant, and scalable than Worldcoin, and more advanced in terms of privacy and Sybil resistance compared to Holonym. This positions Tunnel ID as the next-generation identity solution for Web3, capable of powering decentralized finance, DAO governance, and secure access to the digital economy.

Feature	**Traditional Systems**	**Tunnel ID**
Biometric Storage	Stored (encrypted/sharded)	Never stored
Privacy	Centralized databases	Decentralized, ZKP-based
Quantum Security	Vulnerable	LWE-based resistance
Error Tolerance	High failure rates	2.4% FNMR, 2^{-80} false match rate

Join the Privacy Revolution

Tunnel ID Network isn't just a protocol—it's a movement to reclaim digital trust. By marrying biometrics with cutting-edge cryptography, we empower humans to prove their uniqueness without sacrificing privacy.

Get Involved:

- **Developers**: Integrate Tunnel ID into your dApp.
- **Partners**: Collaborate on use cases for DeFi, DAOs, or IoT.
- **Users**: Join our beta program to experience passwordless authentication.

Contact us at `hello@tunnel.me` to learn more.