Decentralized Biometric Proof-of-Humanity (PoH) System Using Smartphone-Based Data Collection and Zero-Knowledge Proofs (ZKP) for Decentralized Identifiers (DIDs)

Alexander Tkachev (Oleksandr Tkachov)
2025, Odesa, Ukraine
alex.tkachev.odessa@gmail.com

Abstract

This invention describes a decentralized biometric Proof-of-Humanity (PoH) system leveraging smartphones for biometric data collection, processing, and integration into a blockchain-based identity system. The system ensures unique and private identification of individuals through the use of biometric data, processed locally on smartphones, and verified using Zero-Knowledge Proofs (ZKP) to generate Decentralized Identifiers (DIDs). The invention prioritizes privacy, accessibility, and scalability, enabling widespread adoption across Web3 applications such as decentralized finance (DeFi), decentralized autonomous organizations (DAOs), and universal basic income (UBI) systems.

Description

1. Overview

This invention provides a method and system for creating unique digital identities based on biometric data collected and processed via smartphones. The biometric data is hashed and encrypted locally to ensure privacy and is used to generate Zero-Knowledge Proofs (ZKP) for decentralized identity verification. These identities, stored on a blockchain or distributed ledger, form the basis of Decentralized Identifiers (DIDs) that enable sybil-resistant participation in decentralized ecosystems.

2. Components of the System

2.1 Biometric Data Collection

Biometric data is captured using standard smartphone hardware, such as:

- Cameras for facial recognition or iris scanning.
- Fingerprint readers for secure fingerprint collection.
- Microphones for capturing voiceprints, where applicable.
- Optional add-on lenses or software enhancements (e.g., magnification for iris scanning).

2.2 Local Processing

Biometric data is processed locally on the smartphone to:

1. Extract unique features (e.g., fingerprint minutiae, facial landmarks).
2. Hash these features using cryptographic algorithms (e.g., SHA-256).
3. Generate a public-private key pair linked to the hashed biometric data.
4. Produce a Zero-Knowledge Proof (ZKP) to validate the uniqueness of the biometric without transmitting raw data.

2.3 DID Generation

A Decentralized Identifier (DID) is created using:

- The hashed biometric data.
- A public-private key pair.
- A Zero-Knowledge Proof confirming the uniqueness of the identity.
- Conformance to W3C DID standards for interoperability.

2.4 Blockchain Submission

The DID, along with the ZKP and public key, is submitted to a blockchain or distributed storage system (e.g., IPFS, Filecoin). The data is redundantly stored across nodes to ensure immutability and availability.

2.5 Verification and Authentication

Verification occurs when a user needs to prove their identity:

a) For frequent usage scenarios, such as logging into Web3 platforms or interacting with decentralized applications (dApps), the system allows for simplified authentication. Users can enter a 6-digit PIN combined with either:
   - A fingerprint scan (on smartphones).
   - A smartphone confirmation (if accessing from desktop or laptop).
   This lightweight process ensures usability while maintaining security.

b) Periodically, or as required by sensitive transactions, the system requests full biometric verification using the previously described capture and hashing process.

c) The system generates a new hash and ZKP locally, which is matched against the stored ZKP on the blockchain.

d) If the proofs match, the user is authenticated as the unique owner of the DID.

Unique Aspects of the Invention

1. ***Local Biometric Data Processing on Smartphones:***

   Biometric data is processed directly on the user's smartphone, ensuring that raw data never leaves the device. This local approach enhances privacy and reduces the risk of data breaches, differentiating it from systems that require centralized processing.

2. ***Integration of Zero-Knowledge Proofs (ZKP):***
    - Using ZKPs to validate the uniqueness of biometric data without exposing raw data or private information offers a privacy-preserving mechanism. This is a distinguishing feature compared to conventional biometric systems that rely on full data comparison.
3. ***Streamlined Usability via Partial Authentication:***
    - The use of a **6-digit PIN code** combined with partial biometric confirmation (e.g., fingerprint scan or smartphone confirmation) for frequent interactions, with periodic full biometric verification for higher security, balances usability and security. This innovation ensures a smooth user experience while maintaining robust sybil resistance.
4. ***Universal Decentralized Identifier (DID) Creation:***
    - Generating W3C-compliant DIDs based on biometric data and ZKPs ensures interoperability across Web3 platforms. The system enables seamless integration into decentralized ecosystems, which sets it apart from isolated identity management systems.
5. ***Applications Beyond Simple Identity Verification:***
    - Your invention targets specific decentralized use cases like sybil-resistant voting in DAOs, fair distribution in UBI systems, and prevention of market manipulation in DeFi. These targeted applications extend the value proposition beyond generic identity verification systems.
6. ***Blockchain Integration with Distributed Storage:***
    - By storing hashed biometric data and ZKPs on blockchains or distributed storage networks like IPFS or Filecoin, your invention ensures immutability, tamper resistance, and redundancy, which is not commonly addressed in other biometric identity systems.
7. ***Hybrid Authentication System for Web3:***
    - The combination of PIN-based and biometric-based authentication methods offers a hybrid approach that simplifies frequent access while maintaining robust identity verification. This nuanced system is particularly suited to Web3 applications that demand both convenience and security.
8. ***Support for Multiple Biometric Modalities:***
    - The ability to use multiple biometrics (e.g., fingerprint, iris scan, or facial recognition) ensures inclusivity and adaptability to different devices and user needs, making the system accessible globally.