

Sybil-Resistant Identity Systems in Decentralized Environments

Ing. Michal Laš supervised by doc. Ing. Ivan Homoliak Ph.D.



BRNO FACULTY
UNIVERSITY OF INFORMATION
OF TECHNOLOGY TECHNOLOGY

Motivation

- In the physical world, proving identity is simple – **uniqueness** is visible and verifiable.
- Online, individuals cannot independently prove their uniqueness; **verification relies on centralized authorities**.
- Ensuring uniqueness is important in various services, such as banking, social media, and online auctions. The problem lies in **Sybil attacks** [1], in which an attacker creates a large number of fake identities to gain an advantage over the system.
- Centralized solutions collect sensitive data, increasing privacy risks and reducing user autonomy.

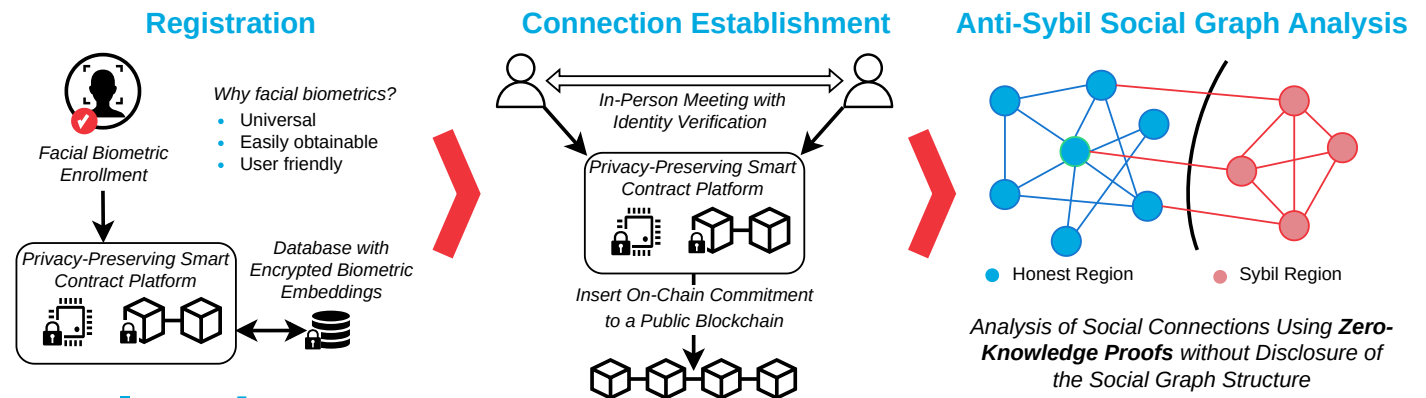
The goal is to design a system that allows individuals to independently verify the uniqueness of online identities **without relying on a trusted authority**. This is another step towards self-sovereign identity management, especially in a world where personal data is a valuable asset.

Objectives

- Explore various approaches and possibilities for creating a decentralized system that would allow a person's uniqueness to be proven in the online space without having to rely on a trusted authority.
- Utilize the identified approaches and design a robust, Sybil-resistant identity management system.
- Focus specifically on decentralization, personal data privacy, anonymity, and security.
- Evaluate the security, properties, and practical usability of the proposed system.

Proposed System

The proposed system utilizes **facial biometric authentication** combined with **anti-Sybil analysis of the social graph**. Users register their facial biometric data using privacy-preserving smart contract platforms, thereby creating a profile on the blockchain. Registered users establish connections with one another, creating a social graph that can be analyzed.



Evaluation

The system was evaluated using a **proof-of-concept implementation** that employs the Oasis network [2] as a privacy-preserving smart contract platform, along with a **social graph analysis simulation**.

- Fast, recursive, zero-knowledge proofs of users' social connections, called **ZK Random Walks**, were implemented using Plonky 2 [3].

Experiments	Circuit Size	Prove Time
ZK Random Walk Linear	8KB + $l^* \times 4.2\text{MB}$	328.56ms
ZK Random Walk Cyclic	8.4MB	630.27ms
Aggregation of 3 Proofs	16.9MB	1.58s

Experiments performed on AMD Ryzen 5 5600H, 16GB RAM
* l is the number of recursion steps (path length)

References

- [1] Douceur, J.R. The Sybil Attack. In: Druschel, P.; Kaashoek, F. and Rowstron, A., ed. Peer-to-Peer Systems online. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, p. 251–260. ISBN 978-3-540-45748-0.
- [2] Oasis Protocol Foundation. The Oasis Blockchain Platform online. Oasis Labs, June 2020. White paper.
- [3] Polygon Zero Team. Plonky2: Fast Recursive Arguments with PLONK and FRI. online, September 2022, p. 16.

- Two approaches were tested: linear and cyclic proofs. Linear uses a different circuit for each recursion step, while cyclic is a single self-referential circuit that verifies its own previous proof via a special Plonky2's recursive method.
- Additionally, there are also proofs for aggregating multiple social connection proofs.
- Three types of synthetic models were used to generate the social graphs: Holmes–Kim, Watts–Strogatz, and Kleinberg small-world.