zk-Census: Privacy-Preserving Decentralized Polling via Zero-Knowledge Eligibility and Verifiable Identity

Tomas Hanak supervised by **doc. Ing. Ivan Homoliak, Ph.D.**

BRNO UNIVERSITY OF TECHNOLOGY — FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2026

Introduction

Traditional centralized surveys rely on **absolute institutional trust**, making them vulnerable to **data manipulation**. Operating as "black boxes," they prevent independent audits of results or participant eligibility.

The Solution & Goals

- **zk-SNARKs (Core Privacy):** Mathematically guarantee user anonymity, eligibility, and Sybil resistance.
- **TEE (Supplementary):** Temporarily encrypts ongoing votes to prevent early results from biasing the outcome.
- **Decentralized:** Ensures independent results without a central authority.

Oasis Sapphire

Confidential execution via **TEE**.

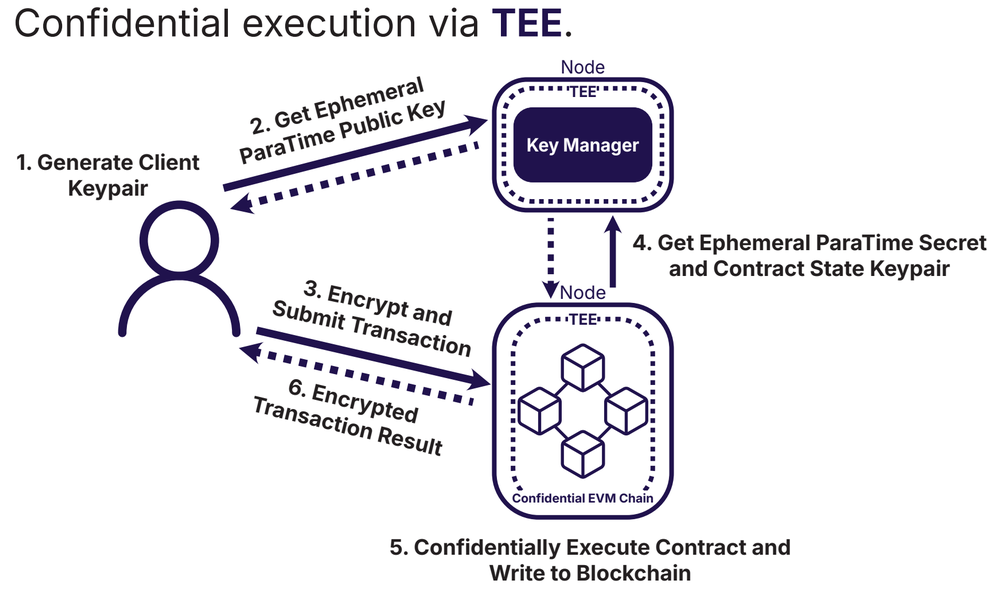

Figure 1: Oasis Sapphire network architecture using TEE

System Architecture

1 Survey Creation

Figure 2: Survey creation and smart contract deployment

2 Identity Provider

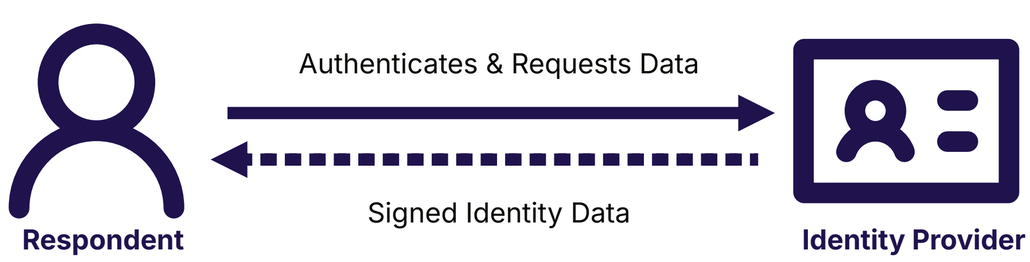

Figure 3: User authentication and issuance of local identity credential

3 zk-SNARK Generation

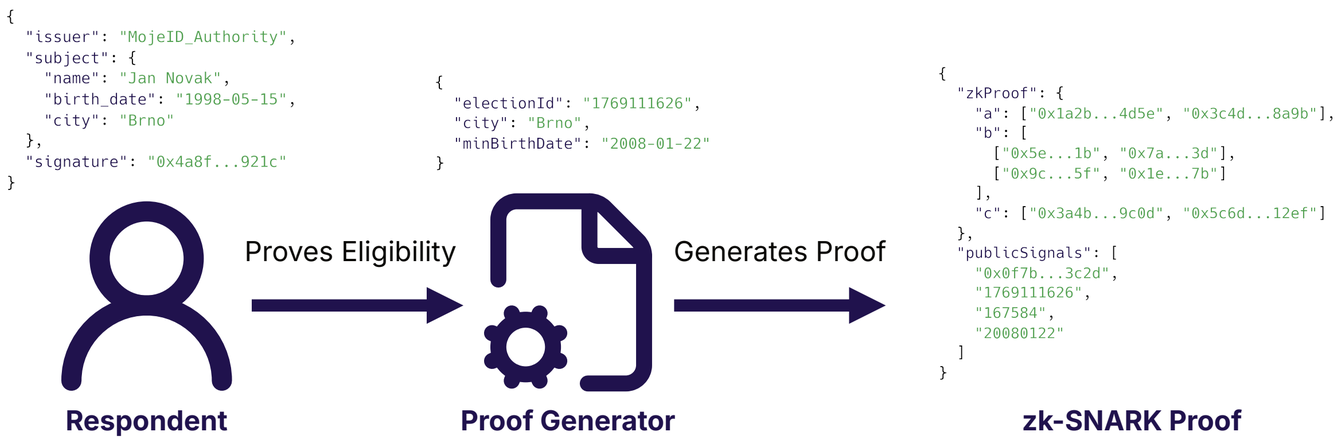

Figure 4: Local generation of zero-knowledge proof

4 Voting & On-Chain Verification

```
// 1. Verify zk-SNARK Proof (Anonymity & Eligibility)
require(verifier.verifyProof(proof), "Invalid Proof");

// 2. Prevent Double Voting
require(!nullifiers[proof.nullifier], "Already Voted");

// 4. Record Nullifier & Increment Vote
nullifiers[proof.nullifier] = true;
results[candidateId]++;
```

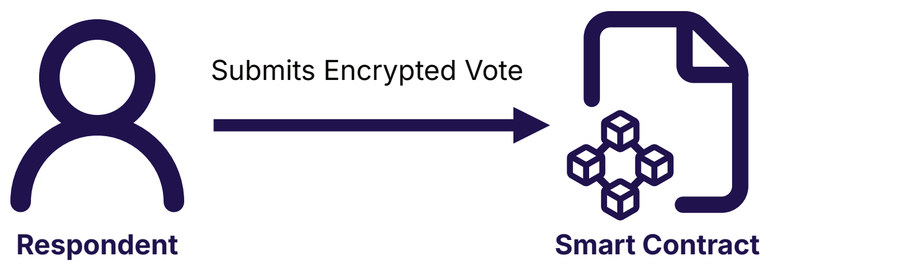

Figure 5: Smart contract verifies the proof and prevents double voting

5 Confidential Tallying & Results

```
// 1. Ensure the survey has officially concluded
require(block.timestamp > electionEnd, "Active");

// 2. Return aggregated results
return results;
```

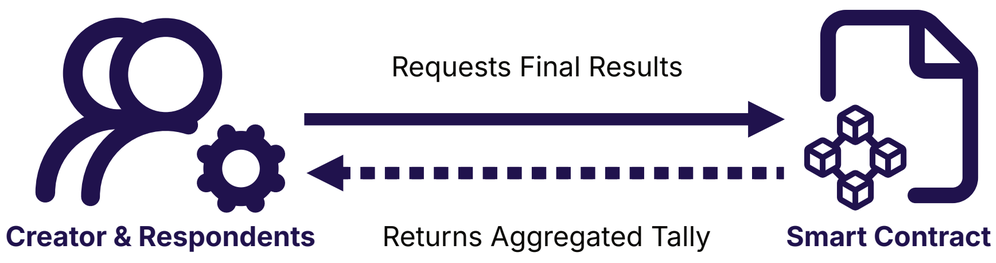

Figure 6: Secure retrieval of aggregated results

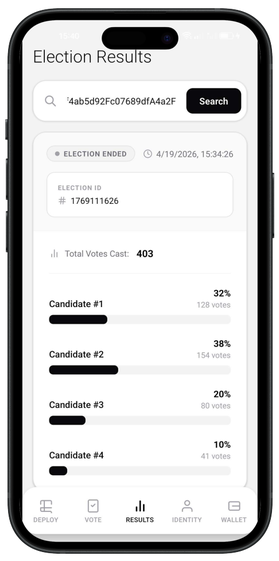

Figure 7: Mobile UI for results

Performance & Costs

Operation	Gas	Price (USD)
Contract Creation (Deploy)	~2 300 000	~$0.0260
Contract Call (Vote)	~400 000	~$0.0046

Table 1: Performance and cost evaluation of the smart contract