BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2026
http://excel.fit.vutbr.cz

Scalability of Decentralized E-Voting on Blockchain

Jaroslav Podmajerský*

Abstract
Traditional elections are expensive, logistically complex, and difficult to audit transparently. This work designs and implements a decentralized e-voting protocol built on blockchain and zero-knowledge proofs, combining threshold encryption with zk-SNARK eligibility verification. The system achieves a per-voter cost of $1.90 in simulation, compared to $2–$91 for real-world national elections, while preserving ballot secrecy and end-to-end verifiability. These results demonstrate that blockchain-based voting can offer a practical, auditable, and cost-effective alternative to conventional election infrastructure.

*xpodmaj00@stud.fit.vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

[Motivation] National elections are among the most critical processes in democratic societies, yet they remain remarkably costly and operationally fragile. The 2020 US Presidential election cost an estimated $14.4 billion, while even smaller-scale elections in Europe routinely require hundreds of millions of dollars in infrastructure, personnel, and logistics. Beyond cost, traditional elections suffer from limited transparency, voters must trust that ballots are counted correctly without any means of independent verification. These shortcomings motivate the exploration of electronic voting systems that could reduce costs, increase accessibility, and provide cryptographic guarantees of correctness.

[Problem definition] The core challenge is to design an e-voting protocol that simultaneously satisfies four properties: *ballot anonymity* (votes cannot be linked to voters), *eligibility verification* (only authorized voters can cast ballots), *threshold trust* (no single party can compromise the election), and *public verifiability* (anyone can audit the election outcome). The system must also be practically deployable and cost-competitive with existing election infrastructure at national scale.

[Existing solutions] Several blockchain-based voting schemes have been proposed in the literature. The BBB-Voting scheme [1] extends the Open Vote Network (OVN) [2] by generalizing it from a binary choice to 1-out-of-k candidate selection while introducing a fault recovery mechanism for stalling participants. The protocol is implemented entirely as Ethereum smart contracts, achieving approximately 13.5% reduction in gas costs compared to OVN. Building upon BBB-Voting, the SBvote protocol [3] addresses its scalability limitations by partitioning voters into groups, each served by an independent booth smart contract, with a main contract aggregating individual booth tallies-enabling elections with up to 1.5 million voters in proof-of-concept experiments. Both protocols operate purely on-chain, with all phases-key generation, vote casting, fault recovery, and tallying-executed via smart contracts without any off-chain component.

[Our solution] We build upon the BBB-Voting and SBvote protocols but depart from their purely on-chain architecture by adopting a hybrid design analogous to the Zcash transaction model [4]: in Zcash, the blockchain records that a valid transaction occurred while concealing the sender, recipient, and amount behind a zero-knowledge proof; similarly, in our protocol the blockchain records that a valid vote was cast while the voter's identity and their choice remain hidden behind a Groth16 zk-SNARK proof. The blockchain thus serves exclusively as an immutable public bulletin board and verification layer, while all computationally intensive operations—eligibility verification via zk-SNARKs, threshold ElGamal encryption for ballot secrecy, and distributed key generation using Feldman Verifiable Secret Sharing are performed off-chain. Proofs of honest computation are published on-chain via Solidity smart contracts deployed through Hardhat, allowing any observer to verify correctness without re-executing the cryptographic work.

[Contributions] The primary contribution is a complete, implemented e-voting system with end-to-end cryptographic guarantees, accompanied by a cost analysis that compares the system against six real-world national elections. The system achieves a simulated per-voter cost of $1.90, making it the cheapest option in the comparison (Figure 2 and Figure 3 on the poster).

2. Protocol Overview

The poster's central diagram (Figure 1) illustrates the five protocol phases and the interactions between the five system actors: the *Voter*, *Voting Authority*, *Tally Authority*, *Backend*, and *Smart Contract*.

Phase 0 – Deployment. The Voting Authority and Backend deploy the necessary smart contracts to the blockchain establishing the election parameters and the on-chain registry.

Phase 1 – Enrollment & Registration. Voters enroll their identity with the Voting Authority, which verifies eligibility. Upon successful verification, the voter registers with the Backend, which freezes and publishes the final voter registry on-chain.

Phase 2 – Setup & Pre-voting. The Backend signals the start of the pre-voting phase. Tally Authorities execute a Distributed Key Generation (DKG) protocol based on Feldman Verifiable Secret Sharing, producing a shared public encryption key without any single party knowing the full private key.

Phase 3 – Voting. Each voter encrypts their ballot using threshold ElGamal under the shared public key and generates a zk-SNARK proof (Groth16, compiled via Circom) demonstrating eligibility without revealing their identity. The encrypted vote and proof are submitted to the smart contract, which verifies the proof and stores the vote along with a nullifier to prevent double-voting.

Phase 4 – Tally. Tally Authorities submit their decrypted shares to the Backend, which reconstructs the secret key via Lagrange interpolation, decrypts all ballots, and publishes the final result on-chain.

3. Security Properties

The poster highlights four security guarantees that the protocol provides, listed in the Security Properties box:

- **Ballot anonymity** – Votes are anonymous and unlinkable to voter identity. The use of ElGamal encryption and nullifiers ensures that no observer can determine how a specific voter voted.
- **Eligibility without identification** – The system verifies voting eligibility via zero-knowledge proofs without revealing voter identity. The Circom circuit proves membership in the registered voter set without disclosing which member the prover is.
- **Threshold trust model** – No single party can compromise the tally. Decryption requires a threshold majority of tally authorities to submit valid decryption shares, preventing unilateral manipulation.
- **Full on-chain verifiability** – All election data, proofs, and results are publicly recorded on the blockchain, enabling any third party to independently verify the election outcome.

4. Cost Comparison

The bottom section of the poster presents two bar charts comparing the system's cost against real-world elections.

Figure 2 shows total election cost on a logarithmic scale. The simulated e-voting system (10 million voters) costs approximately $19 million, compared to $92 million for the 2021 German Federal Election, $190 million for the 2019 UK General Election, and up to $14.4 billion for the 2020 US Presidential Election.

Figure 3 normalizes these figures to a per-voter cost. The e-voting system achieves $1.90 per voter, which is comparable to the $2.00 per voter of the German election and significantly cheaper than the $91.14 per voter of the US election. This comparison demonstrates that a blockchain-based approach can be cost-competitive even when accounting for on-chain transaction fees and proof generation overhead.

It should be noted that the e-voting cost is derived from simulation and does not account for all operational factors present in physical elections (e.g., voter education, dispute resolution, accessibility infrastructure). Nevertheless, the comparison provides a useful baseline for evaluating the economic viability of the approach.

5. Conclusions

This work demonstrates that a decentralized e-voting system combining threshold ElGamal encryption with zk-SNARK eligibility proofs can achieve strong security guarantees while remaining cost-competitive with traditional election infrastructure. The protocol ensures ballot anonymity, eligibility verification without identity disclosure, distributed trust via threshold cryptography, and full public verifiability through on-chain data.

Acknowledgements

I would like to thank my supervisor doc. Ing. Ivan Homoliak, Ph.D. for his guidance throughout this project.

References

[1] Ivan Homoliak, Sarad Venugopalan, Zengpeng Li, and Pawel Szalachowski. BBB-Voting: Self-tallying end-to-end verifiable 1-out-of-k blockchain-based boardroom voting. In *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023.

[2] Feng Hao, Peter Y. A. Ryan, and Piotr Zieliński. Anonymous voting by two-round public discussion. *IET Information Security*, 4(2):62–67, 2010.

[3] Ivana Stančíková and Ivan Homoliak. SBvote: Scalable self-tallying blockchain-based voting. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (SAC '23)*, pages 203–211, Tallinn, Estonia, 2023. Association for Computing Machinery.

[4] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474. IEEE, 2014.