BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2025
http://excel.fit.vutbr.cz

DECENTRALIZED APPLICATION OF SCALABLE ELECTRONIC VOTING FOR NATIONAL ELECTION

Tomáš Švondr

Abstract

Voting is an essential instrument of a democratic system that allows people to express their will and make a collective decision. As technology progresses rapidly, further and further, our voting system deteriorates at almost the same pace, and it is beginning to flounder under ever-increasing requirements and expectations for transparency, security, privacy, and most importantly, trust.

In our work, we focus on exploring and leveraging the main characteristics of blockchain systems, such as trustlessness, immutability, and transparency, to develop a decentralised application that can be utilised in large-scale elections like the parliamentary elections. We have developed a prototype of a decentralised application built on the Ethereum blockchain and utilising the Self-Tallying voting protocol SB-vote, developed at BUT. Currently, the application provides the user with an UI with availability on all standard devices. Furthermore, it maintains the individual phases of the voting protocol, effectively allowing the users to participate in scheduled elections published on the blockchain. The potential of this project lies in intertwining and leveraging modern technology and the fundamental pillar of democracy, voting and together, creating a safe, transparent, trustless, anonymous space for electronic elections.

*xsvond00@vut.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

In modern times, when digitalisation becomes more and more prevalent in the state agenda, our democratic systems also need to adhere to the newly risen standards. This, however, brings up many difficult challenges, such as keeping the casting of a metaphorical ballot anonymous while ensuring that the person casting the ballot is eligible to vote and casts only one ballot and cannot vote multiple times. This, and also maintaining a high level of security.

Such obstacles create an environment where the best solution is a perfectly balanced set of trade-offs between anonymity, security, and transparency.

Currently, the most prevalent solution to this problem is the path of centralised systems, which, while very effective, are potentially vulnerable to a single point of failure and may be exploited for manipulation if the authority controlling the election chooses to do so. There are a few systems which rely on decentralisation to counter these problems. However, such systems often suffer from scalability issues and are suitable only for small-scale applications. The most promising way to tackle these problems seems to lie in blockchain. With solutions like Open Vote Network or BBB-voting, this path looks more and more hopeful. However, even these systems have their flaws - Open Vote supports only voting for one of two options, and BBB-vote, although it supports a larger variety of options to vote for, and has a self-recovery phase, when the system can recover from faulty voting, its scalability remains severely limited[1].

Currently, the most promising solution may arise from a project called Semaphore, which is a platform for Zero-Knowledge signalling on the Ethereum blockchain. This allows for casting a message/or a vote as a provable group member without revealing the submitter's identity. The main bottleneck of this platform lies in the computational difficulty of generating zk-SNARK proofs for large groups, and theoretically, the throughput of the underlying blockchain network. On the other hand, the system's heavy use of zk-SNARK proofs takes advantage of its cost-efficient and easy verifiability[2].

Our approach also bets on decentralisation and blockchain.

It builds on the BBB-voting platform, specifically its more scalable successor SB-Vote. The platform combines a centralised identity verification and phase management, and NIZK-based (Non interactive zero-knowledge proofs) voting, which allows the authority to have the right amount of control on the election management and organisation, while keeping the process decentralised, transparent, anonymous and completely verifiable. [3]

Our work results in a decentralised, multi-platform application for participating and managing large-scale elections.

2. Blockchain

Decentralised applications (dApps) and blockchain technology represent a significant trend in the digital universe with a focus on a secure, transparent, and immutable record of transactions without the need for an intermediary or a central authority. Blockchain is a global distributed ledger where transactions are verified through an internationally distributed network of nodes, with little to no vulnerability to tampering and fraudulent activities. The greatest asset in its favour is that it can deliver data integrity and transparency because each transaction can be cryptographically linked to the last to create an impenetrable chain[4].

dApps, blockchain-powered, run on decentralised networks and utilise smart contracts—self-executing code executing and recording actions according to agreed conditions. A prime example is Ethereum, which enables decentralised systems through its inherent cryptography, eliminating the need for third-party intermediaries. This enhances efficiency and security, reducing costs and the risk of human error. Hence, blockchain and dApps have great potential to disrupt industries, such as the finance industry, by enabling instantaneous transactions and providing users more control over their data[5].

3. Technical solution

The application is divided into three main components:

- Frontend application - codename VoteMate, handling all the user interaction and facilitating communication to the other parts.
- Backend application - operating as a centralised server
- Blockchain smart contracts - functioning as the core of the voting protocol

Votemate is a decentralised application built on a foundation of the Angular framework and web3.js library. It leverages the capabilities and options provided by the web technologies to let the user interact on their terms.

The backend application is developed on Node.js platform, controlling the user's access, and enforcing the scheduled execution of the voting protocol.

Smart contracts - Shifts the reliance from centralised authority and creates the means for users to participate in elections. The smart contracts implement the SB-vote protocol, which operates in several phases - Enrolling and subsequently dividing voters into multiple voting booths (instances of smart contracts), where each booth operates as an independent voting group. The voter submits their cryptographically blinded vote to the booth after the voting phase ends, and a central aggregation smart contract aggregates the results from individual booths. The voting data are publicly verifiable due to the inherent properties of the blockchain (immutability, auditability), and the voting process does not rely on trust in any central authority.

4. Conclusions

We have created a system that brings e-voting decentralised and privacy-preserving to users, offering a practical demonstration of how blockchain and zero-knowledge cryptography can be used in real-world democratic processes. By utilising modern technologies of distributed systems, we have addressed key challenges such as ensuring transparency, immutability, and verifiability of votes, while maintaining the confidentiality of voter choices. This system aims to be a reliable tool for secure elections, eliminating centralisation risks and reducing the potential for fraud or manipulation in traditional voting methods. While it not a perfect solution, and obstacles, mainly in the direction of scalability, are still to be overcome, to gain a full-scale election capability with high candidate and voter participation, the system clearly shows, that there is a way in which we can implement electronic voting with a high degree of security with minimal potential for fraud or manipulation and without compromising the transparency and confidentiality of the voter's choice.

Acknowledgements

I would like to thank my supervisor doc. Ing. Ivan Homoliak, Ph.D., for his help, support and valuable insights.

References

[1] Ivan Homoliak, 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)*, pages 297–306, 2023.

[2] Kobi Gurkan, Koh Wei Jie, and Barry Whitehat. Community proposal: Semaphore: Zero-knowledge signaling on ethereum. [https://semaphore.pse.dev/whitepaper-v1.pdf], February 2 2020. Ethereum Foundation and C Labs.

[3] Ivana Stančíková and Ivan Homoliak. Sbvote: Scalable self-tallying blockchain-based voting, 2022.

[4] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. Accessed: 17 November 2024.

[5] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. *Business & Information Systems Engineering*, 59(3):183–187, Jun 2017.