Towards Secure, Scalable, and Flexible E-Voting in Blockchains

Ivan Homoliak
Brno University of Technololgy,
Faculty of Information Technology

In this talk, we summarize our contributions in the area of e-voting in blockchains. The talk encompasses the system security perspective on design of e-voting systems and it is based on 3 papers of ours, each focusing on different aspect of e-voting in blockchains (security&privacy, scalabilty, flexibility):

1. Homoliak, Ivan, Zengpeng Li, and Pawel Szalachowski. "BBB-Voting: Self-Tallying End-to-End Verifiable 1-out-of-k Blockchain-Based Boardroom Voting." *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023. https://ieeexplore.ieee.org/abstract/document/10411494
2. Stančíková, Ivana, and Ivan Homoliak. "Sbvote: Scalable self-tallying blockchain-based voting." *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*. 2023. https://dl.acm.org/doi/abs/10.1145/3555776.3578603
3. Venugopalan, Sarad, Ivana Stančíková, and Ivan Homoliak. "Always on voting: A framework for repetitive voting on the blockchain." *IEEE Transactions on Emerging Topics in Computing* (2023). https://ieeexplore.ieee.org/abstract/document/10260281

Moreover, the talk tangentially mentions the e-voting related security issues and countermeasures from another paper of us:

1. Homoliak, Ivan, et al. "The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses." IEEE Communications Surveys & Tutorials 23.1 (2020): 341-390. https://ieeexplore.ieee.org/abstract/document/9239372

The default length of the presentation is 60-70 mins and the slides can be viewed at https://drive.google.com/file/d/1nvnMhnZEccQos4TtyaPX0Rpl9CXAbO-q/view?usp=sharing. The presentation can be shortened to arbitrary time according to the requirements but ideally it would need at least 20-30 mins.

Abstract:
We start by briefly introducing the security architecture for blockchains and the application layer categories. We will look in detail at the sub-category of electronic voting, where we discuss relevant properties in terms of security, privacy, and other voting properties. For this category, we summarize the state-of-the-art and extend the existing classification of electronic voting in blockchains. We then discuss our proposed BBB-Voting approach, representing conference voting in blockchains, which is based on two existing voting protocols and allows voting for 2 or more options. We define the attacker

model and assumptions. We then introduce the protocol and the basic BBB-Voting scheme, which we then extend to include robustness. We then present two full implementations and experiments including various proposed optimizations leading to on-chain cost savings as well as increased processing throughput. We compare the results to a competing Open Voting Network approach. We then perform a security analysis of the proposed solution as well as describe the satisfaction of various properties of electronic voting. We then discuss and outline the scalability in terms of the number of participants while maintaining the integrity of the on-chain smart contract data. We implement this variant in our next work, SB-Vote, where we test electronic voting on several different smart contract-enabled blockchains, including a second-level (L2) blockchain, and demonstrate that our approach can be used for millions of users. In the last part of the talk, we discuss our proposed approaches for repeated voting in Always-on-Voting (AoV), which address the problems of peek-end-effect and granularity of the periods between votes, and thus brings more flexibility into the voting itself. We will introduce the attacker model and the goals we want to achieve. We then introduce AoV and the techniques it uses. We then perform a security analysis and discussion in terms of incentive schemes, pluggable voting protocols, changing candidate lists, and the use of different types of blockchains.