Implementing a Blockchain-Based Voting System: Exploring the Use of Decentralized Technology for Transparent and Fraud-Resistant Elections

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the

Degree Bachelor of Science, School of Engineering

Baran Kalaycioglu

Spring, 2024.

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisors

Rosanne Vrugtman, Department of Computer Science

Briana Morrison, Department of Computer Science

Implementing a Blockchain-Based Voting System: Exploring the Use of Decentralized Technology for Transparent and Fraud-Resistant Elections

CS4991 Capstone Report, 2024

Baran Kalaycioglu
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
bk3xgp@virginia.edu

ABSTRACT

The prevalence of fraud and inefficiencies in traditional voting systems calls for a more secure and reliable alternative. I propose a blockchain-based voting system designed to ensure the integrity and immutability of voting records. By leveraging smart contracts for a streamlined design and a decentralized architecture for self-verification, the system would offer a novel approach to secure digital voting. My proposal explores existing decentralized blockchain frameworks designed for cryptocurrencies, analyzing how they can be adapted and enhanced to meet election security requirements and find a feasible implementation. Future work will focus on addressing scalability challenges, enhancing voter anonymity, and conducting extensive field testing to validate the system's efficacy in real-world elections.

1. INTRODUCTION

Traditional centralized voting methods have encountered various forms of fraud and inefficiencies, ranging from voter fraud to the exclusion of eligible voters. The search for a more secure, transparent, and efficient voting mechanism has prompted researchers to investigate the potential of utilizing blockchain technology for this purpose. Additionally, all centralized voting systems face potential risks of government fraud.

Blockchain, a decentralized ledger technology prominent in cryptocurrencies such as Bitcoin and Ethereum, offers a promising solution for reimagining conventional electronic voting systems. Each block includes a timestamp, the transaction data, and a cryptographic hash linking it to the preceding block, essentially serving as a safeguard for both private and public data. Its inherent qualities, such as cryptographic security, immutability, anonymity, provenance, transparency, and decentralization[6], make it a highly suitable candidate for voting systems.

2. RELATED WORKS

Blockchain technology's application in voting has been extensively explored through pilot projects and studies, demonstrating significant potential. Huang et al.'s systematic review analyzes different proposals for incorporating blockchain into voting systems, offering a detailed comparison of strategies and design principles[2].

Research by Jafar et al. evaluates blockchain frameworks such as Bitcoin, Ethereum, and Hyperledger Fabric, pinpointing those most apt for voting purposes[3]. Tas et al. delve into the challenges and prospects of blockchain in e-voting, emphasizing the essentiality of scalability, voter anonymity, and robust security measures, thereby laying down fundamental criteria crucial for guiding this

proposal[4]. Cryptographic frameworks for secure voting, particularly the voting scheme by Fujioka et. al.,'s commonly referred to as FOO, provides the basis of the voting procedure presented in this proposal[5].

Unlike most proposals which presuppose the existence of unique voter identifiers, this paper presents a design which addresses this crucial aspect of an election process. By integrating traditional voting elements with various encryption algorithms and a decentralized system, it offers a unique - albeit highly theoretical - framework for a secure and decentralized voting system.

3. PROPOSED DESIGN

The design proposal outlines the technical elements involved and describes the voting procedure under its implementation. The procedure is divided into three main phases: setup and registration, ballot preparation and submission, and opening and counting. Each section delegates parts of the overall design to specific components or entities, and the roles and responsibilities for each are described.

3.1Key Components of System Architecture

The design integrates smart contracts in place of regulatory entities within the system architecture, similar in concept to servers or clients that manage distinct aspects of the design. The contracts are self-executing programs, automating and regulating the process based on the contract's algorithm[2]. Their use also facilitates separation of concerns, allotting specific tasks to specific entities to prevent collusion and enhance efficiency.

The smart contracts delineated for this proposal are:
Validator: verifies voter eligibility and generates a list of approved voters during the setup and registration phase.
Collector: collects submitted ballots, assigns each a number, and sends the ballot-number pair as a transaction onto the blockchain during the ballot preparation and submission phase.
Counter: processes the ballot-number pairs received from the Collector, unlocking ballots with keys submitted by voters to tally the votes during the opening and counting phase.

Additionally, the proposal acknowledges an *Administer* role, symbolizing the election's governing or organizing entity, such as a government body.

When considering the blockchain system's architecture, critical considerations include optimizing block and transaction sizes, reducing latency, selecting an appropriate consensus mechanism, and deciding public or permissioned access. The system requires high throughput, scalability, minimal mining, a permissioned structure and smart contract support to meet the electoral process's unique needs. Based on Jafar et al.'s evaluation[3], Hyperledger Fabric stands out as the ideal framework due to its ability to fulfill these criteria and offering a modular architecture, allowing for adjustments to tailor the architecture to best fit the requirements of the system.

3.2 Voting Process

3.2.1 Setup and Registration

The setup and registration phase ensures voter eligibility. For setup, the Administrator defines and publicizes eligibility criteria and prepares registration centers, while voters submit their credentials to electronic machines at designated registration centers.

Each center houses its dedicated local client, which serves as an access node to the permissioned blockchain. Each voting machine at the center is connected to the client and relays voter information it receives. The

voters go to their designated venter to submit their vote. Once submitted, the data is transferred to the Validator deployed on the blockchain to verify eligibility based on the established eligibility criteria.

Upon validation, the smart contract signals approval, prompting the client to create a unique private/public key pair via an asymmetric key generation algorithm. The client then shares the public key with other nodes for duplicate and formatting checks. A non-unique or non-compliant key result in transaction rejection, prompting key regeneration. If accepted, the public key is logged on to the ledger to form a permanent registration record, and the key-pair is given to the voter. Finally at the end of the phase, ledger transactions are transferred to the blockchain, publicly listing eligible voters' keys for audit.

3.2.2 Ballot Preparation and Submission

Upon obtaining their keys, voters encrypt their ballots using a bit-commitment scheme similar to the protocol used in FOO[5], ensuring vote secrecy while committing to a choice. This encryption utilizes a unique reveal key, which the voter may generate through applying a randomized shuffling algorithm on their private key, to encrypt their vote. The result is an encrypted "ballot" for submission.

The voter then generates a ring signature with their private key and the public keys list from the registration phase, attaching it to their ballot. This ring signature confirms the voter's eligibility without disclosing their identity, allowing anyone to verify the signature's authenticity - the algorithm is designed such that anyone can check the validity of the signature using the list of public keys, validating they are from the eligible voters list, without revealing their identity[8].
The signed ballot is then sent to the Collector, who catalogs the ballots in a ledger and sequentially assigns each a number before appending the block to the blockchain. At the end of the phase, voters can confirm their vote's recording by re-creating the ballot and ring signature. If their vote is missing, they may craft their ballot and ring signature to prove their absence as an eligible voter.

3.2.3 Opening and Counting

To open their ballot, the voter submits their reveal key and ballot number to the Counter, who retrieves the <ballot, number> pairs from the Collector. Using the reveal key, the Counter unlocks and counts the vote associated with the submitted number. Votes with non-functioning reveal keys or invalid contents are rejected. Valid votes are logged on the ledger, and upon completion of the count, the Counter appends a block of valid votes on the blockchain.

4. ANTICIPATED RESULTS

In this section, I evaluate the benefits offered by my proposal and the limitations of the system design. Although the proposal employs a variety of encryption techniques and provides a robust framework, it lacks a practical foundation and remains largely theoretical.

4.1 Benefits

The system provides a mechanism for generating unique keys for each voter. Most protocols, including FOO, generally presuppose initial voter authentication or a unique identifier without detailing its generation, separating this proposal from the majority.

Requiring voters to register in person with credentials minimizes identification fraud and defines secure blockchain entry points. Only authorized registration centers, acting as permissioned nodes, can conduct transactions, enhancing accountability and preventing

external interference. However, the feasibility of this approach remains largely theoretical.
The system's use of multiple encryption methods enhances its security, while its decentralized nature ensures transaction verification and eliminates single points of failure. Adding blocks to the chain after each phase secures the preceding data.

The system automates each phase through smart contracts, with distinct contracts for different phases distributing responsibilities across entities, ensuring a separation of concerns.

4.2 Limitations

The proposal, while novel, remains largely hypothetical with questionable feasibility. The specifics of smart contract operations and the design of a blockchain supporting transactions with varying formats and other described functionalities are left unexplored.

Aspects of the proposal can be considered convoluted and unnecessarily complex, making auditing difficult. Exploring advanced algorithms like zero-knowledge proofs, not covered in the paper, may offer more efficient solutions for certain steps[6].

Each phase concludes with a block added to the blockchain, securing and rendering the previous data immutable. However, this process prevents real-time broadcasting, allowing voters to audit their information's recording only after a phase ends and before the next begins.

The system's energy and power demands are expected to be substantial. Even with a less resource-intensive permissioned consensus mechanism, the registration process remains computationally demanding. Moreover, generating unique keys may become challenging with a high volume of registrations, potentially leading to numerous flags exchanged between Validators and clients at registration centers, risking system timeouts. Consequently, the scalability of this design is doubtful.

The proposal lacks secure channels for safely transmitting transactions. Although transaction contents are secure, their submission remains vulnerable to attacks. Additionally, much of the auditing, validation and encryption processes depends on the voters' own efforts.

5. CONCLUSION

The proposed design introduces a novel approach to rethink conventional voting systems, leveraging smart contracts to alienate workloads and automate processes. It incorporates numerous encryption techniques alongside blockchain architecture to ensure vote security. While the integration of diverse strategies provided an intriguing exploration of the potential uses of various algorithms for voting systems, in practice, it is likely to overly complicate the process. Overall, exploring and prototyping a theoretical blockchain-based voting system gave me insight into how difficult and computationally intensive such an undertaking would be, and I do not anticipate that such a proposal could feasibly be implemented on a large scale.

6. FUTURE WORK

Future work could focus on specialized implementations of decentralized voting systems where they are most applicable. While the benefits of using decentralized voting are clear, this project has demonstrated that a large-scale deployment, such as for national elections, is practically infeasible. The development and implementation of more advanced and efficient algorithms for this purpose should be explored.

REFERENCES

1. Peralta, R. (2016, May 23). Electronic voting. Encyclopedia Britannica. https://www.britannica.com/topic/eletronic-voting
2. Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K.-K. R. (2022). The application of the blockchain technology in voting systems: A review. ACM Computing Surveys, 54(3), 1–28. https://doi.org/10.1145/3439725
3. Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. Sensors (Basel, Switzerland), 21(17), 5874. https://doi.org/10.3390/s21175874
4. Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for e-voting. Symmetry, 12(8), 1328. https://doi.org/10.3390/sym12081328
5. Fujioka, A., Okamoto, T., & Ohta, K. (1993). A practical secret voting scheme for large scale elections. In J. Seberry & Y. Zheng (Eds.), Advances in Cryptology—AUSCRYPT '92 (pp. 244–251). Springer. https://doi.org/10.1007/3-540-57220-1_66
6. Zero-knowledge proofs in blockchain voting | hackernoon. (2023, November 22). https://hackernoon.com/zero-knowledge-proofs-in-blockchain-voting
7. Bender, A., Katz, J., & Morselli, R. (2006). Ring signatures: Stronger definitions, and constructions without random oracles. In S. Halevi & T. Rabin (Eds.), Theory of Cryptography (pp. 60–79). Springer. https://doi.org/10.1007/11681878_4