ELECTORA WHITEPAPER

JAMES CAMPBELL

Abstract. Presenting a novel voting system designed to maximize privacy and minimize trust, while maintaining comprehensive verifiability. In this system, voters are able to validate their eligibility without disclosing their identities. Votes, securely encrypted, remain private throughout the voting period, and only become public once this period concludes. This feature provides an opportunity for any third party to audit the election process, from verifying the legitimacy of voter eligibility to the authenticity of the final vote tally, thereby promoting a robust and transparent democratic process.

1. Introduction

This paper discusses a voting system that utilises Sismo zkproofs [1], threshold.network's Conditions Based Decryption (CBD) [2], and the Arweave storage blockchain Section 2.3. Sismo zkproofs, based on zero-knowledge proofs, allow voters to validate their eligibility while keeping their identities hidden. In tandem, threshold CBD encrypts all votes, which remain inaccessible until a predetermined time-based condition - the conclusion of the voting period - is met.

The Arweave storage blockchain is used for storing encrypted votes and their associated zkproofs. Arweave's unique blockweave architecture provides a permanent, immutable storage solution, preserving voting records for future audits and verification of the voting process. When the voting period ends and the CBD condition is satisfied, all votes become public, enabling the verification of zkproofs and the counting of eligible votes.

The system is built entirely with public domain, open-source tools, enhancing transparency and offering users with the requisite technical skills the option to participate independently in the voting process. This approach, combining Sismo zkproofs, threshold CBD, and the Arweave storage blockchain, contributes to a voting system that prioritises privacy, verifiability, and minimised trust.

In Section 1.1 we cover the motivation of the project and the state of current voting systems. In Section 2.1, Section 2.2, and Section 2.3 we introduce each of the core components of the protocol. Then, in Section 3 we outline the role of each of the components and how they interact with each other.

1.1. Background.

Electronic voting systems have emerged as a significant area of research and development in the field of information and communication technology, with potential applications in various aspects of governance and political processes. The adoption of such systems, however, is not without its challenges and concerns, particularly in terms of security, infrastructure, and implementation.

The concept of electronic voting has been explored in various contexts, including the potential application of blockchain technology in e-voting systems. A study by Rahmad et al. [3] provides an overview of blockchain technology towards e-voting in Malaysia, highlighting the potential of blockchain as a secure and transparent platform for voting processes. The study underscores the importance of addressing the challenges associated with the implementation of such technology, including issues related to security, privacy, and the digital divide.

Security considerations are paramount in the implementation of electronic voting systems. Limba et al. [4] delve into the peculiarities of cyber security management in the process of internet voting implementation. The study emphasizes the vulnerabilities of personal devices used for e-voting and the potential threats from hackers and foreign intelligence services. It suggests that all votes must be encrypted in a way that ensures that a single person is unable to decrypt them, and recommends rules that limit the ability of system administrators to elevate their own privileges.

The complexity of voting systems within social networks is another aspect of electronic voting that has been explored. Alouf-Heffetz et al. [5] compare different voting systems within social networks, including direct democracy, liquid democracy, and sortition. Their research illustrates how voter competency distributions and levels of direct participation affect group accuracy differently in each voting mechanism, providing valuable insights for the selection of a suitable voting system based on the characteristics of a particular voting setting.

However, the limitations of the current deployed infrastructure for remote electronic voting over the Internet are a significant concern. Rubin [6] discusses the security considerations for remote electronic voting, focusing on the limitations of the current infrastructure in terms of the security of the hosts and the Internet itself. The study concludes that, at the time of writing (2002), our infrastructure was inadequate for remote Internet voting.

In conclusion, while electronic voting systems offer promising opportunities for enhancing democratic processes, they also present significant challenges that need to be addressed. The complexities of these systems, coupled with the security concerns and limitations of the current infrastructure, underscore the need for continued research and development in this field.

2. Components

2.1. **Sismo.** Sismo [1] utilises zero-knowledge proofs (ZKPs) and privacy-preserving technologies to aggregate and selectively disclose personal data to applications. In the context of our voting system, Sismo plays a crucial role in ensuring voters can validate their eligibility without revealing their identities, thus maintaining voter privacy.

Sismo is designed to respond to the challenges of fragmented digital identities, which are dispersed across the internet in a variety of platforms (both web2 and web3). Sismo's communication protocol enables users to consolidate their digital identity data in a private Data Vault, which acts as a secure storage for personal data from various web2 and web3 accounts, credentials, and attestations.

The Data Vault acts as a prover, enabling users to generate ZKPs that attest ownership of granular pieces of data, referred to as Data Gems. Using Sismo's communication protocol, users can generate proofs to verify claims about Data Gems they own. These proofs are accepted and verified by verifiers integrated into applications, such as the voting system discussed in this paper. This allows users to selectively disclose their data without revealing the associated Data Source, underpinning the privacy-preserving feature of the voting system.

2.2. **CBD.** The voting system incorporates Threshold's Conditions Based Decryption (CBD) Section 2.2, a cryptographic technique for safeguarding sensitive information. CBD encrypts all cast votes, rendering them private and inaccessible until a pre-specified condition is fulfilled. In this particular application, the condition for decryption is time-based: the end of the voting period.

CBD operates on the principle of formal verification by a cohort of decentralized nodes within the Threshold network [7]. Only when the predefined conditions are provably satisfied does the data requester gain decryption rights. In the context of our voting system, this means that the votes, initially encrypted by the voter (the data owner), remain completely unreadable to anyone until the voting period concludes.

The conditionality underlying CBD is versatile, allowing the data owner to define a range of access conditions. In this voting system, a time-based condition is employed: votes become accessible for decryption only after a pre-specified period (the voting period) has elapsed. This enhances the privacy of the voting process, ensuring that the votes of individual participants remain confidential until the predetermined time condition is met.

A key component of CBD is the Threshold Decryption scheme, which involves distributing a decryption key into multiple shares amongst decentralized nodes within the Threshold network. A minimum number of these nodes, or a threshold, must participate in partial decryptions which are then combined on the requester's client to reconstruct the original plaintext data - the votes, in this case.

The application of CBD in this voting system represents a leap in privacy-preserving technologies, guaranteeing the confidentiality of votes during the voting process while allowing for public verification once the voting period concludes.

2.3. **Arweave.** Outline arweave [8]

3. Architecture

Describe how everything fits togetherp - probably through the user journey.

3.1. Creating an Election.

- create a sismo group (eligibility criteria)
- set an end date (becomes the cbd decryption condition)
- add voting options/candidates
- write to Ballot Manager contract on scroll

3.2. Participating in an Election.

- navigate to relevant ballot
- generate a sismo proof of eligibility (belonging to the associated sismo group)
- pick choice
- encrypt zk proof + vote in browser
- store on arweave

3.3. Counting an Election.

- check end time
- collect relevant votes from arweave (tagged with ballot id)

- decrypt everything, discard anythig invalid
- verify all proofs, discard anything invalid
- remove any duplicated proofs (proofs will be unique but they return and anonimized user id)
- Publish and count everything that is left

References

[1] Sismo, "Sismo documentation." https://docs.sismo.io/sismo-docs/

[2] threshold.network, "CBD documentation." https://docs.threshold.network/applications/threshold-access-control/conditions-based-decryption-cbd

[3] Fadhilnor Rahmad, Mad Khir Johari Abdullah Sani, and Irni Eliana Khairuddin, "An overview of blockchain technology towards e-voting in Malaysia." [Online]. Available: https://pdfs.semanticscholar.org/c6ec/fb8a6876d742efaf74a9ee1b5b7d28318e79.pdf

[4] Tadas Limba, Konstantin Agafonov, Linas Paukštė, Martynas Damkus, and Tomas Plėta, "Peculiarities of cyber security management in the process of internet voting implementation." [Online]. Available: https://jssidoi.org/jesi/uploads/articles/18/Limba_Peculiarities_of_cyber_security_management_in_the_proce

[5] Shiri Alouf-Heffetz, Ben Armstrong, Kate Larson, and Nimrod Talmon, "How should we vote? A comparison of voting systems within social networks." [Online]. Available: https://www.ijcai.org/proceedings/2022/0005.pdf

[6] A. Rubin, "Security considerations for remote electronic voting over the internet." [Online]. Available: http://arxiv.org/pdf/cs/0108017

[7] threshold.network, "Threshold documentation." https://docs.threshold.network/

[8] S. Williams, V. Diordiiev, L. Berman, I. Raybould, and I. Uemlianin, "Arweave: A protocol for economically sustainable information permanence." [Online]. Available: https://www.arweave.org/yellow-paper.pdf

James Campbell, Amsterdam, Netherlands
URL: https://github.com/theref