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 [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.

1.1. **Background.**

2. Architecture

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) [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 [4]. 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.** [3]

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] 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

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

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