Towards a Fully Mobile, blockchain-based Electronic Voting system using Non-Fungible Tokens

Ricardo Lopes Almeida[1], Fabrizio Baiardi[2], Damiano Di Francesco Maesa[3], and Laura Ricci[4]

[1, 2, 3, 4]Dipartimento di Informatica, Università di Pisa, Italia
[1]Università di Camerino, Italia

September 17, 2024

Abstract

Research in electronic voting systems has been constant and fruitful since the 1970s, when the introduction of commercial cryptography provided the tools and methods for such critical operations. Yet, save for a few exceptions for testing purposes, no remote electronic voting system has been employed systematically.

A significant breakthrough occurred in 2009 with the introduction of the decentralised computational paradigm through Bitcoin, the world's first cryptocurrency, and the distributed ledger technology that supports it. Researchers soon started applying decentralised concepts and using distributed ledger's features to propose e-voting systems from a decentralised approach, which revealed itself superior right from the start. As a consequence, the field moved to use the new paradigm soon after, and new proposals employing the latest distributed ledger features are still appearing.

This article characterises the evolution of e-voting research through the years and presents a novel architecture based on smart contracts and Non-Fungible Tokens (NFTs), a recent addition to the distributed ledger ecosystem. We explore the inherent advantages of this new concept, as well as its development framework, to present the architecture of a fully mobile, decentralised electronic voting system using NFTs as the main vote abstractor.

1 Introduction

The modernization of voting systems is an active area in academic research, namely in electronic based systems that can improve upon the traditional paper and pen system that many modern democracies still rely on. This research has been mainly focused in developing systems that verify a finite set of security criteria that are used to infer in the ability of such system to deliver the choice of a voter to a tally authority in a safe, transparent and private fashion.

Technological evolution in voting systems before the mid 1970's was restricted to improving on existing voting methods, always with the fundamental limitation of requiring the physical presence of the voter to initiate the process. Both paper ballots and modern touch screen voting terminals limit voting activities by imposing a time and place that does not take into account unforeseen circumstances during the limited availability window nor other limitations that can affect a voter and hinder his or her ability to enact this civic duty.

In 1976, a landmark article by Diffie and Hellman [2] provided the basis for the development of commercial cryptography. Until this point, cryptographic research was confined to governmental (i.e., military) applications. The ideas introduced by this publication triggered a flurry in cryptographic research which produced many of the cryptographic schemes and tools that still support online communication to this day. The development of asymmetrical encryptions schemes based in unidirectional problems, i.e., mathematical problems that are trivial to compute in one direction but unfeasible to solve in the opposite direction, produced popular schemes, such as the *Rivest-Shamir-Adleman (RSA)* [6] cryptosystem, which uses the factorization of the product of two large prime numbers as such intractable mathematical problem. The *ElGamal* cryptosystem is another example that provides similar functionalities but relying in the difficulty of computing discrete logarithms as its one-way function.

Commercial cryptography was a boon for e-voting research. The years following Diffie and Hellman's article saw a significant increase in publications proposing voting systems that use cryptographic schemes and tools as these get developed by other researchers. Though technically sound, none of these proposals was able to make it as a real-world application, mainly due to security concerns. One limiting aspect of these proposals was their reliance in server-client architectures, which are prone to creating a single point of failure in the system, often the point of focus in an attack by an adversary party.

The increase in cryptographic based e-voting proposals also increase the attention of the research community to this topic, namely to the conceptualization of security in these systems, which revealed itself with researchers addressing this topic in e-voting proposals or even dedicating entire publications to it, such as [5] or [3], which were among the first defining trust in an e-voting system through the implementation of specific security criteria, with the rationale that trust in the system is proportional to the number of criteria implemented. These criteria add the properties that define them to the system, such as *accuracy* if a system is able to prove that no invalid votes can be added to the final tally, *privacy* if it is able to maintain the secrecy of a vote from the moment it is cast to when it is finally tallied, etc.

The nomenclature as well as the definition of such criteria is still quite subjective among relevant publications, as a consequence of a lack of standardization in this regard, with the same criteria being often referenced in publication by different names. [1] performed an extensive systematic literature review among e-voting proposals spanning several decades with the goal of establishing an unified set for these criteria. These include *accuracy*, *privacy*, *eligibility*, *verifiability* and *robustness* as a **minimal set**, as in the criteria that directly relate to increased overall security. An **additional set** containing the *convenience*, textitflexibility and *mobility* criteria was also included in this publication as criteria that simplify the usage of the system by a voter, but do not directly contribute to a more secure operation.

E-voting research followed the cryptographic stream for around 30 years, until another landmark article was published in 2009. [4] introduced Bitcoin and blockchain to the world, with the latter being a critical development in the development of a new approach to e-voting. Blockchain is also heavily dependent in cryptography, and as such this new development was not as extreme, providing some continuation from the techniques developed thus far. But the new decentralized approach provided a new avenue of research and soon after the first blockchain-based e-voting systems were published in academia. The evolution of such systems is in itself a window into the evolution of blockchain: earlier proposals were limited to find creative ways around cryptocurrency transactions, which for some years was the sole application of blockchain technology, while later proposals use Smart Contracts, as well as functionalities from the Distributed Virtual Machines that support them, extensively.

This proposal follows the blockchain stream by exploring how Non-Fungible Tokens (NFTs), relatively new feature that gained popularity in recent years, can be used to implement a voting system. NFTs are used to establish ownership of digital objects in a blockchain. Up to recently, most NFT applications are reduced to digital collectibles and digital art. Our approach is to use them to represent digital votes and research on how the mechanism in which ownership is established in the blockchain can be used to devise a more secure e-voting system. In addition to this proposal, we also extend this study to include an implementation in Ethereum, the most popular blockchain with smart contract support, and another implementation in Flow, a more recent blockchain implementation that was optimized for NFT operations, namely transactions and storage model used. These two implementations provide valuable insight to the usefulness of Non-Fungible Tokens in an e-voting context.

The rest of this article is structured as follows: the following Section 2 details the current state of related works. Section 3 provides an introduction to the fundamentals workings of a Non-Fungible Token. Sections 4 and 5 detail the implementation of an basic e-voting system that uses NFT metadata to encapsulate vote selections, and Section **??** provides a summary of the results and an objective comparison between the two approaches considered. Section **??** concludes the article.

2 Related Works

TODO: Related Works!

3 Introduction to Non-Fungible Tokens

TODO: Intro to NFTs

4 Solidity Implementation in Ethereum Blockchain

TODO: Solidity Implementation in Ethereum

5 Cadence Implementation in Flow Blockchain

TODO: Cadence Implementation in Flow

6 Results and Implementation Comparison

TODO: Results and System Comparison

7 Conclusion

TODO: Conclusion .

References

[1] Ricardo Lopes Almeida et al. “Impact of Decentralization on Electronic Voting Systems: A Systemic Literature Survey”. In: *IEEE Access* 11 (November 2023), pp. 132389–132423. ISSN: 21693536. DOI: 10.1109/ACCESS.2023.3336593.

[2] Whitfield Diffie and Martin E. Hellman. “New Directions in Cryptography”. In: *IEEE Transactions on Information Theory* 22 (6 Nov. 1976), pp. 644–654.

[3] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. “A Practical Secret Voting Scheme for Large Scale Elections”. In: *Workshop on the Theory and Application of Cryptographic Techniques*. Ed. by Jeniffer Seberry and Yuliang Zheng. Gold Coast, Queensland, Australia: Springer-Verlag, 1992, pp. 244–251.

[4] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”. In: *www.bitcoin.org* (2008), pp. 1–9.

[5] Peter G. Neumann. “Security Criteria for Electronic Voting”. In: *Proceedings of the 16th National Computer Security Conference*. Baltimore, USA, 1993, pp. 1–7.

[6] Ron Rivest, Adi Shamir, and Leonard Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. In: *Communications of the ACM* 26 (1 1983), pp. 96–99.