Dottorato di Ricerca di Interesse Nazionale in Blockchain and distributed Ledger Technology - Social Systems and Smart Societies

Research Plan

Doctoral Student: Ricardo Lopes Almeida[1] [2]

Advisor Team:
Fabrizio Baiardi[1],
Damiano Di Francesco Maesa[1]
Laura Ricci[1]

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

November 15, 2024

1 Research Plan

1.1 Introduction

The project presented in this document is the main research idea presented towards the completion of the Doctoral Program of the 38^{th} cycle of the Italian National Program in Doctoral Research - Blockchain and Distributed Ledger Technology in Social Systems and Smart Societies.

I, Ricardo Almeida, graduated in Physics and Chemistry by the University of Evora, and with a Master's in Electronic Engineering and Telecommunications by the University of Aveiro, both universities in Portugal, from where I'm originally from, was awarded a 3 year scholarship towards the execution of a research plan centered on decentralised (blockchain based) electronic voting systems.

1.2 Doctoral Project Outline

The idea for this project was inspired by personal curiosity for blockchain technology, which was developed prior to the decision of engaging in the PhD program, and another parallel interest in general governance, but also motivated by the novelty of new technology and the potential for new solutions to existing problems through a novel decentralised approach. Initially this project had a more generalist approach due to the lack of support from blockchains to voting systems. A review of existing blockchain-based e-voting proposals in academia revealed an environment where researchers were trying to discover how to use blockchains developed with financial purposes in mind, namely cryptocurrency-centered blockchains, towards different applications. The introduction of smart contracts by the Ethereum blockchain opened significantly the spectrum of research possibilities, but the most significant breakthrough in this context came with the popularisation and standardisation of Non-Fungible Tokens (NFT).

NFTs provide an interesting new approach to developing a blockchain-based voting systems. NFTs are inherently scarce, indivisible and individually unique. Also, the mechanics that regulate transferring them among users are transparent, since these are always smart contract functions that can be publicly verified, and secure. All NFT operations, from when they are minted until when they are burned, are recorded permanently in the blockchain, which makes NFTs highly traceable. These properties happen to be also highly desirable in a voting ballot. From this observation, the idea of including NFTs to abstract voting ballots in a blockchain-based voting system was quite obvious.

Non-Fungible Tokens are a general idea. From the implementation point of view, the last years saw many public blockchains being introduced with explicit NFT support built in, normally through its support for some sort of smart contract programming paradigm that also supports NFT creation and mechanics. As such, it was evident that the specific technology used in the context of this project would be determinant to any conclusions obtained. In this sense, the doctoral project was expanded to also investigate how significantly different

blockchain architectures behave when used to develop a NFT centered voting system and how these differences can influence the intrinsic characteristics of the system itself.

Among the potential choices of blockchains, I'm focused in comparing the most popular of smart contract/NFT supporting blockchains - Ethereum, with Flow [5], a blockchain that, incidently, was created specifically to address scalability and interoperability issues that arose from running the *CryptoKitties* project in the Ethereum blockchain. The *CryptoKitties* smart contract created one of the first interactive NFT projects in Ethereum, one whose sudden and unexpected popularity put the throughput limits of the Ethereum network to a test [2]. The team behind this project tried to overcome the limitations of the Ethereum network, initially by adjusting the Solidity contract, but eventually they decided to create their own blockchain from scratch. Flow was created to the most efficient blockchain to trade NFTs in. Its main difference from Ethereum resides on how these chains store data, specifically, NFT related data. Ethereum uses a *contract-based* storage approach, where all NFT fields are stored on chain with a reference to the minting contract, i.e, the NFT minting contract is the central storage element, while Flow developed a more decentralised, *account-based* storage approach. In Flow, contracts and NFTs are two different data elements and both are saved relative to an *account*, as in a normal blockchain account, akin to the Externally Owned Accounts from Ethereum, rather than a contract address as in Ethereum. Account storage spaces in Flow can only be modifies by the account owner and any external accesses to digital objects in storage must be explicitly given previously by the owner. Flow and Ethereum differ in other aspects, but the method in which data is saved on chain is the most influential for this purpose.

Though both blockchain implement the same construct, they do so in fundamentally different ways. Due to, perhaps, the novelty of the whole context, there are no objective comparisons between these two approaches published academically or otherwise, neither from a generalist point of view, less even from a electronic voting system development perspective, definitely motivation for this project. Ifg. 1 presents a general idea of the approach considered for a NFT based e-voting system.

1.2.1 Collaboration with the University of Surrey

The Italian *Dottorato di Ricerca di Interesse Nazionale* program establishes a period of 6 months minimum to a maximum of one year where the doctoral research must be undertaken in an foreign (non-Italian) university or research institution. The University of Surrey was chosen to this purpose by several reasons:

1. Similar to the University of Pisa, Surrey maintains a dedicated Blockchain and Distributed Ledger Technology research group, as well as researchers active in electronic voting systems development, something that is not yet common in most European universities.

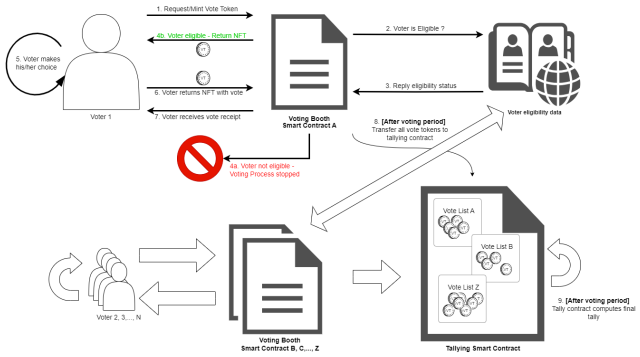

Figure 1: General solution adopted to experiment with the different storage architectures considered.

2. I've collaborated with U. Surrey researchers recently in a research project in a similar area (homomorphic encryption) and the feedback of such collaboration was largely positive.

3. I'm already quite familiar with the United Kingdom, both the country and the culture. I've worked with British organisations and lived in British soil in the past and I have most of my British bureaucratic elements still active, namely a bank account and a valid National Insurance Number which, hopefully, can make a transition back to the UK easier.

1.3 Research Questions

The salient research points indicated in Sec. 1.2 were summarised in the following set of Research Questions:

1. What advantages, if any, does a *account-based* storage architecture provides when compared with a *contract-based* approach regarding implementing Non-Fungible Token based smart contracts?

2. Can Non-Fungible Tokens be used to develop a secure, transparent and private blockchain-based voting system, using these tokens to abstract the voting ballot?

3. If NFTs are indeed useful to be used in a decentralised e-voting context, which of the storage architectures considered produces the better option?

1.4 State of the Art/Related Works

Research in electronic voting systems as been active for several decades now and started parallel to the first breakthroughs in commercial cryptography techniques. Until the 1970s, cryptography was mostly used in a military context, but a landmark article by Diffie and Hellman published in 1976 [3] opened the

doors to commercial applications, as well as laying the groundwork for most of the research in electronic voting systems that followed it.

This field evolved somewhat linearly over the following 30 years, with new proposals to novel voting systems following the introduction of new commercial cryptographic techniques, such as symmetrical and asymmetrical encryption schemes, digital signatures, hash algorithms, blind signatures, homomorphism, mix-nets, etc. This pace was kept until relatively recently, when another landmark publication changed the research landscape. In 2009, the mysterious Satoshi Nakamoto published a white paper detailing Bitcoin, the first instance of a cryptocurrency, also introducing the blockchain concept was critical for the whole process to work [4]. Though this publication had no direct relation to the e-voting research, the applicability of blockchain (and cryptocurrencies by extension) in the voting context was obvious. Soon after, the first blockchain-based e-voting proposals came to light, with the rate of new proposals following new blockchain features and tools, such as smart contracts, consensus algorithms and even new architectural approaches, like it was already happening with commercial cryptography.

The main conclusion and results for this exercise were published in a journal article [1] at the end of year 1 of this program. Following this exercise, further investigation was undertaken towards determining the extent at which academic publications were focusing either in new blockchain architectures and using these new architectures to improve existing voting systems. Though the shift towards the usage of smart contracts was quite evident in new decentralised proposals, as indicated in [1], so far the same does not seem to apply to Non-Fungible Tokens. Up to the time of this writing, I have not been able to find any academic publications detailing any architectural comparisons between blockchain implementations nor any e-voting proposals where NFTs are used explicitly to establish the voting system.

1.5 Proposed Strategy and Timeline

The project timeline was defined with the following sequence of steps and deliverables:

1. Knowledge acquisition phase - year 1 and 2

   Expected milestone: Literature Survey on centralised and decentralised e-voting systems (DONE)

2. Blockchain architecture analysis and comparison based on NFT implementation details - year 1, 2, and 3 **Expected milestone**: Conference paper on the architectural aspects of NFT development and comparison between existing paradigms (IN PROGRESS)

3. Development of a prototype for a NFT-based voting system based on the architectural paradigms considered - year 2 and 3

4. Performance and implementation comparison between the prototypes developed - year 3 **Expected milestone**: Conference/journal article with a proposal for a NFT-based e-voting system. (IN PROGRESS)

5. Doctoral dissertation - year 3 **Expected milestone**: Doctoral dissertation presentation and discussion. (TO DO)

1.5.1 Expected outcomes for the period abroad

The collaboration with the University of Surrey is planned for the beginning of year 3. If agreed, I expect to start this period in the beginning of February 2025. I expect to have the architectural comparison article ready for submission by that time, so I expect to use the bulk of this period for the development of the prototypes suggested and to extract meaningful experimental results. The University of Surrey has developed projects of this kind in the past, so I'm counting with the expertise gathered during those experiences for additional guidance and counseling over the best direction to proceed during the development phase.

Also, the collaboration between Pisa and Surrey undertook in the beginning of the current year was promising. It allowed me to expand my expertise in areas that revealed some application potential to my doctoral project, therefore I'm also expecting to be able to collaborate in similar opportunities, if possible. Blockchain research is still an emerging research area and I'm determined to explore fully every opportunity to explore new source of synergy.

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] bbc.com. *CryptoKitties craze slows down transactions on Ethereum*. URL: https://www.bbc.com/news/technology-42237162 (visited on 06/22/2022).

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

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

[5] Flow blockchain development team. *Flow Prime*. technical report. Flow, 2020. 75 pp. URL: https://flow.com/primer.

Todo list