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

This document presents an abbreviated version of the research plan presented for my application to the 38th cycle of the Italian *Dottorato de Ricerca di Interesse Nazionale*, the international program financed by the Italian government for doctoral research. I graduated in Physics and Chemistry by the University of Evora and a Master's in Electronic Engineering and Telecommunications by the University of Aveiro, both public universities from Portugal from where I'm also originally from. My application to this program was awarded with a 3-year scholarship to develop a research project within the subject "Blockchain and Distributed Ledger Technology -Social Systems and Smart Societies".

With that theme in mind, I proposed a research line focused in the development of e-voting systems and how a decentralised, blockchain-based paradigm introduced by could be to their benefit. Governance and voting were presented as potential applications areas for blockchain academic research. Yet, years after the introduction of blockchain, there was little progress made. This project begun with an exhaustive systematic literary survey centered on both the older, centralised (server-client) architectures that was used to propose early e-voting ideas, and the new and emerging field of decentralised, blockchain-based voting systems. The main outcomes for this exercise where published in an journal article [1], but one of the more relevant conclusions was how largely unexplored blockchains are regarding voting applications. Incidently, while I was focused in this task, blockchains kept evolving and pushing new features, at the same time that researchers were still trying to explore old ones fully. A good example of this is how while most e-voting related papers published around that time were still largely exploring the possibilities brought by the introduction of smart contracts, the blockchain world was ablaze with the sudden popularisation of Non-Fungible Tokens (NFTs) and related applications.

Once I was able to understood the NFT concept properly, I realised how it can potentially beneficial towards the development of a blockchain-based voting system. During the decentralised approach of the literary survey, one of the difficulties made evident by the analysis of early blockchain-based proposals was the abstraction of the ballot itself, or more generally, conceiving a secure, transparent and private method to exchange secure information within the network. I also observed how researchers made the most out of the limited applicability scope of early public blockchains, given that most were based on cryptocurrency-centric blockchains, which required creative approaches to circumvent these limitations. In my perspective, NFTs were particularly apt for this purpose and solved plenty of issues that revealed themselves when applications different than the original were imposed to the chain.

The main purpose with this doctoral project is to develop a functional blockchain-based electronic voting system that uses NFTs as the main data transmission element in the system. Towards that objective, and given the central role NFTs play in this plan, I also suggested expanding this development to use different blockchain architectures for that purpose, namely considering a general purpose blockchain with smart contract and NFT support, and another

blockchain specialised in supporting NFT development and mechanics. I observed how the blockchain world reacted to the 2021/2022 boom in NFT popularity, and one of the outcomes of it was the creation of NFT-centric blockchains that had significantly different architectural definitions that claimed to allow for superior scalability, interoperability and speed regarding NFT operations. As such, I added a new objective to the current plan: explore blockchain architectures that are suitable for this application, towards determining the best development strategy to produce a secure, transparent and private e-voting system. A subsequent search for other academic proposals that were using NFTs towards this objective was unable to find any meaningful results. There's significant academic research being conducted around the applicability of the NFT concept, just not specific to voting systems, at least not presently. This considered, this project intends to respond to the following research question:

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?

In order to find a good answer to this, the doctoral project was subdivided in the following sequence of steps and expected milestones/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)

1.1   Collaboration with the University of Surrey

This doctoral 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 because:

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.

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.

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.

Todo list