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 [26] 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)* [70] 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 [62] or [32], 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. [4] 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. [61] 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 6 provides a summary of the results and an objective comparison between the two approaches considered. Section 7 concludes the article.

2 Related Works

The commercialisation of cryptography triggered a stream of new approaches to e-voting systems using new cryptographic schemes and tools derived from these to implement these ideas. Diffie and Hellman's 1976 publication [26] was followed by new symmetrical and asymmetrical cryptographic schemes proposals, such as [22], [28], and [70], which in turn were instrumental to define cryptographic tools that have been extensively used in e-voting system development, such as blind signatures [19], Mix-Nets [20], Homomorphism in threshold cryptosystems [73] and cryptographic knowledge proofs [34].

Research in e-voting systems progressed towards the establishment of a classification criteria that were then used to compare proposals from a security standpoint. Authors implemented criteria such as *accuracy*, *privacy*, *eligibility*, *verifiability*, *convenience*, *flexibility*, *mobility* and *robustness* using the cryptographic tools indicated thus far. A simple example that illustrates this process is the usage of asymmetrical encryption keys to encrypt voter data, thus protecting the *privacy* of the voter. A proposal that uses such scheme can claim that it establishes voter *privacy*. Yet, a formal definition of such criteria has notorious absent from related literature. [62] was among the first to attempt such characterisation, with subsequent publications, such as [32], [9], [44], [50], [52], [43], [7], and [21], continuing this trend. These articles followed the rationale that the more security of a voting system is proportional to the number of security criteria it implements, which translates in an assurance that a voter can trust his/her choice to it. Over time, these cryptographic tools became a fixture in all e-voting proposals in this initial 30-year window of research in centralised e-voting systems. This is a limiting paradigm since it constrains the whole system by establishing a single point of attack or failure, while also reducing system scalability, due in great part to the demand of a large amount of resources, such as primary and secondary storage, computational power, network bandwidth, etc., to implement these criteria.

Scalability is an crucial characteristic that can hinder a wide adoption of the proposed system. Contemporary elections can go from exercises where the system is only expected to process up to a thousand votes at one point, to national-wide events that might require the processing of millions of votes. The relationship between the scalability of a system and the amount of available resources is evident in the analysed literature. Proposals from this era confirm that the ones that satisfy the most security criteria also establish a computationally complex and demanding system that is often limited to small-scale elections. As an example, in [23], [64], [42], and [63], this trade-off was shifted towards security and transparency at the expense of scalability. The authors do recognize this limitation and, as such, are explicit in restricting the usage of their system to small-scale elections.

On the other side of this spectrum, proposals such as [11], [12], [67], [45], [66], [65], [54] or [59] present scalable systems that are simpler than the ones considered in the last paragraph, but their adoption in large-scale elections implies a sacrifice in security and transparency. Proposals suitable for large-

scale elections implement the lowest number of security criteria.

Several e-voting systems were evaluated in a real-world scenario. For this case, we are only interested in systems that address the criterion of *mobility*, i.e., a voting system that does not restrict voters geographically, in part because these proposals did not follow any of the academic ones that preceded them. Therefore, there was little interest in electronic proposals that limited their users to traditional polling places, since they infuse a degree of privacy and security that derives solely from the surrounding election apparatus. The few notable exercises in recent history were run in Canada in 2013 [35], Estonia in 2005 [39], Switzerland in 2005 [13], Norway in 2011 [30], France in 2012 [68], and Australia in 2015 [36].

The first decentralised e-voting proposals were limited to cryptocurrency-centric blockchain, such as Bitcoin, due to the lack of alternatives in the early years of blockchain development. This proposals were somewhat simple in the sense that they conceived convoluted and impractical methods to exchange information using transactional metadata from cryptocurrency transfers. Proposals such as [81], [24], [15], [53], [72], [79], [27] or [10] used a script function available in Bitcoin transactions to add voting information to the blockchain data, namely the *OP_RETURN* function, which receives an 83-byte wide string as input, and adds it to the transaction metadata as the function's output. Hence, it was used to write non-transactional data directly to the blockchain. This mechanism needs to go around the limited functionalities offered by early blockchain solutions whose scope of operations were limited to cryptocurrency transactions. Furthermore, this method is infeasible for large-scale use because a Bitcoin transaction necessarily involves exchanges worth a considerable amount of money, as well as being notoriously hard-to-scale blockchain due to its low block rate. Bitcoin adds a new block every 10 minutes, which limits the rate of operations that this blockchain can withstand.

The popularisation of public blockchains attracted interest from other platforms, which triggered the development of software frameworks used to create and deploy custom blockchains with proprietary access control and offering more flexibility to applications. As such, researchers such as [48], [6], [18], [16], [80], [46], [60], [31], [47], [37], [41], [55], [82], [5], [38], [75] or [56] adopted private blockchains using custom-made solutions in customisable frameworks such as Hyperledger Fabric, Quorum, and Multichain. As a drawback, the increased flexibility is paid for by a lack of network support. It is difficult to establish a privately accessible network with enough active nodes to establish a satisfactory level of redundancy.

A significant breakthrough arrived with the introduction of the smart contract through the Ethereum blockchain, specifically through the implementation of a *Touring-complete* processing platform, named *Ethereum Virtual Machine (EVM)*, that can execute code scripts in a decentralised fashion by splitting and distributing the instructions through the active nodes in the network. Proposals such as [57], [49], [25], [33], [40], and [58] were among the first to implement a voting system via Ethereum smart contracts.

The same time period also produced some blockchain-based proposals for

e-voting systems in a real-world scenario. Unlike the centralised approach, these solutions have significant overlap with the academic proposals considered. Among these real-world examples, we cite *Follow My Vote* [29], *TiVi* [74], *Agora* [2], and *Voatz* [76]. The difference between the nature of approaches regarding their real-world applications is an indicator of the potential of blockchain in this scenario. Real-world blockchain-based e-voting solutions follow the academic approach closer than their centralised counterparts.

The real-world solutions indicated are end-to-end applications, i.e., they are ready to be used in an election, as long as their limitations are properly addressed (mostly related to scalability). But there are other proposals published in the public domain as protocols that can be used to set up an e-voting systems instead. These are not complete solutions, as the ones indicated thus far, but instead protocols that can be used to establish a secure and transparent e-voting system. [51] presents a concise summary of the most relevant Ethereum based protocols in existence. Most of the logic employed in these protocols is already abstracted through smart contracts already deployed and publicly available in the Ethereum blockchain, such as the *MACI (Minimal Anti-Collusion Infrastructure)* protocol [17], *Semaphore* [69], *Cicada*, and *Plume*. It is important to notice that none of these protocols employs NFTs as an abstraction of votes as well. There are references to NFTs in the protocol description, but these are used to exemplify how the protocols handles ownership of digital objects or using NFT ownership as means to verify the identity of a voter, but never as the main vote element.

So far, none of the proposals considered used, or even mentioned, NFTs in their processes. Nevertheless, a search for recent proposals with this characterizing element was conducted. Any usage of NFTs in any capacity in a remote voting system was considered relevant, yet our search was unable to find a single complete proposal that combined both. For this purpose, we consulted the main academic databases, namely *Google Scholar*, *Science Direct*, *IEEE*, and *ACM*, using a broader search term at first, namely, "e-voting" and "NFT," as well as with expanded acronyms and other variations, without success. The closest article to a NFT-based e-voting system we were able to consider was [71], where the authors use SoulBound NFTs, a special case of non-transferable NFTs that can potentially be used for identification purposes [78], to circumvent the need for a trusted third party to implement voter *eligibility*. The proposed system only interacts with these NFTs during voter validation. The article does not provide enough technical details to determine exactly how blockchain is used in the remainder of the voting process, but it is clear with how limited their use of NFTs is.

Two other proposals, namely [14] and [1], do mention Non-Fungible Tokens, but more so as a product of their literature and technology review and not as an integral component in their solution. To conclude this search process, [3], [8], and [77] produced extensive surveys around the potentials and usage of NFT, as well as providing a list of future challenges where this technology can be determinant. [3] does mention a potential application of NFTs in governance applications, but without specifying voting or even elections in any capacity. [77]

listed challenges limited to purely digital applications, namely gaming, virtual events, digital collectibles, and metaverse applications. [8] provided a broader survey and identified a larger and more specified set of potential applications for NFTs, but none of them related to governance or e-voting.

As far as we were able to determine, no proposals were submitted thus far using NFTs as an integral element of an e-voting system.

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] Samuel Agbesi and George Asante. "Electronic Voting Recording System Based on Blockchain Technology". In: *Proceedings of the 12th CMI Conference on Cybersecurity and Privacy*. Copenhagen, Denmark, 2019. ISBN: 978-1-72812-856-6. DOI: 10.1109/CMI48017.2019.8962142.

[2] Agora. *Agora, Bringing our voting systems into the 21st century*. Tech. rep. www.agora.vote, 2021, p. 41. URL: https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5f37eed8cedac41642edb534/1597501378925/Agora_Whitepaper.pdf.

[3] Omar Ali et al. "A Review of the Key Challenges of Non-Fungible Tokens". In: *Technological Forecasting and Social Change* 187 (2023), pp. 1–13. ISSN: 00401625. DOI: 10.1016/j.techfore.2022.122248.

[4] 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.

[5] Syada Tasmia Alvi et al. “DVTChain: A Blockchain-based decentralized mechanism”. In: *Journal of King Saud University - Computer and Information Sciences* 34 (9 2022), pp. 6855–6871. ISSN: 22131248. DOI: 10.1016/j.jksuci.2022.06.014.

[6] Ahmed Ben Ayed. “A Conceptual Secure Blockchain-based Electronic Voting System”. In: *International Journal of Network Security & Its Applications (IJNSA)* 9 (3 May 2017), pp. 1–9. ISSN: 09752307.

[7] Fabrizio Baiardi et al. “SEAS, a secure e-voting protocol: Design and implementation”. In: *Computers & Security* 24 (8), pp. 642–652. ISSN: 01674048. DOI: 10.1016/j.cose.2005.07.008.

[8] Hong Bao and David Roubaud. “Non-Fungible Tokens: A Systematic Review and Research Agenda”. In: *Journal of Risk and Financial Management* 15 (5 May 8, 2022), pp. 1–9. ISSN: 1911-8074. DOI: 10.3390/jrfm15050215.

[9] Ahmad Baraani-Dastjerdi, Josef Pieprzyk, and Reihaneh Safavi-Naini. “A Practical Electronic Voting Protocol Using Threshold Schemes”. In: *Proceedings of the 11th Annual Computer Security Applications Conference*. New Orleans, Lousiana, USA: IEEE Computer Security Press, 1995.

[10] Silvia Bartolucci, Pauline Bernat, and Daniel Joseph. “SHARVOT: secret SHARe-based VOTing on the blockchain”. In: *WETSEB’18: IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*. 2018, pp. 1–5.

[11] Josh Benaloh and Dwight Tuinstra. “Receipt-Free Secret-Ballot Elections”. In: *26th Annual ACM Symposium on Theory of Computing*. Montreal, Canada, 1994, pp. 544–553.

[12] Josh Benaloh and Moti Young. “Distributing the Power of a Government to Enhance the Privacy of Voters”. In: *Proceedings of the 5th ACM Symposium on the Principles of Distributed Computing*. 1986, pp. 52–62.

[13] Nadja Braun Binder et al. “International Standards and ICT Projects in Public Administration: Introducing Electronic Voting in Norway, Estonia and Switzerland Compared”. In: *The Estonian Journal of Administrative Culture and Digital Governance* 19 (2 2019), pp. 8–22.

[14] Stefano Bistarelli et al. “An E-Voting System Based on Tornado Cash”. In: *Lecture Notes in Computer Science* 13782 (2022), pp. 120–135.

[15] Stefano Bistarelli et al. “An End-to-end Voting-system Based on Bitcoin”. In: *Proceedings of the 32nd ACM SIGAPP Symposium on Applied Computing*. 2017, pp. 1836–1841. ISBN: 9781450344869.

[16] Nur Sakinah Burhanuddin et al. “Blockchain in Voting System Application”. In: *International Journal of Engineering and Technology* 7 (4 2018), pp. 156–162. ISSN: 2227524X.

[17] Vitalik Buterin. *Minimal anti-collusion infrastructure*. URL: https://ethresear.ch/t/minimal-anti-collusion-infrastructure/5413 (visited on 01/05/2024).

[18] Marwa Chaieb et al. “Verify-Your-Vote: A Verifiable Blockchain-based Online Voting Protocol”. In: *Lecture Notes in Business Information Processing*. Limassol, Cyprus, 2018, pp. 16–30.

[19] David Chaum. “Blind Signatures for Untraceable Payments”. In: *Advances in Cryptology* (1983), pp. 199–205. ISSN: 00200255.

[20] David Chaum. “The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability”. In: *Journal of Cryptology* 1 (1 1988), pp. 65–75. ISSN: 09332790.

[21] David Chaum et al. “Secret Ballot Elections with Unconditional Integrity”. In: *Cryptology ePrint Archive* (270 2007), pp. 1–33. ISSN: 00029114.

[22] Chaum1981. “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”. In: *Communications of the ACM* 24 (1981), pp. 84–90. ISSN: 00010782.

[23] Lorrie Faith Cranor and Ron K. Cytron. “Sensus: A Security-Conscious Electronic Polling System for the Internet”. In: *Proceedings of the Thirtieth Hawaii International Conference on System Sciences* (1997), pp. 561–570.

[24] Jason Paul Cruz and Yuichi Kaji. “E-voting System Based on the Bitcoin Protocol and Blind Signatures”. In: *IPSJ Transactions on Mathematical Modeling and Its Applications* 2016-MPS-107 (7 2016).

[25] Gaby G. Dagher et al. “BroncoVote: Secure Voting System using Ethereum’s Blockchain”. In: *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. Funchal, Madeira, Portugal, 2018, pp. 96–107.

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

[27] Tassos Dimitriou. “Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting”. In: *Computer Networks* 174 (February 2020). ISSN: 13891286. DOI: 10.1016/j.comnet.2020.107234.

[28] Taher ElGamal. “A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms”. In: *Advances in Cryptology - Crypto ’84* (1984), pp. 10–18.

[29] Adam Kaleb Ernest. *Follow My Vote*. 2021. URL: https://followmyvote.com (visited on 2021-05-26).

[30] Jordi Barrat i Esteve, Ben Goldsmith, and John Turner. *International Experience with E-Voting: Norwegian E-Vote Project*. Assessment Report. Washington, U.S.A: The International Foundation for Electoral Systems, June 2012. 188 pp.

[31] Nazim Faour. "Transparent E-Voting dApp Based on Waves Blockchain and RIDE Language". In: *Proceedings of the XVI International Symposium on Problems of Redundancy in Information and Control Systems (Redundancy 2019)*. 2019, pp. 219–223. ISBN: 9781728119441. DOI: 10.1109/REDUNDANCY48165.2019.9003336.

[32] 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.

[33] Francesco Fusco et al. "Crypto-voting, a Blockchain based e-Voting System". In: *IC3K 2018 - Proceedings of the 10th International Joint Conference on Knowledge Discovery Knowledge Engineering and Knowledge Management*. Vol. 3. 2018, pp. 223–227. ISBN: 9789897583308.

[34] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. "The Knowledge Complexity of Interactive Proof Systems". In: *Society for Industrial and Applied Mathematics (SIAM) Journal on Computing* 18 (1 1989), pp. 186–208.

[35] Nicole J. Goodman. "Internet Voting in a Local Election in Canada". In: *The Internet and Democracy in Global Perspective: Studies in Public Choice*. Vol. 31. Springer, Cham, 2014. Chap. 1, pp. 7–24. ISBN: 978-3-319-04351-7.

[36] J. Alex Halderman and Vanessa Teague. "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election". In: *Lecture Notes in Computer Science* (9269 Mar. 2015), pp. 35–53. ISSN: 16113349.

[37] Gang Han et al. "Blockchain-Based Self-Tallying Voting System with Software Updates in Decentralized IoT". In: *IEEE Network*. Vol. 34. 2020, pp. 166–172. DOI: 10.1109/MNET.001.1900439.

[38] Ch Anwar ul Hassan et al. "A Liquid Democracy Enabled Blockchain-Based Electronic Voting System". In: *Scientific Programming* 2022 (2022). ISSN: 10589244. DOI: 10.1155/2022/1383007.

[39] Sven Heiberg, Arnis Parsovs, and Jan Willemson. "Log Analysis of Estonia Internet Voting 2013-2015". In: *Lecture Notes in Computer Science* (9269 2015), pp. 19–34. ISSN: 16113349.

[40] Friðrik þ. Hjálmarsson et al. "Blockchain-Based E-Voting System". In: *IEEE International Conference on Cloud Computing*. July 2018, pp. 983–986. ISBN: 9781538672358.

[41] E-Voting System using Hyperledger Sawtooth. "Vivek S. K. and Yashank R. S. and Yashas Prashanth and Yashas N." In: *Proceedings of the 2020 International Conference on Advances in Computing, Communication and Materials (ICACCM 2020)*. 2020, pp. 29–35. ISBN: 9781728197852. DOI: 10.1109/ICACCM50413.2020.9212945.

[42] Kenneth R. Iversen. "A Cryptographic Scheme for Computerized General Elections". In: *Advances in Cryptology* (LNCS 576 1992), pp. 405–419.

[43] Rui Joaquim, André Zúquete, and Paulo Ferreira. "REVS - A Rocust Electronic Voting System". In: *IADIS International Journal of www/Internet* 1 (i 2003), pp. 47–63.

[44] Wen-Shenq Juang and Chin-Laung Lei. "A Secure and Practical Electronic Voting Scheme for Real World Environments". In: *IEICE Transactions Fundamentals* (1997).

[45] Wen-Shenq Juang, Chin-Laung Lei, and Horng-Twu Liaw. "A Verifiable Multi-Authority Secret Election Allowing Abstention from Voting". In: *The Computer Journal* 45 (6 2002), pp. 672–682. ISSN: 00104620.

[46] Kashif Mehboob Kahn, Junaid Arshad, and Muhammad Mubashir Khan. "Secure Digital Voting System based on Blockchain Technology". In: *International Journal of Electronic Government Research* 14 (1 2018). ISSN: 1548-3886.

[47] Christian Killer et al. "Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System". In: *Proceedings of the 2020 IEEE Conference on Local Computer Networks (LNC)*. Vol. November. 2020, pp. 172–183. ISBN: 9781728171586. DOI: 10.1109/LCN48667.2020.9314815.

[48] Kevin Kirby, Anthony Masi, and Fernando Maymi. *Votebook, A proposal for a blockchain-based electronic voting system*. Tech. rep. New York University, Sept. 2016. 14 pp.

[49] Ali Kaan Koç et al. "Towards Secure E-Voting Using Ethereum Blockchain". In: *6th Symposium on Digital Foresinc and Security*. 2018, pp. 1–6. ISBN: 9781538634493.

[50] Wei-Chi Ku and Sheng-De Wang. "A secure and practical electric voting scheme". In: *Computer Communications* 22 (3 1999), pp. 279–286. ISSN: 01403664.

[51] Odysseas Lamtzidis. *The State of Private Voting in Ethereum*. 2023. URL: https://odyslam.com/blog/state-of-private-voting/ (visited on 01/05/2024).

[52] Byoungcheon Lee and Kwangjo Kim. "Receipt-free Electronic Voting through the Collaboration of Voter and Honest Verifier". In: *Proceedings of JW-ISC 2000*. Okinawa, Japan, 2000, pp. 1–8.

[53] Kibin Lee, Joshua I. James, and Tekachew Gobena Ejeta. "Electronic Voting Service Using Block-chain". In: *Journal of Digital Forensics, Security and Law* 11 (2 2017), pp. 123–136. ISSN: 15587223.

[54] Emmanouil Magkos, Mike Burmester, and Vassilis Chrissikopoulos. "Receipt-freeness in Large-Scale Elections without Untappable Channels". In: *IFIP Advances in Information and Communication Technology* 74 (2001), pp. 683–694. ISSN: 18684238.

[55] Aanchal Mani et al. "College Election System using Blockchain". In: *ITM Web of Conference* 44 (2022), pp. 1–5. DOI: 10.1051/itmconf/20224403005.

[56] Raphael Matile et al. "CaIV: Cast-as-Intended Verifiability in Blockchain-based Voting". In: *2019 IEEE International Conference on Blockchain and Cryptocurrency*. Seul, South Korea, 2019, pp. 24–28. ISBN: 9781728113289.

[57] Patrick McCorry, Siamak F. Shahandashti, and Feng Hao. "A Smart Contract for Boardroom Voting with Maximum Voter Privacy". In: *Lecture Notes in Computer Science*. Vol. 10322 LNCS. 2017, pp. 357–375.

[58] Johannes Mols and Emmanouil Vasilomanolakis. "ethVote: Towards secure voting with distributed ledgers". In: *International Conference on Cyber Security and Protection of Digital Services and Cyber Security 2020*. 2020, pp. 1–8. ISBN: 9781728164281.

[59] Tal Moran and Moni Naor. "Receipt-free Universally-Verifiable Voting with Everlasting Privacy". In: *Lecture Notes in Computer Science* 4117 LNCS (2006), pp. 373–392. ISSN: 16113349.

[60] Malik Hamza Murtaza, Zahoor Ahmed Alizai, and Zubair Iqbal. "Blockchain Based Anonymous Voting System Using zkSNARKs". In: *Proceeding of the 2019 International Conference on Applied and Engineering Mathematics*. 2019, pp. 209–2014. ISBN: 9781728123530.

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

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

[63] Valtteri Niemi and Ari Renvall. "Efficient voting with no selling of votes". In: *Theoretical omputer Science* 226 (1 1999), pp. 105–116. ISSN: 03043975.

[64] Hannu Nurmi, Arto Salomaa, and Lila Santean. "Secret Ballot Elections in Computer Networks". In: *Computer and Security* 10 (6 1991), pp. 553–560.

[65] Tasuaki Okamoto. "Receipt.Free Electronic Voting Schemes for Large Scale Elections". In: *Lecture Notes in Computer Science* 1361 (1998), pp. 25–35. ISSN: 16113349.

[66] Tatsuaki Okamoto. "An electronic voting scheme". In: *Advanced IT Tools* (1996), pp. 21–30.

[67] Choonsik Park, Kazutomo Itoh, and Kaoru Kurosawa. "Efficient Anonymous Channel and All/Nothing Election Scheme". In: *Lecture Notes in Computer Science* 765 LNCS (1994), pp. 248–259. ISSN: 16113349.

[68] Tiphaine Pinault and Pascal Courtade. “E-voting at Expatriates’ MPs elections in France”. In: *Electronic Voting* (Feb. 2012), pp. 289–195.

[69] pse.dev. *What is Semaphore*. URL: https://docs.semaphore.pse.dev/ (visited on 01/05/2024).

[70] 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.

[71] Aayush Sagar et al. “SoulBound E-Voting System”. In: *International Journal for Research in Applied Science and Engineering Technology* 11 (3 Mar. 31, 2023), pp. 1520–1525. DOI: 10.22214/ijraset.2023.48548.

[72] Safdar Hussain Shaheen, Muhammad Yousaf, and Mudassar Jalil. “Temper Proof Data Distribution for Universal Verifiability and Accuracy in Electoral Process Using Blockchain”. In: *13th International Conference on Emerging Technologies*. 2017.

[73] Adi Shamir. “How to Share a Secret”. In: *Communications of the ACM* 22 (11 1979), pp. 612–613.

[74] tivi.io. *TiVi*. 2021. URL: https://tivi.io/ (visited on 2021-05-26).

[75] Shantanu Vidwans et al. “Permissioned Blockchain Voting System using Hyperledger Fabric”. In: *Proceedings of the 2022 International Conference on IoT and Blockchain Technology, ICIBT 2022*. 2022, pp. 1–6. ISBN: 9781665424165. DOI: 10.1109/ICIBT52874.2022.9807702.

[76] Voatz. *Voatz - Secure, accessible voting at your fingertips*. 2021. URL: https://voatz.com/ (visited on 2021-05-28).

[77] Qin Wang et al. “Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges”. In: *arXiv* (Oct. 24, 2021). URL: http://arxiv.org/abs/2105.07447.

[78] Eric Glen Weyl, Puja Ohlhaver, and Vitalik Buterin. “Decentralized Society: Fiding Web3’s Soul”. In: *SSRN Electronic Journal* (2022). ISSN: 1556-5068. DOI: 10.2139/ssrn.4105763.

[79] Tifan Wu. “An E-Voting System Based on Blockchain and Ring Signature”. Master’s Thesis. University of Birmingham, 2017. 54 pp.

[80] Wenbin Zhang et al. “A Privacy-Preserving Voting Protocol on Blockchain”. In: *2018 IEEE 11th International Conference on Cloud Computing*. 2018, pp. 401–408. ISBN: 978-1-5386-7235-8.

[81] Zhichao Zhao and T-H. Hubert Chan. “How to Vote Privately using Bitcoin”. In: *Lecture Notes in Computer Science*. Vol. 9543. 2016, pp. 82–96.

[82] Yuanjian Zhou et al. “An improved FOO voting scheme using blockchain”. In: *International Journal of Information Security* 19 (3 2020), pp. 303–310. ISSN: 16155270. DOI: 10.1007/s10207-019-00457-8.