https://doi.org/10.2352/EI.2025.37.3.MOBMU-311

Digital Voting: Blockchain Enabled Democracy

Cristian Eremia[1], *Navaneeth Shivananjappa*[1], *Reiner Creutzburg*[1,2]

[1] *SRH University, School of Technology and Architecture, Sonnenallee 221, D-12509 Berlin, Germany*
[2] *Technische Hochschule Brandenburg, Department of Informatics and Media, Magdeburger Str. 50, D-14770 Brandenburg, Germany*
Email: cristian.eremia2000@gmail.com, navaneeth.shivananjappa999@gmail.de, reiner.creutzburg@srh.de, creutzburg@th-brandenburg.de

Keywords: Blockchain technology, Digital voting systems, Electoral security, Societal impacts, Regulatory compliance, Prototype development

Abstract

The main objective of this paper is to understand what and how deploying a digital voting system in a democratic country would look and what challenges a potential architect of such a system might confront. The study will also focus on using blockchain to solve specific barriers that might appear in the quest for a digitized voting system. By exploring the confluence of technology and democracy, this research underscores the importance of technological innovation in democratic participation and governance.

This paper will cover the fundamentals of blockchain, its integration within electronic voting systems, examination of its technical attributes, societal impacts, regulatory compliance, and a proposed blockchain-based e-voting system. Certain features of blockchain present a promising solution to longstanding challenges in electronic voting systems, such as ensuring security, integrity, compliance, and public trust.

The initial sections of the paper provide an in-depth analysis of blockchain's theoretical basis, emphasizing how its unique attributes can safeguard the electoral process against fraud and manipulation. Even more so, security techniques like cryptography and consensus mechanisms are also studied in this section. Following this inquiry, the study investigates the societal implications of deploying an e-voting system in a democracy, drawing insights from the experiences of various European countries. This exploration reveals the critical role of societal acceptance, efficient technical solutions, and legal frameworks in successfully implementing new voting methods.

Next, the design phase articulates a viable system architecture that balances several components: efficiency, control, security, and transparency. The suggested architecture considers critical factors such as voter anonymity, vote integrity, and the unique ability to modify votes within the voting period while aligning with democratic principles and regulatory standards.

In summary, this paper presents a complete analysis of digital voting, including technical and societal considerations, steps to deploy such a system in a democratic country, and, more importantly, blockchain technology's potential to revolutionize it further. Integrating theoretical knowledge, societal insights, and practical design considerations offers a blueprint or framework for future advancements in creating digital democracies.

Introduction

Safeguarding the authenticity, confidentiality, and availability of priceless information is crucial in the digital landscape. Despite the rapid technological advancements transforming virtually every facet of human life, voting systems have mainly remained archaic, fraught with challenges such as dishonesty, manipulation, fraud, and administrative errors [1]. These issues pose significant barriers to preserving traditional voting methods as nations navigate the transition toward digital economies. Furthermore, in an era marked by concerns about election integrity [4], disinformation [5], and cyber threats [6], a secure e-voting system holds significant promise. By providing a trustworthy and transparent electoral process using blockchain, this research is relevant to academics and cybersecurity experts and policymakers, electoral commissions, and the public.

Aside from the dire need for modernization, there is an alarming trend of low voter turnout in democratic elections [2]. This is caused by several variables, including logistical challenges, accessibility issues, and indifference stemming from mistrust over the integrity of the democratic process [3]. One feasible solution to these issues might be a secure and readily available electronic voting system. Due to its ability to remove geographical restrictions, shorten wait times, and simplify the voting process, digital voting has the potential to expand voter accessibility significantly.

A potential digital voting system can be upgraded by blockchain technology, which offers a transformative solution to specific challenges. By embracing blockchain's decentralized and immutable nature, a digital voting system can effectively mitigate the risks associated with traditional methods. Through cryptographic security and transparent, tamper-proof transactions, blockchain could ensure the integrity of the voting process. Moreover, blockchain technology's decentralization concept divides power among users, eliminating the need for a central authority. In addition to improving security, this decentralization fosters voter trust. Voters may independently confirm the integrity of the voting process and boost trust in the result by logging every transaction in a public ledger.

Because the world is changing so quickly, it is critical to investigate several options that might strengthen democracy's fundamental principles and core. Technologies like blockchain could aid in integrating a secure digital voting system in various nations

by comprehending specific technology and examining real-world use cases.

Methodology and Key Debates

Methodology

This paper adopts a holistic approach, beginning with a theoretical analysis of blockchain and other technological factors, emphasizing its capacity to transform digital transactions through decentralization, immutability, and transparency. This theoretical foundation aids in conceptualizing a framework for a blockchain-based voting system. The study further examines the societal impacts and regulatory challenges of e-voting systems, drawing insights from global examples to highlight technological, social, and legal intricacies in their implementation. The design phase proposes a system based on the Proof of Authority consensus mechanism, ensuring a secure, transparent voting process that aligns with varied electoral requirements.

Key Debates and Controversies

The paper discusses blockchain's scalability and energy efficiency, challenging the balance between privacy and transparency. Questions arise about maintaining election integrity within decentralized systems and the practicality of ensuring voter anonymity. Digital voting systems spur debates over regulation enforcement and the potential exclusion of technologically underserved populations. The paper stresses the need to maintain traditional voting methods alongside digital solutions to ensure inclusivity and neutrality in elections.

Technical Foundations - Blockchain, Security & Consensus

DLTs are digital systems for recording the transaction of assets in which the transactions and their details are recorded in multiple places simultaneously [8]. Unlike traditional databases, DLTs have no central data store or administration functionality. Inside it, the ledger is not maintained by any single entity. Instead, it is spread across multiple nodes (devices or data points connected to the network). Each node replicates, saves a copy of the ledger, and updates itself independently. Blockchain technology is at the heart of DLT's appeal for digital voting systems, characterized by its sequence of blocks linked through cryptographic hashes. Each block contains transaction data, a nonce, a unique hash, and the previous block's hash, ensuring the entire chain's integrity. This immutable chain of blocks is pivotal for recording and maintaining the authenticity and integrity of information. Because no central authority can validate transactions to provide data integrity and security, it is necessary to implement a feature known as a consensus mechanism. This mechanism is essential for maintaining the integrity of the blockchain, ensuring that every transaction, or in the case of e-voting, every vote is accurately recorded and universally agreed upon by all network participants. This works by having a set of protocols used in agreement by all the validation nodes. When a transaction is made, it has to be validated by network participants. If a majority or a specified threshold agrees, it is added to the ledger, which is then updated in all the nodes in the network [9]. There are a lot of possible consensus mechanisms like Proof of Work, Proof of Stake (PoS), Proof of Space, Proof of Burn, and others, but one that this paper will use as a solution will be Proof of Authority.

Cryptography is also crucial in securing blockchain technology and ensuring data integrity, secrecy, and privacy, especially in sensitive applications like electronic voting. Techniques such as hashing, digital signatures, and encryption safeguard data against unauthorized access while allowing for the public validation of transaction integrity. Hash functions like SHA-256 ensure immutability and security by producing a unique hash for each block, making any tampering evident. Digital signatures and encryption, using algorithms like RSA, ECDSA, and EdDSA, ensure the authenticity and confidentiality of transactions, providing a secure, anonymous, and tamper-proof recording of votes on the blockchain.

Societal & Regulatory Foundations - Compliance, Laws, Public Consensus & Practical Case Studies

This chapter explores integrating electronic voting systems or blockchain into society, focusing on their alignment with democratic principles, legal standards, and societal expectations. It scrutinizes the legal frameworks in countries like Germany, Romania, and Estonia, noting their efforts and challenges in adopting electronic voting or blockchain solutions.

Germany's Approach to Electronic Voting: Legal Framework and Challenges

Germany's legal framework, grounded in the Basic Law and Federal Election Act, emphasizes democratic election principles such as the secrecy and privacy of ballots. Its use case of discontinuing electronic voting machines is a good example of how people are very cautious regarding electronic voting. Germany used electronic voting machines from 1998 through 2005, and in 2009, they were dimmed as unconstitutional as they did not comply with the public nature of elections. One of the main arguments for this decision was that voters could only verify the vote count with special expert knowledge [10]. More so, concerns over transparency and public verification were highlighted. Based on this, it becomes apparent that whatever form of digital voting might be implemented, it needs to have transparent processes and records.

Romania's Exploration of Blockchain in Elections

In the 2020 parliamentary elections, Romania's Special Telecommunications Service (STS) implemented blockchain technology to ensure the electoral process's integrity, transparency, and traceability [11]. The solution prevented data alteration and was used to monitor electoral turnout and prevent illegal voting, with all information publicly available in real-time. This system included two key components: the SIMPV for monitoring voter presence and preventing illegal voting and the SICPV for managing voting records. The project was not created with the gold of voters casting their ballots in a digital form, but it was used to record statistical data through fingerprints.

Estonia: A Model for Digital Governance

Estonia is a beacon of digital innovation, with its extensive e-governance system enabling services like e-health, digital education, and online voting. The 'i-Voting system,' introduced in 2005, exemplifies Estonia's commitment to accessible, secure, and transparent digital democracy. Estonia's electronic has faced both appraisal and scrutiny over security concerns, highlighting

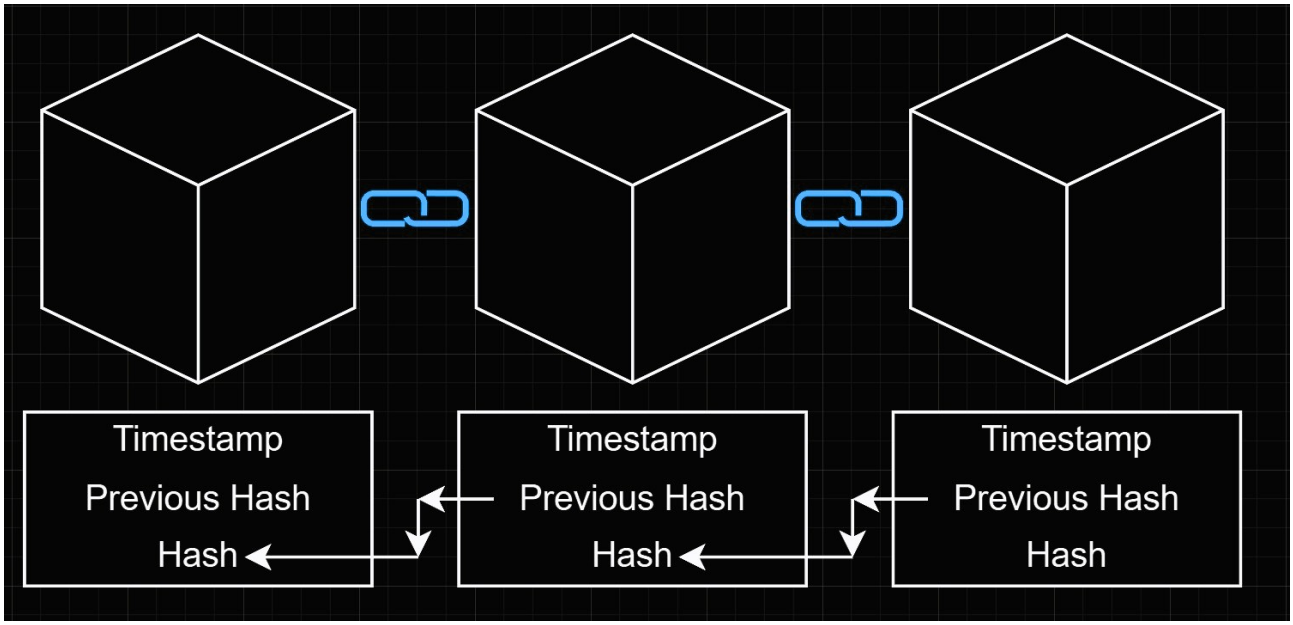


Figure 1. *A Simple Blockchain Diagram*

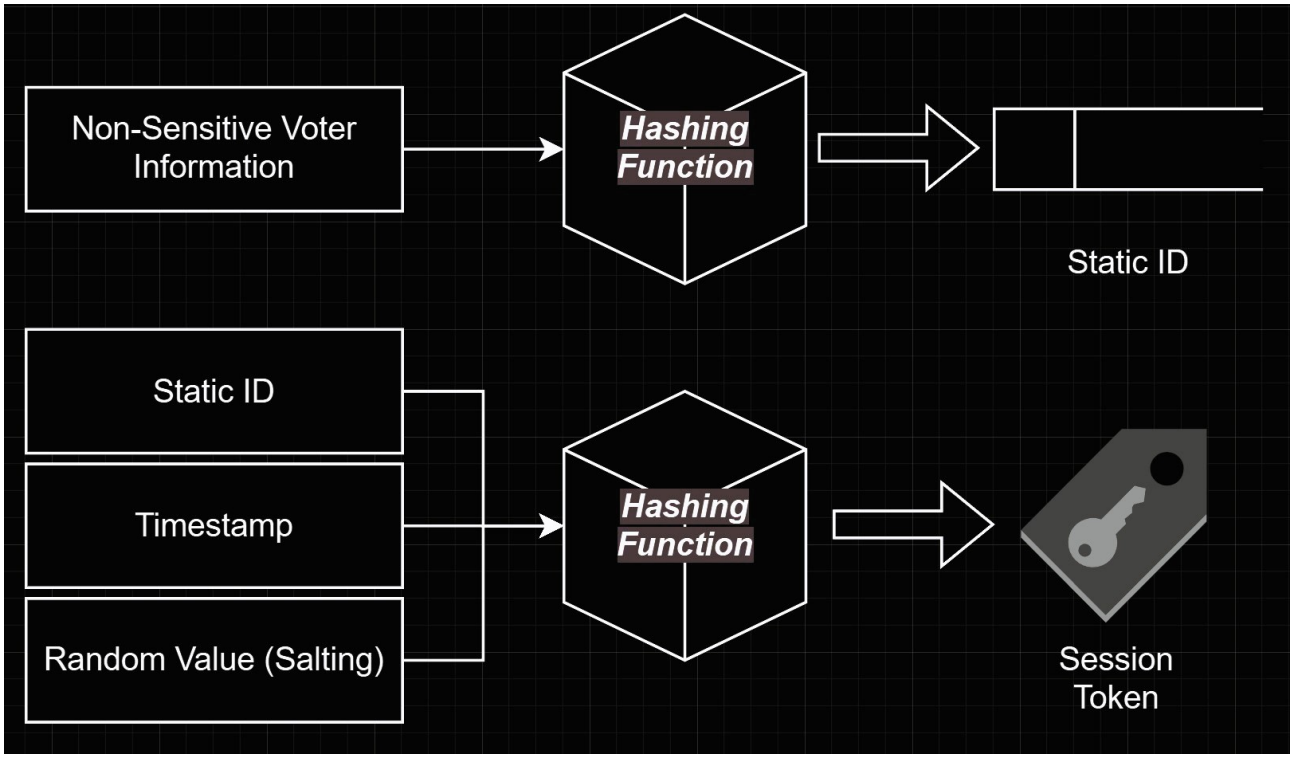


Figure 2. *Token & ID Creation*

the ongoing debate around the security and integrity of electronic ballots [12]. This case underscores the necessity of continuous technological and procedural refinement to address vulnerabilities and maintain public confidence in digital voting systems. Nonetheless, over the years, the electorate started to prefer using the e-voting system in Estonia instead of paper ballots. In 2023, the number of citizens who cast e-votes was higher than the number of paper votes for the first time in history. This transition shows the preference of people to use electronic systems but also the slow adoption of such technology.

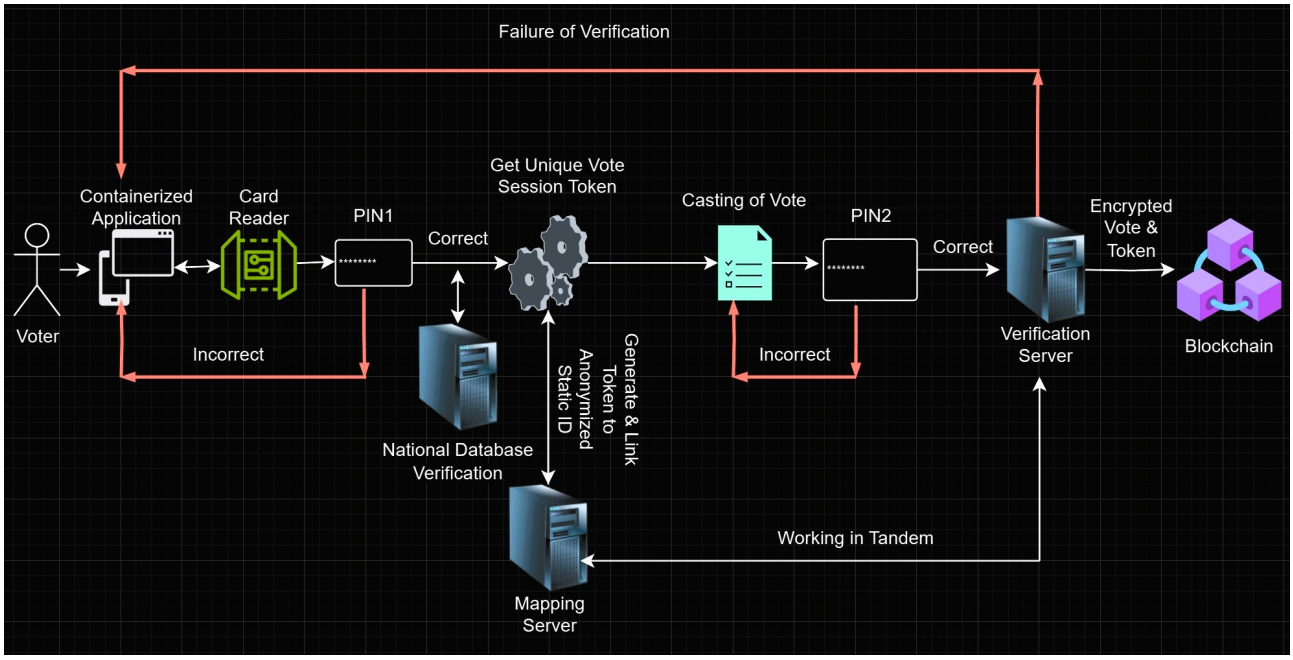


Figure 3. *Schema of the System Before Reaching the Blockchain*

Public Consensus, Educational Impact and Adoption

The adoption of e-voting systems is intricately linked to public consensus and education. Building public trust in new technologies requires clear communication, transparency, and educational initiatives that demystify the technology and emphasize its benefits for the democratic process. Germany, Romania, and Estonia's experiences illustrate the varied paths toward digital voting adoption, each shaped by legal constraints, technological challenges, and societal attitudes toward digital innovation.

In conclusion, exploring societal and regulatory foundations reveals the complex landscape of digital voting system integration. Legal frameworks, public consensus, and technological innovation intersect to shape the possibilities and limitations of e-voting. As countries navigate these challenges, the experiences of Germany, Romania, and Estonia offer valuable lessons on balancing technological advancements with the imperatives of democratic integrity, security, and public trust.

Designing a Blockchain-Based E-Voting System

This chapter transitions from theoretical discussions and case studies to the design of a practical framework for a blockchain-based digital voting system, focusing on European compliance standards. This system incorporates critical principles for democratic voting processes, including voter privacy, system security, legal compliance, transparency, accessibility, scalability, and resilience against technical failures and cyber threats.

Designing the System

While designing the system, certain core factors must be considered. These are ensuring the anonymity of voters while allowing for vote verification, implementing robust security measures to protect against tampering and unauthorized access, adhering to national and international regulations concerning elections and data protection, allowing for transparent processes while ensuring that individual votes remain private and untraceable to voters, ensuring that the system is easily accessible and understandable to all eligible voters, regardless of their technical expertise, designing the system to handle a large number of votes efficiently without compromising security or privacy and incorporating measures to withstand technical glitches and cyber threats.

Voter Registration, Verification, and Casting: Digital IDs and Anonymity

Digital IDs will be the primary method through which each citizen can register for the e-voting system. A digital ID usually involves a unique identifier, including attributes like name, date of birth, biometric data, and other personal information inside a chip. The government or trusted agencies issue them. Because the digital ID validates the citizen, it is the perfect trusted object for building the system.

After a citizen gets his national ID card and activates it using two PINs, he can register in the e-voting platform. After getting his card, the person will be able to scan his card using either Near Field Communication (NFC) or a card reader connected to the device. After that, once the card is scanned, the system reads the encrypted digital certificate in the card's chip, including the voter's unique identification data. The voter is then prompted to enter PIN1, which is used for authentication. This control ensures that the person who scanned said card is the owner. Once that happens, the system verifies their identity against a national database. This database will contain the digital records of all registered voters. The verification process checks the digital certificate from the ID card against the voter's details in the database, ensuring the person is eligible to vote in that specific election or referendum. After that, the citizen can vote using PIN2, and the vote is encrypted and sent. The registration and verification process is

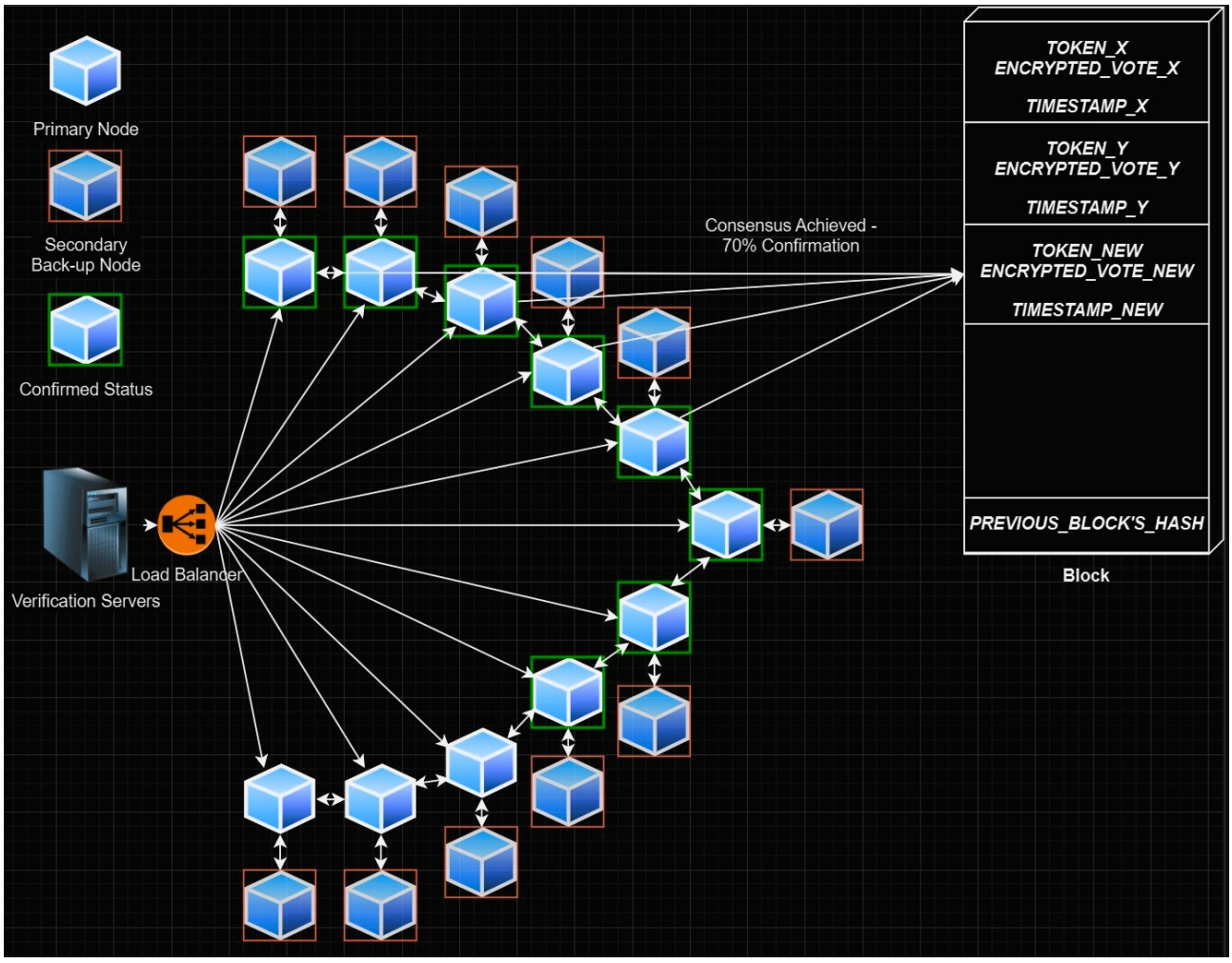


Figure 4. *Schema of an Achieved Consensus*

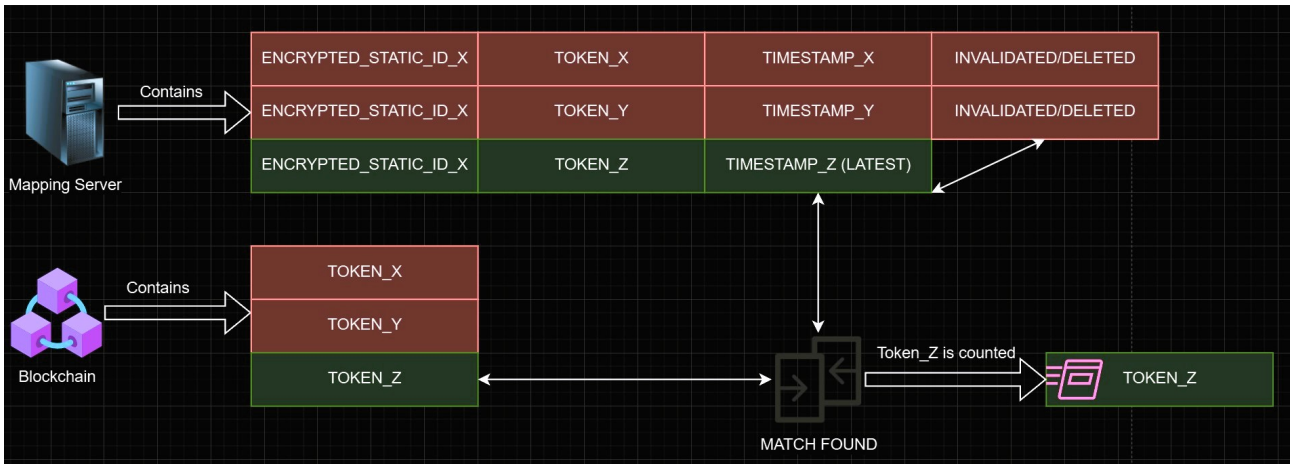


Figure 5. *Schema Illustrating the Tallying*

secured based on MFA requirements, as one will need a first factor: the card itself, respectively "Something You Have," and two PINs, "Something You Know."

When a successful registration and verification occurs, a unique token for the voter must be created, acting as a one-time identifier for the voting session. This token will be generated using a cryptographic algorithm, such as a hash function like SHA-256, which combines inputs, including the voter's dynamically

created static ID, a timestamp, and a random value (known as salting [7]), into a fixed-size string of characters. Hashing ensures the token is non-reversible, meaning it's computationally infeasible and practically impossible to trace back to the voter's identity. Simultaneously, a dynamic creation of the static ID occurs in the server. This static ID is generated based on consistent, non-identifying inputs unique to the voter, ensuring it remains the same across different voting sessions. Once generated, the static ID must be securely stored within the server's encrypted database and used internally to link to the tokens. However, only the token, not the static ID, must be returned to the application. After that, the user can cast their vote, which will be encrypted and sent, along with the voting session token, to the verification server/s. The verification server/s, adept at handling these tokens, verifies their authenticity and validity, acting as a first line of defense against potential fraudulent activities or errors. This verification checks that the token matches the expected format, is not a duplicate, and falls within the designated voting period. Notably, the system does not store any direct mapping between the token and the voter's identity on the blockchain, maintaining strict adherence to the principles of privacy and anonymity. Instead, it upholds a separate, secure, and encrypted mapping system. This system links each voter's anonymized static ID, which also cannot be directly linked to a person's identity, to the latest valid token associated with it, ensuring that the integrity of the voting process is maintained. Each voter's final choice is accurately reflected in the election results while preserving the confidentiality of voter identities and making the changing of votes possible.

The mapping and verification servers work together to manage the voting process in the theoretical e-voting system. The verification server ensures that each vote entering the system is authentic and valid. At the same time, the mapping server manages the ongoing relationship between voters and their votes, maintaining each voter's integrity and anonymity throughout the voting period.

The system's design will also allow voting changes within an amount of time. If voters decide to change their vote within the permissible period, they must re-authenticate, generating a new token. This new token is utilized for the subsequent vote. When a vote change occurs, the new token and vote are added as a new transaction on the blockchain. Simultaneously, the system invalidates the previous token in its secure record. This mechanism ensures that only the vote linked to the latest valid token is considered during vote tallying without altering the previous blockchain transaction. This method sustains the integrity and confidentiality of the voting process, accommodating vote changes while securing every vote transaction.

The Design of The Blockchain: Transparency, Security and Immutability

Once verified, votes are sent to the blockchain network without identifiable information, maintaining voter anonymity. The blockchain network, composed of several servers operated by diverse entities (preferably under different political parties, NGOs, and other such entities), validates transactions based on a consensus mechanism. This mechanism ensures the integrity and security of the voting process, with decentralization acting as a fundamental defense against manipulation. The choice of consensus mechanisms, such as Proof of Authority (PoA), balances efficiency, security, and compliance requirements.

Tallying of the Votes - The End of the Voting Period

At the voting period's end, the Mapping Server orchestrates the final vote counting, prioritizing the most recent votes for each voter. Because the system supports multi-voting, it must first identify the latest valid vote per encrypted static ID. Only the last one (filtered by time) will be considered in the final tally, such that the system prevents double voting and maintains integrity while checking both the blockchain and the Mapping Server while invalidating old votes. This phase includes secure decryption and tallying of votes, emphasizing accuracy and impartiality in election results.

In summary, the proposed blockchain-based digital voting system framework addresses the multifaceted requirements of modern democratic elections. By integrating advanced technological solutions with stringent security and privacy measures, the system aims to enhance the integrity, transparency, and accessibility of the voting process, paving the way for greater public trust and participation in democratic governance.

Conclusion

This research aimed to dissect and illuminate the transformative potential of e-voting systems and blockchain technology in democratic countries. The founding ideas of blockchain technology—decentralization, transparency, and security—were discovered to be consistent with voting fundamental values, making it highly suitable for such a system.

While analyzing examples of other nations' experiences with e-voting systems and blockchain-integrated voting processes, opportunities and challenges were observed; in the short term, numerous problems were noted, ranging from technological and possible system vulnerabilities to the population's delayed acceptance of new technology and constitutional problems. Nonetheless, additional opportunities for democracies to evolve were found in the long term. People appeared more willing to vote digitally while technology and security practices improved. The clearest example of this was seen in Estonia, where, despite sluggish acceptance of the e-voting system, more than half of the electorate now utilizes it to vote.

Even in successful cases like Estonia, close vulnerability management and constant monitoring of processes must be implemented. In critical processes like voting, where there is no room for error, protocols, practices, and technology must be implemented cautiously and with a security focus. Even if blockchain-based digital voting is very promising because of its basic principles, every system must be fixed. Still, it can always be improved and made more secure, always staying one step ahead of potential threats.

Acknowledgments

The European Union partially supported this work through ERASMUS MUNDUS, Project CyberMACS (Project No. 101082683) (https://cybermacs.eu).

References

[1] Dawson, S. (2020). " Electoral fraud and the paradox of political competition", in Journal of Elections, Public Opin-

ion and Parties, Volume 32(4), pp. 793-812. https://doi.org/10.1080/17457289.2020.1740716.

[2] Lijphart, A. (1998). "The problem of low and unequal voter turnout - and what we can do about it", in Institut für Höhere Studien. Vol. 54. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-246720.

[3] Blais, A. (2005) "WHAT AFFECTS VOTER TURNOUT?", in Annual Review of Political Science, Vol. 9, pp. 111-125. https://doi.org/10.1146/annurev.polisci.9.070204.105121.

[4] Vail, K.E., Harvell-Bowman, L., Lockett, M. (2023) "Motivated reasoning: Election integrity beliefs, outcome acceptance, and polarization before, during, and after the 2020 U.S. Presidential Election", in Motiv Emot, Vol. 47, pp. 177–192. https://doi.org/10.1007/s11031-022-09983-w.

[5] Pavlíková, M., Šenkýřová, B., Drmola, J. (2021). "Propaganda and Disinformation Go Online", in Challenging Online Propaganda and Disinformation in the 21st Century. Political Campaigning and Communication, pp. 43-47. https://doi.org/10.1007/978-3-030-58624-9_2.

[6] Kamat, P., Gautam, A.S. (2018). "Recent Trends in the Era of Cybercrime and the Measures to Control Them", in Handbook of e-Business Security. https://www.taylorfrancis.com/chapters/edit/10.1201/9780429468254-11/electronic-wastage-prospects-challenges-next-generation-sudan-jha-le-hoang-son-raghvendra-kumar-manju-khari-jyotirmoy-chatterjee?context=ubx.

[7] P. Gauravaram. (2012). "Security Analysis of salt——password Hashes" in International Conference on Advanced Computer Science Applications and Technologies (ACSAT), pp. 25-30. https://doi.org/10.1109/ACSAT.2012.49.

[8] Antal, C., Cioara, T., Anghel, I., Antal, M., Salomie, I. (2021). "Distributed Ledger Technology Review and Decentralized Applications Development Guidelines" in Future Internet, Vol. 13(3), p. 62. https://doi.org/10.3390/fi13030062.

[9] Bhardwaj, R., Datta, D. (2020). "Consensus Algorithm", in Decentralised Internet of Things. Studies in Big Data, Vol. 71, pp. 91-107. https://doi.org/10.1007/978-3-030-38677-1_5.

[10] Seedorf, S. (2016). "Germany: The Public Nature of Elections and its Consequences for E-Voting" in E-Voting Case Law, pp. 23-44. https://books.google.de/books?hl=en&lr=&id=MLC1CwAAQBAJ&oi=fnd&pg=PA23&dq=Bundeswahlgesetz+(Federal+Election+Act)&ots=svQkXYZZtL&sig=SnNbnG4jtUbPIZAQ2sM1BdNzbs8&redir_esc=y#v=onepage&q=Bundeswahlgesetz%20(Federal%20Election%20Act)&f=false.

[11] Pascu, E. "STS a implementat tehnologia BLOCKCHAIN care garantează integritatea sistemelor informatice pentru alegerile parlamentare" DefenseRomania, 27 Aug. 2020. https://m.defenseromania.ro/sts-a-implementat-tehnologia-blockchain-care-garanteaza-intergitatea-sistemelor-informatice-pentru-alegerile-parlamentare_606603.html.

[12] Springall D., Finkenauer, T., Durumeric Z. (2014) "Security Analysis of the Estonian Internet Voting System", in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 703-715. https://doi.org/10.1145/2660267.2660315.

Author Biography

Cristian Eremia is an Information Security Engineer with hands-on experience in SOC operations, Penetration Testing, Threat Analysis and Compliance. He holds a Master of Science degree from SRH Berlin University of Applied Sciences, Berlin School of Technology and is passionate about exploring new and innovative solutions to address real-world challenges.

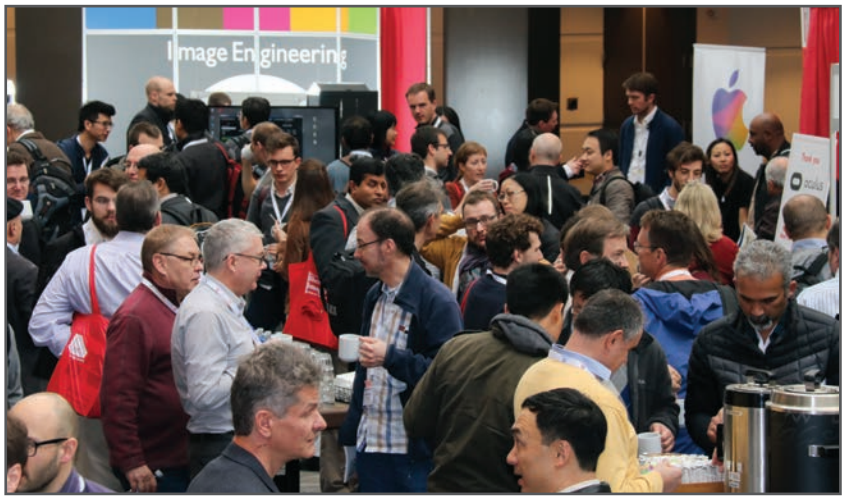
Navaneeth Shivananjappa is a Lecturer at SRH University of Applied Sciences, Berlin School of Technology and Architecture, specializing in the field of Web Application Pentesting and Cyber Security. His research interests include Cybersecurity, Cybersecurity tools, Penetration Testing, Web Application Security, Kubernetes Security, Cloud Security, and Cybersecurity Awareness.

Reiner Creutzburg is a Retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019, he has been a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Device (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interests include Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory architecture, and Modern Digital Media and Imaging Applications.

JOIN US AT THE NEXT EI!

electronic IMAGING

Imaging across applications . . . Where industry and academia meet!



• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org

ADVANCING IMAGING SCIENCE 75 1947 IS&T 2022 imaging.org