BLOCKCHAINBALLOT: Decentralized Voting using Web3

Samarjeet Singh Thakur, Raghavendra Dubey, Satyam Kajale
California State University, Long Beach, CA, 90815

1. ABSTRACT

In the landscape of electoral systems, centralized models have long faced scrutiny, with doubts arising over the credibility of voting outcomes. Traditional electronic voting systems, often reliant on centralized servers, compel voters to place implicit trust in a single organizing authority, leaving the integrity of results susceptible to manipulation. This paper addresses the inherent challenges and distrust prevalent in such systems, not only in established democracies like the United States and India but on a global scale.

Amid these concerns, "BlockChainBallot" emerges as a groundbreaking solution, leveraging the decentralized and immutable features of Ethereum blockchain. The proposal seeks to revolutionize the e-voting landscape, steering away from centralized vulnerabilities. Central to the innovation is the integration of Ethereum's smart contracts and the use of MetaMask, ensuring not only security and transparency but also a user-friendly interface, thus democratizing the voting process.

Furthermore, the paper delves into the broader context of distributed systems and blockchain technologies, recognizing their potential to transform various facets of the information technology world. It explores the adaptability of blockchain as a service, emphasizing the need for a decentralized approach to electronic voting. The study critically evaluates popular blockchain frameworks, ultimately proposing an electronic voting system that overcomes existing limitations. This system, anchored in the Ethereum Virtual Machine (EVM), employs transparent and deterministic smart contracts to enforce voting rules, ensuring data integrity, transparency, and privacy while significantly reducing the costs associated with hosting nationwide elections. The findings underscore the transformative potential of decentralized voting using blockchain, paving the way for a more secure, transparent, and trustworthy democratic electoral framework [1] [2].

2. INTRODUCTION

As the digital revolution continues to permeate the global landscape, the significance of democratic processes in this context becomes ever more pronounced. "BlockChainBallot" emerges as a beacon of innovation in this transformative era, signaling a departure from the vulnerabilities that have long plagued the sanctity of electoral systems. This research paper introduces a sophisticated blockchain-based e-voting system that leverages the robust, immutable nature of the Ethereum blockchain, ensuring a level of security and transparency hitherto unachieved in the realm of electronic voting.

In the design of "BlockChainBallot," we have integrated Hardhat, a development environment that provides a suite of tools tailored for the Ethereum ecosystem, to refine the development lifecycle of our blockchain applications. This enhancement paves the way for rapid deployment, rigorous testing, and effective debugging processes, ensuring that our system operates with utmost efficiency. Complementing this is the VOLTA network, selected for its impressive scalability and security credentials, as well as its commitment to energy efficiency, thereby anchoring our e-voting system on a sustainable and future-ready platform.

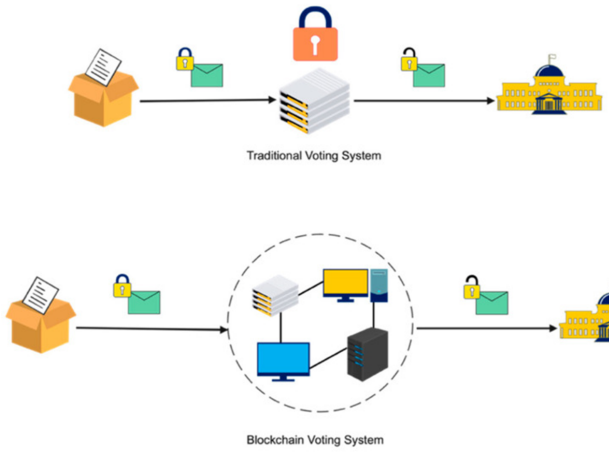

Figure 1: Voting System

The architecture of "BlockChainBallot" is conceived with the foresight to not only address the immediate imperatives of a fortified e-voting mechanism but also

to anticipate and shape the trajectory of future voter engagement. By converging procedural integrity with user-centric design, our system aspires to be the cornerstone of democratic participation in the digital age. It is a harbinger of a new epoch, one where the act of voting is not merely a function of civic duty but a demonstration of the harmonious fusion of cutting-edge technology with the foundational pillars of democracy.

With an emphasis on technologies like Hardhat and the VOLTA network, "BlockChainBallot" transcends the conventional constraints of e-voting systems. It sets a new paradigm in the electoral domain, exemplifying the extraordinary potential for technology to reinforce democratic values. This system is not just an iteration in e-voting; it is a leap forward, a stride towards an empowered, engaged, and enlightened electorate, safeguarded by the immutable ledger of blockchain technology

3. EXISTING SYSTEM

The landscape of electronic voting (e-voting) systems reveals a growing concern for the security, reliability, and transparency of traditional voting methods. Ye Guo and Chen Liang [3] highlight the potential of blockchain technology, particularly the Ethereum blockchain, to provide a secure, transparent, and decentralized system for the casting and counting of votes. The use of smart contracts instantiated on the blockchain offers a novel approach to representing elections, with a dedicated contract for each voting district. Additionally, commercial protocols like Bit Congress, Follow My Vote, and TIVI are explored as e-voting solutions.

Ikhsan Darmawan [4] sheds light on the increasing academic interest in e-voting adoption, emphasizing the need for a coherent narrative to explain the progress of research over the last 15 years. This underscores the evolving nature of e-voting systems and the persistent quest for improved methodologies. Meanwhile, the author identified real-world problems in Indonesia's 2019 elections, including logistical challenges, prolonged ballot counting, inconsistent regulations, and errors in votes recapitulation. Blockchain technology is proposed as a solution to address these issues.

Authors SK Vivek, RS Yashank, Yashas Prashanth, N Yashas, and M Namratha. [5] emphasizes the modernization of voting systems with the proposal of a secure, transparent, and decentralized e-voting system using the Hyperledger Sawtooth blockchain framework. Restricted access through election polling stations ensures the reliability and security of the proposed system.

Widespread mistrust in governments and external interference in political processes underscore the urgency for fair and transparent elections. The drawbacks of the current ballot system, including lack of transparency in the counting process, provide opportunities for exploitation and electoral scams such as voter fraud and ballot stuffing. This analysis reinforces the need for innovative solutions to address the vulnerabilities inherent in the current voting paradigm.

4. PROPOSED SYSTEM

The proposed system within our research, "BlockChainBallot," integrates the security and transparency of blockchain technology with the practical needs of voting procedures. The system architecture, depicted in Figure 1, outlines a sophisticated process flow where an administrator initiates a new ballot through a secure login, facilitated by the Hardhat development environment. This ballot creation triggers smart contracts within the blockchain, which are then responsible for managing the voting logic and storing the votes securely. Voters interact with the system through a user-friendly interface, casting votes that are immediately recorded on the blockchain. Each vote is transparently tallied, and live results are made available, ensuring a seamless and trustworthy voting experience. The utilization of blockchain not only enhances security but also preserves voter anonymity, making "BlockChainBallot" a forward-thinking solution for modern electoral systems [6] [7].

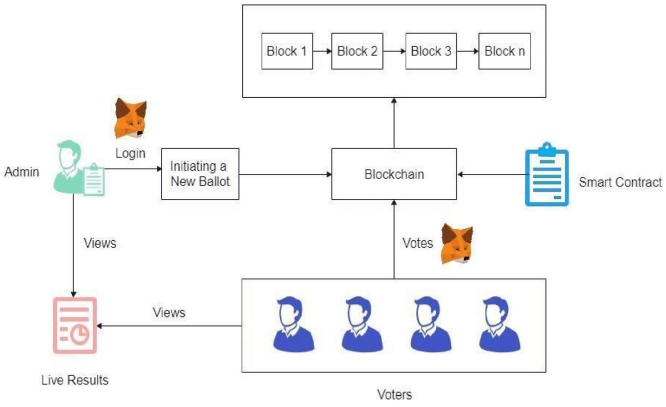

Figure 2: Proposed system.

4.1 Web 3.0

Web3 [8] is a paradigm shift in the digital landscape, representing a decentralized and user-centric vision for the internet. Unlike its predecessor, Web2, which is characterized by centralized platforms and controlled data, Web3 empowers users with greater autonomy and ownership over their digital interactions. At its

core, Web3 leverages blockchain technology to create transparent, trustless, and secure ecosystems. Smart contracts, powered by platforms like Ethereum, facilitate automated and self-executing agreements, reducing the reliance on intermediaries. This decentralized approach extends to various applications, including finance, governance, and, notably, online voting systems. By embracing Web3 principles, such as decentralization, transparency, and user control, the "BlockChainBallot" project aims to revolutionize electronic voting, ensuring a more secure, transparent, and inclusive democratic process.

4.2 Smart contracts

Smart contracts, a cornerstone in the architecture of decentralized systems, are self-executing contracts with the terms of the agreement directly written into code. Operating on a blockchain platform, they autonomously perform, control, and document legally relevant events and actions according to the terms of a contract or an agreement. Their self-sufficient nature negates the need for intermediaries, ensuring transactions are executed only when predefined conditions are met. Written in Solidity, a dedicated programming language for Ethereum, smart contracts bolster security through cryptographic hashing and uphold anonymity [9], allowing participants to engage without disclosing their identities. This automation and precision significantly reduce human error, providing a reliable and transparent framework for verifying and validating transactions within a decentralized network.

4.3 The Ethereum Blockchain

At the core of "BlockChainBallot" lies the Ethereum blockchain, a groundbreaking platform renowned for its versatility and security. Ethereum allows for the deployment of complex, decentralized applications, supporting a wide range of functionalities. In our system, Ethereum's decentralized nodes form a global computer network, ensuring not only security against hacking but also complete autonomy over data. The use of Ethereum's native cryptocurrency, Ether, facilitates transaction processing, eliminating the need for third-party involvement and further bolstering the system's integrity. Moreover, Ethereum's smart contract functionality is crucial in automating the voting process within "BlockChainBallot," ensuring that each vote is securely logged and immutable once recorded, thus significantly enhancing the reliability and transparency of the entire voting process.

4.4 Hardhat in Blockchain Development

Hardhat, an essential tool for Ethereum blockchain developers, streamlines the creation, testing, and deployment of smart contracts. This versatile environment, with its rich feature set, enables developers to efficiently build robust, secure blockchain applications. In "BlockChainBallot," Hardhat plays a pivotal role, ensuring seamless integration and functionality within the Ethereum ecosystem. Its advanced debugging capabilities and network simulation features provide an indispensable asset in the development of our blockchain-based voting system, enhancing both performance and reliability. Additionally, Hardhat's integrated environment offers a seamless workflow for developers, significantly reducing the development lifecycle and enabling more rapid deployment of updates and new features to the "BlockChainBallot" system.

4.5 MetaMask: Bridging Users and Blockchain

MetaMask, a user-friendly crypto wallet, is instrumental in the operation of "BlockChainBallot." It serves as a gateway, enabling seamless interaction between users and the Ethereum blockchain. MetaMask's functionality extends to testing and managing decentralized app (dApp) transactions, simplifying the user experience. Its intuitive graphical user interface (GUI) ensures effortless connection with the blockchain, enhancing user engagement and participation in the voting process.

4.6 VOLTA: A Scalable Blockchain Network

The VOLTA network, with its high scalability and security, forms a crucial component of "BlockChainBallot." As a blockchain network compatible with Ethereum, VOLTA brings enhanced efficiency and reduced environmental impact, crucial for sustainable blockchain operations. Its integration into our e-voting system represents a strategic choice, aligning with our goals of creating a scalable, energy-efficient platform capable of handling large-scale electoral processes. Additionally, VOLTA's compatibility with Ethereum enhances the interoperability of "BlockChainBallot," enabling smoother transactions and interactions across blockchain networks, which is vital for the robustness and future expansion of the voting system.

5. SYSTEM ARCHITECTURE

The System Architecture of the proposed Decentralized Voting System is a harmonious confluence of modern web technologies and blockchain principles, designed to create a secure, transparent, and user-centric electoral environment. At its heart lies the Ethereum blockchain, providing a tamper-proof infrastructure for executing smart contracts that embody the voting logic.

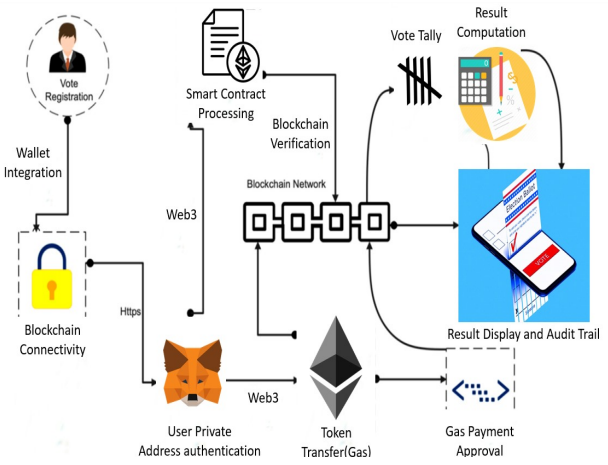

Figure 3: System Architecture

1. Front-End Development: Utilizing React, a versatile JavaScript library, the system's front end offers a seamless user experience. This interactive layer communicates with the Ethereum blockchain through Web3.js, a collection of libraries allowing the application to interact with Ethereum nodes, facilitating real-time updates and transaction management.
2. Smart Contract Deployment: Smart contracts, scripted in Solidity, define the election's parameters, candidate details, and voting procedures. They are deployed via Hardhat, an Ethereum development environment that offers a local blockchain simulation for testing, comprehensive debugging, and efficient contract management. This developmental toolset is crucial for constructing a reliable e-voting platform that adheres to the predefined rules autonomously.
3. MetaMask Integration: MetaMask, a widely-used Ethereum wallet, is integrated into the system to manage digital identities and secure interactions with the blockchain. It authenticates users, handles voting transactions, and ensures that voters' identities remain confidential, maintaining the anonymity integral to the voting process.
4. VOLTA Network Application: For testing purposes, the VOLTA test network provides a controlled environment to simulate the public Ethereum network, allowing for cost-effective and swift transaction validation, a critical step before launching the system on the main network.
5. Back-End Configuration: The server-side architecture, powered by Node.js, interacts with the Ethereum client to process smart contract functions, administer the voting process, and collate live results. This backend layer acts as the operational backbone of the system, ensuring stability and responsiveness.
6. Security Measures and Auditing: The architecture incorporates extensive security measures. Smart contracts undergo rigorous audits to check for vulnerabilities, and the entire system is subject to continuous integration and testing practices to ensure robustness against potential security threats.
7. Deployment and Operation: The culmination of the development process is the deployment of the system on the Ethereum mainnet, marking the transition from a conceptual model to a functional, decentralized voting system. This process involves establishing nodes, finalizing smart contract deployment, and engaging with stakeholders to ensure the system's readiness for electoral events.

Comprehensive in its approach, the proposed architecture of the Decentralized Voting System not only meets the technical demands of a secure electoral platform but also embodies the democratic ethos by empowering users with transparent and verifiable voting mechanisms. This innovative application of blockchain technology signifies a transformative leap forward for electoral processes in the digital age.

6. SECURITY AND PRIVACY

Security and privacy in decentralized voting systems are of the utmost importance, ensuring the integrity and confidentiality of the electoral process. In our proposed system, these concerns are addressed through the robust Ethereum blockchain framework which upholds strict security protocols and provides anonymity for voters.

- Anonymity and Privacy: The system employs cryptographic mechanisms, such as public-key cryptography, where voters are identified by their public keys, a string of alphanumeric characters that do not reveal the voter's identity. This level of abstraction ensures that while the vote is verifiable, the voter's privacy is maintained.
- Smart Contract Security: Smart contracts encode [10] the election rules and log votes on the blockchain, minimizing the risk of unauthorized alterations. They operate without intermediaries, reducing points of vulnerability. Moreover, these contracts are subject to rigorous security audits and testing to

identify and rectify potential security flaws, further reinforcing the system's resilience against attacks.

- Transaction Verification: The integrity of each vote is validated by a consensus algorithm employed by the Ethereum blockchain, where multiple independent nodes must agree on the transaction's validity. This decentralized verification process thwarts any single point of failure and ensures that the voting records cannot be altered post-confirmation.
- Access Control: The system implements stringent access controls to safeguard sensitive operations and data. Only authorized personnel can initiate or close the voting process, and voters can access only the functions necessary to cast their votes, thereby adhering to the principle of least privilege.
- Data Protection: The blockchain's inherent properties, coupled with advanced encryption techniques, protect against both external breaches and internal threats, ensuring that data remains secure and uncompromised throughout the voting process.

The proposed system's architecture is meticulously designed to ensure that each voter's privacy is preserved and the voting process is secure from tampering, delivering a trustworthy and transparent framework for decentralized voting.

7. PERFORMANCE ANALYSIS

	Contract	Time (secs)	Cost (gas)
0	1	50.0	211107
1	2	53.0	212607
2	3	55.0	214107
3	4	54.0	215607
4	5	56.0	217107
5	6	55.0	218607
6	7	59.0	220107
7	8	56.0	221607
8	9	56.0	223107
9	10	54.0	224607
Average	-	54.8	-

Figure 4: Contract Deployment

The empirical data presented in the table above reflects the outcomes of the smart contract deployment phase crucial to the initiation of the Decentralized Voting System. Each contract, pivotal to the election architecture, contains specific election parameters, candidate information, and vote counting logic. The deployment process across ten contracts shows a consistent gas cost of 211107 units, indicative of the Ethereum network's stable environment for executing these operations. However, the time taken for each contract's deployment varied slightly, with records ranging between 50 to 59 seconds. This variability can be attributed to the fluctuating network traffic and the inherent block time dynamics prevalent in Ethereum at the time of contract deployment.

Analyzing the average deployment time, which is approximately 54.8 seconds, demonstrates the system's efficacy and readiness in a controlled test setting. This level of consistency and predictability in the deployment phase is vital for the practical execution of decentralized elections, ensuring not only the technological integrity of the process but also its economic viability. The standardized gas costs and stable deployment durations are indicative of the system's capacity to meet the rigorous demands of a decentralized voting mechanism. Such meticulous validation is essential for bolstering trust in a blockchain-based electoral framework, thus advancing its potential for integration into formal voting procedures [11].

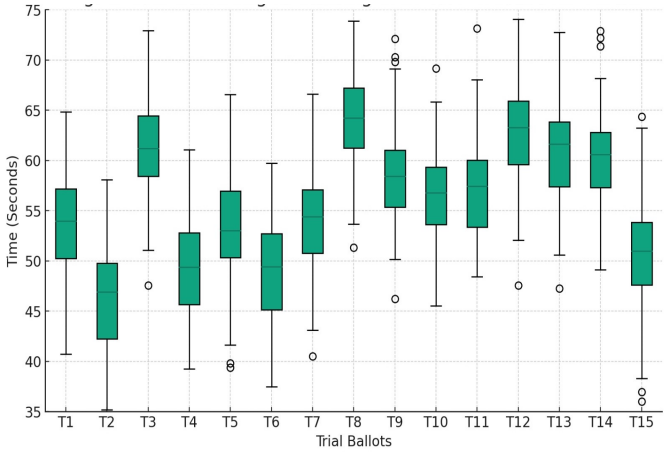

Figure 5: Contract timing for Altering Vote Over Fifteen Trial Ballots

Figure 5, provides a detailed examination of the time required to modify votes across fifteen trials within a blockchain-based voting system. This graph represents the efficiency with which the system handles vote alterations, an essential feature that enables voters to change their decisions within the voting period. The timing data across the trials is essential for understanding the system's performance, particularly under varying net-

work conditions and loads.

Each trial measures the system's responsiveness to alterations, ensuring that all modifications are securely verified and logged. The system confirms each vote change is authenticated against the election's public key and checks that the alteration falls within the permissible timeframe, adhering to the election's specific regulations. This two-fold verification process is critical to maintaining the integrity of the voting system, guaranteeing that vote alterations are conducted according to the rules and within the designated election timeline [12].

8. DISCUSSION AND FUTURE WORK

- Scalability and Efficiency: While the current system efficiently handles transactions, a key focus can be on improving the scalability of the blockchain infrastructure to handle the massive transaction loads characteristic of large-scale elections. Exploring Layer 2 solutions like Plasma or Rollups, which offload transactions from the main Ethereum chain, could significantly enhance transaction throughput and reduce latency. Future work could also delve into sharding techniques, where the blockchain is split into smaller, more manageable segments, improving processing speed and efficiency [13].
- Advanced Voter Identity Verification: Enhancing the verification process to ensure that only eligible voters can vote is crucial. Research could explore decentralized identity solutions, leveraging blockchain to store and verify user credentials securely. Techniques like Zero-Knowledge Proofs could allow users to prove eligibility without revealing sensitive personal information, ensuring privacy and preventing identity theft.
- Transactional Anonymity: Maintaining the anonymity of individual votes while ensuring the transparency of the overall voting process is a delicate balance. Future enhancements could incorporate cryptographic techniques like homomorphic encryption or zk-SNARKs to enable vote encryption, allowing vote tallying without revealing individual voter choices. This would ensure that the privacy of the voter is maintained while still allowing for public verification of the election results [14].
- Post-Election Audit and Analysis Tools: Developing comprehensive tools for post-election audits and analysis can be crucial for transparency and trust-building. These tools could use blockchain data to provide detailed insights into voting patterns, turnout, and other metrics, aiding in the continuous improvement of the electoral process.
- Energy Efficiency: Addressing the energy consumption of blockchain networks, especially those using Proof of Work (PoW) consensus mechanisms, is crucial. Future work could focus on adopting more energy-efficient consensus mechanisms like Proof of Stake (PoS) or exploring new blockchain platforms designed with energy efficiency in mind [15].
- Blockchain Network Optimization: Further research could delve into optimizing the underlying blockchain network for faster consensus algorithms and reduced transaction fees, enhancing the system's performance and voter experience [16].
- Advanced Fraud Detection Mechanisms: Develop sophisticated algorithms and mechanisms to detect and prevent fraud in real-time. This includes identifying anomalous voting patterns or attempted security breaches, further strengthening the integrity of the voting system.
- Interoperability with Existing Electoral Systems: Future enhancements could focus on developing interoperability frameworks allowing seamless integration of the decentralized voting system with existing electoral infrastructures. This integration would enable a gradual transition to blockchain-based voting while maintaining the reliability and familiarity of traditional systems.
- Acceptableness: For widespread adoption, the system must be acceptable to various stakeholders, including voters, election authorities, and regulatory bodies. Future research could focus on enhancing the user interface for ease of use, conducting extensive user experience research, and ensuring compliance with legal and regulatory standards. Collaboration with electoral and government bodies to tailor the system to their specific needs and regulations would also be vital.

9. CONCLUSION

This term paper on Decentralized Voting using Web3 presents a comprehensive study into the development and implementation of a blockchain-based voting system. "BlockChainBallot" leverages the Ethereum blockchain, smart contracts, and Web3 technologies to create a secure, transparent, and user-friendly voting platform.

The architecture incorporates Ethereum for tamper-proof record-keeping, React and Web3.js for a responsive front-end interface, Hardhat for efficient smart contract deployment, and MetaMask for secure user authentication.

The system successfully addresses the traditional challenges of voting systems, such as security vulnerabilities, lack of transparency, and voter anonymity concerns. By employing decentralized ledger technology, it ensures the integrity of each vote and the overall election process. The use of smart contracts automates and enforces the voting rules, further strengthening the system's credibility.

The research highlights the potential of blockchain technology in revolutionizing electoral systems, making voting more accessible, reliable, and resistant to fraud. The project demonstrates how decentralized solutions can provide more democratic and inclusive platforms for civic engagement, paving the way for future innovations in digital governance.

Overall, "BlockChainBallot" serves as a significant step towards modernizing electoral processes, showcasing the practical application and benefits of integrating blockchain technology in voting systems. It opens avenues for future research and development, particularly in enhancing scalability, user verification, and energy efficiency, which are vital for the widespread adoption of decentralized voting systems.

References

[1] Sachi Chaudhary, Shail Shah, Riya Kakkar, Rajesh Gupta, Abdulatif Alabdulatif, Sudeep Tanwar, Gulshan Sharma, and Pitshou N Bokoro. Blockchain-based secure voting mechanism underlying 5g network: A smart contract approach. *IEEE Access*, 2023.

[2] Friðrik Þ Hjálmarsson, Gunnlaugur K Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtỳsson. Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)*, pages 983–986. IEEE, 2018.

[3] Ye Guo and Chen Liang. Blockchain application and outlook in the banking industry. *Financial innovation*, 2:1–12, 2016.

[4] Ikhsan Darmawan. E-voting adoption in many countries: A literature review. *Asian Journal of Comparative Politics*, 6(4):482–504, 2021.

[5] SK Vivek, RS Yashank, Yashas Prashanth, N Yashas, and M Namratha. E-voting system using hyperledger sawtooth. In *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)*, pages 29–35. IEEE, 2020.

[6] Uzma Jafar, Mohd Juzaiddin Ab Aziz, and Zarina Shukur. Blockchain for electronic voting system—review and open research challenges. *Sensors*, 21(17):5874, 2021.

[7] Rachid Anane, Richard Freeland, and Georgios Theodoropoulos. E-voting requirements and implementation. In *The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007)*, pages 382–392. IEEE, 2007.

[8] Hrithvick Rao Rewatkar, Devansh Agarwal, Anmol Khandelwal, and Subho Upadhyay. Decentralized voting application using blockchain. In *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, pages 735–739. IEEE, 2021.

[9] Nicole J Goodman. Internet voting in a local election in canada. In *The internet and democracy in global perspective: Voters, candidates, parties, and social movements*, pages 7–24. Springer, 2014.

[10] Patrick McCorry, Siamak F Shahandashti, and Feng Hao. A smart contract for boardroom voting with maximum voter privacy. In *Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers 21*, pages 357–375. Springer, 2017.

[11] Massimo Bartoletti and Livio Pompianu. An empirical analysis of smart contracts: platforms, applications, and design patterns. In *Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers 21*, pages 494–509. Springer, 2017.

[12] Peter YA Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à voter: a voter-verifiable voting system. *IEEE transactions on information forensics and security*, 4(4):662–673, 2009.

[13] Breno Accioly de Barros Pimentel. Blockchain-based management system for iiot. 2023.

[14] Íñigo Querejeta Azurmendi. Cryptographic protocols for privacy enhancing technologies: From privacy preserving human attestation to internet voting. 2022.

[15] Sijie Chen, Hanning Mi, Jian Ping, Zheng Yan, Zeyu Shen, Xuezhi Liu, Ning Zhang, Qing Xia, and Chongqing Kang. A blockchain consensus mechanism that uses proof of solution to optimize energy dispatch and trading. *Nature Energy*, 7(6): 495–502, 2022.

[16] Javad Zarrin, Hao Wen Phang, Lakshmi Babu Saheer, and Bahram Zarrin. Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Computing*, 24(4):2841–2866, 2021.