AMERICAN JOURNAL OF INNOVATION IN SCIENCE AND ENGINEERING (AJISE)

ISSN: 2158-7205 (ONLINE)

VOLUME 3 ISSUE 3 (2024)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Innovation in Science and Engineering (AJISE)

Volume 3 Issue 3, Year 2024
ISSN: 2158-7205 (Online)
DOI: https://doi.org/10.54536/ajise.v3i3.3876
https://journals.e-palli.com/home/index.php/ajise

Advancing E-Voting Security: Biometrics-Enhanced Blockchain for Privacy and VerifiAbility (BEBPV)

Gbenga Alex Ajimatanrareje[1*]

Article Information

Received: October 07, 2024

Accepted: November 09, 2024

Published: December 10, 2024

Keywords

BEBPV, Blockchain, E-Voting, Receipt-Freeness, Verifiability

ABSTRACT

Achieving individual verifiability and receipt-freeness in e-voting systems poses a complex challenge. Mechanisms that allow voters to confirm their votes may also inadvertently enable them to show proof of their choices to others, thus jeopardizing vote privacy. This creates a critical tension between two essential objectives: enabling individual verifiability, where voters trust the system to accurately count their votes, and maintaining receipt-freeness, where the system prevents exploitation and coercion. The Biometrics-Enhanced Blockchain for Privacy and Verifiability (BEBPV) system proposed in this study addresses this challenge by employing facial biometric authentication and trusted node centres for post-voting verification; the biometric facial authentication reduces risks associated with the resale of voting credentials and removes the need for voters to recall complex passwords, while the post-voting verification process available at secure, trusted node centers allows voters to confirm their votes without retaining any proof that could be shared with third parties, thus upholding receipt-freeness. These mechanisms collectively ensure that individual votes are verifiable, while simultaneously safeguarding against coercion and vote-buying through receipt freeness. The feasibility of the BEBPV system is demonstrated through smart contract implementation for both the voting phase and post voting phase. Additionally, the system is validated on several essential attributes of an e-voting, including fairness, universal verifiability, eligibility and privacy. A technical evaluation indicates a transaction cost of 166,662 gas per vote cast.

INTRODUCTION

According to Tas and Tanriover (2020), blockchain technology is increasingly getting accepted as a transformative solution for e-voting, offering enhanced trust and security in electoral systems (Tas & Tanriover, 2020). E-voting frameworks can offer a secure, verifiable, and transparent platform for voting and storing of votes by leveraging blockchain's capabilities. This modernized technique not only enhances the integrity of elections but also increases confidence of voters by making sure that each vote cast is securely recorded, accurate, and free from tampering (Soni *et al.*, 2020).

Among the fundamental requirements for e-voting systems are individual verifiability and receipt-freeness, both essential for building trust and preventing exploitation (Benabdallah *et al.*, 2022). Individual verifiability ensures that people that voted can independently confirm that the candidates they voted for were recorded as they originally voted, thus affirming the legitimacy of election results. Conversely, receipt-freeness is critical to maintaining the confidentiality of votes, as it prevents voters from proving how they voted, thereby mitigating risks of coercion or vote-selling. Most existing e-voting systems struggle to fully satisfy both of these requirements, as mechanisms for verifying individual votes can often be exploited to reveal voting choices to third parties (Garg *et al.*, 2019). Consequently, there is a need for a system that achieves both receipt-freeness and individual verifiability without compromising other essential e-voting attributes.

This paper introduces the BEBPV system, an e-voting solution that incorporates advanced computer vision for biometric voter identification, enhancing both security and user convenience. The primary contribution of the BEBPV model lies in its post-voting verification mechanism, enabling voters to verify their individual votes without retaining any evidence that could be shown to others. This approach addresses the critical balance between individual verifiability and receipt-freeness, ensuring a secure and trustworthy voting experience.

LITERATURE REVIEW

A number of researchers have explored blockchain-based approaches for enhancing e-voting systems. Sallal *et al.* (2023) introduced the PVPBC system (Privacy and Verifiability Preserving E-Voting Based on Permissioned Blockchain), which prioritizes voter privacy and verifiability. In this model, voter identification is managed by a VID (Voter ID) assigned by a TTP (Trusted Third Party) and linked to a capability access token stored on the blockchain. Although the PVPBC model fully addresses the privacy of voters and verifiability of individual votes, it fails to address the issue of receipt freeness, thus the system can be exploited for vote buying and coercion. An Anonymous Decentralized E-Voting model presented by Kurbatov *et al.* (2019), incorporating ring signatures and blockchain to maintain integrity of the system and anonymity of the voter. In this system, each voter is referenced with a unique key pair and public keys. However, its scalability is limited due to the computational load associated with ring signatures, and

[1] Department of Data Science and AI, Bournemouth University, United Kingdom
[*] Corresponding author's e-mail: s5552175@bournemouth.ac.uk

users may need prior blockchain knowledge to engage effectively with the system.

In another approach, Hardwick *et al.* (2018) developed a protocol for E-Voting focused on decentralization and ensuring privacy of voters. This protocol leverages blockchain to improve transparency, fairness, and security in voting processes. The process is started by generation of pseudonymous identities for the blind signatures; this is achieved by the generation of public-private keys by voters, which are essential to protect voter privacy. This system enables a voter to alter their vote, it also allows a voter to personally verify their vote but it also fails to address the issue of receipt-freeness. Sallal *et al.* (2020) also proposed the Verify My Vote model (VMV), integrating the verifiability protocol of selene into an internet voting framework to bolster transparency and trust without requiring an overhaul of existing infrastructure. To create a tamper-resistant and verifiable record of votes, this system employs a permissioned DLT (distributed ledger technology); however, it falls short in fully ensuring receipt-freeness, additionally, privacy of voters is a concern, as the Election Authority (EA) can access certain data.

Khoury *et al.* (2018) introduced a platform for voting that is decentralised leveraging the Ethereum blockchain to create a trustless voting environment that emphasizes transparency, data integrity, and voter privacy. This system relies on the Ethereum Virtual Machine to execute smart contracts, which enforce voting protocols without the need for third-party intervention. Nevertheless, this platform also faces challenges in achieving both receipt-freeness and individual verifiability.

MATERIALS AND METHODS

Components of the BEBPV system

1. TTP (Trusted Third Party): During the initial phase, this entity manages the registration process, overseeing the front end system.

2. Front end system: The front end system contains multiple pages dedicated to various functions: the first page facilitates registration, the second page supports authentication, and the third is the voting page used for the casting, among other functions.

3. VFD (Voter's Face ID Numerical Data): A unique identifier generated for each voter's face using SHA256, created by the front-end system upon biometric recognition.

4. Voters: Individuals who participate in the election by casting a vote for their selected candidate.

5. Candidates: The individuals running for an elected position from which voters must choose.

6. Election Authority: The EA organizes and oversees the election, ensuring that all voters meet the eligibility criteria.

7. Capability Token: This token is stored on the Authentication Distributed Ledger Technology (DLT) alongside the VFD of each eligible voter, providing authorization for participation.

8. Trusted node centers (locations): These secure physical centers serve two primary functions. First, they allow voters to cast their votes in person if they lack a compatible device or prefer a physical voting experience, thus preventing voter disenfranchisement. Second, these centers facilitate individual vote verification. Each center is equipped with a device registered to one of the addresses specified in the smart contracts, enabling individual vote verification. Access to these locations is restricted to one voter at a time, and all personal electronic devices are prohibited to prevent any photographic evidence of the selected candidate. This arrangement enables the system to maintain receipt-freeness while allowing for individual verification.

Blockchain Structure

The functionality of the DLT (Distributed Ledger Technology) of the BEBPV system draws inspiration from the PVPBC system, with significant modifications that enhance its unique application in this work. (Sallal, *et al.*, 2020).

Authentication DLT

Identities and records of voters are stored on the authentication distributed ledger technology which uses a permissioned ledger.

Election Permission Distributed Ledger

It functions as a repository to secure verification-related data of votes, including the Voter's Face ID Numerical Data (VFD), encrypted votes, and tracking numbers, thereby supporting the verification process for each voting transaction.

How the BEBPV model works

Just like the PVPBC system by Sallal *et al.* (2023), the BEBPV e-voting process has three(3) key stages: Registration phase, Voting phase, and Post-Election phase.

Registration Phase

- As shown in Figure 1, the registration stage starts with the voter engaging with the front end system, where they provide their email address, ID and importantly, their facial biometric information. The front end system then captures a live photo of the voter's face, generating a unique VFD (Voter Face ID Numerical Data) from it.
- This is followed by the automatic forwarding of the voter's information to the Trusted Third Party. The next stage involves the Trusted Third Party verifying the voter's credential and confirming their eligibility to participate in the election. Once eligibility is confirmed, the TTP records a capability token, the VFD and the biometric face data of the person on the blockchain.
- Following this, an automated email is sent to the voter to confirm successful registration. If registration is denied, the TTP sends an email explaining the reason for rejection, which may include ineligibility of the person.

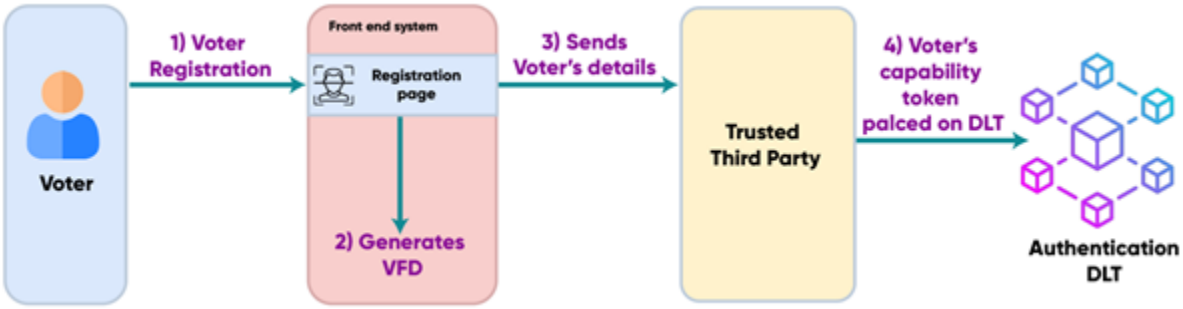

Figure 1: Process of voter registration

Voting Phase

• The voting phase (depicted in Figure 2 below) is initiated by the voter authentication phase. The voter begins by authenticating with the front end system, permitting it to capture a live facial photograph. The system (front-end) then utilizes computer vision technology to search the Authentication DLT for a matching facial record. Once the system locates the same face on the authentication distributed ledger technology, retrieval of the VFD is followed and then confirmation of the presence of an attached access token. Upon successful verification, the system then automatically directs the voter to the page where voting takes place.

• As illustrated in Figure 3, the voter views a list of candidates on the voting page. After selecting a candidate, encryption of the vote takes place, the encrypted vote is then forwarded to the EA (Election Authority) for signing, which is done digitally. The VFD, along with the signed ballot and a tracking number that is encrypted (which was generated by the front end system), is subsequently stored on the Election distributed ledger technology.

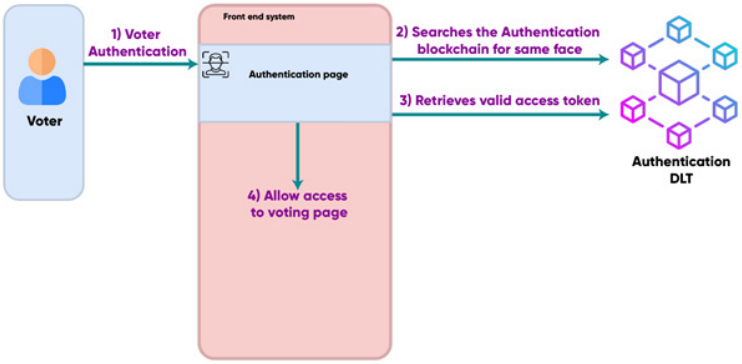

Figure 2: Process of authenticating a voter

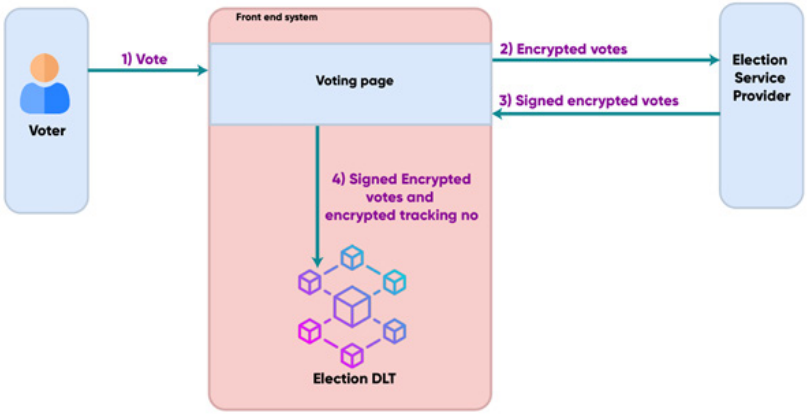

Figure 3: Process of voting

Post Election Phase

• Once the voting is concluded, the voting stage is closed by the EA (Election Authority) before the election results are available for viewing. Upon the EA ending the voting phase, the tracking numbers are decrypted by the front end system, showing each vote in plain text together with its corresponding tracking number. The election results are publicly available for everyone to see. Figure 4 details this process.

• To confirm the accuracy of their individual vote,

a voter visits the nearest trusted node center. At the center, the voter interacts with the system (front end), which captures their live face photo. This is followed by the system searching the Authentication distributed ledger technology automatically using computer vision technology to locate a matching facial record. A retrieval of the VFD takes place once the system is able to find the face on the authentication distributed ledger technology. This VFD is subsequently used to query the Election distributed ledger technology. Once the system is able to find a match of the VFD on the Election distributed ledger technology, then a decryption of the associated tracking number is followed, and finally the front end system reveals the decrypted tracking number and the choice for which the voter made during the casting of vote.

• Each trusted node center is assigned a unique address, and only these approved nodes permit interaction with the system (front-end) for accessing individual tracking numbers and chosen candidates. Attempts to view this information from any device or location other than a trusted node center will result in an error message prompting the voter to locate the closest trusted node center. Figure 5 depicts this process.

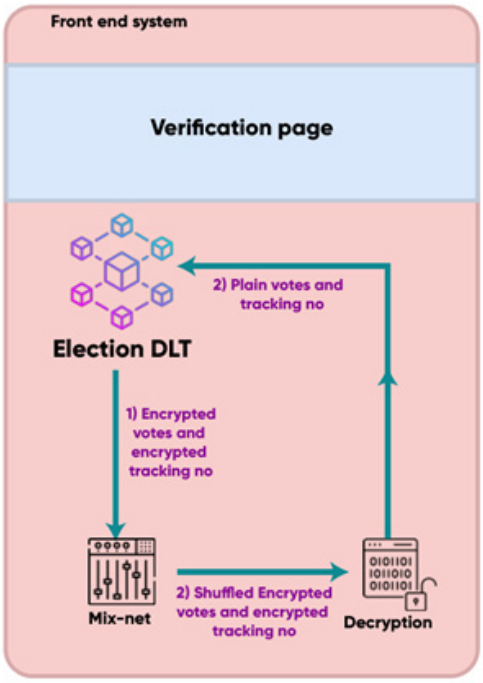

Figure 4: System process for revealing plain text votes after the election concludes.

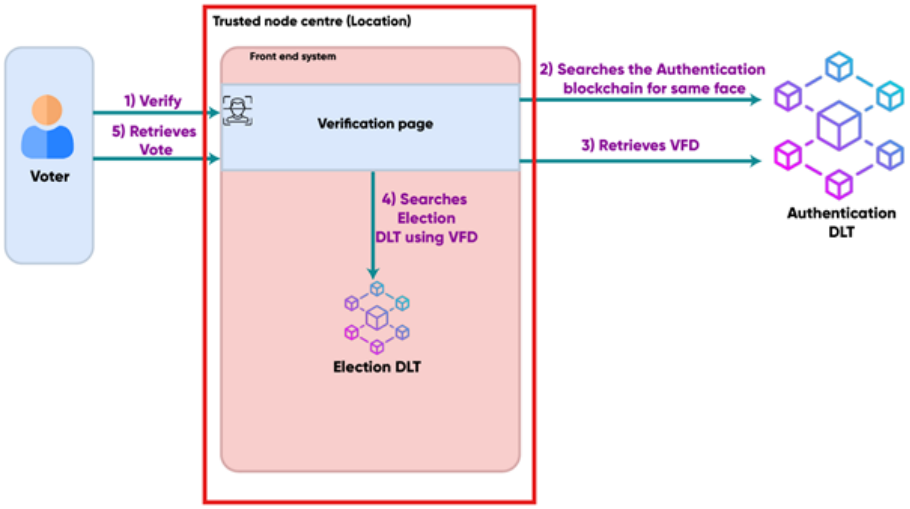

Figure 5: Voter's verification of their vote accuracy

RESULTS AND DISCUSSION

Theoretical Evaluation

Audit (Universal Verifiability)

This property allows an independent party to audit the system, assess the overall election performance, and verify the system's functionality as described (Sadia *et al.*, 2020). The BEBPV model achieves universal verifiability by making election results publicly available in plain text once the election is concluded by the EA. Additionally, the use of smart contracts enables anyone to review the source code and verify the system's functionality.

Eligibility

According to McCorry *et al.* (2017), the Eligibility property restricts voting participation to authorized individuals who meet predefined criteria. The BEBPV model upholds this requirement by approving only eligible voter registrations through the Trusted Third Party (TTP), while unqualified registrations are rejected, accompanied by an email explaining the reason for denial.

Individual Verifiability

Individual verifiability provides voters the ability to confirm that their votes were correctly cast and counted (Benabdallah *et al.*, 2022). The BEBPV model enables this by allowing participants to verify their individual votes at any of the designated trusted node centers.

Receipt Freeness

This is a principle designed to prevent vote-buying by ensuring that voters cannot produce proof of how they voted (Marwa Chaieb *et al.*, 2019). Achieving both

individual verifiability and receipt-freeness can be challenging, but the BEBPV system addresses this by enabling verification of individual votes exclusively at trusted node centers, ensuring complete receipt-freeness.

Privacy

The privacy property protects voter information from unauthorized access or leaks (Larriba *et al.*, 2021). In the BEBPV system, voter privacy is ensured during registration, as the TTP only accesses the VFD without additional personal information, safeguarding voter confidentiality.

Fairness

Fairness ensures that votes are not tallied progressively, preventing premature indications of which candidate is leading and ensuring that ongoing results do not influence subsequent voters (Li *et al.*, 2022). The BEBPV model maintains fairness by revealing results only after the election is officially closed by the EA, ensuring that no results are visible until voting is complete.

Technical Evaluation

The voting and post-election phases of the BEBPV system were implemented in a smart contract. The implemented components are those that align with the capabilities of Remix. Table 1 and Figure 6 below show the evaluation of costs of transaction and execution for the 'voteCandidate' function of the smart contract developed for the BEBPV model, tested over ten(10) experiments on the Goerli network.

Table 1: Voting cost per voter (utilizing the voteCandidate function) across 10 experimental trials.

Trial Number	Transaction Cost (gas)	Execution Cost (gas)
1	172337	150301
2	141715	119679
3	145293	123257
4	148871	126835
5	152449	130413
6	193317	171281
7	162698	140662
8	166276	144240
9	207143	185107
10	176522	154486

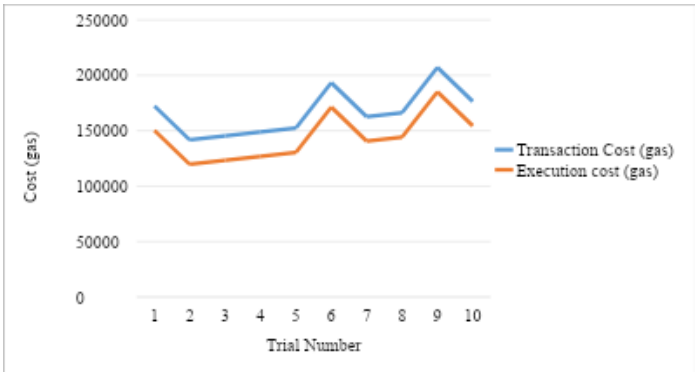

Figure 6: Graph of cost evaluation of voting per voter (using the vote Candidate function) over 10 experiments (Trials).

CONCLUSIONS

The BEBPV system introduced in this paper offers significant advantages in achieving individual verifiability and receipt-freeness, facilitated through facial biometric authentication for voter registration and the use of trusted node centers for vote verification. This approach enhances the usability of the e-voting system by allowing voters to authenticate using biometric data, removing the need to remember complex credentials. To demonstrate the BEBPV system's implementability, smart contracts were developed and deployed for the election and verification phases within Remix. The system was rigorously evaluated against key e-voting attributes, including universal verifiability, eligibility, privacy, receipt-freeness and individual verifiability. Additionally, the transaction cost of casting a vote was analyzed through the voting function in the smart contract to assess average gas consumption.

REFERENCES

Alotaibi, O. (2024). Role of Artificial Intelligence in Enhancing Metaverse Gaming Experience and Human Interaction. *International Journal of Metaverse, 2*(1), 11–19. https://doi.org/10.54536/ijm.v2i1.2933

Alvi, S. T., Uddin, M. N., & Islam, L. (2020). Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract. *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT).* https://doi.org/10.1109/icssit48917.2020.9214250

Bellini, E., Ceravolo, P., Bellini, A., & Damiani, E. (2020). Designing Process-Centric Blockchain-Based Architectures: A Case Study in e-voting as a Service. *Lecture Notes in Business Information Processing*, 1–23. https://doi.org/10.1007/978-3-030-46633-6_1

Benabdallah, A., Audras, A., Coudert, L., Madhoun, N. E., & Badra, M. (2022). Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. *IEEE*

Access, 10, 70746–70759. https://doi.org/10.1109/access.2022.3187688

Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2019). Verify-Your-Vote: A Verifiable Blockchain-Based Online Voting Protocol. *Lecture Notes in Business Information Processing*, 16–30. https://doi.org/10.1007/978-3-030-11395-7_2

D. MohanaPriya, G. Devadharshini, S Divya, & J. Rajalatchumy. (2021). Towards A Privacy-Preserving Voting System Through Blockchain Technologies. *2021 International Conference on System, Computation, Automation and Networking (ICSCAN)*. https://doi.org/10.1109/icscan53069.2021.9526542

Garg, K., Saraswat, P., Bisht, S., Aggarwal, S. K., Kothuri, S. K., & Gupta, S. (2019, April). A comparitive analysis on e-voting system using blockchain. In *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)* (pp. 1-4). IEEE. https://doi.org/10.1109/iot-siu.2019.8777471

Hardwick, F. S., Gioulis, A., Akram, R. N., & Markantonakis, K. (2018). E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. *ArXiv* (Cornell University). https://doi.org/10.1109/cybermatics_2018.2018.00262

Hui, H., & Sang, L. T. (2024). Integrating Financial and Textual Indicators for Enhanced Financial Risk Prediction: A Deep Learning Approach. *American Journal of Financial Technology and Innovation, 2*(1), 15–24. https://doi.org/10.54536/ajfti.v2i1.2489

Khoury, D., Kfoury, E. F., Kassem, A., & Harb, H. (2018, November). Decentralized voting platform based on ethereum blockchain. In *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)* (pp. 1-6). IEEE. https://doi.org/10.1109/imcet.2018.8603050

Kurbatov, O., Kravchenko, P., Poluyanenko, N., Shapoval, O., & Кузнецова, Т. (2019). Using Ring Signatures For An Anonymous E-Voting System. *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*. https://doi.org/10.1109/atit49449.2019.9030447

Larriba, A. M., Cucó, A. C., Sempere, J. M., & López, D. (2021). Distributed Trust, a Blockchain Election Scheme. *Informatica* (Lithuanian Academy of Sciences), 321–355. https://doi.org/10.15388/20-infor440

Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M. (2022). A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT. *IEEE Transactions on Dependable and Secure Computing, 19*(1), 119–130. https://doi.org/10.1109/tdsc.2020.2979856

McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy. *Lecture Notes in Computer Science,* 357–375. https://doi.org/10.1007/978-3-319-70972-7_20

Sadia, K., Masuduzzaman, M., Paul, R. K., & Islam, A. (2020). Blockchain-Based Secure E-Voting with the Assistance of Smart Contract. *Blockchain Technologies,* 161–176. https://doi.org/10.1007/978-981-15-4542-9_14

Sallal, M., de Fréin, R., & Malik, A. (2023). PVPBC: Privacy and Verifiability Preserving E-Voting Based on Permissioned Blockchain. *Future Internet, 15*(4), 121–121. https://doi.org/10.3390/fi15040121

Sallal, M., Owenson, G., Salman, D., & Adda, M. (2022). Security and performance evaluation of master node protocol based reputation blockchain in the bitcoin network. *Blockchain: Research and Applications, 3*(1), 100048. https://doi.org/10.1016/j.bcra.2021.100048

Sallal, M., Schneider, S., Casey, M., Dupressoir, F., Treharne, H., Dragan, C., ... & Wright, P. (2020, November). Augmenting an internet voting system with selene verifiability using permissioned distributed ledger. In *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1167-1168). IEEE. https://doi.org/10.1109/icdcs47774.2020.00124

Soni Vivek, Yashank, R. S., Yashas Prashanth, N Yashas, & M Namratha. (2020). E-Voting Systems using Blockchain: An Exploratory Literature Survey. *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA).* https://doi.org/10.1109/icirca48905.2020.9183185

Taş, R., & Tanrıöver, Ö. Ö. (2020). A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting. *Symmetry, 12*(8), 1328–1328. https://doi.org/10.3390/sym12081328