Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 7-Issue 1, January 2024
Paper: 45

Secured Blockchain Voting System using Ring Signatures and Blind Signatures

Shashwat Rai[1] and Dr. T Senthil Kumar[2*]

[1] Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India, 603203.

[2] Associate Professor, Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India,603203.

[1] sr6183@srmist.edu.in, [2]senthilt2@srmist.edu.in

*Corresponding Author: Dr. T Senthil Kumar

Keywords— Blockchain, Voting, Blind Signatures, Ring Signatures, ECC.

Abbreviations - SEC: Secure Election Cryptography; ECC: Elliptical Curve Cryptography; RSA: Rivest-Shamir-Adleman; FOO: Fujioka-Okamoto-Ohta; AES: Advanced Encryption Standard.

***Abstract*—Online voting systems have encountered significant challenges such as voter privacy, security, and tampering. This paper proposes a secure online blockchain voting system that addresses these issues by utilizing blind signatures and ring signature techniques. Our system ensures voter privacy by using ECC blind signatures that enable voters to sign their ballots anonymously without disclosing their identities. The system's integrity is ensured by ring signatures that allow any member of the tallying group to sign a message anonymously, making it impossible to identify the signer. The proposed system is implemented on a blockchain network that provides decentralization, immutability, and transparency. The voting process involves several steps, including registration, authentication, and ballot casting. The security of the proposed system is analyzed using threat modeling, and simulation results demonstrate its scalability and efficiency.**

INTRODUCTION

Online voting systems have become increasingly popular as the internet and technology continue to advance. With this growth, it is necessary to create systems that are both reliable and secure. Blockchain technology has shown great potential in providing a secure and transparent platform for voting. However, challenges remain in ensuring voter privacy and preventing double voting in blockchain-based voting systems.

This research paper proposes a solution to these challenges by using Elliptic Curve Cryptography (ECC) Blind Ring Signatures and Ring Signatures in a secure online blockchain voting system. The proposed system allows voters to cast their votes anonymously and securely, preventing their identity or voting choice from being revealed. Additionally, the system employs ring signatures to protect the identity of the voting commission member to sign messages anonymously as a member of the commission.

The paper is organized as follows. Section 2 provides a review of related works in online voting systems and blockchain technology. Section 3 explains the proposed voting system in detail, including its architecture, the ECC Blind Signature scheme, and the Ring Signature scheme. Section 4 provides the results of the experiments conducted and their implications. Finally, Section 5 concludes the paper by summarizing the contributions and outlining potential areas for future research in this field.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 45

LITERATURE REVIEW

In [1], an effort to create a scheme for e-voting that achieves end-to-end verifiability and successfully demonstrates its usefulness is made by the authors Kashif Mehboob Khan et al. They attempt to utilize features of blockchain including cryptographic underpinnings and transparency. In order to demonstrate how well their suggested digital voting system works in practice and to guarantee the integrity of the voting process, the authors conclude by presenting a case study of the system in use. In [2] by scholars Uzma Jafar et al provides further criteria for scalable voting solutions and enables future research to bear in mind all the electoral requirements, benefits, and demerits of the offered solutions before proposing or developing any solutions. In [3], by Ruhi Tas, Ö. Ö. Tanriöver, it was suggested that blockchain systems can actually offer answers to several issues that plague the existing electoral process, and that distant participation, safety and agility should be enhanced for long-term blockchain based electronic voting. The paper [4] by Nhan Tam Dang et al uses attribute-based encryption and the blockchain to propose a method for sharing protected data on P2P-based apps. The suggested approach was tested on a mobile p2p network that offers services for sharing and storing data securely. The authors go on to discuss how ABE may be utilized to overcome these restrictions by enabling fine-grained access control based on factors like user roles, locations, and times. The authors outline their solution, which utilizes ABE to exchange and encrypt data on P2P apps.

The paper [5] by Diego Cagigas et al emphasizes the key potential advantages, costs, and dangers of blockchain for government, civil servants, and people while identifying the public services most likely to be impacted by its deployment. The application of blockchain for digital identification, public financial management, and the provision of public services are a few of the major topics that the authors notice in the research on blockchain in public services. They also bring attention to the difficulties and restrictions associated with deploying blockchain in the public sector, such as legal restrictions and the requirement for system interoperability.In the paper [6] by Yan Xu et al, the obstacles in applying food safety were studied, as well as the limitations with the blockchain technology itself. By identifying the tremendous potential of blockchain technology and its implications for food safety regulation, this study adds to the body of knowledge already available in the field of food safety.In the paper [7] by Rifa Hanifa Tunnisa and Budi Rahardjo, the recording technique is more secure as hash values and digital signatures are used to save the results of each polling place that is connected to the others. The proposed sequence in this system's blockchain creation process takes into account the fact that all nodes that take part in the process must be included in the Bitcoin system. The paper [8] implements a proof that allows voters to cast their ballots using a smartphone application that uses fingerprint and password biometric identification.

In the paper [9] by Chaum D et al, the voters mark their ballots using optical scan technology in the first step of the two-stage voting procedure, and then they confirm their choices using a cryptographic receipt in the second. In order to ensure openness and accountability throughout the voting process, the receipts may subsequently be utilized to perform voter-variable audits of the election outcomes. Similarly, [10] by Dalia et al proposes both a commitment round to ensure fairness and a recovery round to allow for the disclosure of the election outcome if voters abort. It also provided a computational demonstration of the security of ballot secrecy. The authors of paper [11] discussed the implementation of blockchain-based electronic voting in real-world settings and extracted a set of qualities that it must possess. These attributes must be both publicly and individually verifiable. The author of [12] N. Baranov concludes that if people understand the benefits of distant electronic voting and

other digital advances in the political process, and if technical issues are resolved, it is feasible to legitimise the use of blockchain and other digital advancements in the conduction of remote elections.

The objective of Richard Essah and Issac Ampofo Sr in [13] is to categorize trends and other indications in order to provide research bibliometric analysis on biometric voting using IoT to send votes to a central system. The sample comprised of 267 different components. The data was processed, and the results were visually shown. Per the study, the body of knowledge on biometric voting which uses Internet of Things to transfer votes to a central system, is growing quickly, based on several relevant parameters. The paper [14] combines visual cryptography with picture steganography to provide a revolutionary method of online voting that increases system security without sacrificing system usability or speed. The voting system also uses a threshold decryption approach and a password hashing algorithm. The programme is created using web-based Java EE, and MySQL and Glassfish are integrated as its application server and database server, respectively. [15] implements a proof-of-concept of Bingo Voting, a novel voting system that is both verifiable and free of coercion. Bingo Voting is built on a reliable random number generator, demonstrating the usefulness of the system by allowing all expensive calculations to be relegated to a pre-voting phase that is not time-sensitive. Two coercion/vote buying attacks on voting systems are shown as justification for the new approach and demonstrate how risky it may be to allow the voter to add randomization to the voting system.

The paper [16] by M Rosenfield examines the likelihood of success of common assaults in Bitcoin and the stochastic mechanisms that underlie them, while [17] demonstrates a secure voting system employing the RSA Key Encapsulation Mechanism, using a key derivation function together with unrelated keys for encryption and decryption. It has two levels: symmetric and public key layers. The three components of RSA are key creation, encryption, and decryption. The induction function of RSA-KEM, KDF3 built on SHA-256, is mostly used for key creation. AES key wrap provides key-wrapping capabilities. In [18] by Marino Tejedor-Romero et al, end-to-end vote verification is made possible by a distributed, remote e-voting system based on mixnets, operations in the Galois field, and Shamir secret sharing. Due to their competing interests, parties take part in the network as nodes, safeguarding their own interests and preserving process integrity. The novelty is the secret-sharing among the political parties, which assures that no party may undermine the integrity of the ballot without being identified and identified in real time, and the computational and architectural scalability of the idea, which make it easy to execute. By contrasting and analyzing current security measures, separating the security risks in blockchain technology's six layers, and exploring and defining the various security attacks and challenges when implementing blockchain technology, the study [19] by R. F. Olanrewaju et al encourages theoretical research and the development of robust security protocols in the present and future distributed work environment. In project [20] the major goal is to create an E-voting system that is more secure, verifiable, and doesn't necessitate the presence of reliable individuals on every level. In addition to leveraging ring signature and fingerprint authentication for added protection, blockchain is used to make voting significantly safer.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 45

PROPOSED WORK

The proposed secure online blockchain voting system architecture is designed based on the MVC pattern as follows:

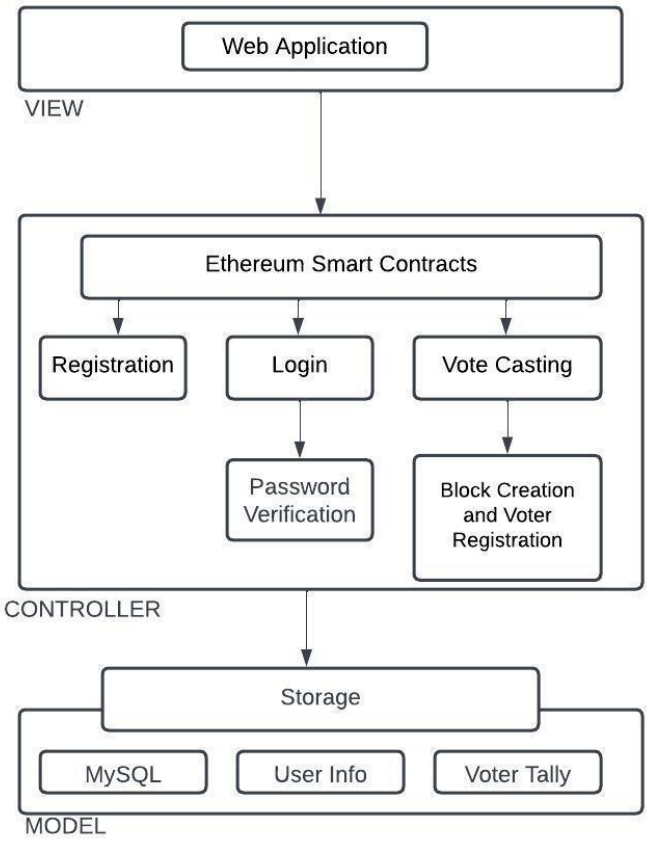

Figure 1. MVC Architecture

- The Model component of the system is the Ethereum blockchain, which provides secure and transparent data storage for the voting process. The blockchain serves as a tamper-proof database for storing voting data, ensuring data integrity and transparency, with the Ethereum network providing a framework for blockchain creation and storage..
- The Controller component is the smart contracts, which define the voting process logic and interact with the Model component to implement the voting process. The smart contracts ensure that each voter can cast only one vote and that the results are accurately counted and verified. They also utilize ECC Blind Signature and Ring Signatures to protect voter anonymity and prevent fraud. The public key provided by the blockchain is used for verification purposes by the ledger, while the private key is with the host.
- The View component is the web application, which provides a user-friendly interface for voters to interact with the system. The web application communicates with the Controller to perform the necessary operations related to the voting process. It ensures that the user interface is intuitive and easy to use, while also enforcing security and privacy measures to protect voter anonymity and prevent double voting.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 45

By separating the system into these three components, we can ensure that each component performs its specific function effectively, leading to a more reliable and efficient voting system. The web application platform allows users to register and cast their vote securely and transparently. The registration phase requires voters to provide their unique ID, name, roll number, and mobile number, which are stored in a database.

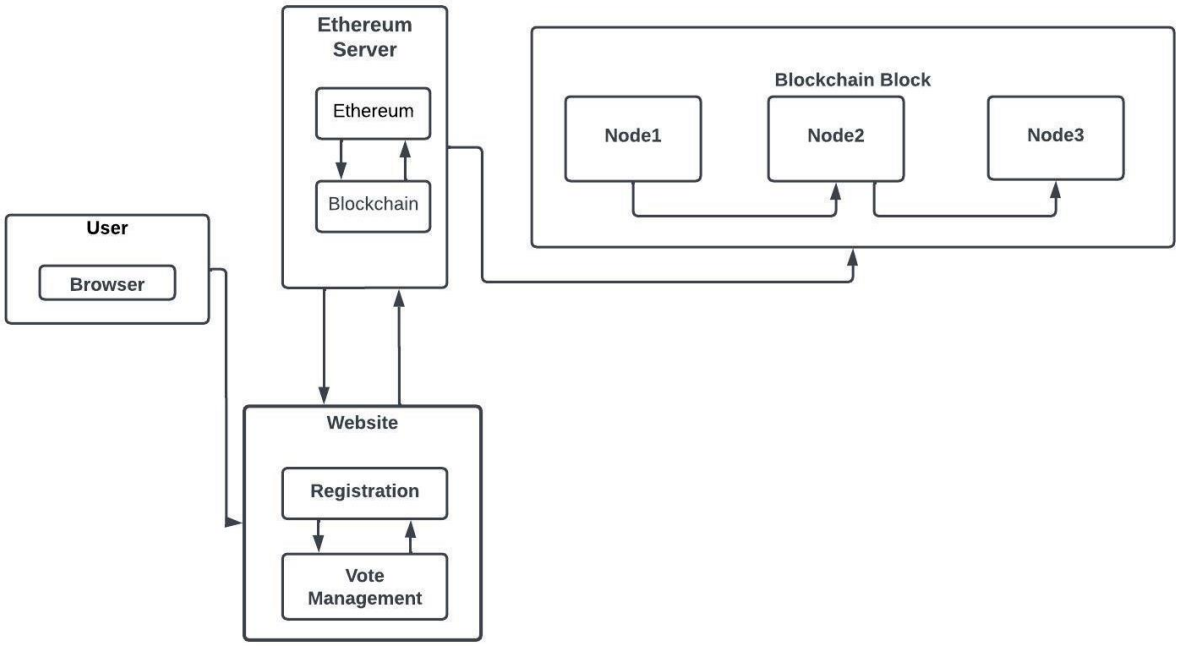

Figure 2. Basic Structure of the Web-Application

To ensure the legitimacy of transactions, electronic digital signatures are used. These signatures verify that transactions are initiated by the rightful sender, as they are signed using the corresponding private key of the sender's public k.

ECC is a public-key cryptographic algorithm widely used in secure communication and data protection. ECC relies on the properties of elliptic curves over finite fields to encrypt and decrypt messages. ECC is an efficient cryptographic algorithm and is well-suited for resource-constrained environments like blockchain-based systems. The ECC algorithm is based on defining a set of points on an elliptic curve over a finite field and a group operation to combine these points. A private key is used to generate a public key, which is a point on the curve. To encrypt a message, the sender generates a random number to create a point on the curve, which is then added to the recipient's public key to produce the ciphertext. The ciphertext can only be decrypted using the recipient's private key.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 45

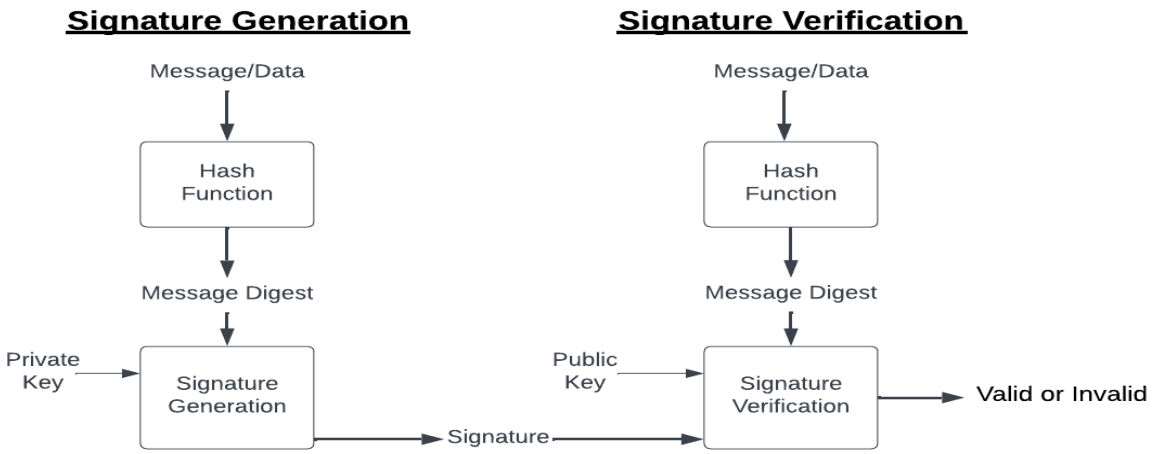

Figure 3. Signature Block

Blind signatures are a form of digital signature that enables a message to be signed without disclosing its content. In ECC Blind Signatures, the message is encrypted using the sender's public key to generate a ciphertext. The ciphertext is then signed using the sender's private key to create a blind signature. The recipient can use their private key to decrypt the ciphertext, revealing the original message without disclosing the signature or the signer's identity.

- Setup: Two parties, A and B, agree on a cryptographic hash function H, an elliptic curve E, and a generator point G on E.
- Key generation: A generates a public/private key pair (P_A, d_A) on the elliptic curve E. B generates a public/private key pair (P_B, d_B) on the same elliptic curve E.
- Blinding: A wants B to sign a message m for them without revealing the contents of the message. They choose a random blinding factor b and compute the blinded message m' = H(m||b) * G, where || denotes concatenation. A sends m' to B.
- Signing: B receives the blinded message m' and signs it using their private key d_B to get s' = d_B * m'. B sends s' back to A.
- Unblinding: A receives s' from B and unblinds it using their blinding factor b to get s = s' + b. A sends s to B.
- Verification: B receives s from A and verifies that s * G = P_A + H(m||P_A) * P_B, where + denotes the elliptic curve point addition operation. If the verification succeeds, then B has blindly signed the message m for A.

In this algorithm, the requester generates a blinding factor b and blinds the message M by multiplying it with b. The requester sends the blinded message M' and a randomly generated point R = rP to the signer. The signer computes the inverse of the blinding factor b, computes the point R' = R + b^-1Q, where Q is the signer's public key, and signs the blinded message with the private key d. The signer sends the unblinded signature S = S' + br to the requester. The requester unblinds the signature by multiplying it with the inverse of the blinding factor b and verifies the signature by computing the verification point V = S'b^-1P + brP. The requester checks whether V = kP, where k is the signer's public key. If V = kP, the signature is valid.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 45

Ring signatures allow anonymous signatures, where the signer is a member of a group but their identity is kept confidential. Ring Signatures use a group of public keys, and the signer generates a signature that is valid for any of the public keys in the group using their private key. This makes it impossible to identify the specific member of the group who signed the message, providing anonymity.

- Setup: A wants to sign a message m anonymously, and there are n possible signers: {P_1, P_2, ..., P_n}. A knows the public keys of all signers.
- Key generation: Each signer j (1 <= j <= n) generates a public/private key pair (P_j, d_j) on the same elliptic curve E.
- Signing: A chooses a random index i (1 <= i <= n) and a random blinding factor r. The value c = H(m || P_i || R) is computed , where R = r * G is a random point on the elliptic curve E and H is a cryptographic hash function. Then the signature value s = r - c * d_i (mod order(E)) is computed, where order(E) is the order of the elliptic curve group.
- Verification: To verify the ring signature, anyone can compute s * G = R + c * P_i and check if it equals any of the public keys P_1, P_2, ..., or P_n.

We have implemented a modified and upgraded version of the base cryptographic functions henceforth referred to as SEC.

A self-executing digital contract known as a "smart contract" enables two or more parties to reach an agreement and automate the implementation of that agreement. In Ethereum, smart contracts are employed for a number of functions, including the creation and management of digital assets, the execution of financial transactions, and the automation of decentralized organization governance. By doing away with middlemen and lowering the possibility of fraud and mistake, they provide a more transparent and efficient method of doing business. Implementing blind signature in Ethereum using smart contracts provides security, transparency, efficiency, immutability, and cost-effectiveness in executing the signature process. Ether, the Ethereum network's native coin, is used to carry out smart contracts. A consensus algorithm is used by a network of nodes to validate a smart contract after it has been performed.

Using smart contracts, we can implement blind and ring signatures to the contract.

- Generate public and private keys for the signer using the secp256k1 curve. This is the same curve used in Ethereum for generating account addresses and signatures.
- Create a smart contract that defines the parameters of the blind signature protocol. This can include the public key of the signer, the message to be signed, and the blinding factor.
- The user generates a random blinding factor and uses it to blind the message. The blinded message is then sent to the smart contract for signature.
- The smart contract receives the blinded message, verifies that the blinding factor is valid, and signs the blinded message using the signer's private key.
- The smart contract returns the blinded signature to the user.
- The user unblinds the signature using the inverse of the blinding factor and obtains the final signature.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 45

```
function requestBSign(uint256 bVote) public {
  require(eligibleVoter[msg.sender].eligible);
  bVotes[bVote] = msg.sender;
  RequestToBlindlySign(msg.sender);
}

//requested bsign is recorded on the blockchain for auditing purposes
function writeBSign(address _voters, uint256 bSign) onlyOwner public {
  eligibleVoter[_voters].signedBlindedVote = bSign;
  eligibleVoter[_voters].eligible = false;
}


function Vote(uint256 choiceCode, uint256 vote, uint hashVote, uint256 c, uint256 s) public {
  verifyBSign(hashVote, c, s);
```

Figure 4. Sample Smart Contract

The consensus mechanism in a blockchain network helps to ensure that all the distributed ledgers maintained by the network's peers are identical copies. This minimizes the risk of fraudulent transactions by preventing any unauthorized changes to the ledger. A cryptographic hash function, the SHA3 hashing algorithm, is used to generate a unique checksum for each block in the chain. This checksum serves as an indicator of any tampering with the data in the block, as even the slightest modification in the input data of a transaction will result in a different hash value. This makes it difficult for malicious actors to corrupt the transaction data.

SHA3 algorithm is chosen for its various advantages over previous hashing algorithms such as SHA256. It is more secure, uses a different hashing approach, making it less vulnerable to attacks such as length extension attacks, and more resistant to collision attacks. SHA3 is also faster on some hardware due to its parallel processing optimization, unlike SHA256, which is optimized for sequential processing. Lastly, it is more flexible than SHA256, with a variable output size, allowing it to produce hashes of different lengths. The benefits of SHA3 over previous hashing algorithms make it a more efficient and secure consensus mechanism for blockchain-based applications like e-voting.

The voting scheme is divided into four phases:

- During preparation the voter fills in a ballot and sends it after blinding and signing to the validator.
- In the administration phase the validator signs the message and sends it back to the voter.
- The voter in the voting phase then unblinds the signature and casts his vote onto the immutable ledger. After the vote is finished the voter opens his vote by sending his commitment key.
- In the results phase, the processing and tallying of votes are performed, and the results are displayed on the website. Users can verify their votes using their public key, which provides transparency to the voting system.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 45

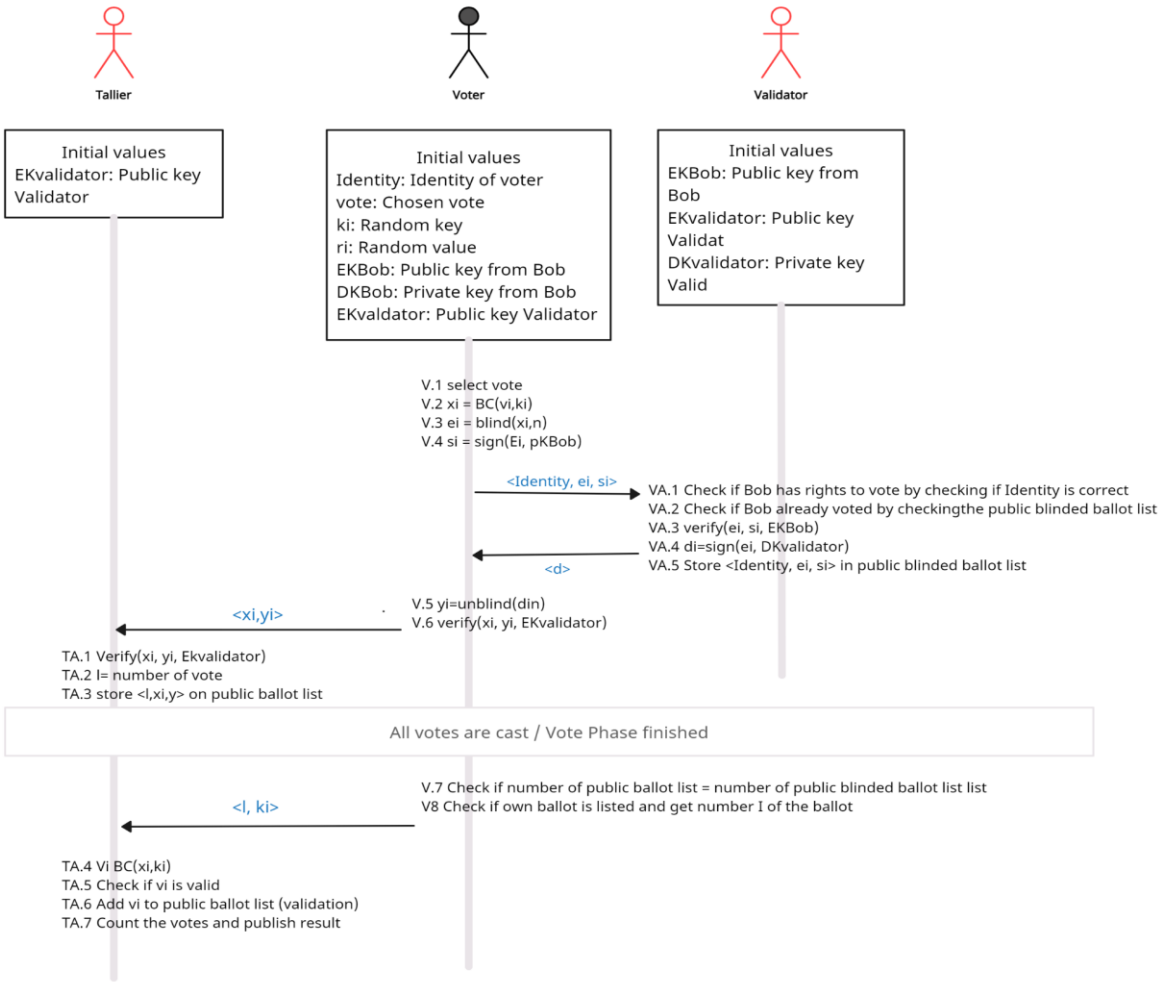

Figure 5. Voting Scheme

When a user logs in and accesses the app, they are shown a voting interface that lists the candidates for office or the ballot items up for vote. After choosing their chosen candidate or viewpoint, the user would next cast their ballot. The vote would then be transmitted by the app to the backend, which would use the Ethereum blockchain to interact with it and record it on a secure ledger. The election's regulations, such as how many votes are needed to win and how long the voting session will last, will be encoded in the smart contracts. Moreover, the smart contracts would stop double voting.

The validator does not know the contents of the message being signed, as it is blinded by the user. However, the validator is responsible for ensuring that the signature is valid and has not been tampered with. To do this, the tallier verifies the signature using the signer's public key, which they previously obtained during the setup phase. Once the validator has verified the signature, they send it back to the voter, who then unblinds the signature to obtain the valid signature for the original message. The validator plays an important role in ensuring the validity of the signature while maintaining the privacy of the signer. They act as a trusted intermediary between the voter and the tallier, and their main responsibility is to verify the validity of the signature and maintain the privacy of the voter.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 45

The administrator in the e-voting system with blockchain technology has the responsibility of managing the election. They have access to a dashboard that allows them to set up the voting rules, candidates or issues being voted on, monitor the voting process and results. During the voting period, the administrator would oversee the process and address any issues or irregularities. They would then analyze the results and declare the winner using the transparent and auditable record provided by the blockchain ledger

This approach ensures the integrity of the voting system, preventing any potential fraudulent activities while providing a secure and transparent voting experience for users.

RESULTS AND DISCUSSION

Our research results show that this voting system achieves a high level of security and transparency. ECC Blind Signature is used to ensure voter anonymity and prevent tampering with votes during transmission. Ring Signature further enhances security by allowing group signatures that make it difficult to trace the origin of a vote, further providing a degree of protection against attempts at outside coercion and interference in a voting scenario.

We evaluated the performance of our system using several metrics, including voting process accuracy, transaction verification speed, and security level. Our research findings indicate that the system is highly accurate and secure, with a low error rate and no tampering detected during testing. The use of blockchain technology ensures that all transactions are recorded on the network, which increases transparency and prevents the manipulation of election results. The blockchain network also enables transparent and auditable voting processes, which are essential for ensuring election integrity.

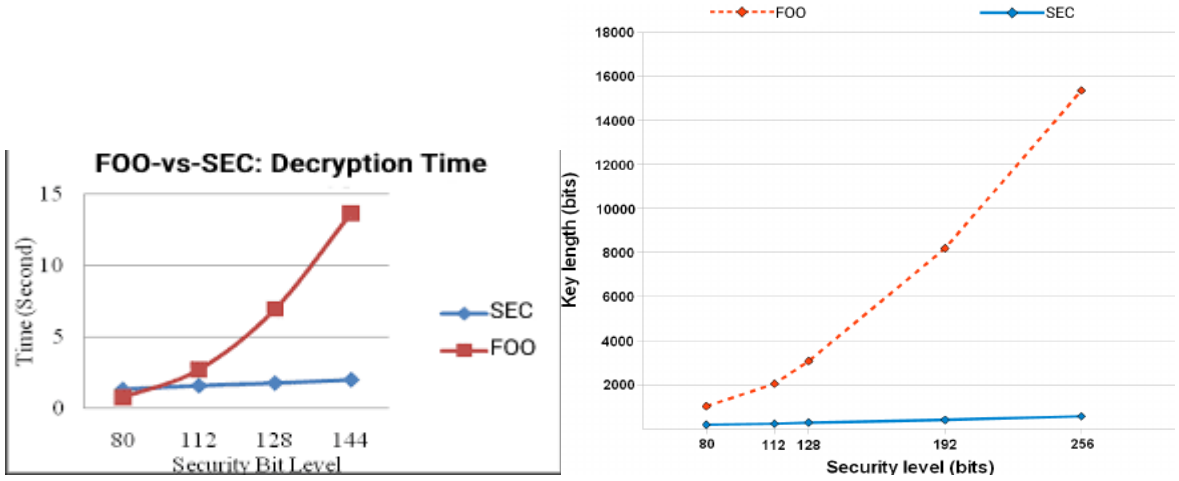

Figure 6. FOO vs SEC contrast- Time and Key Length parameters

Compared to previous interpretations of the concept, our implementation shows considerable improvement. Contrasting our implementation to FOO as implemented in [21], we see our project shows marked improvements on several parameters.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume7-Issue1, August 2023
Paper: 45

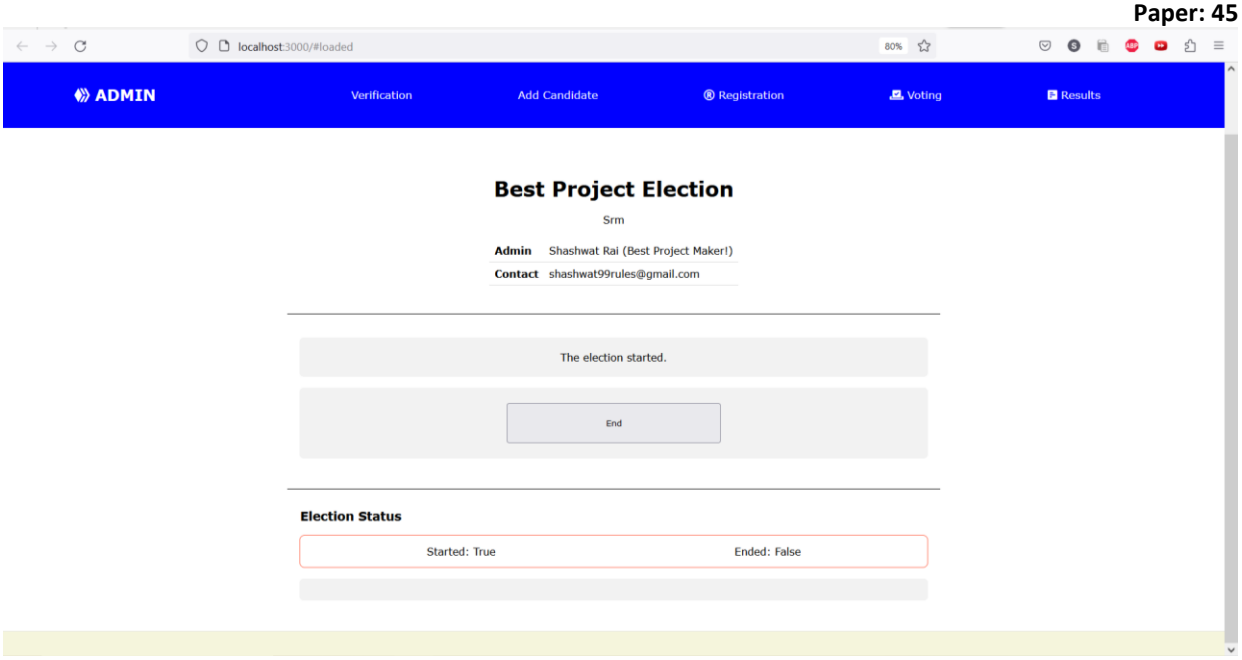

Figure 7. Screenshot of the Web-Application

CONCLUSION

The proposed system offers a secure online voting solution that maintains voter privacy and ensures the integrity of the vote. The use of ECC blind and ring signature techniques provides an additional layer of security to the voting process, making it more resilient to attacks. The system's implementation is flexible and can be adapted to various applications, including shareholder voting, college and other institution elections, and other online voting systems. It is important to note that our contracts are executed on the Ethereum blockchain, which means that the voting application can be accessed from anywhere that can run a browser, regardless of location, platform, or device. This allows for a high degree of flexibility in terms of accessibility and convenience for voters.

The scope of our project is limited to small-scale polls and elections, such as those held within a college or corporation. We acknowledge that a larger voting process with millions of voters may present different challenges that need to be addressed. One of the main limitations of the Ethereum network is its scalability, which is still an area that requires further research. Therefore, we cannot yet recommend the use of our contracts for nation-wide elections or other large-scale voting processes. Nonetheless, the accessibility and flexibility of the voting application we have developed makes it a useful tool for other small-scale voting processes in a variety of contexts.

REFERENCES

1. Khan, Kashif Mehboob et al. “Secure Digital Voting System Based on Blockchain Technology.” Int. J. Electron. Gov. Res. 14 (2018): 53-62.

2. Jafar U, Ab Aziz MJ, Shukur Z, Hussain HA. A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. Sensors

(Basel). 2022 Oct 6;22(19):7585. doi: 10.3390/s22197585. PMID: 36236684; PMCID: PMC9572428.

3. Taş R, Tanrıöver ÖÖ. A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting. Symmetry. 2020; 12(8):1328.

4. Dang, Nhan & Tran, Ha & Nguyen, Sinh & Maleszka, Marcin & Dương, Hải. (2021). Sharing secured data on peer-to-peer applications using attribute-based encryption. Journal of Information and Telecommunication. 5. 1-20. 10.1080/24751839.2021.1941574.

5. A. Aliti, E. Leka, A. Luma and M. A. Trpkovska, "A Systematic Literature Review on Using Blockchain Technology in Public Administration," 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2022, pp. 1031-1036, doi: 10.23919/MIPRO55190.2022.9803797.

6. Xu Y, Li X, Zeng X, Cao J, Jiang W. Application of blockchain technology in food safety control : current trends and future prospects. Crit Rev Food Sci Nutr. 2022;62(10):2800-2819. doi: 10.1080/10408398.2020.1858752. Epub 2020 Dec 12. PMID: 33307729.

7. D. Khoury, E. F. Kfoury, A. Kassem and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain," 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), Beirut, Lebanon, 2018, pp. 1-6, doi: 10.1109/IMCET.2018.8603050.

8. Ueda, Eduardo & Silva, Marcelo & Silva, Anderson & Junior, Norisvaldo & Pereira, Fabio & Santos, Alessandro & Guelfi, Adilson & Kofuji, Sergio. (2021). A Proposed Blockchain-Based Voting System with User Authentication through Biometrics. Journal of Information Security and Cryptography (Enigma). 8. 1-11. 10.17648/jisc.v8i1.78.

9. AChaum, David; Aleks Essex; Richard T. Carback III; Jeremy Clark; Stefan Popoveniuc; Alan T. Sherman; Poorvi Vora (May–June 2008), "Scantegrity: End-to-End Voter Verifiable Optical-Scan Voting" (PDF), IEEE Security & Privacy (6:3): 40–46, archived from the original (PDF) on 2016-01-16, retrieved 2016-11-23

10. Khader, Dalia & Smyth, Ben & Ryan, Peter & Hao, Feng. (2012). A Fair and Robust Voting System by Broadcast. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI). 205.

11. Pathak, Prof & Suradkar, Amol & Kadam, Ajinkya & Ghodeswar, Akansha & Parde, Prashant. (2021). Blockchain Based E-Voting System. International Journal of Scientific Research in Science and Technology. 134-140. 10.32628/IJSRST2182120.

12. Baranov, Nikolay. (2022). From Distrust to Legitimization: The Difficult Path of Digital Electoral Technologies, an Evidence from Russia. RUDN Journal of Political Science. 24. 433-446. 10.22363/2313-1438-2022-24-3-433-446.

13. Essah, Richard & Senior, Isaac. (2023). A Bibliometric Overview of IoT-Based Digital Voting. Asian Journal of Computer Science and Information Technology. 15. 10-23. 10.9734/AJRCOS/2023/v15i3321.

14. Rura, Lauretha & Issac, Biju & Haldar, Manas. (2016). Implementation and Evaluation of Steganography Based Online Voting System. International Journal of Electronic Government Research. 12. 71-93. 10.4018/IJEGR.2016070105.

15. Bohli, Jens-Matthias & Müller-Quade, Jörn & Röhrich, Stefan. (2007). Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator. Cryptology ePrint Archive, Paper 2007/162

16. Rosenfeld, Meni. "Analysis of Hashrate-Based Double Spending." ArXiv abs/1402.2009 (2014): n. pag.

17. Ahubele, B.O., & Oghenekaro, L.U. (2022). Secured Electronic Voting System Using RSA Key Encapsulation Mechanism. European Journal of Electrical Engineering and Computer Science.

18. Tejedor-Romero, M., Orden, D., Marsá-Maestre, I., Junquera-Sánchez, J., & Giménez-Guzmán, J.M. (2021). Remote E-Voting System Based on Shamir's Secret Sharing Scheme. Electronics 10, no. 24: 3075. https://doi.org/10.3390/electronics10243075

19. Olanrewaju, Rashidah & Khan, Burhan & Kiah, Miss & Abdullah, Nor & Goh, Khang Wen. (2022). Decentralized Blockchain Network for Resisting Side-Channel Attacks in Mobility-Based IoT. Electronics. 11. 3982. 10.3390/electronics11233982.

20. Suralkar, S., Udasi, S., Gagnani, S., Tekwani, M., & Bhatia, M. (2019). E-Voting Using Blockchain With Biometric Authentication. International Journal of Research and Analytical Reviews 6 (1), 72-81

21. Cranor, Lorrie Faith and Ron Cytron. "Sensus: a security-conscious electronic polling system for the Internet." Proceedings of the Thirtieth Hawaii International Conference on System Sciences 3 (1997): 561-570 vol.3.