Secure Electronic Voting (E-voting) System Based on Blockchain on Various Platforms

K. Varaprasada Rao and Sandeep Kumar Panda

Abstract In today's world, online voting is becoming more popular. It has a lot of potential for lowering administrative expenses and increasing voter turnout. It eliminates the need for voters to travel to polling locations or print ballot papers because they can vote from anywhere with Internet criteria having been a struggle. In an E-voting system to provide security, we are using various cryptography techniques. In the existing E-voting system, all participants depend on a third-party entity for analysis and publishing of the voting results. To address this problem, many existing approaches use blockchain technology. These existing approaches face various problems like security issues and constraints on the number of voters. To address the two difficulties noted above, we offer a platform-agnostic, decentralized trust, and more secure E-voting mechanism that can be implemented on a platform-independent blockchain-based approach that supports smart contract execution.

Keywords E-voting · Blockchain · Security · Decentralization · Linkable ring signature · Paillier technology

1 Introduction

Election security is a concern of national security in any democracy. For more than a decade, the computer security industry has investigated the possibility of an E-voting system [1], to lower election costs while preserving and improving election security. Since the commencement of democratically electing candidates, the voting system has been based on pen and paper. A new election technology must replace the traditional pen and paper approach to eliminate fraud and make the voting process traceable and verifiable [2]. This is where blockchain technology comes into the

K. Varaprasada Rao (✉) · S. K. Panda
Department of Computer Science and Engineering, Faculty of Science and Technology, ICFAI Foundation for Higher Education, Hyderabad, India
e-mail: varaprasad.fst@ifheindia.org

S. K. Panda
e-mail: sandeeppanda@ifheindia.org

S. C. Satapathy et al. (eds.), *Computer Communication, Networking and IoT*,
Lecture Notes in Networks and Systems 459,
https://doi.org/10.1007/978-981-19-1976-3_18

picture. Blockchain provides distributed decentralized data sharing among authorized users in a network [3]. Blockchain consists of collections of blocks, each block connected with the previous block and form like a chain [4].

These technological elements use modern encryption to provide a level of security equal to or greater than any other database. Several blockchain-based E-voting systems have recently been built by utilizing the technology's inherent capabilities.

2 Background and Literature Review

When Satoshi Nakamoto invented the first cryptocurrency, Bitcoin, in 2008, he introduced blockchain technology. The bitcoin blockchain technology combines a decentralized public ledger with a proof-of-work (PoW)-based stochastic consensus system, as well as financial incentives, to create a completely ordered sequence of blocks known as the blockchain. Nick Szabo coined the term "smart contracts" in the 1990s, describing them as "a set of promises, stated in digital form, including protocols within which the parties fulfill on these promises" [5]. A smart contract is a code that expresses logic, and it can operate as an unconditionally trusted third party [6]. It cannot be changed once it has been written, and all network members must check all stages. The beauty of smart contracts is that anyone with the ability to set up a blockchain node to confirm the results.

2.1 Blockchain Architecture's Basic Elements

The blockchain provides various basic components. Figure 1 describes the major components of blockchain are as follows.

Node: Node is a user or computer in the blockchain network.
Transaction: It's a unit of records in the blockchain network.
Block: It's a collection of data that are used to complete network transactions and distributed to all nodes.
Miners: in blockchain miners play a very important role to approve the transactions in the network [7].
Chain: A sequence of blocks in a specific order.
Consensus: A group of instructions that work together to complete blockchain procedures.

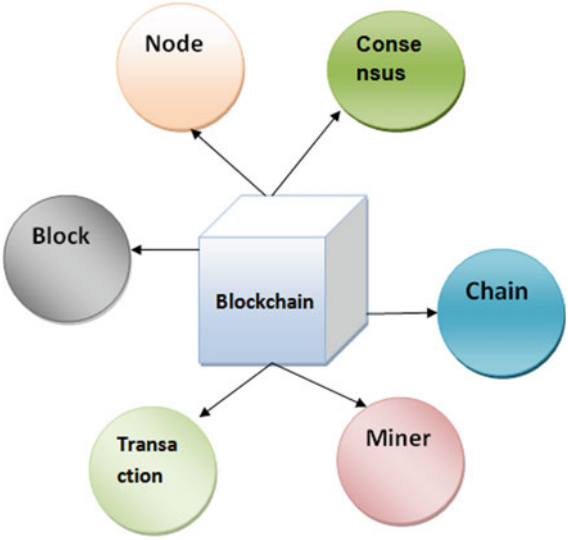

Fig. 1 Blockchain components

2.2 *Blockchain Architecture's Crucial Characteristics*

For all sectors that use blockchain, the architecture has numerous advantages. As shown in Fig. 2, there is a range of embedded characteristics:

Cryptography: It is used to provide security to each transaction in the blockchain network. Immutability: No changes or deletions can be made to blockchain records [2, 4, 8].
Decentralization: All participants of the blockchain network may have access to the complete distributed database. As seen in the core process, a consensus method enables system control [9–12].
Anonymity: Blockchain provides an address to every participant in the network [13].

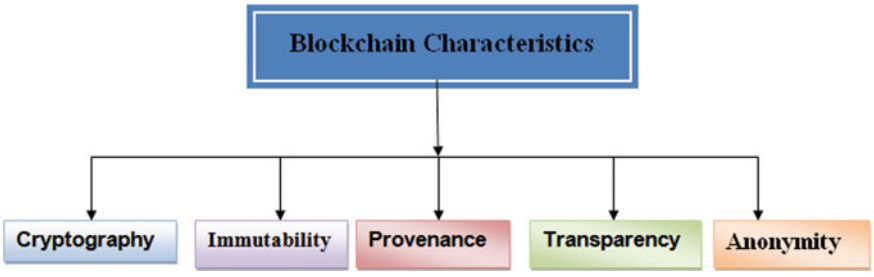

Fig. 2 Blockchain characteristics

Transparency: It means that the data in the network cannot be manipulated. It is not possible since erasing the blockchain network would need enormous computational resources.

2.3 Review of Related Literature

In recent years, several publications have been published that have highlighted various security and privacy issues in blockchain-based E-voting systems. Here, we present a few blockchain-based electronic voting techniques below:

Shahzad et al. [14] were proposed BSJC proof of completeness as a trustworthy electronic voting technique. They utilized a process model to describe the overall structure of the system. This approach addresses various security and privacy issues but this approach is capable of the small-scale election. However, a slew of other issues has been raised. The polling procedure may be delayed if the block is generated and sealed on a big scale [15–19].

Yi [20] presented the BES approach for proving security in an E-voting system in a P2P blockchain-based network. To prevent vote tampering, distributed ledger could be used. On UNIX systems in a peer-to-peer network, the system was tested and designed. Counter-measurement assaults are a key difficulty in this strategy. A distributed procedure, such as the use of secure multipart computers, may be able to solve the problem. However, if the computation function is sophisticated, and there are too many participants; computing costs become increasingly substantial and possibly prohibitive [21].

3 Deployment of the System

Our voting mechanism is compatible with any blockchain-based platform that supports smart contracts and achieves the same level of security [4, 15]. Other factors that may influence platform selection include vote latency and flexibility requirements [3]. In our scenario, we use the Hyperledger Fabric blockchain technology, which is based on Byzantine Fault Tolerance (BFT), to deploy our voting system in a real-world setting. Our approach supports the four requirements listed below.

1. **Encode and decode messages**
   We need to encrypt the candidate ID before voting begins so that it is suitable for the vote count [22].
2. **Our voting mechanism does not depend on a centralized trustworthy entity to count polls and announce results**
   The existing E-voting systems rely on a centralized third party to evaluate the polls and produce the results. In this approach, we use a blockchain decentralized approach to evaluate the ballots and produce the results [23].

3. **Our voting technology is platform agnostic and offers extensive security protections**

   Our voting method is secure because it uses cryptographic approaches offered by our voting protocol; as a result, this approach is used in any smart contract-supported blockchain-based platform [24]. In this approach, Paillier technology is used to conduct the polling and provide privacy without revealing voter information, which helps us meet our goal of offering total security [25].

   Generate Key: by using this function the voting administrator a secret key for every voter based on their public key [26].
   Encryption: It is necessary to encrypt the plaintext ballot. This function is used to encrypt the voter polls during the blockchain network [27].
   Decryption: By using this function, the voting administrator decrypts the votes polled by the voters and publishes the results.
   Proof-of-work: This function is used to generate proof-of-work that indicates only authorized voter can encrypt their vote.
   Decryption validates proof-of-work: By using this function, the voting administrator generates key-value pair to decrypt the votes and publish the polling results [20].

   This function uses a linkable ring signature method to validate the voters and decrypt the votes, even if the owner of the ballot cannot be traced.
   Linkable ring signature (LRS): LRS is used to preserve voters' privacy. By using this method, we use short linkable ring signature (SLRS), which eliminates constraints on the voting system. This LRS approach contains the following features: (1) check whether the voter is a valid user or not, (2) voters can verify whether their votes are polled by blockchain network or not, (3) to provide scalability maintain signature size, and (4) avoid double/duplicate voting. We use the tuple function in our voting system (Setup, KeyGen, Sign, Verify, Link).

4. **Our voting platform is adaptable and expandable**: We offer two optimized SLRS key accumulation methods that allow voting scalability and achieve latency in large-scale voting.

4 Voting Protocol

Figure 3 describes the architecture of the E-voting system; the voting system comprises various voters, vote administrator (VA), front-end smart contract server (SCA), and numerous smart contract validation nodes. A smart contract validation node's job is to accurately simulate the execution of smart contract codes. The validation nodes for practical voting could be controlled by many stockholders, implying that all ballots on the blockchain have been confirmed by various stockholders.

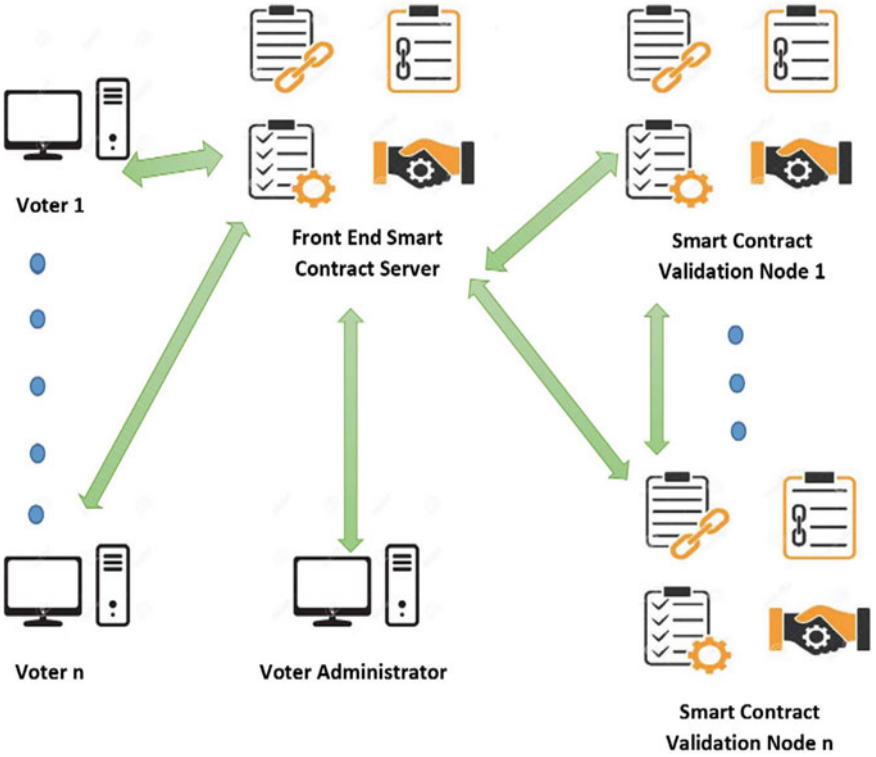

Fig. 3 Blockchain-based independent E-voting system

4.1 Voting Process Entities

In our voting system (shown in Fig. 3), there should be four entities participating, with the following details:

Smart Contract Administrator (SCA): **SCA can access the blockchain platform and apply or terminate smart contracts**. The membership service in Hyperledger Fabric authorizes this account, and the authority to apply or dismiss the smart contract is provided. In this approach, we required at least one SCA to install the voting smart contract.
Voter Administrator (VA): The VA manages the votes by establishing polling settings, initiating the counting and results in publication phases. SLRS is used to prevent administrators from associating ballots to users, although Hyperledger has underlying means for authenticating users.
Smart contract: A smart contract's job is to (1) store encrypted ballots. (2) Check the ballots for legitimacy. (3) Count the ballots that have been encrypted. (4) Verify that the vote results are valid. (5) Make the vote results public and gives a platform for people to check the results of the election.

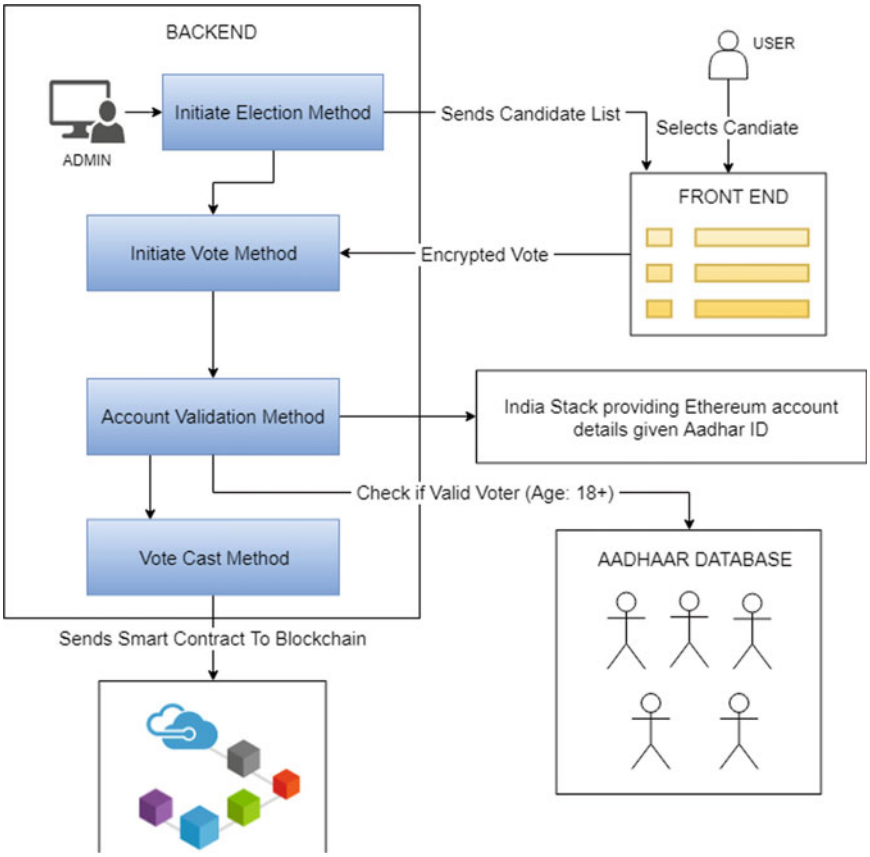

Fig. 4 Blockchain-based E-voting process

Voter: Voters are those who can exercise their right to vote. Before anyone can vote, individuals must first register with the voting system.

Figure 4 describe the E-voting system process using blockchain.

4.2 Registration of Voters

The user must register his identification using this voting mechanism. The registration information could include: (1) Email Id and password, (2) voter Id and password, (3) an administrator-sent invitation URL with the desired password. After passing the savvy agreement's personality check, the client can sign in with the ideal secret key to download the SLRS param and the executive public key, then, calls the KeyGen() function to produce the SLRS key pair (); then the user transfers the public key to

the ballet. If his SLRS public key is acknowledged, the shrewd agreement puts his public key on the blockchain, finishing his/her enrollment step.

5 Conclusions

E-voting is a method of casting and tallying votes that use computers. It is a time- and cost-effective method of conducting a voting operation, with the advantages of large amounts of data in real time and a high level of security. It takes out the requirement for citizens to go to surveying areas or print voting form papers since they can cast a ballot from any place with Internet standards that have been a battle. In the existing E-voting system, all participants depend on a third-party entity for analysis and publishing of the voting results. To resolve the issue that the current blockchain casting a ballot framework needs thorough security highlights, and most of them are stage subordinate, we proposed a blockchain-based democratic framework in which electors' protection and casting a ballot accuracy are ensured by homomorphic encryption, linkable ring marks, and proof-of-work between the citizen and blockchain. Our approach eliminates security attacks and eliminates the constraints on the number of voters and candidates supported during polling and provides secure architecture. Our voting system's correctness and security are examined. This approach provides that our voting method performs well even in large-scale voting.

References

1. Alaya B, Laouamer L, Msilini N (2020) Homomorphic encryption systems statement: trends and challenges. Comput Sci Rev 36:100235
2. Murala DK, Panda SK, Swain SK (2019) A novel hybrid approach for providing data security and privacy from malicious attacks in the cloud environment. J Adv Res Dyn Control Syst 11(06-Special Issue)
3. Liu Y, Wang Q (2017) An E-voting protocol based on blockchain. IACR CryptolEprint Arch 1043, Racsko P (2019) Blockchain, and democracy. Soc Econ 41:353–369
4. Murala DK, Panda SK, Swain SK (2019) A survey on cloud computing security and privacy issues and challenges. J Adv Res Dyn Control Syst 11(06-Special Issue)
5. Szabo N (2017) Formalizing and securing relationships on public networks. First Monday 1997, 2, 9. The Economist. EIU Democracy Index. 2017. Available online: https://infographics.economist.com/2018/DemocracyIndex/. Accessed on 18 Jan 2020
6. Fernández-Caramés TM, Fraga-Lamas P (2020) Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. IEEE Access 8:21091–21116
7. Zhao Z, Chan T-HH (2016) How to vote privately using Bitcoin. In: Qing S, Okamoto E, Kim K, Liu D (eds) ICICS 2015, vol 9543. LNCS. Springer, Cham, pp 82–96
8. Murala DK, Panda SK, Swain SK (2019) Secure dynamic groups data sharing with modified revocable attribute-based encryption in cloud. Int J Recent Technol Eng (IJRTE) 8(4), Nov 2019. ISSN: 2277-3878
9. Yu B et al (2018) Platform-independent secure blockchain-based voting system. Cryptology ePrint Archive, change me (2018). http://eprint.iacr.org/201

10. Panda SK, Satapathy SC (2021) An investigation into smart contract deployment on Ethereum platform using Web3.js and solidity using blockchain. In: Bhateja V, Satapathy SC, Travieso-González CM, Aradhya VNM (eds) Data engineering and intelligent computing. Advances in intelligent systems and computing, vol 1. Springer, Singapore. https://doi.org/10.1007/978-981-16-0171-2_52
11. Panda SK, Rao DC, Satapathy SC (2021) An investigation into the usability of blockchain technology in internet of things. In: Bhateja V, Satapathy SC, Travieso-González CM, Aradhya VNM (eds) Data engineering and intelligent computing. Advances in intelligent systems and computing, vol 1. Springer, Singapore. https://doi.org/10.1007/978-981-16-0171-2_53
12. Sathya AR, Panda SK, Hanumanthakari S (2021) Enabling smart education system using blockchain technology. In: Panda SK, Jena AK, Swain SK, Satapathy SC (eds) Blockchain technology: applications and challenges. Intelligent systems reference library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_10
13. Gao S, Zheng D, Guo R, Jing C, Hu C (2019) An anti-quantum E-voting protocol in blockchain with audit function. IEEE Access 7:115304–115316
14. Shahzad B, Crowcroft J (2019) Trustworthy electronic voting using adjusted blockchain technology. IEEE Access 7:24477–24488
15. Lai WJ, Hsieh YC, Hsueh CW, Wu JL (2018) Date: a decentralized, anonymous, and transparent e-voting system. In: Proceedings of the 2018 1st IEEE international conference on hot information-centric networking (HotICN), Shenzhen, China, 15–17 Aug 2018
16. Jena AK, Dash SP (2021) Blockchain technology: introduction, applications, challenges. In: Panda SK, Jena AK, Swain SK, Satapathy SC (eds) Blockchain technology: applications and challenges. Intelligent systems reference library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_1
17. Lokre SS, Naman V, Priya S, Panda SK (2021) Gun tracking system using blockchain technology. In: Panda SK, Jena AK, Swain SK, Satapathy SC (eds) Blockchain technology: applications and challenges. Intelligent systems reference library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_16
18. Panda SK, Mohammad GB, Nandan Mohanty S, Sahoo S (2021) Smart contract-based land registry system to reduce frauds and time delay. Secur Priv e172. https://doi.org/10.1002/spy2.172
19. Panda SK, Satapathy SC (2021) Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers. Pers Ubiquit Comput. https://doi.org/10.1007/s00779-021-01588-3
20. Yi H (2019) Securing e-voting based on blockchain in the P2P network. EURASIP J Wirel Commun Netw
21. Hopwood D, Bowe S, Hornby T, Wilcox N (2016) Zcash protocol specification. Technical report, 2016–1.10. Zerocoin Electric Coin C
22. Tivi Voting. https://tivi.io/. Accessed 24 June 2017
23. Torra V (2019) Random dictatorship for privacy-preserving social choice. Int J Inf Secure 19:537–543
24. Tsang PP, Au MH, Liu JK, Susilo W, Wong DS (2010) A suite of non-pairing IDbased threshold ring signature schemes with different levels of anonymity (extended abstract). In: Heng S-H, Kurosawa K (eds) ProvSec 2010, vol 6402. LNCS. Springer, Heidelberg, pp 166–183
25. Jafar U, Ab Aziz MJ, Shukur Z, Blockchain for electronic voting system—review and open research challenges
26. Wood G (2014) Ethereum: a secure decentralized generalized transaction ledger. Ethereum Proj Yellow Pap 151:1–32
27. Yaga D, Mell P, Roby N, Scarfone K (2020) Blockchain technology overview. arXiv 2019. arXiv:1906.11078. The Economist. EIU Democracy Index, 2017. Available online: https://infographics.economist.com/2018/DemocracyIndex/. Accessed on 18 Jan 2020