Proceedings of the 7th International Conference on Trends in Electronics and Informatics (ICOEI 2023)
IEEE Xplore Part Number: CFP23J32-ART; ISBN: 979-8-3503-9728-4

Blockchain based e-voting system

Aarti C. Naik
Electronics and Computer Science
Shree LR Tiwari College of Engineering
Mumbai, India
aartinaik72@gmail.com

Ankit Mukesh Prajapati
Electronics and Computer Science
Shree LR Tiwari College of Engineering
Mumbai, India
ankit.m.prajapati@slrtce.in

Shivam Nilesh Pandey
Electronics and Computer Science
Shree LR Tiwari College of Engineering
Mumbai, India
shivam.n.pandey@slrtce.in

Ashish Chandraprakash Mishra
Electronics and Computer Science
Shree LR Tiwari College of Engineering
Mumbai, India
ashish.c.mishra@slrtce.in

2023 7th International Conference on Trends in Electronics and Informatics (ICOEI) | 979-8-3503-9728-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICOEI56765.2023.10125883

***Abstract*—Voting is an important aspect for democratic countries. It is a process of expressing the choice or opinion of people on a particular matter. Voting can take place in a variety of contexts, such as in national or local elections, within organizations or associations, or in public surveys. Voting is a fundamental right in many democratic societies, and it allows citizens to participate in the governance of their country or community by selecting representatives or making decisions on important issues. It is an important way for people to have a say in the policies and laws that affect their lives, and to hold those in power accountable. Voting decide which candidate is capable and also decides the future of that country therefore voting should be as transparent as possible and should have high level of security. But the existing voting system have some flaws like Security concerns, Centralization, Limited Audibility etc. Due to this inclination, voters is decreasing towards voting and voting percentage decreases. There is a solution to these issues is strong requirement of a system which has High level of security, Transparency, Decentralization, etc.**

***Keywords*—blockchain, e-voting, security, consensus, ballot**

I. Introduction

Voting plays a significant role in democratic countries. By participating in elections, citizens can select their government through voting. A safe and transparent voting mechanism must be in place in order to guarantee the accuracy and integrity of the election results.[1] This approach must guarantee voter privacy while also promoting openness and accountability during the electoral process.[1] This is specifically crucial in nations with large-scale elections since human vote counting consume more time and is prone to mistakes. The adoption of a safe and open e-voting system can prevent fraudulent activities and guarantee that the election results fairly represent the preferences of the electorate. [2]

II. Literature Review

Voting systems built on blockchains have also attracted interest with its potential means of enhancing voting process security and transparency. Blockchain technology makes it possible to share data in a secure, transparent manner and does away with the necessity for a central authority to supervise elections.[3] The decentralised and impenetrable properties of blockchain can help to ensure that the voting process's integrity is upheld and that the outcomes cannot be tampered with.[4] Additionally, as votes can be recorded and tallied in real-time without the need for middlemen, blockchain-based electronic voting systems can facilitate a more streamlined and effective procedure.[4] Yes, there have been elections that have used blockchain technology in some capacity. Blockchain technology offers several potential benefits for elections, such as increased transparency, immutability of records, and enhanced security.[7]

As Table 1 shows, blockchain-based solutions have been deployed for corporate, community, city, and national voting, For example In 2018, West Virginia successfully conducted a primary election using blockchain technology. This was a significant milestone for the state and the country as a whole, as it demonstrated the potential for secure and transparent electronic voting systems.[14] West Virginia primary blockchain elections represent a positive step forward for democracy and technology, and we should celebrate this achievement as we continue to explore new ways to ensure fair and transparent elections.

Furthermore, many Moscow residents don't have time to attend face-to-face meetings. So, meetings have moved to the Digital Home online platform. In December 2017, residents began using a blockchain to vote, and the results were publicly auditable.[6] City officials believed that neighbors should have a convenient environment in which to influence their living conditions. The officials also believed that a blockchain would increase trust between citizens and government. Each question discussed by the community is moved to blockchain based election system.[6] After the polling is finished, the results are provided. To assess blockchain based election system trustworthiness, the city of Moscow commissioned the accounting firm PwC to conduct an audit. PwC looked at the possibility that the polling's outcome could be manipulated by internal employees and external attacks. The audit found no reason to be concerned for polls that involved more than 300,000 votes. [6]

Setting	Context	Remark
West Virginia primary elections (2018)	The state of West Virginia used a blockchain-based mobile voting platform called Voatz in its primary elections. This platform allowed military personnel stationed overseas to cast their votes using their smartphones.	The successful use of blockchain technology in the West Virginia primary elections is still a significant achievement and demonstrates the potential for technology to improve the voting process. It is important to continue to address and mitigate any potential risks and challenges associated with electronic voting systems, while also exploring new ways to enhance the security and accessibility of our democratic processes.
Moscow city council elections (2019)	The city of Moscow, Russia, used a blockchain-based system called "Active Citizen" to allow residents to cast non-binding votes on various city issues.	The Moscow City Election Commission used a blockchain-based system called "Transparent Elections" to record and store the results of the electronic voting pilot project. the use of blockchain technology in the Moscow city council elections was a significant step forward in terms of ensuring transparency and accuracy
Utah Republican Party primary elections (2020)	The Utah Republican Party used a blockchain-based mobile voting platform called Voatz in its primary elections. This platform allowed voters with disabilities, military personnel, and overseas voters to cast their votes using their smartphones.	the Utah County Republican Party conducted a pilot project in 2019 that utilized blockchain technology for mobile voting in their local elections. This pilot project was considered a success, and the Utah State Legislature passed a bill in 2020 that allowed certain counties to conduct mobile voting using blockchain technology in future elections.

TABLE I
BLOCKCHAIN-BASED SOLUTIONS DEPLOYED FOR E-VOTING.

III. IMPLEMETATION OF E-VOTING USING BLOCKCHAIN

In the blockchain, data is recorded in a distributed ledger that cannot be altered or erased and is an append-only data structure.8 The ledger is now impervious to change.[12] Assuring immutability is achieved by chaining the blocks so that each block has a hash that is a function of the previous block and, by induction, the entire prior chain. There are two distinct blockchain types, each with varying degrees of limitations on who can read and write blocks. [11] Everyone in the world can read and write on a public blockchain. Popular with cryptocurrency users is this variety. [11]

The ability to read or interact with a blockchain is limited with a private blockchain. In permissioned blockchains since only certain nodes are allowed to communicate with them. Blockchain offers a platform for creating distributed and immutable apps, or smart contracts, in addition to cryptocurrencies. [8]

Smart contracts are programmed agreements that go into effect automatically when certain criteria are met. Smart contracts are used as a legally enforceable agreement between parties, just like traditional written contracts. [5] Smart contracts eliminate the need for a middleman by automating transactions and enabling direct, automatic agreement-making between parties. Comparing smart contracts to traditional written contracts, cost savings, increased efficiency, and risk reduction are three major advantages. [5]

Smart contracts reinvent trust since they are readily verifiable and accessible to all blockchain users. In this paper, we define our smart contract-based electronic voting system. [5]

A. Problems With Public Blockchain

Although blockchain technology has a lot of potential benefits, there are also a lot of problems and restrictions that need to be worked out. [13] The primary issues with blockchain are as follows:

1) Scalability: Scalability is one of the primary issues with blockchain. The time and resources needed to validate transactions and maintain the blockchain grow as the blockchain's size rises. It is less practicable to utilise in high-transaction applications because of the potential for slower transaction times and higher transaction costs.[8]

2) Energy consumption: The quantity of energy needed to maintain blockchain is another significant issue. Several blockchains use the proof-of-work consensus algorithm, which necessitates a substantial amount of computer power and high energy usage. This has prompted questions about how blockchain technology would affect the environment. [10]

3) Interoperability: The capacity of several blockchains to connect and communicate with one another is referred to as interoperability. Currently, there is no standardized way for different blockchains to interoperate, which makes it difficult for different blockchain-based applications to work together. [13] This limits the potential benefits of blockchain technology and makes it harder to develop new applications that can leverage the advantages of different blockchains. [13]

4) Security: While blockchain is designed to be secure, it is not immune to attacks. There have been instances of 51% attacks, where a single entity gains control of more than half of the computing power in a blockchain network, enabling them to manipulate the blockchain. Additionally, smart contracts, which are used to automate the execution of transactions in some blockchain-based applications, can contain bugs or vulnerabilities that can be exploited by attackers. [10]

5) Regulatory challenges: The decentralized nature of blockchain makes it difficult for governments and regulators to

monitor and control the use of blockchain-based applications. This can create regulatory challenges. [13]

B. Private Over Public Blockchain

Private blockchain technology has several advantages over public blockchain technology when it comes to e-voting.

1) Security: Private blockchains have more control over the network and who has access to it. This makes them more secure compared to public blockchains, where anyone can participate in the network. [9]

2) Privacy: Private blockchains can be designed to ensure that the identity of voters is kept confidential, which is not possible in public blockchains where transactions are visible to everyone. [9]

3) Scalability: Private blockchains can handle a large number of transactions, making them suitable for large-scale e-voting systems. [9]

4) Speed: Transactions on private blockchains can be processed much faster than on public blockchains, which is important for real-time election results. [9]

5) Cost-effective: Private blockchains are more cost-effective than public blockchains because they do not require the resources to maintain a large network of nodes. [9]

6) Compliance: Private blockchains can be designed to meet specific regulatory requirements, making them suitable for use in countries where there are strict laws regarding the conduct of elections. [9]

Overall, the use of private blockchain technology in e-voting can provide a more secure, transparent, and accessible voting system that can address many of the gaps and challenges associated with Public blockchain. [9]

IV. Methodology

The only way to interact with ledger data on the blockchain is through a smart contract. When e-voting is implemented using blockchain, the smart contract will contain a number of features to make voting safe, transparent, and client-side compatible.

- Transfer Vote
- Get Election State
- Dispose Election

before begining of election, there should be a voter and candidate. Both voter and candidate will have there account. user have to provide its basic as well as additional details (adhar number, pan number, state, country etc). so that we can define criteria for election.

Election will created by a trusted admin. An Election will have three phase Upcoming, Current and Past election.

A. Upcoming Phase

The first phase of the election is coming up. All users must apply to be candidates in this phase if they choose to run in the election. The user's cryptographic ID, local ID, and election ID in which he or she wants to run as a candidate are requirements for this phase.

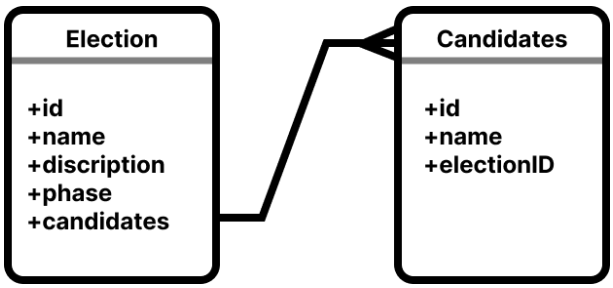

Fig. 1. Election ER Diagram

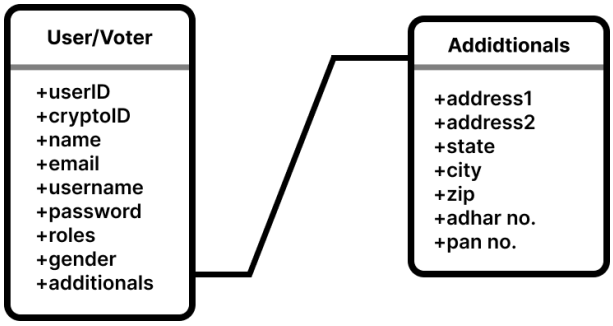

Fig. 2. User ER Diagram

B. Current Phase

The voters will select their candidate throughout the current phase. No user registration or candidate participation in a specific election will be permitted during this phase. Voting in this election will require a voter's cryptographic, local, and candidate's cryptographic and local ids in addition to an election id. With the voter-provided specifications, the current phase of the election will carry out the smart contract's Transfer Vote function and generate a blockchain transaction. The blockchain ledger will contain this transaction after it has been further confirmed.

C. Past Phase

Election results are calculated in the past phase, candidate votes are tallied, and delete transactions are initiated. Calculated results were sent back to the server for local database storage.

Fig 1 shows Election Entity, Election entity's primary key is its ID, and its description will provide further information about the election, like its name and phase (current, past and upcoming phase). Elections include a list of candidates who are competing, along with other information. A candidate has an election-ID, crypto-ID, and ID as the primary key.

Fig 2 shows ER Diagram of User. Each voter or candidate is a user in this network, and as such, they each have some related property. Name, email, username, password, gender, role, and crypto-ID are a user's primary information. Address, Adhar Number, Pan Number, City, State, and Zip are additional information that is used to construct election criteria so that only those voters who meet those criteria are able to vote in an election.

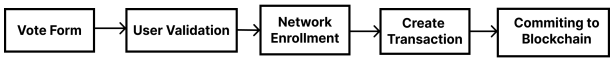

Fig. 3. Transactions Flow

V. Transferring vote

In current phase of election user must have to be logged-in in system to give vote to candidate. Voter will use crypto-ID and user-ID to select candidate. Block diagram of transferring vote is shown in Fig 3.

A. Vote Form

A form in which voter must have to fill the election ID, select a candidate according to his choice and enter his credentials for authentication.

B. User Validation

This request will be accepted by server with voters credentials. voter will be authenticated with its credentials provided with database credentials. On successful authentication, Voter have to enter an 6 digit OTP sent on his registered mobile number or email address on this same vote form.

C. User Enrollment

After user validation request is passed to blockchain network gateway client to enroll user with certificate Authority to obtain user's cryptographic information. till now a user is only authenticated to access its private informations like profile page, apply for candidate in election, give vote in election, but after network enrollment user is eligible to interact with blockchain.

D. Create Transaction

On successful enrollment of user, gateway client will raise transaction with user's private key to sign transaction and user's cryptographic ID will passed in smart contract function as a parameter along with selected candidate cryptographic ID, user-ID and election-ID.

E. Commiting to Blockchain

After successful transaction creation, a transaction id will be returned to user. the transaction will be verified and validated by peers and then added to blockchain and vote transfer cycle will complete. the vote counts are immediately reflect on client side. with the transaction id a user can verify his vote.

VI. Conclusion

Comparing the use of an e-voting system with a private blockchain to one that uses an EVM and a public blockchain, there are a number of potential advantages. Private blockchain reduces the possibility of unauthorised access, fraud, and manipulation with the voting process by restricting access to approved participants and confirming transactions through pre-selected validators. Moreover, private blockchain enables more effective and economical transaction processing, leading to quicker and more trustworthy voting outcomes.

A private blockchain can be modified to fit the unique requirements of the electronic voting system, offering a solution that is created to satisfy the needs of the organisation. Also, private blockchain lessens the possibility of network delays and congestion, which may be a major problem with public blockchain systems. In a private blockchain, there is less chance of fraud or malevolent conduct because the institution or organisation that owns the network has more control over who may participate and how transactions are validated.

In conclusion, integrating a private blockchain into an e-voting system can offer improved security, efficiency, customizability, less network congestion, and better control, making it a practical option for businesses and institutions wishing to establish a trusted e-voting system.

References

[1] Orhan Cetinkaya and Deniz Cetinkaya. "Verification and validation issues in electronic voting". In: *Electronic journal of e-government* 5.2 (2007), pp117–126.

[2] J Alex Halderman and Vanessa Teague. "The New South Wales iVote system: Security failures and verification flaws in a live online election". In: (2015), pp. 35–53.

[3] Rifa Hanifatunnisa and Budi Rahardjo. "Blockchain based e-voting recording system design". In: (2017), pp. 1–6.

[4] Fridrik Hjalmarsson, Gunnlaugur K Hreiarsson, and Mohammad Hamdaqa. "Blockchain-based e-voting system". In: (2018), pp. 983–986.

[5] Bhabendu Kumar Mohanta, Soumyashree S Panda, and Debasish Jena. "An overview of smart contract and use cases in blockchain technology". In: *2018 9th international conference on computing, communication and networking technologies (ICCCNT)*. IEEE. 2018, pp. 1–4.

[6] "Moscow's Blockchain Voting Platform Adds Service for High-Rise Neighbors". In: (). URL: https://www.coindesk.com/moscows-blockchain-voting-platform-adds-service-for-high-rise-neighbors.

[7] Ryan Osgood. "The future of democracy: Blockchain voting". In: *COMP116: Information security* (), pp. 1–21.

[8] Suporn Pongnumkul, Chaiyaphum Siripanpornchana, and Suttipong Thajchayapong. "Performance analysis of private blockchain platforms in varying workloads". In: *2017 26th International Conference on Computer Communication and Networks (ICCCN)*. IEEE. 2017, pp. 1–6.

[9] Chang-Hyun Roh and Im-Yeong Lee. "A study on electronic voting system using private blockchain". In: *Journal of Information Processing Systems* 16.2 (2020), pp. 421–434.

[10] Johannes Sedlmeir et al. "The energy consumption of blockchain technology: Beyond myth". In: *Business & Information Systems Engineering* 62.6 (2020), pp. 599–608.

[11] Harsh Sheth and Janvi Dattani. "Overview of blockchain technology". In: *Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146* (2019).

[12] Bikramaditya Singhal et al. "How blockchain works". In: *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions* (2018), pp. 31–148.

[13] Toqeer Ali Syed et al. "A comparative analysis of blockchain architecture and its applications: Problems and recommendations". In: *IEEE access* 7 (2019), pp. 176838–176869.

[14] "west virginia blockchain voting". In: (). URL: https://slate.com/technology/2019/07/west-virginia-blockchain-voting-voatz.html.