Advancements in Blockchain Based Architecturefor E-Voting System

Prof. Sumit Shevtekar[1], Radhey Saykar[2]

[1]Assistant Professor Department of Computer Engineering, Pune Institute of Computer Technology, Pune, India.

[2]Student, Department of Computer Engineering, Pune Institute of Computer TechnologyPune, India

Abstract

Blockchain based E-voting system can be revolution- ary in terms of security and tamper proof, transparent elections and hence empower the democracy. Blockchain E-voting is already implemented at organisational level. But at state/national level it faces challenges such as privacy, stability, latency etc. To counter them we require advanced implementation techniques from multiple disciplines. These techniques are 2-layer-solution, sharding for scalability issue, optimizing consensus algorithm and off-chain transaction for reducing latency, zero knowledge proof, using multiple protocols for user privacy etc. General architecture of blockchain is explained in details which combines election creation, voter registration, voter transaction, tallying the results and vote verification. We have discussed how integrating E-voting with blockchain document verification system can be benificial. It is complicated to implement at state, national level and need additional research and implementation to make blockchain E- voting acceptable in elections across the world. Through research and innovation we can make blockchain voting mainstream.

Keyword*:* E-Voting, Blockchain, Electronic Voting, Architecture, Limitations, Smart Contracts, Applications

I. INTRODUCTION

The foundation of any thriving democracy lies in its ability to conduct free, fair, and transparent elections. However, as the digital age ushers in unprecedented opportunities, it also introduces new challenges to the integrity of electoral processes. Traditional voting mechanisms, relying heavily on paper-based ballots and manual counting, face growing concerns over issues such as voter impersonation, miscounts, logistical inefficiencies and security. In response to these challenges, blockchain technology has emerged as a potential game-changer in the realm of e-voting.

A. Electronic voting

Electronic voting (E-voting) is modern voting system in which voting procedure is conducted using electronic means and IT services to conduct voting procedures. General struc- ture of E-voting contains these parts: registration, authen- tication and authorization, vote casting, vote counting and vote verification. E-voting provides acceleration of results processing, prevention of fraud, by reducing human involve- ment, increase involvement in democratic process, reduction of cost. Electronic voting machines are considered vulnerable to security attacks by experts. These machines can be sabotaged by intruder who has physical access to the machine and potentially manipulate data of votes casted as well as steal voters private data.

B. Essential requirements from an E-voting

Every E-voting system has to comply with following essen-tial requirement to be used in national election.

1) Voter should be able to vote in complete freedom andvoter should not be forced to vote.
2) No one should be able to know voters identity and hisvote and secrecy should be maintained.
3) Voter should be able to correctly verify that his vote hascounted and it was correctly counted with clear proof.
4) E-voting system should be tamper-proof, i.e. no oneshould be able to change vote of a voter.
5) Anyone should be able to tally votes and should beallowed to do so.
6) Only valid and registered voter should be allowed tovote.
7) voting system should be accessible to every valid voter.Every valid voter should be able to avail the voting right.

C. Necessity of blockchain for E-voting

A blockchain is a immutable, distributed, incontrovertible, public ledger. Blockchain is based on advanced cryptography. This cryptographic provides security better than databases. Main features of blockchain are:

1) No single point of failure: The ledger exists in many different locations. So system and data is always avail- able.
2) Authentication of user is done by distributed system.
3) Every block contains reference to previous block and these blocks are chained together in chronological order.This chain is immutable because of the encryption and because one change in a block corrupts entire chain.
4) Through consensus majority nodes in network decide whether new block should be permanently appended or not

That is why blockchain technology is considered ideal byexperts to create electronic voting system. The strongest potential for BEV is in organisational contexts. Indeed, they have already been used for the internal elections of political parties in Denmark and shareholder votes in Estonia.

D. *Limitations in blockchain E-voting*

Implementing BEV at large scale is complicated and it has other cons. Some of the key technical limitations of blockchainvoting include:

1) **Scalability**:Blockchain networks, especially public ones, face challenges in handling a large volume of trans-actions simultaneously. As the number of voters and transactions increases, it can lead to network congestion and slower processing times..
2) **Latency**: The time required to validate and record a transaction on the blockchain, known as block con- firmation time, can vary depending on the blockchain platform.
3) **Privacy Concerns**: While blockchain transactions are pseudonymous (linked to cryptographic addresses), they are also transparent and immutable. This transparency can potentially compromise voter privacy, as all trans- actions are visible on the ledger. Efforts must be made to implement

cryptographic techniques to protect voter identities.

4) **Voter Authentication**: Ensuring that voters are who they claim to be in an online environment can be challenging. Implementing secure and user-friendly authentication methods is crucial to prevent impersonation and ensure the integrity of the voting process.
5) **User Experience**: Designing a user-friendly interface and providing clear instructions is essential to ensure widespread adoption.
6) **Security Risks**: While blockchain itself is considered secure, vulnerabilities can arise from the surrounding ecosystem, such as weaknesses in smart contracts, flaws in the implementation of the voting system, or attackson the network infrastructure.
7) **Environmental effects**: Blockchain transactions results in high carbon emission because of high energy con- sumption.
8) **Cost**: Running a blockchain network, especially a public one, can be costly. This includes costs associated with transaction fees, network maintenance, and infrastruc- ture.
9) **Regulatory Compliance**: Blockchain-based voting sys- tems may need to comply with legal and regulatory frameworks, which can vary by jurisdiction. Ensuring compliance with existing election laws and regulationsis a complex task.
10) **Risk of Forks**: In the event of a blockchain fork (a split in the blockchain's history), there could be uncertainty about which chain represents the true and valid history. This could potentially lead to disputes in the validity of votes.
11) **Accessibility and Inclusivity**: Not all voters may have equal access to the technology required to participate in a blockchain-based voting system.

II. METHODOLOGY

By casting votes as transactions, tallies of the votes can be stored on blockchain and keeps track of the tallies of the votes. This way, everyone can agree on the final count because they can count the votes themselves, and because of the blockchain audit trail, they can verify that no votes were changed or removed, and no illegitimate votes were added.

A. Addressing Limitations in blockchain E-voting

Here are strategies to address the key limitations:

1) Scalability:

- **Use Layer 2 Solutions**: Implement Layer 2 so- lutions like state channels or sidechains to handle a large volume of transactions off-chain while still benefiting from the security of the main blockchain.
- **Sharding**: Utilize sharding techniques to partition the blockchain network into smaller, manageable parts, each capable of processing its own set of transactions.

2) Latency:

- **Consensus Algorithm Optimization**: Choose con- sensus algorithms (e.g., Proof of Stake) that offer faster block confirmation times. This reduces the time it takes for a transaction to be validated.
- **Off-chain Transactions**: Consider using off-chain transactions for certain operations that do not require the same level of security as on-chain trans- actions.

3) Privacy Concerns:

- **Zero-Knowledge Proofs**: Implement cryptographic techniques like zero-knowledge proofs to allow for private transactions while still ensuring the integrity of the voting process.
- **Mixing Services**: Integrate mixing services or pro- tocols that allow users to combine their

transactionswith others to increase privacy.

4) Voter Authentication:

- **Biometric Verification**: Incorporate biometric au- thentication methods, such as fingerprint or facial recognition, to enhance voter identity verification.
- **Multi-factor Authentication (MFA)**: Require vot- ers to use multiple forms of authentication, such asa combination of a password, OTP, and biometric data.

5) User Experience:

- **Intuitive User Interfaces**: Design user-friendly interfaces with clear instructions to guide voters through the process.
- **Education and Training**: Provide resources and training materials to familiarize users with the blockchain-based voting system.

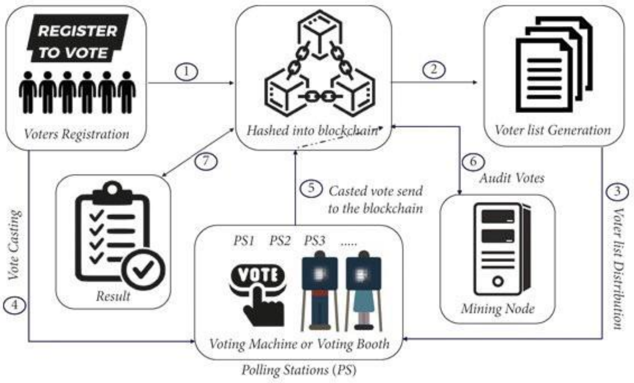

Fig. 1. Block-chain voting systems architectural overview

6) Security Risks:

- **Code Audits and Security Testing**: Conduct thor- ough code audits and security testing to identify andrectify vulnerabilities in the voting system’s smart contracts and infrastructure.
- **Penetration Testing**: Regularly perform penetration tests to assess the security posture of the entire system and identify potential weaknesses.

7) Risk of Forks:

- **Consensus Protocol Stability**: Choose a well- established consensus mechanism and monitor the blockchain network’s stability to minimize the risk of forks.

B. Architecture

General architecture of Blockchain voting system is as follows,

1) **Election creation**: Election administrators create elec- tion ballots using a decentralized app.When the election is created. Each district node is given permission tointeract with its corresponding ballot smart contract. This means that the blockchain network is structuredin a way that each district has its own node, and each node has access only to the information related to its specific district. This helps in maintaining the integrity and confidentiality of the election.
2) **Voter registration**: The registration of voter phase is conducted by the election administrators. Registration requires government identity verification. Admin re- leases list of eligible voters. Smart card technology can be used to give each voter a unique identity. This smart card contains voters public key
3) **Vote transaction**: Voter can authenticate himself using smart card combined with personal

identification num- ber(PIN). Voter interacts with a ballot smart contract with the same voting ID. Zero knowledge protocol is used by blockchain system to verify if valid voter has casted a vote or not and this process is carried out while protecting voter's privacy, that is voter's information and vote is not revealed. This smart contract appends the vote to the block-chain if consensus is reached between the majority. This is how the new block is created in the blockchain containing transaction details. These details are encrypted to preserve voter's privacy

4) **Tallying results**: Each ballot smart contract does their own tally in its own storage and declares result when election is over. When the elections are over the results are declared automatically using smart contracts.
5) **Verifying vote**: Before verifying the vote voter has to authenticate himself. This can be done at the district election center using voter ID, voting reset and other documents. Authenticated Voter can verify if his vote has counted and has counted correctly. This verification may not be needed to be equally efficient over long period of time. Because few voters are going to use this service and there number will decrease overtime. We can take advantage of this by saving the storage on blockchain and storing the whole election data on a server. To ensure integrity of that server blockchain and digital signature can be used. Digital signature of the server data will be created frequently and this digital signature will be stored on public blockchain. So when voter data manipulation happen voter will know that through change in digital signature of server data. To trace-back the manipulated data Markle tree can be implemented over the server data.

1) Combining BEV with document verification system: Combining blockchain voting with document verification ser- vices can make voting more secure and transparent. At state/national level implementing blockchain voting can have various obstacles. We can reduce them by using existing system of government approved documents in voter regis- tration and voter verification steps. Government documentare going to be required at the stage of proving validity ofvoter(based on age, nationality, domicile etc.). These document can be verified using document verification system based onblockchain technology.

III. CONCLUSION

Block-chain based E-voting system has tremendous poten- tial in every sector. It is already been used in small scale elec- tions and the are proven to be reliable. In large scale elections on the other hand process of implementing such system is complicated and new issues arises. Amongst them technical issues are scalability, latency, privacy concerns, access to authorized voter, security risk, cost and accessibility. These issues can be solved by implementing new techniques and following innovative approaches. These implementations are crucial to make blockchain voting mainstream and henceforth can help make elections more democratic.

REFERENCES

1. Fririk . Hjálmarsson, Gunnlaugur K. Hreiarsson School of Computer Science Reykjavik University, Iceland fridrik14, gunnlaugur15@ru.is. Blockchain-Based E-Voting System
2. S. W. Draper M. I. Brown Departments of Psychology and Computing Science, University of Glasgow, Glasgow, UK. Increasing interactivity in lectures using an electronic voting system
3. Taban Habibu, Konde Sharif, Sebwato Nicholas Department of Com- puter and Information Science, Muni University, Arua Uganda. Design and Implementation of Electronic Voting System

4. How blockchain technology could change our lives, In-depth Analysis,February 2017, PE 581.948
5. Ahmed Ben Ayed, Department of Engineering and Computer Science, Colorado Technical University, Colorado Springs, Colorado, USA; a conceptual secure blockchain- based electronic voting system. Interna- tional Journal of Network Security Its Applications (IJNSA) Vol.9,
6. No.3, May 2017 DOI: 10.5121/ijnsa.2017.9301 1
7. Francesco Fusco1, Maria Ilaria, Lunesu2, Filippo Eros Pani and Andrea Pinna 1NET SERVICE SPA, Via Montegrappa, Bologna, Italy, Depart- ment of Electrical and Electronic Engineering, Piazza dArmi, Cagliari,
8. Italy. Crypto-voting, a Blockchain based e-Voting System
9. Hanady Hussien , Hussien Aboelnaga Electronic and Communication Department. AAST, Cairo, Egypt. Design of a Secured E-voting System
10. Michał Pawlak, Aneta Poniszewska- Mara´ndaa, Natalia Kryvinska Institute of Information Technology, Lodz University of Technology, Lodz, Poland, School of Business, Economics and Statistics, University of Vienna, Vien, Austria, Comenius University in Bratislava, Bratislava, Slovakia. Towards the intelligent agents for blockchain e-voting system. The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2018)
11. Mochamad Heru Riza, Chakim University of Raharja; Aliyah Cen- dekia, Abditama University; M. Adhit Dwi Yuda, University of Ra- harja; Rifqi Fahrudin Catur, Insan Cendekia University; Dwi April- iasari, Univeristy of Raharja; Secure and Transparent Elections: Ex- ploring Decentralized Electronic Voting on P2P Blockchain DOI: https://doi.org/10.34306/ajri.v5i1Sp.959
12. S.K. Vivek; R.S. Yashank; Yashas Prashanth; N. Yashas; M. Namratha; E-Voting Systems using Blockchain: An Exploratory Literature Survey DOI: 10.1109/ICIRCA48905.2020.9183185
13. Sarvesh Tanwar, Neelam Gupta, Prashant Kumar Yu-Chen Hu, Mul- timedia Tools and Applications(2023) Implementation of blockchain- based e-voting system
14. Wei Fu, Xuefeng Wei Shihua Tong, An Improved Blockchain Consensus Algorithm Based on Raft, Arabian Journal for Science and Engineering volume 46, pages 8137–8149 (2021)
15. Hongyu Zhu; Libo Feng; Jianzhao Luo; Yani Sun; Bei Yu; Shaowen Yao; BCvoteMDE: A Blockchain-based E-Voting Scheme for Multi-District Elections; Publisher: IEEE