IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

E-VOTING DAPP USING SMART CONTRACT

Prateek Meshram, Krishna Varma, Mayur Mahajan, Tejas Purohit, Rishabh Waghmare

Assistant Professor, Student, Student, Student, Student
Computer Engineering,
Dr. D. Y Patil Institute of Engineering, Management, and Research, Akurdi, Pune, India

Abstract: This Electronic voting(e-voting) is an electronic means of casting and counting votes. It's an effective and cost-effective way of conducting a voting procedure, which has characteristics of being chivalrous data and real-time and requesting high safety. Blockchain is a disruptive technology of the current period and promises to ameliorate the overall adaptability of voting systems. espousing blockchain in the distribution of databases one-voting systems can reduce one of the infidelity sources of database manipulation. The physical voting systems have numerous excrescencies in it as well as the digital voting systems aren't perfect enough to be enforced on a large scale. This paper presents an overview of Blockchain- grounded voting systems. We suppose that blockchain could be used in colorful interactive online systems, similar as the Internet of effects, force chain systems, advancing systems, etc. The compass of this check is to exfoliate light on some recent benefactions of the security and sequestration issues associated with e-voting grounded on the blockchain. At the end of this paper, we handed a comparison of the security and sequestration conditions of the being-voting systems grounded on the blockchain.

INTRODUCTION

Voting is a system to make a collaborative decision or express an opinion among a group, a meeting, or electorates (1). Voting generally follows debates, conversations, and election juggernauts. During voting, the person to be tagged is the seeker of an election, and the person who casts a ballot for their chosen seeker is the name (2). ultramodern republics are erected upon traditional ballot or electronic voting(e-voting). In these recent times, a bias which are known as EVMs is monstrously blamed due to irregular reports of election results. There have been numerous questions regarding these biases' design and internal armature and how they might be susceptible to attacks. thus, a safe and robust voting system can be developed with the use of blockchain. Fig.1 shows thee-voting system stages grounded on blockchain technology. The paper aims to familiarize recently interested scientists. either, streamlining the compendiums with some previous understanding of Blockchain, including the rearmost security and sequestration issues in thee-voting systems grounded on the blockchain. This study approach will present a check of the state-of-the-art papers in which the Blockchain is used to give voting schemes with some position of sequestration and security.

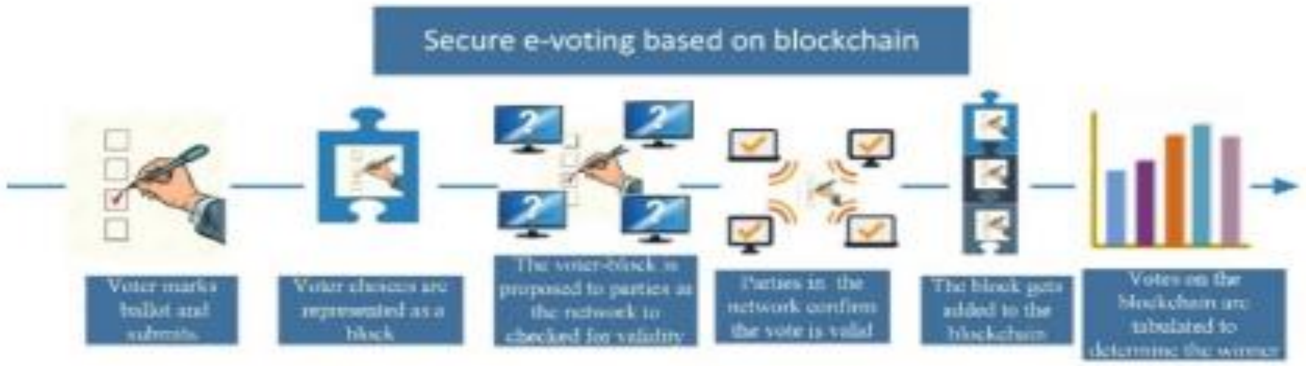
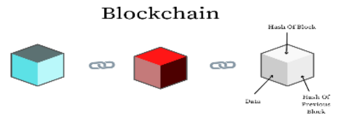

Secure e-voting based on blockchain
Voter marks ballot and submits.
Voter choices are represented as a block
The voter-block is proposed to parties as the network to checked for validity
Parties in the network confirm the vote is valid
The block gets added to the blockchain
Votes on the blockchain are tabulated to determine the winner

Figure 1. E-voting system stages based on blockchain technology.

SOME TERMS USED IN THE VOTING SYSTEM

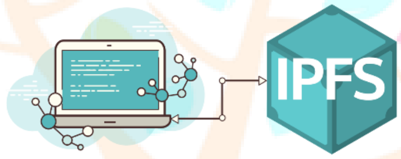
- **Blockchain** - The blockchain is a digital platform for digital means. It consists of a continuously growing list of records known as blocks that are linked and secured using cryptography. The major operation of Blockchain has been in all cryptocurrency deals, substantially Bitcoin. still, they're decreasingly being used in several other operations because of their essential resistance to revision to the sale/ block/ whole distributed tally – Blockchain.



- **Smart Contract** - A smart contract is an automated digital agreement, written in the law, that tracks, verifies, and executes the list deals of a contract between colorful parties. The deals of the contract are automatically executed by the smart contract law when destined conditions are met. A smart contract is a short program whose inputs and labors are deals with on a blockchain.

SMART CONTRACT
PARTIES
SMART CONTRACT
EXECUTION

- **IPFS** - The Inter-Planetary Train System, IPFS is a decentralized train-participating platform that identifies lines through their content. The Inter Planetary train System, or IPFS for short, is a peer-to-peer hypermedia protocol designed to make the web briskly, safer, and more open. When a train is uploaded to IPFS, it's resolved into gobbets, each containing at most 256 kilobytes of data and/ or links to other gobbets.



LITERATURE REVIEW

The author in [7] proposed that Blockchain-enabled e-voting (BEV) could reduce voter fraud and increase voter access. Eligible pickers cast a ballot anonymously using a computer or smartphone. BEV uses an encrypted key and tamper-proof personal IDs. The blockchain's audit trail ensures that no vote has been changed or removed and that no fraudulent and illegitimate votes have been added. In this system to address voter tampering, blockchains generate cryptographically secure voting records. Votes are recorded accurately, permanently, securely, and transparently. So, no one can modify or manipulate votes.

Authors in Voting System Using Blockchain: Vaibhav Anasune, Pradeep Choudhary, MadhuraKelapure, and Pranali Shirke Prasad Halgaonkar, "Online Voting: Voting System Using B-chain",2019, the article gives a short review on various methodologies that are used in current voting. The paper will help to build a system that will face the present and upcoming challenges and will remove drawbacks from these previous architectures [6].

The authors in [1] have discussed E-Voting and how it can be used or integrated with Blockchain [1]. the authors have not only focused on some inherent features of Blockchain DApps which includes privacy, and transparency, but their paper has proposed a solution to verify the users' identities which is done in the registration phase. The first step of the protocol is a registration, and this is required for identity verification. However, a server is centralized (Centralized Authority) is involved in the verification process and the same is also used to add the users' information to the database.

The author in [11] introduced an e-voting system based on blockchain technology. The system utilizes smart contracts that make cost-efficient and secure elections possible. Not only this but the voter's privacy is also guaranteed by this system. The authors have discussed how blockchain technology can overcome the limitations of e-voting systems. The authors have discussed how blockchain-based e-voting systems have laid the ground for transparency and how these systems ensure election integrity and security**.**

In [5], authors have proposed Votereum, an Ethereum-based E-voting system that utilizes blockchain technology and smart contract. The authors in their system have introduced the concept of verifiable E-voting platforms and have discussed the evaluation and security concerns of the system. Not only this, the authors have discussed the requirements, architecture, and design of the system.

The authors in [16], proposed a voting protocol based on Quantum Blockchain. This protocol provides essential security requirements such as anonymous, binding, nonreusable, verifiable, eligible, fair, and self-tallying. Besides this Quantum Blockchain, they used other quantum techniques such as:

- Quantum Secure Communication (QSC).
- Quantum Bit commitment (QBC).
- Quantum Key Distribution (QKD)

The authors in [19], proposed likewise an e-voting protocol based on the blockchain without a trusted third party, which affords a safe and adaptable voting technique. The protocol provides Public Verifiability, Individual Verifiability, Dependability, Consistency, Auditability, Anonymity, and Transparency.

The authors in [20], proposed voting protocol preserves end-to-end privacy based-blockchain and maintains detectability and correctability against defrauding without a third party committed. The protocol implementation respecting the hyper ledger structure proves the validity and practical applicability.

The authors in [24] proposed a methodology of combining the secret sharing scheme and homomorphic encryption with the blockchain to build up a decentralized e-voting framework without a trusted third party. Moreover, the framework provides a transparent voting manner while preserving the anonymity of the voter's identity. The author during the billing phase preserves the data transmission privacy and verifies the ballots.

BLOCKCHAIN TYPES AND THEIR COMPARISON

In Blockchain Technology, there exist three major types: Private, Consortium, and Public blockchain. Since a network will have to be created, a comparison must be made on what kind of network must be used for the same. The types are compared based on Consensus determination, read permission, Immutability, Efficiency, whether it is centralized or not, and the Consensus process. Depending upon the operation, an innovator must decide what kind of blockchain should be used. This helps in keeping the data tampered- with substantiation. Table I shows a comparison between the types of blockchains.

Property	Types of Blockchain		
	Private	Consortium	Public
Consensus determination	Single Organization	Selected nodes	All participating miners
Read permission	Could be public or restricted	Could be public or restricted	Public
Immutability	Could be tampered	Could be tampered	Nearly impossible to tamper
Efficiency	High	High	Low
Centralized	Yes	Partial	No
Consensus process	Permissioned	Permissioned	Permissionless

CHARACTERISTICS OF BLOCKCHAIN

1. **Cost effective***:* In traditional systems, there is a need for some central organization to verify the validity of transactions. Blockchain is a peer-to-peer network(P2P). The absence of a central agency reduces the cost per transaction.
2. **Persistence***:* Blockchain has one important property of persistence, each block can maintain its records. This helps in keeping the data tamper-proof.
3. **Validity***:* The execution is not carried out every time. You need to register your identity. This system has three roles, proposer, acceptor, and learner.
4. **Anonymity** *& Identity:* The centralized systems require knowing you as a person. You need to register your identity proof with those authorities. Whereas with blockchain, the user data remains anonymous.
5. **Auditability***:* The block added to the blockchain remains there ever. This helps in checking transaction history. In a private blockchain, the audibility is the least and depends on the central entity. In a permissioned blockchain, there is a little bit of audibility. In public blockchains have the most audibility.

The authors in [18], designed a secure online e-voting protocol-based blockchain named Verify-Your-Vote (VYV). This protocol guarantees the following features:

- Eligibility: Just the acceptable elector can vote.
- Fairness: No essential results that could affect other electors' choices are made available.
- Vote privacy: privately keep the votes; this can likewise be demonstrated as no link between the elector and his ballot.
- Receipt-freeness: The elector cannot create a certificate that enables him to back to the third party to inform them he voted for a particular candidate. That is to stop vote selling.
- Verifiability: Each elector can verify whether his/her vote has been counted rightly.
- Robustness: The Protocol can allow a set number of offending electors.

BLOCKCHAIN-BASED E-VOTING SYSTEM: OPEN ISSUES AND CHALLENGES

This paper analyses the current disquisition on blockchain electronic voting systems and identifies issues in it. E-Voting defines the process that uses electronic tools in the process of choices for voting and counting purposes. The procedure for electronic voting varies from country to country. These may include voting machines in polling stations, centralized accounting of paper bills, and online voting. In many countries, centralized calculations are used. This paper also talks about several factors that make an e-voting system secure like,

a. Anonymity*:* Any correlation between listed pickers and picker individualities shall be anonymous.

b. Auditability and Accuracy: The results should be accurate and should precisely correspond to the picker sentiment.

c. Democracy/Singularity: Every eligible person should be suitable to vote. There shall be no duplication of votes.

d. Vote Privacy: No particular person should be suitable to associate a particular vote with an existent.

e. Robustness and Integrity: It is proof that registered voters will abstain without problems. It also encourages others to cast their legitimate votes.

f. Transparency and Fairness: No one outside voter involved with the counting process can find out about the results before they are announced.

g. Availability and Mobility: The systems should always be available during the electoral process and maintaining security during voting.

PROS AND CONS OF SOME OF THE REFERENCES

Protocol	**Pros**	**Cons**
Based on Quantum Blockchain.	anonymous, binding, non-reusable, verifiable, eligible, fair and self-tallying	The main disadvantage of it does not provide audibility consistency
Used blockchain as a transparent ballot box	Abide by the underlying e-voting properties. Allow a degree of decentralization. Provide for the elector to modify/update their vote within the allowable voting phase	It does not provide privacy, consistency, and audibility
Design a blockchain-based protocol named Verify-Your-Vote (VYV)	Eligibility, Fairness, Vote privacy, Receipt-freeness, Verifiability	This protocol does not support anonymity.
Design the blockchain-based protocol without a trusted third party	Public Verifiability, Dependability, Dependability, Consistency, Auditability, Transparency, Anonymity.	The robustness and fairness are the limitations
The proposed protocol preserves end-to-end privacy.	Detectability, correct ability.	It does not provide consistency and fairness
Design smart contracts using the Ethereum wallets and the Solidity language	Design Android application for the voting system	The main disadvantage not support robustness and the receipt freeness feature.

FUTURE WORK

A successful e-voting system requires several key features to balance out. Security and privacy issues are undoubtedly one of the most critical factors because we want to avoid being able to manipulate the outcomes of any adversaries or self-interested parties and maintain election integrity. We believed that blockchain had improved some of the security and privacy aspects. However, there is still room for improvement. The other properties that need to be included in e-voting systems based on blockchain are:

1) **Anonymity:** In e-voting systems, the need for anonymity is complicated because, in all aspects, we don't want anonymity. To stop people from voting multiple times and committing certain types of fraud, they need to be able to verify who is voting. However, we want the votes themselves to be anonymous and no exposed voted to count. It can lead to bullying or coercion if the government, opposition party, or anyone else can find out whom a person voted for.

2) **Accessibility:** Accessibility must be considered by all voters. It would be nice to encourage everyone to vote and make voting from their location easier. At the same time, we don't want an overly technical system that makes voting impossible for some segments of the population.

3) **Scalability**: Blockchain scalability is still in its early days. So, the time to put a transaction in the block and the time to reach the consensus still needs improvement.

4) **Speed**: It is best if, in a relatively short period, we will obtain the results. If it took a long time to determine the final vote count, people's will at the time of the results differ greatly from when the votes were cast.

CONCLUSION

Blockchain has recently drawn remarkable attention in decentralized application systems because of its decentralized nature and safety function. It provides an entirely different way to store, distribute, and update data and will play a vital role in the future interactive internet system. This paper has presented and compared the recent researcher's contributions to security and privacy issues for the existing e-voting mechanisms based on blockchain. However, the developing need for security and privacy protections may be a barrier to emerging real blockchain applications.

REFERENCES

[1] [J] P. Tarasov and H. Tewari, “The future of e-voting.” IADIS International Journal on Computer Science & Information Systems, vol. 12, no. 2, 2017

[2] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[3] S. Shukla, A. N. Thasmiya, D. O. Shashank and H. R. Mamatha, "Online Voting Application Using Ethereum Blockchain," 2018 International Conference on Advances in Computing, Communications, and Informatics (ICACCI), Bangalore, 2018, pp.

[4] 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, 2018, pp. 1-6, doi: 10.1109/IMCET.2018.8603050

[5] Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao and Tuan A. Nguyen,(2019), Votereum: An Ethereum-based E-voting system :

[6] Vaibhav Anasune, Pradeep Choudhary, Madhura Kelapure and Pranali Shirke Prasad Halgaonkar, “Online Voting: Voting System Using B-chain”,(2019), Online Voting: Voting System Using Blockchain

[7] Ashish Singh; Kakali Chatterjee, "SecEVS: Secure Electronic Voting System Using Blockchain Technology", 2018 International Conference on Computing, Power and Communication Technologies (GUCON).

[8] Salanfe, Setup your own private Proof-of-Authority Ethereum network with Geth, Hacker Noon, 2018. Available at: https://tinyurl.com/ y7g362kd.

[9] Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth. ethereum.org/

[10] Vitalik Buterin. (2015). Ethereum White Paper Available at https: //github.com/ethereum/wiki/wiki/White-Paper.

[11] Ethdocs.org. (2018). What is Ethereum? — Ethereum Homestead 0.1 documentation. [online] Available at: http://ethdocs.org/en/latest/ introduction/what-is-ethereum.html

[12] Agora (2017). Agora: Bringing our voting systems into the 21st century Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf

[13] Patrick McCorry, Siamak F. Shahandashti, and Feng Hao. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy Available at: https://eprint.iacr.org/2017/110.pdf.

[14] Andrew Barnes, Christopher Brake and Thomas Perry. (2016). Digital Voting with the use of Blockchain Technology is Available at https://www. economist.com/sites/default/files/plymouth.pdf

[15] Jonathan Alexander, Steven Landers, and Ben Howerton (2018). Netvote: A Decentralized Voting Network Available at https://netvote. io/wp-content/uploads/2018/02/Netvote-White-Paper-v7.pdf

[16] Jelurida,"Jelurida",2017. Available at: https://www.jelurida.com/sites/ default/files/JeluridaWhitepaper.pdf

[17] Lee, K., James, J.I., Ejeta, T.G., et al.: Electronic voting service using blockchain. J. Digit. Forensics Secur. Law: JDFSL 11(2), 123 (2016)

[18] Jason, P.C., Yuichi, K.: E-voting system based on the bitcoin protocol and blind signatures. Trans. Math. Model. Appl. 10(1), 14–22 (2017)

[19] Ayed, A.B.: A conceptual secure blockchain-based electronic voting system. Int. J. Netw. Secure. Appl. (IJNSA) 9(3), 1–9 (2017)

[20] McCorry, P., Shahandashti, S.F., Hao, F.: A smart contract for board room voting with maximum voter privacy. In: International Conference on Financial Cryptography and Data Security, pp. 357–375. Springer (2017)

[21] Dong, Y., Zhang, D., Han, J., et al.: Board electronic voting system based on alliance blockchain. J. Netw. Inf. Secure. (12) (2017)

[22] Wu, Y.: An e-voting system based on blockchain and ring signature. Master, University of Birmingham (2017)

[23] P. Akritidis, Y. Chatzikian, M. Dramitinos,E.Michalopoulos, D. Tsigos, and N. Ventouras, “The vote secure secure internet voting system,” in International Conference on Trust Management, vol. 3477. Springer, 2005, pp. 420 – 423.

[24] G. Beroggi, “Secure and easy internet voting,” Computer, vol. 41, no. 2, pp. 52 – 6, 2008.

[25] L. Weinstein, “Risks of internet voting,” Communications of the ACM, vol. 43, no. 6, pp. 128–128, 2000.

[26] M. Di Pierro, “What is the blockchain?” Computing in Science &Engineering, vol. 19, no. 5, pp. 92–95, 2017.

[27] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, “Decentralized applications: The blockchain empowered software system,” IEEE Access, vol. 6, pp. 53 019–53 033, 2018.

[28] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. D. A. Rocha, “A survey of how to use blockchain to secure internet of things and the stalker attack,” Security and Communication Networks, vol. 2018, 2018.