Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 01 Issue: 05 | MAY-2023

ONLINE VOTING SYSTEM USING BLOCKCHAIN

Omkar Kajale [1], Roshani Pagare [2], Dhanashree Pawar [3], Ankita Shelke [4] &

Prof. J.Y.Kapadnis [5]

Department of Computer Engineering of Pune Vidyarthi Griha's College of Engineering & S. S. Dhamankar Institute of Management, Nashik

---

Abstract - Online voting is a trend that is gaining momentum in modern society. It has great potential to decrease organizational costs and increase voter turnout. It eliminates the need to print ballot papers or open polling stations—voters can vote from wherever there is an Internet connection. Despite these benefits, online voting solutions are viewed with a great deal of caution because they introduce new threats. A single vulnerability can lead to large-scale manipulations of votes. Electronic voting systems must be legitimate, accurate, safe, and convenient when used for elections. Nonetheless, adoption may be limited by potential problems associated with electronic voting systems. Blockchain technology came into the ground to overcome these issues and offers decentralized nodes for electronic voting and is used to produce electronic voting systems mainly because of their end-to-end verification advantages. This technology is a beautiful replacement for traditional electronic voting solutions with distributed, non-repudiation, and security protection characteristics. The following article gives an overview of electronic voting systems based on blockchain technology.

Key Words: electronic voting; security; blockchain-based electronic voting;

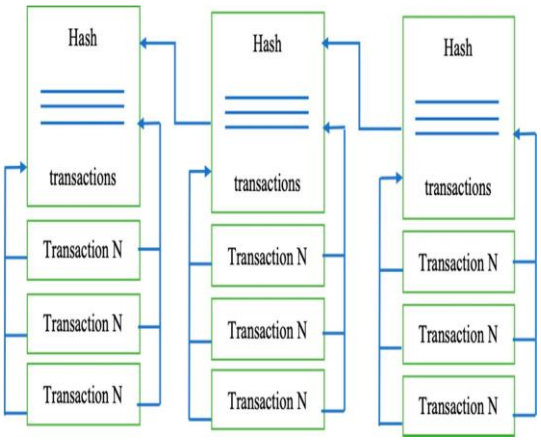
INTRODUCTION

Electoral integrity is essential not just for democratic nations but also for state voter's trust and liability. Political voting methods are crucial in this respect. From a government standpoint, electronic voting technologies can boost voter participation and confidence and rekindle interest in the voting system. As an effective means of making democratic decisions, elections have long been a social concern. As the number of votes cast in real life increases, citizens are becoming more aware of the significance of the electoral system [1,2].The voting system is the method through which judges judge who will represent in political and corporate governance. Democracy is a system of voters to elect representatives by voting [3,4]. The efficacy of such a procedure is determined mainly by the level of faith that people have in the election process.

Engineers across the globe have created new voting techniques that offer some anti- corruption protection while still ensuring that the voting process should be correct. Technology introduced the new electronic voting techniques and methods [9], which are essential and have posed significant challenges to the democratic system. Electronic voting increases election reliability when compared to manual polling. In contrast to the conventional voting method, it has enhanced both the efficiency and the integrity of the process [10]. Because of its flexibility, simplicity of use, and cheap cost compared to general elections, electronic voting is widely utilized in various decisions.

BACKGROUND Today, we call a blockchain a set of technologies combining the blockchain data structure itself, distributed consensus algorithm, public key cryptography, and smart contracts [18]. Below we

describe these technologies in more detail. Blockchain creates a series of blocks replicated on a peer-to-peer network. Any block inblockchain has a cryptographic hash and timestamp added to the previous block, as shown in Figure 1. A block contains the Merkle tree block header and several transactions [19]. It isa secure networking method that combines computer science and mathematics to hide data and information from others that is called



cryptography. It allows the data to be transmitted securely across the insecure network, in encrypted and decrypted forms.

Blockchain solutions are developed to be used in a distributed environment. It is assumed that nodes contain identical data and form a peer-to-peer network without a central authority. A consensus algorithm is used to reach an agreement on blockchain data that is fault-tolerant in the presence of malicious actors. Such consensus is called Byzantine fault tolerance, named after the Byzantine Generals' Problem [25]. Blockchain solutions use different Byzantine fault tolerance (BFT) consensus algorithms: Those that are intended to be used in fully decentralized self-organizing networks, such as cryptocurrency platforms, Public key cryptography is used mainly for two purposes: Firstly, all validators own their keypairs used to sign consensus messages, and, secondly, all incoming transactions (re-quests to modify blockchain data) have to be signed to determine the requester. Anonymity in a blockchain context relates to the fact that anyone wanting to use cryptocurrencies just needs to generate a random keypair and use it to control a wallet linked to a public key [28]. The blockchain solution guarantees that only the keypair owner can manage the funds in the wallet, and this property is verifiable [29,30]. As for online voting, ballots need to be accepted anonymously but only from eligible voters, so a blockchain by itself definitely cannot solve the issue of voter privacy.

Smart contracts breathed new life into blockchain solutions. They stimulated the application of blockchain technology in efforts to improve numerous spheres. A smart contract itself is nothing more than a piece of logic written in code. Still, it can act as an unconditionally trusted third party in conjunction with the immutability provided by a blockchain data structure and distributed consensus [31]. Once written, it cannot be altered,and all the network participants verify all steps. The great thing about smart contracts isthat anybody who can set up a blockchain node can verify its outcome.

Core Components of Blockchain Architecture:

These are the main architectural components of Blockchain as shown in Figure 2.

Node: Users or computers in blockchain layout (every device has a different copy of acomplete ledger from the blockchain);

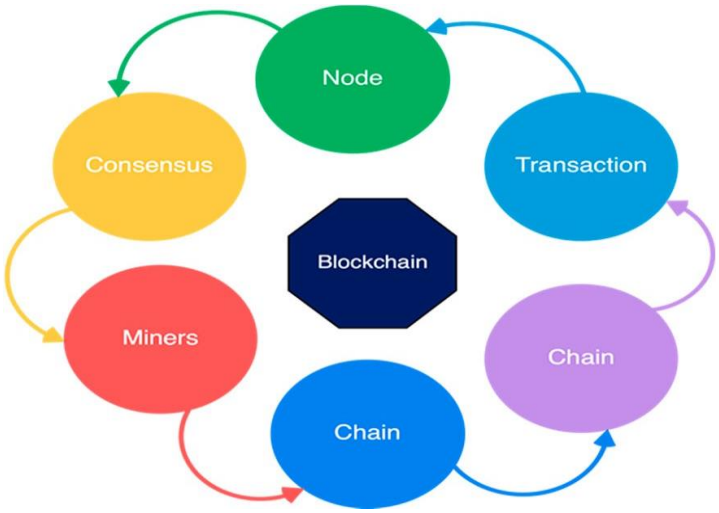
Transaction: It is the blockchain system's smallest building block (records and details),which blockchain uses;

Block: A block is a collection of data structures used to process transactions over the network distributed to all nodes.

Chain: A series of blocks in a particular order;

Miners: Correspondent nodes to validate the transaction and add that block into the blockchain system;

Consensus: A collection of commands and organizations to carry out blockchain processes.



CORE COMPONENT OF BLOCK CHAIN

Critical Characteristics of Blockchain Architecture

Blockchain architecture has many benefits for all sectors that incorporate blockchain

Cryptography: Blockchain transactions are authenticated and accurate because of computations and cryptographic evidence between the parties involved;

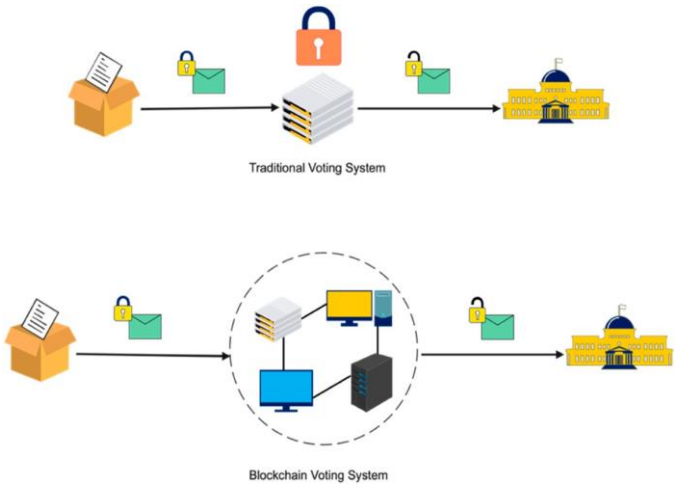
Decentralization: The entire distributed database may be accessible by all members of the blockchain network. A consensus algorithm allows control of the system, as shown in the core process

Anonymity: A blockchain network participant has generated an address rather than a user identification. It maintains anonymity, especially in a blockchain public system; Transparency: It means being unable to manipulate the blockchain network. It does not happen as it takes immense computational resources to erase the blockchain network.

Charactricts of block chain

How Blockchain Can Transform the Electronic Voting System

Blockchain technology fixed shortcomings in today's method in elections made the polling mechanism clear and accessible, stopped illegal voting, strengthened the data protection, and checked the outcome of the polling. The implementation of the electronic voting method in blockchain is very significant [35].



However, electronic voting carries significant risks such as if an electronic voting system is compromised, all cast votes can probably be manipulated and misused. Electronic voting has thus not yet been adopted on a national scale, considering all its possible advantages. Today, there is a viable solution to overcome the risks and electronic voting, which is blockchain technology. In Figure 4, one can see the main difference between both of the systems. In traditional voting systems, we have a central authority to cast a vote. If someone wants to modify or change the record, they can do it quickly; no one knows how to verify that record. One does not have the central authority; the data are stored in multiple nodes. It is not possible to hack all nodes and change the data. Thus, in this way, one cannot destroy the votes and efficiently verify the votes by tally with other nodes.

Traditional vs. blockchain voting system.

If the technology is used correctly, the blockchain is a digital, decentralized, en- crypted, transparent ledger that can withstand manipulation and fraud. Because of the distributed structure of the blockchain, a Bitcoin electronic voting system reduces the risks involved with electronic voting and allows for a tamper-proof for the voting system. A blockchain-based electronic voting system requires a wholly distributed voting infrastruc- ture. Electronic voting based on blockchain will only work where the online voting system is fully controlled by no single body, not even the government [36]. To sum-up, elections can only be free and fair when there is a broad belief in the legitimacy of the power held by those in positions of authority. The literature review for this field of study and other related experiments may be seen as a good path for making voting more efficient in terms of administration and participation. However, the idea of using blockchain offered a new model for electronic voting.

Problems and Solutions of Developing Online Voting Systems

Whether talking about traditional paper-based voting, voting via digital voting ma- chines, or an online voting system, several conditions need to be satisfied:

Eligibility: Only legitimate voters should be able to take part in voting;

Unreusability: Each voter can vote only once

Privacy: No one except the voter can obtain information about the voter's choice;

Fairness: No one can obtain intermediate voting results

Eligibility:

The solution to the issue of eligibility is rather apparent. To take part in online voting, voters need to identify themselves using a recognized identification system. The identifiers of all legitimate voters need to be added to the list of participants. But there are threats: Firstly, all modifications made to the participation list need to be checked sothat no illegitimate voters can be added, and secondly, the identification system should be both trusted and secure so that a voter's account cannot be stolen or used by an intruder. Building such an identification system is a complex task in itself [37]. However, because this sort of system is necessary for a wide range of other contexts, especially related to digital government services, researchers believe it is best to use an existing identificationsystem, and the question of creating one is beyond the scope of work

Fairness:

Fairness in terms of no one obtaining intermediate results is achieved straight forwardly: Voters encrypt their choices before sending, and those choices are decrypted at the end of the voting process. The critical thing to remember here is that if someone owns a decryption key with access to encrypted decisions, they can obtain intermediate results. This problem is solved by distributing the key among several keyholders [41]. A system where all the key holders are required for decryption is unreliable—if one of the key hold- ers does not participate, decryption cannot be performed. Therefore, threshold schemes are used whereby a specific number of key holders are required to perform decryption. There are two main approaches for distributing the key: secret sharing, where a trusted dealer divides the generated key into parts and distributes them among key holders (e.g., Shamir's Secret Sharing protocol); and distributed key generation, where no trusted dealer is needed, and all parties contribute to the calculation of the key (for example, Pedersen's Distributed Key Generation protocol).

Soundness and Completeness:

On the face of it, the completeness and soundness properties seem relatively straight- forward, but realizing them can be problematic depending on the protocol. If ballots are decrypted one by one, it is easy to distinguish between valid and invalid ones, but things become more complicated when it comes to homomorphic encryption. As a single ballot is never decrypted, the decryption result will not show if more than one option was chosen or if the poll was formed so that it was treated as ten choices (or a million) at once. Thus, we need to prove that the encrypted data meets the properties of a valid ballot without compromising any information that can help determine how the vote was cast. This taskis solved by zero-knowledge proof [46]. By definition, this is a cryptographic method of proving a statement about the value without disclosing the value itself. More specifically,range proofs demonstrate that a specific value belongs to a particular set in such cases.

This section provides some background information on electronic voting methods. Electronic voting is a voting technique in which votes are recorded or counted using electronic equipment. Electronic voting is usually defined as voting that is supported by some electronic hardware and software. Such regularities should be competent in supporting/implementing various functions, ranging from election setup through

vote storage. Kiosks at election offices, laptops, and, more recently, mobile devices are all examples of system types. Voter registration, authentication, voting, and tallying must be incorporated in the electronic voting systems

One of the areas where blockchain may have a significant impact is electronic voting. The level of risk is so great that electronic voting alone is not a viable option. If an electronic voting system is hacked, the consequences will be far-reaching. Because a blockchain network is entire, centralized, open, and consensus-driven, the design of a blockchain-based network guarantees that fraud is not theoretically possible until adequately implemented [66]. As a result, the blockchain's unique characteristics must be taken into account. There is nothing inherent about blockchain technology that prevents it from being used to any other kind of cryptocurrency. The idea of utilizing blockchain technology to create a tamper-resistant electronic/online voting network is gaining momentum [67]. End users would not notice a significant difference between a blockchain-based voting system and a traditional electronic voting system.

Related Literature Review

Several articles have been published in the recent era that highlighted the security and privacy issues of blockchain-based electronic voting systems. Reflects the comparison of selected electronic voting schemes based on blockchain.

The open vote network (OVN) was presented by [76], which is the first deployment of a transparent and self-tallying internet voting protocol with total user privacy by using Ethereum. In OVN, the voting size was limited to 50–60 electors by the framework. The OVN is unable to stop fraudulent miners from corrupting the system. A fraudulent voter may also circumvent the voting process by sending an invalid vote. The protocol does nothing to guarantee the resistance to violence, and the electoral administrator wants to trust

Acknowledgments: This research was funded by the Malaysia Ministry of Education (FRGS/1/2019/ ICT01/UKM/01/2) and Universiti Kebangsaan Malaysia (PP-FTSM-2021)

Reference:

1. Liu, Y.; Wang, Q. An E-voting Protocol Based on Blockchain. *IACR Cryptol. Eprint Arch.* **2017**, *2017*, 1043.
2. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access* **2019**, *7*, 24477–24488. [CrossRef]
3. Racsko, P. Blockchain and Democracy. *Soc. Econ.* **2019**, *41*, 353–369. [CrossRef]
4. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.
5. The Economist. EIU Democracy Index. 2017. Available online: https://infographics.economist.com/2018/DemocracyIndex/ (accessed on 18 January 2020).
6. Cullen, R.; Houghton, C. Democracy online: An assessment of New Zealand government web sites. *Gov. Inf. Q.* **2000**, *17*, 243–267. [CrossRef]
7. Schinckus, C. The good, the bad and the ugly: An overview of the sustainability of blockchain technology. *Energy Res. Soc. Sci.* **2020**, *69*, 101614. [CrossRef]
8. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. *IEEE Access*

2019, *7*, 115304–115316. [CrossRef]

9. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, A.; Di, J.; Li, Q.; Lee, Y. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**. [CrossRef]
10. Hang, L.; Kim, D.-H. Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors* **2019**, *19*, 2228. [CrossRef] [PubMed]
11. Chang, V.; Baudier, P.; Zhang, H.; Xu, Q.; Zhang, J.; Arami, M. How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. *Technol. Forecast. Soc. Chang.* **2020**, *158*, 120166. [CrossRef] [PubMed]
12. Wang, B.; Sun, J.; He, Y.; Pang, D.; Lu, N. Large-scale election based on blockchain. *Procedia Comput. Sci.* **2018**, *129*, 234–237. [CrossRef]
13. Ometov, A.; Bardinova, Y.; Afanasyeva, A.; Masek, P.; Zhidanov, K.; Vanurin, S.; Sayfullin, M.; Shubina, V.; Komarov, M.; Bezzateev, S. An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends. *IEEE Access* **2020**, *8*, 103994–104015. [CrossRef]
14. Hakak, S.; Khan, W.Z.; Gilkar, G.A.; Imran, M.; Guizani, N. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. *IEEE Netw.* **2020**, *34*, 8–14. [CrossRef]
15. Çabuk, U.C.; Adiguzel, E.; Karaarslan, E. A survey on feasibility and suitability of blockchain techniques for the e-voting systems. *arXiv* **2020**, arXiv:2002.07175. [CrossRef]
16. Szabo, N. Formalizing and securing relationships on public networks. *First Monday* **1997**, *2*, 9. [CrossRef]
17. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
18. Tan, W.; Zhu, H.; Tan, J.; Zhao, Y.; Da Xu, L.; Guo, K. A novel service level agreement model using blockchain and smart contract for cloud manufacturing in industry 4.0. *Enterp. Inf.Syst.* **2021**. [CrossRef]

,