Leveraging Blockchain Technology for Secure Online Voting Systems: A Comprehensive Review

Astha Sah, Ankit Kumar* and Bharat Bhushan

Department of Computer Science and Engineering, School of Engineering and Technology Sharda University, Greater Noida 201310, India
E-mail: asthasah7091@gmail.com; ak1485602@gmail.com; bharat_bhushan1989@yahoo.com
**Corresponding Author*

Received 08 January 2025; Accepted 01 May 2025

Abstract

In a democratic society, no mechanism better expresses the ideas than the voting system. Voting procedures have been made as safe as feasible over the years, with an emphasis on efficiency, impartiality, and dependability. When e- voting systems are utilized in elections, they must be lawful, precise, secure, and accessible. However, usage could be hampered by potential issues with automated voting systems. Blockchain technology emerged to address these challenges, providing decentralized platforms for electronic voting. Blockchain technology improves the and guaranteeing the fairness of elections. This essay offers a thorough introduction to the idea of voting systems, it examines a variety of significant research problems, Including the benefits, problems, and consequences of such structures. Additionally, it conveys a complete review of the blockchain relies e-voting systems that are now utilized in different nations and organizations. It further compares the blockchain voting system with traditional and e-voting.

Keywords: Voting system, blockchain, democracy, security, integrity.

Journal of Mobile Multimedia, Vol. 21_3&4, 535–554.
doi: 10.13052/jmm1550-4646.213412

1 Introduction

The word "blockchain" implies that it is a network of blocks. A distributed, transparent method of logging & validating transactions is provided by the blockchain system. Typically, a centralized body contends, records, and verifies the credentials. Every node in the decentralized platform that utilizes such technology is able to interact with any additional node and maintains a duplicate of the ledger detailing all of the transactions. Electronic voting constitutes one amongst the sectors whereby blockchain could potentially have major consequences. The architectural layout of a network built on a blockchain ensures that deception is not conceivable unless the system is entirely centralized, functioning, & consensus-driven [1].

As an online voting to be utilized for balloting, it needs to be reputable, precise, secure, and intuitive. However, possible issues with automated voting machines can prevent widespread adoption. Blockchain technology was introduced to look after these problems & provides distributed voting via internet nodes [2]. Considering features like decentralized voting, confidentiality, and security safeguards, this technology is a viable substitute for conventional electronic voting systems. Since it contains numerous blocks, changing the hash will affect the data in its entirety. Any illegal conduct can be identified via this method. Hashing algorithm strategy, block production & securing, data collection & event proclamation through a flexible blockchain approach are required to create a end-to-end network which offers security and confidentiality. Every vote is verified via blockchain consensus procedure, & the entire votes are accessible to all on decentralized replicas of the blockchain database [3].

All nations that conduct democracy values, voting and election processes occurs significantly. Plenty of issues with elections exist, such as duplicate voting, inaccurate calculating, imitation, stolen or ruined ballots, and limited record-keeping. With the advent of online voting, casting votes has become simplified, the electorate may employ the platform if they choose, and they are forbidden to vote several times or for oneself.

Additionally, voting will require validation of an Aadhar number, and that will save the work and time on the part of human workers, improvements to voting as well as simple navigation. The principal notion the system for voting should be simple enough for everyone to. It speaks to the system's compatibility with many platforms and technologies by allowing it to adjust to a range of formats, dialects and voting boxes. This statement stresses on allowing a variety of ballot issue forms, including broad enquiries in order to create a versatile and adaptable voting experience.

This paper provides a thorough analysis of the existing body of knowledge regarding blockchain-based electronic voting systems. The aims to examine a variety of associated research fields, such as the advantages, obstacles, and possible future fields of study in this area. This study performs a thorough examination of the amount of material currently available on blockchain-based electronic voting systems. It also includes the system which are used by companies as well as government. The security properties needed by the OVS and various cryptographic techniques needed to preserve CIA is also discussed. In particular, the study seeks to accomplish the following goals:

- Determine and evaluate the advantages and disadvantages of blockchain-based electronic voting systems relative to conventional voting and other electronic voting systems.
- Offer a summary of findings and suggestions for further study and advancement in this area.

The entire paper presents as

- Section 2 introduce the concept of OVS and its security properties along with the characteristics and technology description of the system which further discuss about the benefit and limits of OVS.
- Section 3 discusses the concept of blockchain and its properties, security requirements for the OVS is also high- lightened in the further subsections.
- Section 4 represents the frameworks of BC based voting system and its use in online voting system which further discuss the advantages and the system used by government and companies.
- Section 5 provides a comparison between BC based voting system with traditional.
- Section 6 explains recent advances and Section 6 conclude the paper.

2 Online Voting System

In today's world, online voting is becoming more and more popular. Voters can cast their ballots from any location with a web connection, doing away with having to print out ballots or visit polling locations. Voting online solutions are seen with significant care as they present new risks, even with these advantages. Large-scale election fraud is possible with just one weakness. Fig.1 demonstrates the online voting system.

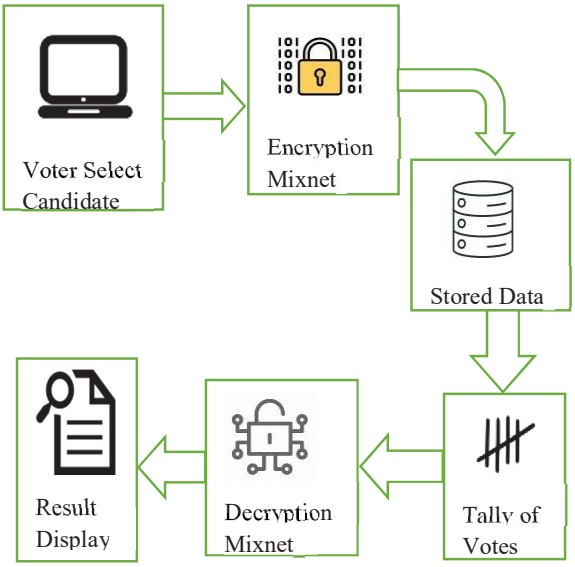

Figure 1 Online voting system.

Technology description

OVS is integrated with a variety of software tools, software kits, and coding languages, including Hypertext Preprocessor (PHP), CSS, WAMP Server & MYSQL, which was used alongside HTML to specify the style and arrangement of text and other elements. Smartphones were equipped with Java programmes (MIDlet's) and were simulated to assist the voting procedures. The system's screen elements and user interface layouts created using Extensible Markup Language (XML). Inspections for several system modules were created using XML coding, and the parse framework () was utilised to deliver services to the backend.

2.1 Security Properties of Online Voting System

According to a number of published studies, the following characteristics should be taken into account while developing a system that provides advanced safety in the online voting platform [4].

Authentication. It is ensured by this characteristic that voting is restricted to those who are authorized. **Integrity.** The integrity attribute contributes to the voting transparency and fairness. Voters have the ability to verify that their votes are not being influenced. **Verifiability.** Verifiability is a feature which

ensure that every vote is accurately counted. Every voter ought to confirm that their ballot was cast for the appropriate party.

2.2 Advantage of Online Voting System

Compared to conventional voting methods, OVS has numerous of benefits that improve community access to political processes and promote involvement. The benefits are outlined below: -

Lower expenses.

Conventional Voting System: Costs associated with printing, staffing, and security total $7 on average per voter. Blockchain Voting System: This system includes transaction fees and infrastructure costs, with an average cost of $3 per voter.

Safety precautions.

Conventional System: Each electoral board has 15 fraud cases to report. Blockchain System: Two times the amount of fraud cases for every election. Conclusion: The use of blockchain voting technologies resulted in an approximate 87% decrease in fraud instances. Give the problem statement again.

Numerous voting choices and higher participation.

Conventional System: 60% of voters cast ballots on average. Blockchain Voting System: The average voter turnout for the Blockchain Pilot Project is 70%. In conclusion, ten percent more people used blockchain voting methods than traditional ones.

Faster and more precise vote placement & scoring. The methodical procedures of online voting reduce the number of incorrect votes. Vote tabulation and result delivery time are shortened by electronic ballot collection and accounting.

Improved accessibility for the sick & disabled. Online voting systems, which include a range of platforms and accessibility enhancements, enable those with disabilities particularly the visually impaired to vote in a private and autonomous manner.

2.3 Limit & Issues of Online Voting System

Compared to document systems, OVS are far more effective and have fewer instances of error. However, a number of issues, including privacy, security,

and accountability, come up when we use online voting methods. Blockchain is the perfect solution to these problems. Voters can participate in a more transparent form of democracy.

Inadequate voter information. According to the information in their pupil database, the vast majority of voters during the software testing experiment did not have mailing addresses or contact numbers. Furthermore, a large percentage of voters neglected to update and validate this information in advance of Election Day, as required. The electoral board was forced to arrange for the changes to be completed on the precise day of voting in order to accommodate the voters.

Delay of SMS gateway. Additional difficulties were related to the SMS gateway's delay. Voters anticipated instant messages, so when they took a little longer than anticipated, they asked for a password or additional verification code. It was necessary to modify the systems resends in order to stop several messages via being sent in less than five minutes.

3 Blockchain

Blockchain is a P2P network-based distributed database of activities. It consists of a number of blocks, typically containing a collection of established transaction details. When a significant node in a network made up of peers come to a consensus, each contributing peer, or nodes, verifies the newly acquired block and adds the authenticated blocks to the network. Without the consent of the majority, no entity may add or change an item in the database. Furthermore, each node in the chain may not alter or remove any data from the blockchain since they are immutable. To guarantee the legitimacy of the system, blockchain integrates the benefits of cryptographic and consensus approaches [5]. The immutability of the blockchain prevents new users from joining the network, reading its contents, submitting operations, confirming the accuracy of current blocks, or participating part in the decision-making process that adds additional blocks.

3.1 Popular Consensus Protocols

The purpose of this section is to outline and offer a brief explanation of the most widely used protocols [6] as in Table 1.

Table 1 Consensus protocol in online voting system

Consensus Protocol	Computational Power	Energy Consumption	Scalability	Efficiency
Proof of Work (PoW)	High	High	Limited	Low
Proof of Stake (PoS)	Low	Low	High	High
DPoS	Low	Low	High	High
PBFT	Moderate	Moderate	Moderate	High

Proof-of-Work (PoW)

The primary consensus mechanism used in prior blockchains, such a version 1.0 of Ethereum and Bitcoin. This system rewards the first node for solving a highly complex encrypted puzzle, hence creating rivalry between nodes. These nodes can only use brute force methods to figure out this puzzle, which requires them to locate the hash digest that fits a preset format. Since all hash calculations for lost nodes are merely discarded, this protocol is accountable for a huge amount of unused power.

Proof-of-Stake (PoS)

When PoW started to have issues because of its excessive energy consumption, this protocol was developed as an alternative. By accumulating more network stake that is, by keeping tokens from the relevant blockchain in their accounts nodes in a proof of stake (PoS) improve the likelihood that they will be chosen by the protocol. The greater the stake, the greater the likelihood that they will be chosen to append the subsequent block and get paid for that block. The consensus method used by Ethereum was modified from the PoW to PoS in version 2.0.

Delegated Proof of Stake (DPoS)

The same stake premise as the initial protocol is utilised in this version, but the right to vote is acquired instead of money, and block verifiers those who actually make new blocks are chosen. Due to their claim to ownership in the network, nodes essentially assign the power they possess, thus the name.

Practical Byzantine Fault Tolerance (PBFT)

A node in the protocol recommends a block to the prime node, as serves as the system supervisor, and the principal node forwards the proposal to several backup nodes. The suggested block is added to the network if sufficient standby nodes concur. If not, it is thrown away.

3.2 Blockchain Property

Immutability. BC data is repeated across all of the nodes that make up the network at every moment. The confidentiality of the data is preserved although the blocks are functionally "linked" to one another by this data coupling.

Pseudo-Anonymity. Limited confidentiality is provided when every transaction is represented by a series of seemingly arbitrary bits. It is feasible to de-anonymize the user via those monitored interfaces and/or perform statistical evaluation of the transactional data. For this reason, the attribute has been preceded by a "pseudo" for accuracy's sake.

Verifiability. The consensus method is use to preserve a single, cohesive representation of the data structures even in such a dynamic network, enabling unsynchronized nodes to come together to the consensus picture held by the majority of the network.

Smart Contracts. smart contracts operate in a distributed simulated machine. Blockchains guard against code that may intercept & squander network bandwidth (infinite cycles, unoptimized programming, etc.), smart contracts give developers a great deal of programming freedom.

3.3 Security Attacks

This section provides a summary of the main obstacles facing Blockchain systems and discusses the different security risks associated with them.

51% Percentage Attack: This type of attack gives the attacker control over hash values in an effort to determine other messages they want to send first. In this instance, the attacker controls over 51% of the network's total hash values or mining power. We call it a 51% percentage attack.

Centralization attack: Since the Blockchain is a decentralized network, it functions peer-to-peer. In this case, the attacker attempts to sabotage decentralization and presents a false impression of centralization.

DDoS assault: When several systems overload the targeted system's bandwidth and resources, a distributed denial of service attack occurs. The system overloads, preventing the target node from completing the transaction.

Insider attacks: Unauthorized access to a computer system or network allows someone to enter untrusted data into a program that is then interpreted by an interpreter. Someone who has administrative credentials and in-depth

knowledge of the system manipulates the data and creates a special challenge. In order to remove any evidence of the attack and make it more difficult to detect, an attacker with administrator rights can change login information and records. This is known as an insider attack.

3.4 Security Requirements

One of the most important things that a system for voting online needs to have been confidentiality. Cryptographic techniques are utilized to provide this functionality, and frequently multiple techniques are used simultaneously [7].

Hashing. Mapping an arbitrary, variable-sized intake to a fixed-sized outcome is called hashing. It makes use of mathematical functions to convert data into a string that is unintelligible to recipients who are not the intended ones.

Blind signature. A blind signature is an algorithmic method that is used to confirm the legitimacy of digital interactions or records that are acknowledged but have their content hidden prior. Without requiring decryption, it is used to sign encrypted messages. Before the recipient signs the message, the sender blinds them.

Secure Hashing Algorithms (SHA). SHA exists in several variations. A 256-bit fixed-length hashing algorithm is produced by SHA-256 with a source of any length. A cryptographic attack known as a collision attack looks for two inputs that have an identical hash value. Hash routines that are considered secure and resistant to collision attacks are SHA-256 and SHA-512.

Zero-knowledge proof (ZKP). ZKP, is a cryptographic technique wherein a prover (a party) can demonstrate to a validator (a party) that a specific signal is true without disclosing the message's content. There must be the demonstrator and a validator for this system to work. ZKP raises a system's degree of transparency. It is applicable to any confidential information. ZKP can be connected to various other blockchain systems provides an extra layer of protection to the BC database.

4 Blockchain in Voting System

Election management as a whole can be made effective by implementing blockchain technology for online voting. For example, users may utilise it for tallied votes or verify if voters have cast ballots. Additionally, we can use

virtual management. According to Kim, H.R., the following are the benefits of the blockchain based OVS [8]:

1. Reduction of time and expenses
2. Heightened public involvement
3. Dependability and safety.

The primary features of the blockchain network led us to conclude that it is an excellent choice for systems for voting. The network's hashing and linkage of blocks ensures that data cannot be changed, guaranteeing the immutability of entries. The issue related to the centralised point's collapse also gets fixed because the primary server is swapped out for a collection of separate network nodes. Additionally, if necessary, it offers voters' confidentiality and transparency. There needs to be agreement among the nodes of a block for inclusion to the system. Smart contracts enable the setting up of transparent election regulations, so averting multiple disputes. Compared to the conventional voting method, which stores votes in a centralized database, the blockchain offers numerous benefits. These benefits lower the dangers connected with online voting, and a high level of secrecy can be attained by combining cryptographic techniques.

These are some of the tools which could be utilized to put forward a BC based voting system.

Ganache. Ganache is used to test and create distributed Ethereum applications [9]. It is used to generate blockchain users with Ether locally on the computer and provides ten accounts for use in the regional Ethereum chain.

Go-Ethereum/Geth. It is an Ethereum BC implementation which uses the programming language Go to run apps & smart contract applications. It features a decentralized system that can be chosen based upon the PoW, the PoS, or the PoA.

MetaMask. It is a Google Chrome browser extension that creates a link among the browser & the blockchain, allowing to link to the Ethereum ledger to regulate smart contract functionality. With their own accounts, voters will be enabled to connect to the localized Ethereum blockchain and interact with smart contract.

Truffle. The Truffle framework serves to validate smart contracts before deploying them to blockchain. The Truffle Framework facilitates the development, testing, and deployment of decentralised applications. It serves as an experimental atmosphere for the distributed ledger network. It is capable of

Table 2 Blockchain framework

Name	Consensus	Description
Bitcoin	PoW	Function as public blockchain. Scaling and programming Bitcoin is challenging. Information is distributed on a besteffort basis inside an ad-hoc distributed network of volunteers, as required by the protocol.
ZCash	PoW	ZCash uses zero-knowledge proof to facilitate secure transactions with two different kinds of addresses. These addresses are the z-address.
Ethereum	PoW	Ethereum is programmable, allowing users to create and run decentralised apps on its peer-to-peer network.
Exorum	Custom-built Byzantine algorithm	It is a publicly available blockchain that operates decentralized and it is capable of handling 5,000 tps.
Quorum	QuorumChain	Quorum use a Structured P2P network to store past transactions and authenticate certain communications within of an alcove.

creating smart contracts, compiling, linking, and saving them to the system. Ganache is a component of the truffle ecology.

Some of the framework of Blockchain is elaborated in Table 2.

4.1 Advantage of Blockchain Voting System

- Voting becomes more prevalent since it is an easier approach considering today's busy schedules.
- As block voting never employs unsecured ballots and biometric identity is a particularly secure form of authentication, it is more reliable than ID proof. Additionally, vote safety at the data storage level is provided by blockchain.
- Full-fledged setup and management is quicker and simpler since it saves time. in order to free up time for other activities
- Although the voting programme is decentralised, it tends to erode public confidence in the system and people's confidence in the voting system will grow as a result of its clarity.

4.2 Challenges of Blockchain Based Voting System

Although the blockchain relies e-voting systems have obvious benefits like reliability, safety, and decentralization, they also confront numerous

obstacles. Security issues encompass cyber-attacks involving as hash-based, authenticity attacks and smart contract flaws. The absence of scaling is a serious concern. Online access is needed to customize these preferences as it is not available everywhere, which is especially problematic in rural areas where off-the-shelf online voting alternatives will be challenging to implement. Full decentralization, on the other hand, is still a long way off because it requires developing and executing an effective consensus process that assures transparency and security without sacrificing speed. A related issue to consider for a successful decentralization strategy is the adoption of an adequate consensus mechanism capable of properly and quickly validating confirm transactions.

4.3 System Used by Govt Institutions and Companies

Governments and other institutions have embraced a number of commercial BC e- voting systems in addition to those created by businesses. Several of the more well-known ones in this part are reviewed in this publication.

The Systems That Government Institutions Use

Australia. Approximately 280,000 people used the Scytl app to conduct blockchain-based electronic voting during the 2015 State General Election in New South Wales [10]. Once the application process is complete, the voter registers with the proper authorities, receives their voter ID, and selects a 6-digit pin. After submitting their vote, they enter the system with their ID and PIN to receive a 12-digit receipt number. Voters obtain their voter information using the ID, PIN, and ticket number in order to validate their vote.

Russia. *In 2014, over two million persons were able to vote online.* In order to elect council members in 2017, citizens of Moscow employed blockchain. Additionally, Waves' blockchain e-voting system was utilised by Russia [11]. A consensus method based on Proof of Authority is u by the system to tolerate crashes. The voting procedure's regulations, voter verification, and registration data are stored in smart contracts.

Switzerland. held local elections utilizing Luxoft developed electronic voting devices. Most national voting procedures in Switzerland, including state-wide elections and polls, employ the electronic voting system [12]. Utilising a Short Message Service (SMS) approval, the suggested approach is a mobile application. Entering a PIN and comparing the authentication sign with the one they received in the mail; voters use their ID to connect onto the

e-voting website then follow the prompts to cast their vote. The mechanism acknowledges the vote if the two match. Following that, voters input codes for the PIN, the referendum's name, and their choice of yes or no.

Commercial Blockchain-Based E-Voting Systems.

This section describes some of the well-known commercial blockchain e-voting systems that businesses have created, along with their applications.

- A safe, decentralised online voting tool called Follow My Vote lets people checks the voting booth. Voters may find their individual voter ID at an authentication part of the process, which guarantees their eligibility to cast a ballot. To verify that a person's identity matches the information on their papers stored in the database, it uses a digital camera and user ID [13]. The procedure enables the user to locate the vote, open the box for voting, and verify that it is accurate. The "voting booth" required all voters to download it on a computer system, phone, or tablet. After that, they had to authenticate themselves by presenting official proof of identity, such as their passport, and a Personal Identification Identifier that had previously been authorised by the election-organizing body.
- Kaspersky Lab developed the polling system Polys, which works on blockchain. The organiser panel, voter the application, and observation application are its three primary parts. The election organiser can start and halt voting with the help of this panel. Three methods are used by the voter app: open voting, PIN, and voter authorization emails. The organiser provides a link to vote on behalf of the participants. Voter ID verification, vote encryption and blockchain integration, and accurate results counting are all guaranteed by Polys. The observer application enables all participants & outside observers to watch the polling process live. Voters can confirm that the blockchain has accurately recorded and tallied their ballots [14].
- The first customised BC e-voting system was developed by Luxoft, a multinational IT service supplier, in collaboration with the town of Zug and the Lucerne University of Applied Sciences in Switzerland [15]. To improve security and lower the chance of data loss, the system is installed in three separate data centres – two in Switzerland and one in Ireland. Whereas Voters can cast anonymity ballots remotely via Voatz, a BC based mobile voting system, and confirm that the vote they cast was correctly tabulated. According to reports, the technique has been employed in elections across the United States by a number of governments and political parties.

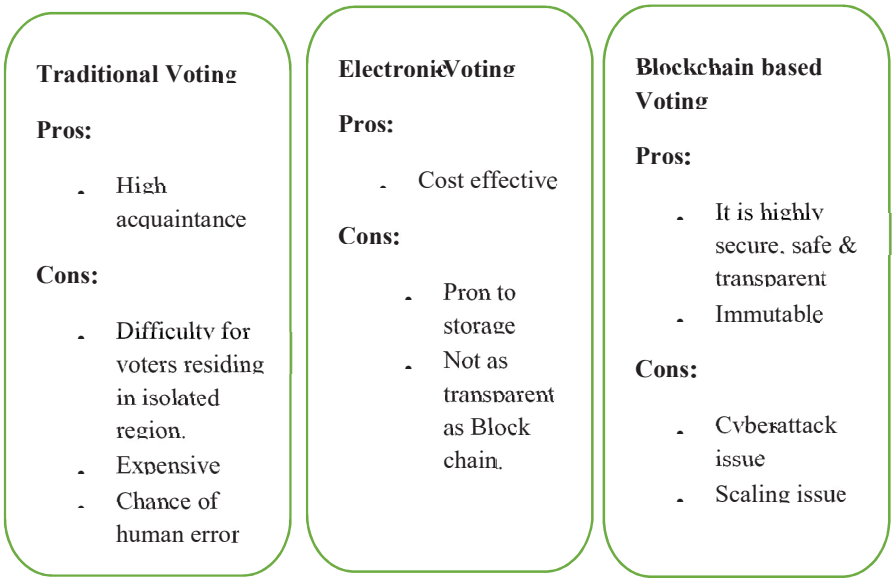

Figure 2 comparison between traditional, e-voting, online voting system.

5 Recent Advances

Jacob et al. [16] evaluated and coordinated online elections across various legal and regulatory frameworks. Alsadi et al. [17] constituted the initial phase of a step-by-step process that minimizes business risk while showcasing the benefits of verifiability. Vladucu et al. [18] presented a thorough summary of the BC -based online polling methods that are being adopted by a number of nations and businesses. Almeida et al. [19] detailed the development of the software as a whole as well as all the components, both concentrated and distributed, developed and utilised for implementing voting systems. Venugopalan et al. [20] proposed With Always on Voting (AoV), users can cast multiple ballots and modify chosen candidates or programmes without having to wait for the next campaign. Chaudhary et al. [21] proposed a voting system work on blockchain that uses 5G and IPFS to enable voters to choose a safe, dependable, and affordable candidate. Additionally, the use of 5G networks by voters and candidates allows for faster reaction times and greater dependability in communication. Singh et al. [22] evaluated some of the popular blockchain frameworks and presents an alternative that addresses some of the shortcomings and restrictions of existing systems. Joseph et al. [23] proposed a online voting platform that is transparent, impenetrable &

Table 3 Recent advances.

Author	Year	Description
Jacob et al. [16]	2024	Evaluated and coordinated online elections across various legal and regulatory frameworks.
Alsadi et al. [17]	2023	Represented the initial phase of a step-by-step strategy electronic voting methods.
Vladucu et al. [18]	2023	Gave an extensive description of the blockchain-based
Almeida et al. [19]	2023	Offered an analysis of the way research on voting technology has developed, based on a thorough examination of the literature.
Venugopalan et al. [20]	2023	Suggested Always on Voting (AoV), a framework for recurrent polling.
Chaudhary et al. [21]	2023	Proposed a BC-based voting system that uses 5G & IPFS.
Singh et al. [22]	2023	Evaluated some of the popular blockchain frameworks.
Joseph et al. [23]	2023	Proposed a online voting platform that is transparent, impenetrable & capable of ensuring the accuracy and authenticity
Khaleelullah et al. [24]	2023	Provided an introduction to the fundamental characteristics and structure of the blockchain in relation to electronic voting
Farooq et al. [25]	2022	Offered a platform built on cutting-edge blockchain technology that maximises system dependability and transparency

capable of ensuring the accuracy and authenticity of the voting procedure is implemented using blockchain technology. Khaleelullah et al. [24] provided an introduction to the fundamental characteristics and structure of the blockchain in relation to electronic voting. Farooq et al. [25] offered a platform built on cutting-edge blockchain technology that maximises system dependability and transparency to foster a relationship of trust amongst voters and election officials.

6 Conclusion

The establishment of BC based polling systems is becoming intensively popular due to the technology's rapid growth and acceptance. An overview of BC based, electronic, and conventional polling methods is provided by this survey. This paper reviewed cryptography, consensus algorithms, assessment of performance, qualities of an effective system, and tools for putting such systems into place. This paper offers a current summary of the blockchain

electronic polling systems that have been utilized by businesses, governments & academic organizations. This paper provides a thorough analysis of the existing body of knowledge regarding blockchain based electronic voting systems. Along with technology, the study explores a number of important research issues, such as the advantages, obstacles, and possible future fields of study in this area. Future work involves developing an inclusive and accessible blockchain e-voting system for all qualified voters. Blockchain e-voting implementations commonly address user authentication and registration difficulties. Consider using IoT, biometrics, and other secure methods for user authentication in blockchain e-voting systems.

References

[1] Yavuz, E., Koc, A. K., Cabuk, U. C., and Dalkilic, G. (2018). Towards secure e-voting using Ethereum Blockchain. 2018 6th International Symposium on Digital Forensic and Security (ISDFS). https://doi.org/10.1109/isdfs.2018.8355340.

[2] Sheer Hardwick, F., Gioulis, A., Naeem Akram, R., and Markantonakis, K. (2018). E-voting with Blockchain: An E-voting protocol with decentralisation and voter privacy. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). https://doi.org/10.1109/cybermatics_2018.2018.00262.

[3] Seifelnasr, M., Galal, H. S., and Youssef, A. M. (2020). Scalable open-vote network on Ethereum. Lecture Notes in Computer Science, 436–450. https://doi.org/10.1007/978-3-030-54455-3_31.

[4] A. Abu Aziz, A., N. Qunoo, H., and A. Abu Samra, A. (2018). Using homomorphic cryptographic solutions on e-voting systems. International Journal of Computer Network and Information Security, 10(1), 44–59. https://doi.org/10.5815/ijcnis.2018.01.06.

[5] Bouraga, S. (2021). A taxonomy of Blockchain Consensus Protocols: A Survey and Classification Framework. Expert Systems with Applications, 168, 114384. https://doi.org/10.1016/j.eswa.2020.114384.

[6] Zhang, S., and Lee, J.-H. (2020). Analysis of the main consensus protocols of Blockchain. ICT Express, 6(2), 93–97. https://doi.org/10.1016/j.icte.2019.08.001.

[7] Goldreich, O., and Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. Journal of Cryptology, 7(1), 1–32. https://doi.org/10.1007/bf00195207.

[8] Kim, H. R., Min, K., and Hong, S. (2017a). A study on ways to apply the blockchain-based online voting system. International Journal of Control and Automation, 10(12), 121–130. https://doi.org/10.14257/ijca.2017.10.12.11.

[9] Teja, K., Shravani, M., Simha, C. Y., and Kounte, M. R. (2019). Secured voting through Blockchain technology. 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). https://doi.org/10.1109/icoei.2019.8862743.

[10] Kshetri, N., and Voas, J. (2018). Blockchain-enabled voting. IEEE Software, 35(4), 95. https://doi.org/10.1109/ms.2018.2801546.

[11] Akcagündüz, E. (2022). Can Blockchain technology increase participation in local governments? A review on blockchain-based voting systems in local governments. R&S – Research Studies Anatolia Journal, 5(1), 121–147. https://doi.org/10.33723/rs.1048182.

[12] Beroggi, G. E. G. (2008). Secure and easy internet voting. Computer, 41(2), 52–56. https://doi.org/10.1109/mc.2008.60.

[13] Abuidris, Y., Kumar, R., and Wenyong, W. (2019). A survey of blockchain based on e-voting systems. Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications. https://doi.org/10.1145/3376044.3376060.

[14] (2022). Polys Blockchain-the Technology for 21st Century Elections. [Online]. Available: https://polys.vote/blockchain.

[15] Ohammah, K. L., Thomas, S., Obadiah, A., Mohammed, S., and Lolo, Y. S. (2022). A survey on electronic voting on Blockchain. 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON). https://doi.org/10.1109/nigercon54645.2022.9803127.

[16] Jacob, S. S., Varghese, L. J., Jaisiva, S., Kumar, S. D., Lakshana, R., and Keerthana, R. (2024). Intelligent data storage in electronic voting machine using blockchain system. *"Intelligent Data Storage in Electronic Voting Machine Using Blockchain System,"* 1–5. https://doi.org/10.1109/icstsn61422.2024.10670942.

[17] Alsadi, M., Casey, M., Dragan, C. C., Dupressoir, F., Riley, L., Sallal, M., Schneider, S., Treharne, H., Wadsworth, J., and Wright, P. (2024). Towards end-to-end verifiable online voting: Adding verifiability to established voting systems. IEEE Transactions on Dependable and

Secure Computing, 21(4), 3357–3374. https://doi.org/10.1109/tdsc.2023.3327859.

[18] Vladucu, M.-V., Dong, Z., Medina, J., and Rojas-Cessa, R. (2023). E-voting meets Blockchain: A survey. IEEE Access, 11, 23293–23308. https://doi.org/10.1109/access.2023.3253682.

[19] Almeida, R. L., Baiardi, F., Di Francesco Maesa, D., and Ricci, L. (2023). Impact of decentralization on electronic voting systems: A systematic literature survey. IEEE Access, 11, 132389–132423. https://doi.org/10.1109/access.2023.3336593.

[20] Venugopalan, S. (n.d.). Always on Voting: A Framework for Repetitive Voting on the BLOCKCHAIN_SUPP13315748.PDF. https://doi.org/10.1109/tetc.2023.3315748/mm1.

[21] Chaudhary, S., Shah, S., Kakkar, R., Gupta, R., Alabdulatif, A., Tanwar, S., Sharma, G., and Bokoro, P. N. (2023). Blockchainbased secure voting mechanism underlying 5G network: A smart contract approach. IEEE Access, 11, 76537–76550. https://doi.org/10.1109/access.2023.3297492.

[22] Singh, S., Singh, A., Verma, S., and Dwivedi, R. K. (2023). Designing a Blockchain-Enabled methodology for secure online voting system. *"Designing a Blockchain-Enabled Methodology for Secure Online Voting System,."* https://doi.org/10.1109/idciot56793.2023.10053410.

[23] Joseph, S., Pandey, P., Khari, M., Kumar, K., and Singh, P. P. (2023). Ether Vote: Revolutionizing elections with BlockchainPowered Electronic Voting System. *Ether Vote: Revolutionizing Elections With Blockchain-Powered Electronic Voting System*. https://doi.org/10.1109/smartgencon60755.2023.10442887.

[24] Khaleelullah, S., Hemanth, D. S., Kavitha, E., Viswadutt, B., and Teja, B. S. V. (2023). A novel blockchain based decentralised ballot system. *"A Novel Blockchain Based Decentralised Ballot System," 20*, 1491–1496. https://doi.org/10.1109/icscss57650.2023.10169163.

[25] Farooq, M. S., Iftikhar, U., and Khelifi, A. (2022). A framework to make voting system transparent using blockchain technology. IEEE Access, 10.

Biographies

Astha Sah received the bachelor's degree in computer science engineering from Sharda University in 2025. Her research areas include Blockchain, Internet of things, Artificial Intelligence and deep learning.

Ankit Kumar is a graduate with a Bachelor of Technology (B.Tech) in Computer Science and Engineering from Sharda University. His academic interests lie in emerging technologies such as artificial intelligence, machine learning, and data science. During his undergraduate studies, he actively participated in technical projects and research initiatives, showcasing a strong inclination toward innovation and problem-solving.

Bharat Bhushan is an Associate Professor in the Department of Computer Science and Engineering at Sharda University, India. He holds a Ph.D. in Computer Science and Engineering from BIT Mesra, Ranchi, and has completed his M.Tech in Information Security with distinction. His professional background includes academic and industry experience, and he holds certifications such as MCTS, MCITP, and CCNA. His research interests include cybersecurity, computer networks, and emerging technologies.