ISSN No:-2456-2165

An Exploratory Literature Study on Homomorphic Encryption in Electronic Voting using Blockchain Technology

Anushka Sharma

Abstract:-Over the years, there has been a increase in the usage of distributed ledger technology (DLT), such as blockchain. In the storage and sharing of personal information, privacy is a fundamental concern. Homomorphic en- cryption is a method of securely sending and storing private data between and inside computer systems. Homomorphic encryption has emerged as a potential solution , in which a client's data is encrypted in such a way that some search and manipulation operations can be performed without the need for proper decryption . A lot of researchers have been working or trying to identify real-life usecases of Blockchain technology since peo- ple discovered its potential in several fields . As a consequence of this study, it was discovered that blockchain systems can help solve some of the issues that now plague election systems . In this study, we give a thorough survey of homomorphic encryption research papers or research articles that have been published in the blockchain based e-voting . The primary purpose of this exploratory research article is to assess the current state of blockchain-based voting research, as well as associated possible roadblocks , in order to forecast future trends.

Keywords:- *Blockchain; E-voting system; Encryption; Homomorphic Encryption; Privacy.*

I. INTRODUCTION

Homomorphic encryption is a technique or a method of encrypting text which allows for arbitrary calculations and returns the output in encrypted form . Homomorphic encryption methods have a particular trait called homomorphic evaluation and can be asymmetric or symmetric key encryption techniques . It includes functions for evaluation , decryption , encryption and key generation [26].

- Key←keygeneration (give parameters)
- Cipher ← Encrypt (key, plain) plain ← Decrypt (Key, cipher)
- Cipher res←Evaluate (Cipher1, Cipher2)

On encrypted data, one can perform the basic operations of addition and mul- tiplication where (A) represents or stands for homomorphic addition, while (M) represents or stands for homomorphic multiplication. Below is the operations which are represented as follows:[15]

- ➢ *Adding Two Ciphers in a Homomorphic Manner*:

Given two cipher c1= Encryption(Key, plaintext1) and c2 = Encryption(Key, plaintext2) for two plain texts p1 and p2, addition = c1 (A) c2 = Encryption(Key, p1+p2).

- ➢ *Adding Cipher and Plain texts in a Homomorphic Manner*:

Given two cipher c1=Encryption(Key, plaintext1) and a plain text p1, addition = c1 (A) c2=Encryption(Key, p1+p2).

- ➢ *Multiplication of Two Ciphers in a Homomorphic Manner:*

Given two cipher c1 = Encryption(Key, plaintext1) and c2 = Encryption(Key, plaintext2) for two plain texts p1 and p2, addition = c1 (M) c2 = Encryption(Key, p1 × p2).

- ➢ *Multiplication of Cipher and Plain Texts in a Homomorphic Manner*:

Given two cipher c1 = Encryption(Key, plaintext1) and a plain text p1, multi- plication=c1 (M) c2 = Encryption(Key, p1 × p2).

Blockchain technology has developed vastly in the past years. Blockchain tech- nology has continued to evolve, expanding its scope to include a wide range of applications and exceeding even its developers' hopes. It's capable of generating trustworthy transactions amongst parties who don't trust one other. The use of cryptographic algorithms in blockchain has increased the data's security.These are bundled or packed together as blocks and this is the reason they tamper- proof.

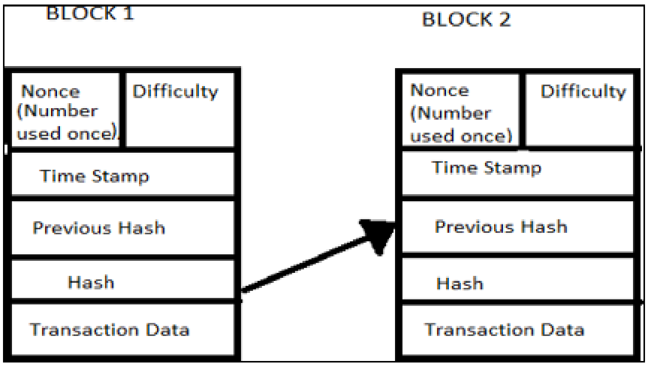
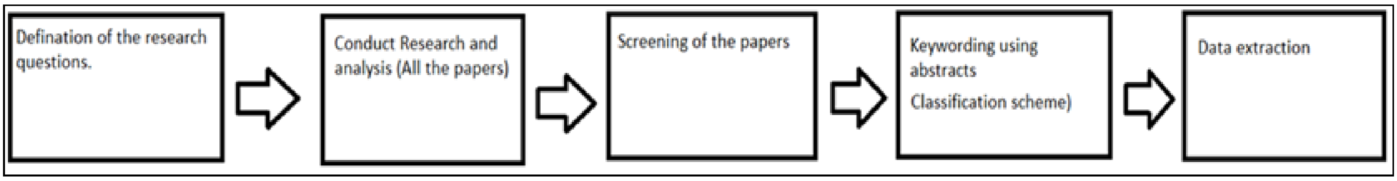


Fig 1 Structure of Block in Blockchain

Blockchain can be useful in the design of distributed systems.The privacy re- lated concerns like the disclosure of transaction amount or true identity should not be neglected or missed for the protection of the user and their interests. When the blockchain is linked into a Business Logistics Management(BLM) or SCM(supply chain management), for example, if the supplier-buyer relation- ships or any more information for each conversation are not protected, the secrets about the trade of suppliers may be leaked [24].Based on the above, a comprehensive review and assessment of blockchain's privacy preservation is required.

In the contemporary years, electronic voting based on block-chain based tech- nology has grown in importance as a means of overcoming some of the issues that arise with e-voting. Because of the blockchain's immutable nature it is con- sidered as decentralised ballot box which is distributed in nature. Online voting, also known as decentralised voting, is a good illustration of how the blockchain may be used. The concept of digital balloting structures brings in general pub- lic electoral procedure quicker and undemanding in the cutting-edge society. It normalizes it withinside the voters, eliminates a positive energy hurdle among the voter and the elected candidate, for this reason making it a powerful man- ner for casting vote on this era of technology[86].When using blockchain, voter anonymity can be achieved through cryptographic techniques and the use of tamper-proof structures.

➢ *Selection of Results*


Defination of the research questions.
Conduct Research and analysis (All the papers)
Screening of the papers
Keywording using abstracts
Classification scheme)
Data extraction

- *Research Questions*

✓ Is blockchain along with or when combined with Homomorphic encryption good enough to support electronic voting?
✓ What are the latest or ongoing research topics and proposed solutions or potential solutions ?
✓ What are the next steps or phases in the blockchain-based e-voting system's research?

- *Data Extraction*

Research articles that were peer-reviewed, conference proceedings papers, book chapters, journal articles and focused on Blockchain Technology e-voting and Homomorphic encryption both were considered for this exploratory paper or survey paper. The publications should have good impact factor(IF) or score in which they were published in. One more factor was considered that the Re- search Articles should be communicated and published in English - Language. The papers that have been chosen have all been published after 2014. These findings or results demonstrates that blockchain-based electronic voting is a very new field of study.

While doing the extensive analysis of the research articles it was found that there has been a rapid increase or growth in the e-voting based on blockchain.

Table 1 Year-wise Research Articles/Papers

Year	**Paper**
2015	[89]
2016	[54],[73],[18],[14]
2017	[30],[74],[48],[6],[65]
2018	[59],[87],[80],[68],[81],[32],[44]
2019	[85],[70],[47],[59],[70],[80],[86]
2020	[56],[12] [46],[75],[82],[1],[22],[8],[64],[25],[75]
2021	[16],[55],[76],[16],[36],[58],[29],[10],[55],[62],[72],[51],[71],[20]
2022	[23],[5],[79],[50],[39],[2],[19],[27],[9],[57],[7],[17],[49],[35],[53],[52],[63],[3],[40],[11],
	[61],[77],[45],[60],[4],[37], [28],[67],[78]

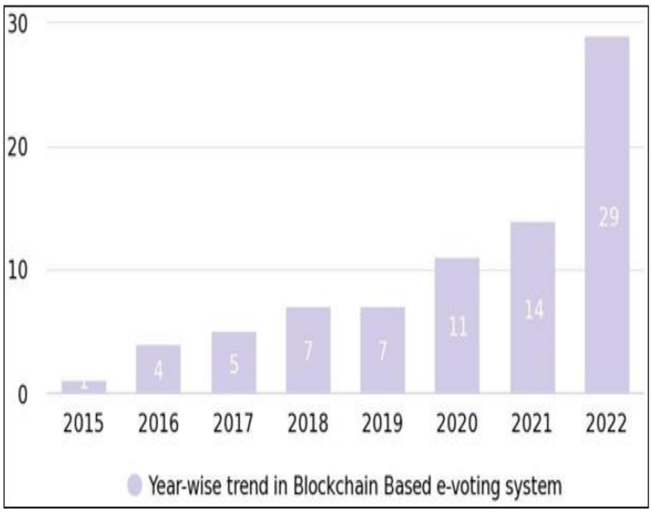


Fig 2 Graph Representing Year-Wise Trend

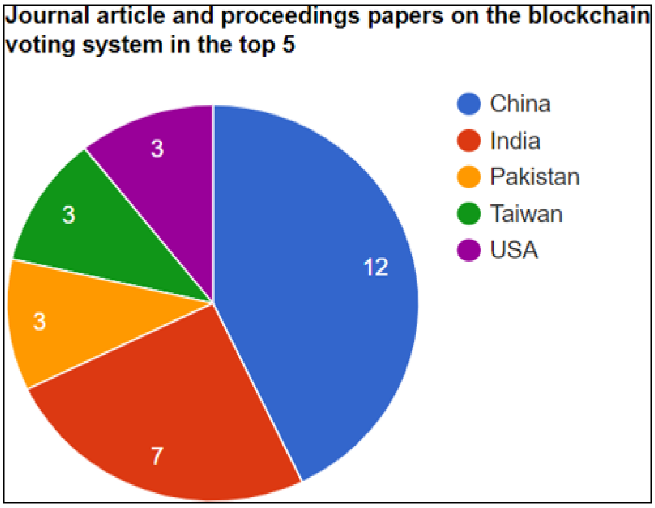


Fig 3 Top Five Countries in on the Blockchain based Electronic Voting System that Published Articles and Proceedings

The contribution to the number of articles and the research done in this domain of block-chain e-voting published by China and India are remarkable. So, this can be considered as the new blooming era in the field of Blockchain based secure e-Voting.

➢ *Background*

A P2P(peer-to-peer) network's nodes maintain a blockchain. The blockchain's basic structure might be divided into three levels: databases,the underlying P2P(peer-to-peer) network,and various applications. The P2P(peer-to-peer) network is in-charge of ensuring that blockchain nodes can easily communi- cate with one another, despite the fact that they are geographically scattered and yet equally privileged participants in the application. In a P2P network, there is no centralised server, and each node is both an information consumer and a source of information.The P2P network's ”flat” topology is a crucial foun- dation of the blockchain's decentralized characteristic [34]. The main objective of blockchain is to send messages consistently and securely between account addresses. The global ledger is in charge of this. The account address which is an non-repeated digital pseudonym that is produced by the user using public key cryptography (for example, elliptic curve encryption). Each communica- tion is done with a transaction, essentially a record including the sender's and receiver's addresses,signatures,messages and from associated parties and so on. The blocks are linked in chronological sequence hence the name blockchain. Blockchain's immutability, transparency, and distributed properties provides a solution to the 'trust problem. There are three types of blockchains based on permissioning:consortium blockchain, public blockchain and private blockchain.

- *Consortium Blockchain:*

  A consortium blockchain (e.g., the HyperLedger) is the one in which the consensus procedure or process which is based on pre- selected grouping of nodes.

- *Public Blockchain :*

  Public blockchain (such as Ethereum or Bitcoin) is one that anyone can submit the transations,read the transactions and to check if the added blocks are genuine. Public blockchain are completely transparent ledger in nature.

- *Private Blockchain:*

  In all key attributes, a private type of or catergory of blockchain is the opposite of a public type of or catergory blockchain, where the rights to write are kept centralised to one organisation and the read rights can be restricted or public to an arbitrary extent. Finally, the term ”private blockchain” refers to anything that isn't totally public. It allows you a lot of flexibility in terms of governance and management.

E-voting has a number of advantages over traditional voting systems, including reduced human error, lower operating costs, and speedier results. Furthermore, due to the accessibility of the elderly and reticent adolescents, online voting developments are improving voter engagement. Furthermore, voters who live abroad or in other countries are permitted to vote more freely. Furthermore, voters who live abroad or in other countries are permitted to vote more freely. E-voting systems, on the other hand, have the potential to vulnerabilities like software, hardware and infrastructure [75]. Furthermore,practically all election systems have the possibility for insider assaults.

The following are the most critical features of an ideal electronic voting sys- tem:

- *Accuracy:*

  The electronic voting system should be capable of accurately count- ing and recording each ballot.[41]

- *Nonrepeatability* **:**

  A voter can caste only one vote.[31]

- *Eligibility* **:**

Only eligible and permitted voters are allowed to vote.[87]

- *Impartiality*:

The voting results should accurately reflect the voter's will and should not be influenced by anyone.

- *Privacy*:

The ballot should be protected from unauthorised access.

- *Integrity*:

The election result cannot be changed in any way.Once the vote is casted by the voter it should be unaltered.[13]

- *Noncoercibility*:

None should have the ability to track down or to know the person who voted for which candidate.[21]

- *Blockchain-based E-Voting Systems issues Difficulties which are listed below:*

For a limited or lesser number of candidates or voters or users blockchain works well. But in the case of large-scale elections when the number of candi- dates or voters or users on the network increases, resulting in a larger transaction cost and duration which ultimately leads to the problem of scalability.

While operating and maintaining online voting systems is much less expen- sive than traditional elections, initial deployments can be costly, especially for companies.Blockchain based e-voting has costly initial setup.

➢ *Privacy Threats*

As stated earlier, a blockchain consists of or hash of the last or the previous transaction, trade values, timestamp , sender's signature and address of participants. Two essential e-vote casting programs, evolved in current years, have also recognized essential protection risks. Below are some of the threats or pos- sible attacks.

- *DoS Attacks*:

A denial-of-service assault is a type of cyber threat in which a malicious attacker tries to make assets unavailable at the community to its clients with the aid of using interrupting the provider of a number that is linked to the Internet.The use of anonymity is one of the methods for hiding IP ad- dresses in P2P networks.

- *Sybil Attacks*:

It is a cyber assault wherein an attacker subverts a P2P net- work's recognition machine with the aid of producing a large wide variety of pseudonymous identities and making use of them to attain an unfair advantage. In phrases of blockchain de-anonymization, Sybil assaults may want to harm or block decentralised anonymity protocols, consequently growing the threat of coming across users actual identities.

One outstanding cryptographic algorithms that supply a technique to this chal- lenge is homomorphic encryption, which allows information to be shared amongst gadgets with out compromising protection. Blockchain can contribute, specif- ically to make sure confidentiality and following information integrity can be specified as contributions of blockchain structures.

- Blockchain structures promise an inexpensive fee within side of the lengthy run. Installing and running a stable information garage machine in allotted structure involves high fee and protection risks. Blockchain is alleged to be more secure and inexpensive than other programs.
- It affords immediate consequences. In a few methods, ballots or votes must be reviewed in diverse vote casting regions after which collected in valuable units. While those tactics take a long time, determining the election's ramifications can take even longer. The election results can be reliably released in minutes rather than hours by combining vote casting with blockchain.
- After the primary vote casting process, with increased confidence, extra electorate can take part in elections.

➢ *Motivation*

With the growing resource and popularity resource of cryptocurrencies ,such as, Ethereum and Bitcoin, they are being forced to consider a fundamental flaw in the original design: scalability. The number of transactions is growing exponentially as cryptocurrencies become more widespread.The graph below demonstrates that cryptocurrencies are being accepted at a rapid rate, but as they have grown in popularity, a number of difficulties have arisen, the most serious of which being the issue of scalability. The fundamental issue is that the Bitcoin theory is founded on the core principle that mining nodes must validate all the transactions that occurs in the network.

Scalability, storage , data protection, cost-effectiveness, bogus entries and se- curity are all aspects of blockchain operations that need to be improved, as seen by the aforementioned observations.

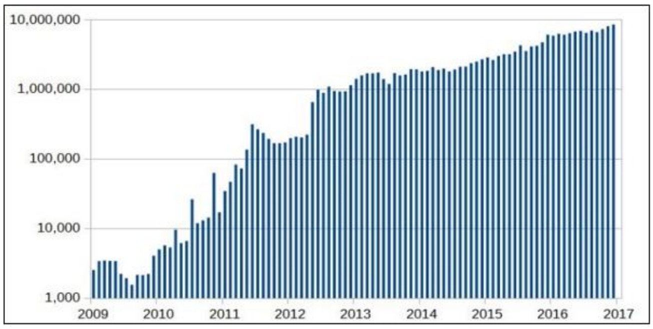


Fig 4 Graph Informing the Increase in Bitcoin Transactions (10 years).
Source : Blockgeeks.com

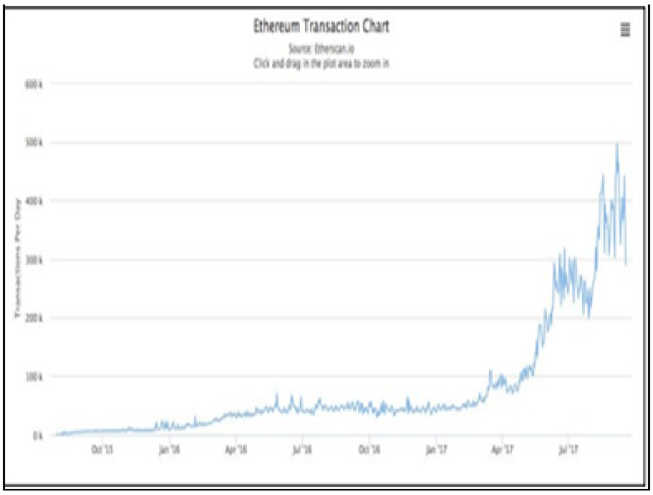


Fig 5 Graph Informing the Escalation in Ethereum Transactions (10 years)
Source : blockgeeks.com

Due to this issue, Bitcoin's developers have proposed Lightning Protocol which can enhance the speed of the process of verification, and Ethereum's creators have offered the sharding solution to solve the problem.

Because techniques demand significant computational requirements, scalability is a major concern when using homomorphic encryption for blockchain. Al- though fully homomorphic encryption is adequate for ensuring data privacy and is compliant with many existing privacy laws, it has not yet been developed to meet all of the desired features. Large computational overhead, noise, and a disproportionately large memory size are all issues that must be addressed.

- *Organization of Paper*

The remaining of this paper is organised in the following manner. To be- gin, had gone through the basics of the blockchain ideas, knwoledge , con- cepts and the extent of current blockchain applications. Section 2 gives the overview of the methodologies put in and used by researchers .We have dis- cuss different techniques for security requirements of the system Cryptographic technique(Homomorphic Encryption) for transaction privacy are classified and compared against blockchain. In addition, we outline these strategies and iden- tify future research topics that need to be investigated further along with the drawbacks of this type of system in order to address blockchain problems in e-Voting. Finally, this paper comes to a close along with conclusion.

II. METHODOLOGY

A blockchain proposal called Hawk uses ZKPs to verify transactions and ex- ecutes private smart contracts off-chain. In blockchain applications, homo- morphic encryption can be used to successfully provide transaction authenti- cation. A homomorphic cryptosystem (HC) is a cryptographic technology that adheres to homomorphism in order to preserve ciphertext arithmetic opera- tions.Transaction authentication can be effectively implemented using homo- morphic encryption. By permitting statistical analysis on encrypted records maintained by blockchain technology, homomorphic encryption provides a so- lution to this problem. Large computational overhead, noise, and a dispropor- tionately large memory size are all issues that must be addressed.

➢ *Literature Survey*

- *According to Author [33],*

This research uses smart contracts to verify and record the votes in the ballots which eventually increases the voters reliability and trust on the voting process. Discussing about the methodology proposed by the author, the overall process has 7 stages. The RSA encryption algorithm has been used which increases the space in the overall process. Homomorphic encryption standard has also been used to stop the reliability of third-party in the elections to count the votes casted and announce winner. The overall system reduces the wastage of election resources. This proposed methodology or system can be enhanced by using other encryption standard which requires lesser space like ECC (Elliptic-curve cryptography) because RSA requires more length of key space. The scalability is less in the case of RSA. More-over, ECC has low CPU consumption as well as memory usage.

- *According to Author [43],*

The proposed system is useful in all the types of elections like student elections, parliament elections etc. It should ideally be based on a public blockchain. Other types of blockchain can be used in place of the public blockchain, but the recorded data or the stored data (votes) must be accessible. Any user can verify it. Any person or citizen who is interested in block-chain voting is represented by the user. The author has used homomor- phic encryption to encrypted the data and the data is stored in a blockchain. Thus, here homomorphic encryption standard is used to hide the voter's data. Nobody knows what's going on because the outcomes aren't revealed until the end. We employed Zero-knowledge proof to ensure that the votes contained valid values, such that a voter can only cast one vote and cannot cast two or more. The proposed system has the demerit or disadvantage of using public blockchain because the votes will be visible to anyone and can be manipulated for the party getting lesser votes. So, live vote showing or sharing is not a good idea.

- *According to Author [69],*

The proposed system includes homomorphic encryption and cloud data storage. The vote will be encrypted and associated with the candidate for whom he or she voted, and this data or information will be preserved. All of the encrypted ballots or votes are then re-encrypted us- ing homomorphic encryption. When data is stored in the cloud, homomorphic encryption will help to enhance and improve the integrity of the data. The proposed system can be enhanced by including other features. In the future, Aadhar-based identification of the citizen or user could be added into the system to allow for a more efficient and harmonious voting procedure

- *According to Author [38] ,*

There are 5 phases in the system naming them as initialization, Registration, Voting, Tallying, and Results Announcement are all aspects of the online voting system, but security must be maintained throughout. Authorities, candidates, voters, and the Public Bulletin Board are the institutions participating in this system (PBB). A pair of keys must be generated by each authority. Assuming at least one authority is trustworthy, all of the authorities should create a public key called Cumulative Public Key (CPK). Voters are verified and registered using their Voter ID in the Voters List Database. The findings are computed using Elliptic ElGamal's homomorphic characteristic. The ballots are not decrypted separately, the ballots are summed and decrypted using Elliptic ElGamal Cryptography's additive characteristic. The votes are calculated using ECC and homomorphic encryption. The results can be verified by checking the PBB to see if their ballot has been changed or not. This research will be further upon with the notion of using Blockchain framework for poll behaviour prediction using classification and deep learning techniques.

- *According to Author [56],*

To disguise or hide ballots and count votes, homomorphic signcryption is utilised. The voting results may be calculated rapidly using smart contracts. There is no third-party involvement. When multiple candidates are engaged, electronic voting based on blockchain can achieve vote counting without the involvement of a third party, and it tackles the problem of maintaining anonymity and public verifiability. Simultaneously, depending on the number of candidates, the protocol can modify the length of the ballot, allowing for more flexible and convenient voting. In terms of security analysis, the electronic voting protocol proposed in this research is secure and trustwor- thy.

- *According to the Author [83],*

By confirming parameters (such as the elec- tion's public key), the election administrator launches a voting contract. With the usage of the voting contracts votes can be casted. The transaction reverts if the vote is not verified as valid by the checks conducted in the smart contract. The vote is regarded final once it has been mined by the blockchain's consensus mechanism. There is a risk that our system will experience an unsuccessful or erroneous or abortive issue. Because any voter can stop or abort the tally without submitting his or her vote. So, it must be assumed that all registered voters submit legal votes.

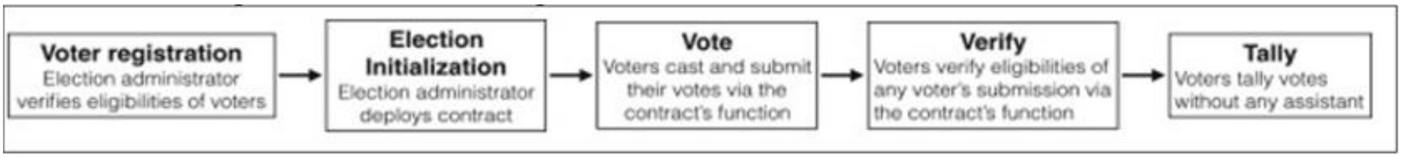

Voter registration
Election administrator verifies eligibilities of voters
Election Initialization
Election administrator deploys contract
Vote
Voters cast and submit their votes via the contract's function
Verify
Voters verify eligibilities of any voter's submission via the contract's function
Tally
Voters tally votes without any assistant

Fig 6 Steps to Cast Vote [83]

- *According to the Author [88],*

The suggested protocol preserves voters' pri- vacy and allows for the identification and rectification of cheating without the involvement of a third party. The Hyperledger Fabric implementation demon- strates that the protocol is workable and practical for small to medium-scale voting concerns.

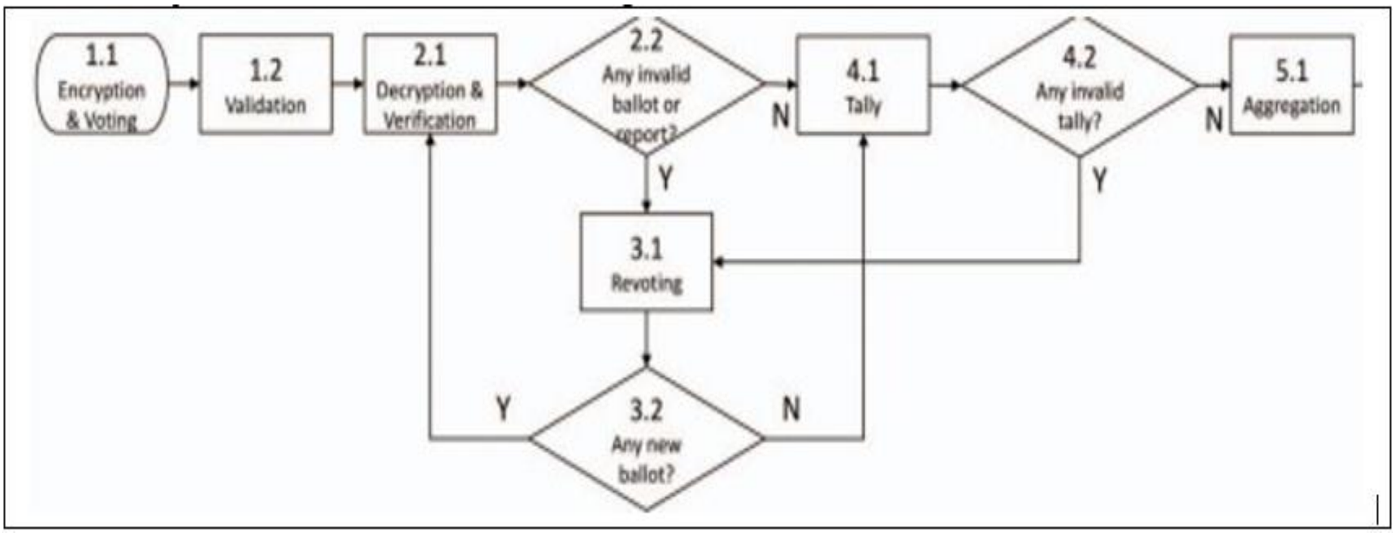


Fig 7 Over-all Flow of the Voting Process [88]

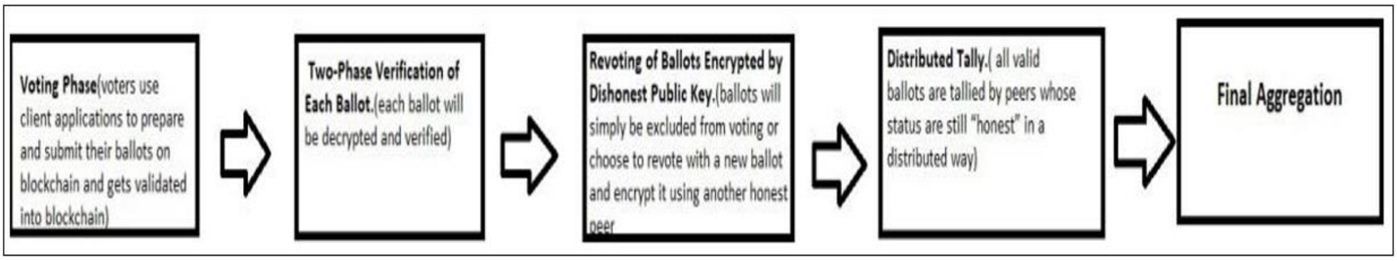

Voting Phase(voters use client applications to prepare and submit their ballots on blockchain and gets validated into blockchain)
Two-Phase Verification of Each Ballot.(each ballot will be decrypted and verified)
Revoting of Ballots Encrypted by Dishonest Public Key.(ballots will simply be excluded from voting or choose to revote with a new ballot and encrypt it using another honest peer
Distributed Tally.(all valid ballots are tallied by peers whose status are still "honest" in a distributed way)
Final Aggregation

Fig 8 Steps to Cast Vote

- *According to the Author [84],*

Instead of using only ElGamal encryption only the author has proposed a new scheme which is mergeing or combining ElGamal encryption and group-based encryption into single umbrella or one scheme. The information on ballots or votes is protected or encrypted using each voter's secret key, and the candidates' public keys are used to conceal the information.These hidden shares of the voters further obscure the homomorphic encryptions of the votes. Because the secret shares multiply to 1, the entire sum of all votes can be decrypted at the end of the election.

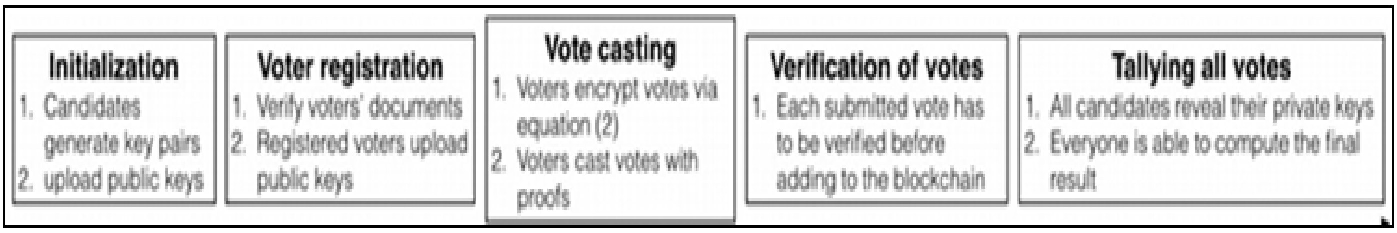

Initialization
1. Candidates generate key pairs
2. upload public keys
Voter registration
1. Verify voters' documents
2. Registered voters upload public keys
Vote casting
1. Voters encrypt votes via equation (2)
2. Voters cast votes with proofs
Verification of votes
1. Each submitted vote has to be verified before adding to the blockchain
Tallying all votes
1. All candidates reveal their private keys
2. Everyone is able to compute the final result

Fig 9 Steps to Cast Vote [84]

- *According to the Author [66],*

The proposed article uses tamper proof Blockchain Technology to achieve universal transparency, verifiability and correctness of electoral data. Using control mechanisms and secure group communication, the work of distributing electoral data in the form of blocks and tamper proof Blockchain ledger was completed. The suggested scheme's offline aspect shields the electoral process from attacks that may occur in an online environment. Its locality-specific feature limits a voter's ability to vote solely in a registered ward. The futher research may be developing a test bed for the suggested vot- ing scheme, offer a security study of NTRU , and attempt to build a mobility-oriented mechanism in the upcoming years.

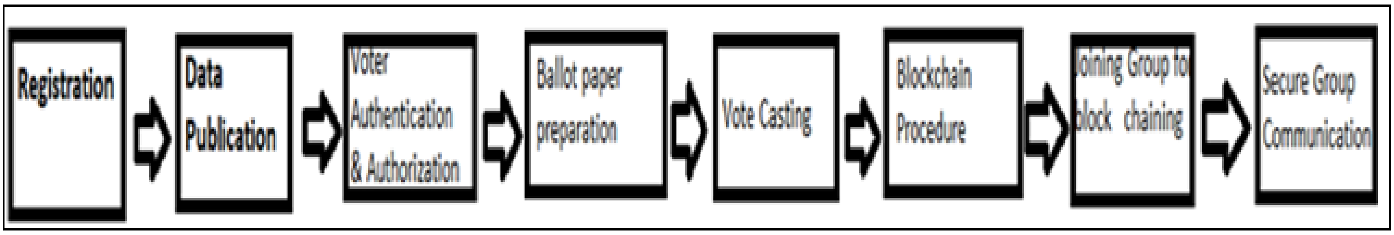

Registration
Data Publication
Voter Authentication & Authorization
Ballot paper preparation
Vote Casting
Blockchain Procedure
Joining Group to block chaining
Secure Group Communication

Fig 10 Steps to Cast Vote

- *According to the Author [76],*

They have come up with a private network and the Ethereum blockchain API. The reason for this decision is because Ethereum is a well-known and safe blockchain application architecture. Smart contracts, on the other hand, are not suited for keeping sensitive data because they are visible and transparent to all voting participants. Because of its privacy proper- ties, homomorphic encryption is preferred in this system. The homomorphism functionality allows you to manipulate ciphertexts without having to decrypt them. This characteristic allows any third party to count encrypted ballots without exposing any information on the ballot in a voting system.

- *According to the Author [42],*

The proposed system looks into the bene- fits of the votes casting the votes by encrypting the votes data. It is different from the voting systems proposed till now. The fundamental advantage of this new electronic voting system is that it enables for statistical analysis of vote results while protecting voter anonymity. The e-voting system may ask vot- ers questions about their age, gender, and educational background in order to conduct extensive statistical analysis. Voters' responses to these questions very definitely contain personal information about them; but, because each response is homomorphic encrypted, voters can react without fear of disclosing them- selves. The acquired data does not need to be decrypted even during statistical analysis, illustrating the strength of homomorphic encryption. Existing systems count votes in encrypted formats, whereas the new method counts votes in plain text format. To put it another way, present methods necessitate the addition of encrypted data, whereas the new approach does not. The disadvantage is that this e-voting system requires larger data size for each block compared to other systems.

- *Drawbacks of Blockchain based System*

The methods outlined above are summarised and discussed in this section. Our comparison focuses on their impact on privacy protection, significant shortcomings, and current implementations. Finally, we outline potential future research directions in the field of blockchain privacy preservation.

- *Legal Accountability and Traceability*

Not all countries supports and have the resources for blockchain based technol- ogy. New set of legal regulatories will be needed to be done.

- *Scalable*

While considering small number of the users it is easy and good to have blockchain as the system. But if we consider large elections like in India or USA where the population of the country is huge it is very difficult and even important to consider scalability of the system. Suppose, elections are to take place in USA today. in the 2020 elections in United States of America (USA), the elec- tion authority declared 15,80,00,000 voters out of the eligible 24,00,00,000. At least, it is nec- essary to have an ability to use ((15,80,00,000/8 h)/60 m)/60 s =(19750000)/60 m)/60 s=5486.11 votes or in other words transactions per second.

- *Lack of Knowledge*

In developing and under-developed countries where the access of simple human necessities is scarce it is very difficult to arrange mobile or computer or any other electronic devices for all the citizens of the country. If the country is ar- ranging voting in respective area booths then also most of the people will not have the knowledge of voting in this type of system. So, training the voters is another work which will be needed to be done.

- *Energy Usage*

The energy consumption is very high in blochchain based systems. So, countries which don’t have the provision of the simple human necessities will not be able to bear the cost of these expenses.

III. FUTURE RESEARCH DIRECTIONS

- *Use of Machine Learning and Deep Learning*

Machine learning algorithms offer incredible learning potential. These features can be used to make the blockchain smarter than it was previously. This connec- tion may aid in the enhancement of the security of the blockchain’s distributed ledger. Additionally, the computational power of ML can be leveraged to re- duce the time it takes to determine the golden nonce, as well as to improve data sharing pathways. Furthermore, the decentralised data architecture feature of blockchain technology allows us to create many better machine learning mod- els. The integration of data science with blockchain can be helped to do the predictive analysis of the trends of the voting and the voters.

- *Storage*

Storing of large number of casted votes along with each voters data requires high volume of data storage. So, moving towards cloud storage should be considered as an option.

- *Voter Data Protection*

While casting the votes, there are many types of questions or data which are required by the voters to enter. These data includes some of the information which if got into wrong hands can be harmful for the voter citizen as well as the country. So, while also allowing for the keeping of a separate record of those who voted along with the casted votes.

A number of study or research gaps in e-voting have emerged, which must be addressed in future studies. Scalability attacks, energy consumption, the usage of untrusted systems, storage, and voter data protection are all potential draw- backs that should be addressed. Blockchain voting techniques may-be exposed to un- foreseen security risks and vulnerabilities.

- *Bogus Registration or Votes Entry*

If a voter without casting the vote leaves the application where the votes were being casted then those votes will be considered bogus. It is very important to exclude these votes can be used in other types of ways which may not be in the trust of voters and the democracy.

IV. CONCLUSION

Due to its decentralised nature and safety function, blockchain has recently at- tracted a lot of interest in decentralised application systems. It offers a whole new approach to store, disseminate, and update data, and it will be critical to the future interactive internet system’s success. The goal of this research survey or exploratory research is to explore and evaluate recent research on blockchain- based voting systems using the homomorphic encryption scheme. The report is a study that highlights existing in e-voting research using blockchain technology along with the homomorphic encryption scheme. The blockchain concept and

Table 2 Security Requirements

<table>
<tr><th>Security Requirements</th><th colspan="11">References</th></tr>
<tr><th colspan="2">[33]</th><th>[43]</th><th>[69]</th><th>[38]</th><th>[56]</th><th>[83]</th><th>[88]</th><th>[84]</th><th>[66]</th><th>[76]</th><th>[42]</th></tr>
<tr><td>Eligibility</td><td></td><td></td><td>✓</td><td>✓</td><td>✓</td><td></td><td></td><td>✓</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>Verifiability</td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Privacy</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Non-Repeatability</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td></td><td>✓</td><td></td><td></td><td></td><td>✓</td><td></td></tr>
<tr><td>Authentication</td><td></td><td></td><td></td><td></td><td></td><td></td><td>✓</td><td></td><td>✓</td><td></td><td></td></tr>
<tr><td>Accuracy</td><td></td><td>✓</td><td></td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Tamper Proof</td><td></td><td></td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td></td><td></td></tr>
<tr><td>Anonymity</td><td>✓</td><td></td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td></td><td></td><td></td></tr>
<tr><td>Integrity</td><td></td><td>✓</td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Data Immutability</td><td>✓</td><td></td><td>✓</td><td>✓</td><td>✓</td><td></td><td>✓</td><td>✓</td><td>✓</td><td></td><td></td></tr>
<tr><td>Confidentiality</td><td></td><td>✓</td><td></td><td>✓</td><td>✓</td><td>✓</td><td></td><td>✓</td><td></td><td></td><td></td></tr>
<tr><td>Transparency</td><td>✓</td><td></td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td></td><td>✓</td></tr>
</table>

Its uses are introduced first, followed by information on current e-voting sys- tems using the homomorphic encryption scheme. The inadequacies in present e-voting systems are then highlighted and examined, as well as the potential of the blockchain idea to improve e-voting, current solutions for blockchain-based e-voting, and prospective research paths on blockchain-based e-voting systems.

At the end, considering the scope of the blockchain based e-voting systems, it is necessary to transition to this type of system but slowly and keeping in mind the scalability issues and the security issues. There is still more to be achieved in this domain. It is a long way to come for the governments as well as the developers and the researchers to look into the shortcommings of the system.

REFERENCES

[1]. Nurul Hanis Abd Rasid. Blockchain technology in e-voting: Comparative study.

[2]. Jacob Abegunde. Adeva: A decentralized electronic voting application using blockchain technology. 2022.

[3]. Taiwo Adekeye. Securing the electoral e-voting system using blockchain technology.

[4]. Yasser Asrul Ahmad, Muhammad Fadhil Shaharuddin, Teddy Surya Gu- nawan, and Fatchul Arifin. Implementation of an e-voting prototype using ethereum blockchain in ganache network. In *2022 IEEE 18th International Colloquium on Signal Processing & Applications (CSPA)*, pages 111–115. IEEE, 2022.

[5]. Lukman Adewale Ajao, Buhari Ugbede Umar, Daniel Oluwaseun Olajide, and Sanjay Misra. Application of crypto-blockchain technology for securing electronic voting systems. In *Blockchain Applications in the Smart Era*, pages 85–105. Springer, 2022.

[6]. Elham Akbari, Qing Wu, Wenbing Zhao, Hamid R Arabnia, and Mary Qu Yang. From blockchain to internet-based voting. In *2017 International Con- ference on Computational Science and Computational Intelligence (CSCI)*, pages 218–221. IEEE, 2017.

[7]. Basharat Ali, Fawad Iqbal, Irshad Hussain, and Muhammad Younas. An efficient e-voting algorithm and dapp using blockchain technology.

[8]. Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, and Sajib Ahamed. Classification of blockchain based voting: Challenges and solutions. In *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, pages 1–6. IEEE, 2020.

[9]. Ch Anwar ul Hassan, Muhammad Hammad, Jawaid Iqbal, Saddam Hus- sain, Syed Sajid Ullah, Hussain AlSalman, Mogeeb AA Mosleh, and Muhammad Arif. A liquid democracy enabled blockchain-based electronic voting system. *Scientific Programming*, 2022, 2022.

[10]. Neha S Aswale, Manasi S Mali, Shraddha S Irale, Saakshi S Dhoka, Tan- ishqua H Mudaliar, Gurunath G Machhale, and Rahul G Sonkamble. Privacy preserved e-voting system using blockchain. *Available at SSRN 3852951*, 2021.

[11]. Ankita Bansal, Abha Jain, and Pardeep Kumar. Ensuring security of digi- tal voting through blockchain technology. In *A Fusion of Artificial Intelli- gence and Internet of Things for Emerging Cyber Systems*, pages 317–331. Springer, 2022.

[12]. Albin Benny. Blockchain based e-voting system. *Available at SSRN 3648870*, 2020.

[13]. LC Bollinger and MA McRobbie. Ensuring the integrity of elections. *Se- curing the Vote: Protecting American Democracy; National Academies of Sciences: Washington, DC, USA*, pages 103–105, 2018.

[14]. Vanessa Bracamonte, Shigeichiro Yamasaki, and Hitoshi Okada. A dis- cussion of issues related to electronic voting systems based on blockchain technology. 2016.

[15]. Ratnakumari Challa. Homomorphic encryption: Review and applications. *Advances in Data Science and Management*, pages 273–281, 2020.

[16]. Seiwoong Choi, Jihun Kang, and Kwang Sik Chung. Design of blockchain based e-voting system for vote requirements. In *Journal of Physics: Con- ference Series*, volume 1944, page 012002. IOP Publishing, 2021.

[17]. Rishikesh Choudhari, M Shivakumar, Shreyas Nandavar, Shruti Maigur, Saroja V Siddamal, Suneeta V Budihal, and Shrishail M Pattanshetti. Decentralized and secured voting system with blockchain technology. In *Security, Privacy and Data Analytics*, pages 167–182. Springer, 2022.

[18]. Jason Paul Cruz and Yuichi Kaji. E-voting system based on the bitcoin pro- tocol and blind signatures. *IPSJ Transactions on Mathematical Modeling and Its Applications*, 10(1):14–22, 2016.

[19]. Camilo Denis González, Daniel Frias Mena, Alexi Massó Muñoz, Omar Rojas, and Guillermo Sosa-Gómez. Electronic voting system using an enterprise blockchain. *Applied Sciences*, 12(2):531, 2022.

[20]. V Dhiman, U Kumar, A Narla, A Kumar, V Sharma, and NP Singh. An election system using blockchain. In *Smart Computing: Proceedings of the 1st International Conference on Smart Machine Intelligence and Real- Time Computing (SmartCom 2020), 26-27 June 2020, Pauri, Garhwal, Uttarakhand, India*, page 48. CRC Press, 2021.

[21]. Tassos Dimitriou. Efficient, coercion-free and universally verifiable blockchain-based voting. *Computer Networks*, 174:107234, 2020.

[22]. Moritz Eck, Alex Scheitlin, and Nik Zaugg. Design and implementation of blockchain-based e-voting.

[23]. Muhammad Shoaib Farooq, Usman Iftikhar, and Adel Khelifi. A framework to make voting system transparent using blockchain technology. *IEEE Access*, 2022.

[24]. Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. A survey on privacy protection in blockchain system. *Jour- nal of Network and Computer Applications*, 126:45–58, 2019.

[25]. Amol D Gaikwad, Pankaj Hatwar, et al. Online voting system using blockchain. *IJRAR-International Journal of Research and Analytical Re- views (IJRAR)*, 7(1):374–379, 2020.

[26]. Craig Gentry. *A fully homomorphic encryption scheme*. Stanford university, 2009.

[27]. Daria Golnarian, Kimia Saedi, and Behnam Bahrak. A decentralized and trustless e-voting system based on blockchain technology. In *2022 27th International Computer Conference, Computer Society of Iran (CSICC)*, pages 1–7. IEEE, 2022.

[28]. Rajat Gupta and Shallu Bashambu. Blockchain for online voting sys- tem. *EPRA International Journal of Research and Development (IJRD)*, 7(5):61–63, 2022.

[29]. Suraj Pratap Gupta and Ankur Mani Tripathi. E-voting using blockchain. In *Journal of Physics: Conference Series*, volume 1911, page 012001. IOP Publishing, 2021.

[30]. Rifa Hanifatunnisa and Budi Rahardjo. Blockchain based e-voting record- ing system design. In *2017 11th International Conference on Telecommuni- cation Systems Services and Applications (TSSA)*, pages 1–6. IEEE, 2017.

[31]. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Kon- stantinos Markantonakis. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In *2018 IEEE International Con- ference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Com- puting (CPSCom) and IEEE Smart Data (SmartData)*, pages 1561–1567. IEEE, 2018.

[32]. Friorik P. Hjalmarsson, Gunnlaugur K. Hreioarsson, Mohammad Hamdaqa, and G´ısli Hjálmtýsson. Blockchain-based e-voting system. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 983–986, 2018.

[33]. Jen-Ho Hsiao, Raylin Tso, Chien-Ming Chen, and Mu-En Wu. Decentral- ized e-voting systems based on the blockchain technology. In *Advances in Computer Science and Ubiquitous Computing*, pages 305–309. Springer, 2017.

[34]. Junjie Huang, Liang Tan, Sun Mao, and Keping Yu. Blockchain network propagation mechanism based on p4p architecture. *Security and Communication Networks*, 2021, 2021.

[35]. Mayuri Jadhav, Nupur Patil, Manali Gharat, and Vilas Jadhav. Blockchain technology in voting.

[36]. Uzma Jafar, Mohd Juzaiddin Ab Aziz, and Zarina Shukur. Blockchain for electronic voting system—review and open research challenges. *Sensors*, 21(17):5874, 2021.

[37]. Akshat Jain, Sidharth Bhatnagar, and Amrita Jyoti. Blockchain-centered e-voting system. In *Innovative Data Communication Technologies and Ap- plication*, pages 267–276. Springer, 2022.

[38]. Chandrapriya Jayabal, S. Swarnalaxmi, A. Safa, and I. Elakkiya. *Blockchain Centered Homomorphic Encryption: A Secure Solution for E- Balloting*, pages 811–819. 01 2020.

[39]. Amrita Jyoti, Rashmi Mishra, Rupa Rani, and Ravi Kalra. Evoting us- ing blockchain technology. In *Advances in Computational Intelligence and Communication Technology*, pages 71–83. Springer, 2022.

[40]. Nur Hafizah Mohamed Kassim and Noraini Ibrahim. Uthm e-voting system using blockchain. *Journal of Soft Computing and Data Mining*, 3(1):34–44, 2022.

[41]. Adel Khelifi, Yasmin Grisi, Dima Soufi, Dalya Mohanad, and PVS Shas- try. M-vote: a reliable and highly secure mobile voting system. In *2013 Palestinian International Conference on Information and Communication Technology*, pages 90–98. IEEE, 2013.

[42]. Hyunyeon Kim, Kyung Eun Kim, Soohan Park, and Jongsoo Sohn. E- voting system using homomorphic encryption and blockchain technology to encrypt voter data. *arXiv preprint arXiv:2111.05096*, 2021.

[43]. Kristián Košt'ál, Rastislav Bencel, Michal Ries, and Ivan Kotuliak. Blockchain e-voting done right: Privacy and transparency with public blockchain. In *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)*, pages 592–595. IEEE, 2019.

[44]. Nir Kshetri and Jeffrey Voas. Blockchain-enabled e-voting. *IEEE Software*, 35:95–99, 07 2018.

[45]. V Lalitha, S Samundeswari, R Roobinee, and Lakshme S Swetha. De- centralized online voting system using blockchain. In *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, pages 1387–1391. IEEE, 2022.

[46]. Huilin Li, Yannan Li, Yong Yu, Baocang Wang, and Kefei Chen. A blockchain-based traceable self-tallying e-voting protocol in ai era. *IEEE Transactions on Network Science and Engineering*, 2020.

[47]. Jing Li, Xianmin Wang, Zhengan Huang, Licheng Wang, and Yang Xiang. Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. *J. Parallel Distributed Comput.*, 130:91–97, 2019.

[48]. Kejiao Li, Hui Li, Hanxu Hou, Kedan Li, and Yongle Chen. Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain. In *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th Interna- tional Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/Smart City/DSS)*, pages 466–473. IEEE, 2017.

[49]. Mrs Pushpa Mahapatro. Voting system based on blockchain technology. 2022.

[50]. Muskan Malhotra, Amit Kumar, Suresh Kumar, and Vibhash Yadav. Un- tangling e-voting platform for secure and enhanced voting using blockchain technology. In *Transforming Management with AI, Big-Data, and IoT*, pages 51–72. Springer, 2022.

[51]. Leslie Mark, Vasaki Ponnusamy, Arya Wicaksana, Basilius Bias Christy- ono, and Moeljono Widjaja. A secured online voting system by using blockchain as the medium. *The Smart Cyber Ecosystem for Sustainable Development*, pages 405–430, 2021.

[52]. Sandeep Mishra, Kishore Thapliyal, S Krish Rewanth, Abhishek Parakh, and Anirban Pathak. Anonymous voting scheme using quantum assisted blockchain. *arXiv preprint arXiv:2206.03182*, 2022.

[53]. Solomon Negash. Improving egovernment services with blockchain: Restor- ing trust in e-voting systems. In *International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, pages 265–275. Springer, 2022.

[54]. Ryan Osgood. The future of democracy: Blockchain voting. *COMP116: Information security*, pages 1–21, 2016.

[55]. Micha-l Pawlak and Aneta Poniszewska-Marańda. Trends in blockchain- based electronic voting systems. *Information Processing & Management*, 58(4):102595, 2021.

[56]. Wenlei Qu, Lei Wu, Wei Wang, Zhaoman Liu, and Hao Wang. A elec- tronic voting protocol based on blockchain and homomorphic signcryption. *Concurrency and Computation: Practice and Experience*, page e5817, 2020.

[57]. Md Raufur Rahman, Aanjey Mani Tripathi, and Greater Noida. E-voting with blockchain technology.

[58]. Divya Rathore and Virender Ranga. Secure remote e-voting using blockchain. In *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pages 282–287. IEEE, 2021.

[59]. Kazi Sadia, Md Masuduzzaman, Rajib Paul, and Anik Islam Abhi. Blockchain based secured e-voting by using the assistance of smart con- tract. 03 2019.

[60]. Olga A Safaryan, Kirill S Lemesko, and Elena V Pinevich. Blockchain in the field of voting. 2022.

[61]. Yash Sangolkar, Nikita Marode, Vikas Meshram, Pranav Sarve, Akhilesh Shambharkar, and Sujit Meshram. Online voting system using blockchain.

[62]. MD Sanjaya. *A Blockchain Based Approach for Secure E-Voting System*. PhD thesis, 2021.

[63]. R Savitha, KB Ashwini, and K Prashanth. Blockchain-based online voting system. *ECS Transactions*, 107(1):13195, 2022.

[64]. Srinivasan Selvaraj, P Shobha Rani, A Gnanasekar, and Vignaraj Anand. A blockchain based online voting system: An indian scenario. In *International Conference on Advanced Informatics for Computing Research*, pages 329–338. Springer, 2020.

[65]. Safdar Hussain Shaheen, Muhammad Yousaf, and Mudassar Jalil. Temper proof data distribution for universal verifiability and

accuracy in electoral process using blockchain. In *2017 13th International Conference on Emerging Technologies (ICET)*, pages 1–6. IEEE, 2017.

[66]. Safdar Hussain Shaheen, Muhammad Yousaf, and Mudassar Jalil. Temper proof data distribution for universal verifiability and accuracy in electoral process using blockchain. In *2017 13th International Conference on Emerging Technologies (ICET)*, pages 1–6, 2017.

[67]. Prakhar Sharma, Dev Agarwal, Omkar Jagdale, Shreya B Kadlag, and Nehali Shinde. Blockchain based e-voting decentralized application.

[68]. Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Kon- stantinos Markantonakis. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Com- puting (CPSCom) and IEEE Smart Data (SmartData)*, pages 1561–1567, 2018.

[69]. C Sravani and G Murali. Secure electronic voting using blockchain and homomorphic encryption. *International Journal of Recent Technology and Engineering (IJRTE)*, 8, 2019.

[70]. Xin Sun, Quanlong Wang, Piotr Kulicki, and Mirek Sopek. A simple vot- ing protocol on quantum blockchain. *International Journal of Theoretical Physics*, 58(1):275–281, 2019.

[71]. Yueren Sun, Haoqi Wang, and Dandan Xu. Blockchain: A method to improve voting system. *Academic Journal of Business & Management*, 3(6):95–99.

[72]. Yueren Sun, Dandan Xu, Haoqi Wang, et al. Improved voting system based on blockchain. *Academic Journal of Computing & Information Science*, 4(4), 2021.

[73]. Yu Takabatake, Daisuke Kotani, and Yasuo Okabe. An anonymous dis- tributed electronic voting system using zerocoin. *IEICE Technical Report*, 116(282):127–131, 2016.

[74]. Pavel Tarasov and Hitesh Tewari. Internet voting using zcash. *IACR Cryptol. ePrint Arch.*, 2017:585, 2017.

[75]. Ruhi Ta¸s and Ö mer Ö zgür Tanrıöver. A systematic review of challenges and opportunities of blockchain for e-voting. *Symmetry*, 12(8):1328, 2020.

[76]. Ruhi Ta¸s and Ö mer Ö zgür Tanrıöver. A manipulation prevention model for blockchain-based e-voting systems. *Security and Communication Networks*, 2021, 2021.

[77]. M Thangavel, Pratyush Kumar Sinha, Ayusman Mishra, and Bhavesh Ku- mar Behera. Enabling data security in electronic voting system using blockchain. In *Biologically Inspired Techniques in Many Criteria Decision Making*, pages 119–129. Springer, 2022.

[78]. Manav Tiwari, Utkarsh Thaokar, Sahil Sangwan, and Shubham Gupta. Secure voting system using blockchain method. *International Journal of Research in Engineering, Science and Management*, 5(1):104–105, 2022.

[79]. Cristian Toma, Marius Popa, Catalin Boja, Cristian Ciurea, and Mihai Doinea. Secure and anonymous voting d-app with iot embedded device using blockchain technology. *Electronics*, 11(12):1895, 2022.

[80]. Baocheng Wang, Jiawei Sun, Yunhua He, Dandan Pang, and Ningxiao Lu. Large-scale election based on blockchain. *Procedia Computer Science*, 129:234–237, 01 2018.

[81]. Wei-Jr Wu. An efficient and effective decentralized anonymous voting sys- tem. 04 2018.

[82]. Ze Xu and Sanxing Cao. Efficient privacy-preserving electronic voting scheme based on blockchain. In *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pages 190–196. IEEE, 2020.

[83]. Xuechao Yang, Xun Yi, Surya Nepal, and Fengling Han. Decentralized vot- ing: a self-tallying voting system using a smart contract on the ethereum blockchain. In *International Conference on Web Information Systems Engineering*, pages 18–35. Springer, 2018.

[84]. Xuechao Yang, Xun Yi, Surya Nepal, Andrei Kelarev, and Fengling Han. Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities. *Future Generation Computer Systems*, 112:859–874, 2020.

[85]. Haibo Yi. Securing e-voting based on blockchain in p2p network. *EURASIP Journal on Wireless Communications and Networking*, 2019(1):1–9, 2019.

[86]. Shufan Zhang, Lili Wang, and Hu Xiong. Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*, 19(3):323–341, 2020.

[87]. Wenbin Zhang, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra, and Sheng Huang. A privacy-preserving voting protocol on blockchain. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 401–408, 2018.

[88]. Wenbin Zhang, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra, and Sheng Huang. A privacy-preserving voting protocol on blockchain. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pages 401–408. IEEE, 2018.

[89]. Zhichao Zhao and T-H Hubert Chan. How to vote privately using bitcoin. In *International Conference on Information and Communications Security*, pages 82–96. Springer, 2015.