End to end secure e-voting using blockchain & quantum key distribution

Article *in* Materials Today Proceedings · August 2021

DOI: 10.1016/j.matpr.2021.07.254

Sweta Gupta
Jagran Lakecity University
6 PUBLICATIONS **103** CITATIONS

Dr. Ishan Y. Pandya
Gujarat Ecological Education and Research Foundation (GEER)
50 PUBLICATIONS **218** CITATIONS

Abhishek Bhatt
Symbiosis Skill and Professional University
37 PUBLICATIONS **389** CITATIONS

Dr.Komal Mehta
itm universe vadodara https://scholar.google.co.in/citations?hl=en&user=WGtBzd…
46 PUBLICATIONS **73** CITATIONS

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

End to end secure e-voting using blockchain & quantum key distribution

Sweta Gupta [a,*], Aparna Gupta [b], Ishan Y. Pandya [c], Abhishek Bhatt [d], Komal Mehta [e]

[a] *School of Engineering & Technology, Jagran Lakecity University, Bhopal, India*
[b] *Lakshmi Narain College of Technology & Science, Bhopal, India*
[c] *Department of Management, A.M.I.I, Pebble Hills University, United States*
[d] *Electronics & Telecommunication Engineering, College of Engineering, Pune, India*
[e] *Civil Engineering and Deputy Director R&D, Drs. Kiran and Pallavi Patel Global University (KPGU), India*

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Electronic voting (e-voting)
Blockchain
Network
Digital voting
System
Technique
Accuracy

ABSTRACT

A blockchain is a revolutionary computational data structure that enables an open, public, distributed ledger with a wide range of uses. Any new cryptographic application, on the other hand, should take into consideration expected technical improvement during the lifetime of any possibly deployed systems, many of which will be in use for decades. This document addresses the weaknesses of blockchain technology as a result of the development of quantum computers, as well as general recommendations for making blockchain more resistant to such technological breakthroughs. As a result, utilizing a special approach, this work shows many steps of the suggested electronic voting system. The method contains the idea of electronic voting using Quantum key distribution and blockchain security. Explicitly an extended version of the blockchain-based e-voting system to several networks applications. This work also describes the architecture, design, and design constraints of such a voting system in our society with implementation implications.

Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

1. Introduction

Election usually accompanies debates, discussions, and campaigns for elections. The voter will typically choose corresponding to candidates' directory or election for the other people he/she prefers. To preserve the vote's namelessness, voting ballots should be unidentified and numbered with the voters in-camera booths. By the seventeenth century, voting had become a widespread occurrence because of the modern parliamentary democracy [1] (Fig. 1).

A vote is additionally used in various alternative personal associations and teams, parties, organizations, companies, and charitable societies. Blockchain is a free, distributed records archive or public records library of all transactions or digital events that have occurred and are exchanged between network-connected participating parties [2]. A blockchain is a sequence of blocks where blocks are linked to form a chain of blocks that contains information or information about any event [3].

It is specified that in e-voting systems, the following features should be included. They are:

- Receipt-Freeness does not create a receipt to show the preference of the voter for a particular candidate.
- Justice, it was not possible to obtain preliminary results influencing other voters' decisions.
- Data Reliability certifies to each vote, once registered, is verified as planned and can't be present manipulated in any way [4].
- Privacy/Voter Anonymity does not disclose the identity of voters and for whom they vote. Only suitable electors should be allowed to vote on an eligibility basis.
- Reliability/Robustness, without loss of votes, elective systems must work securely. It is essential to build software and methods in such a way without any malicious code or faults.
- Individuality makes it hard for electors to vote other than once
- Verifiability**:** Electors must be capable of verifying that their votes are appropriately calculated [5].

[*] Corresponding author.
E-mail address: 6.shwetagupta@gmail.com (S. Gupta).

https://doi.org/10.1016/j.matpr.2021.07.254
2214-7853/© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

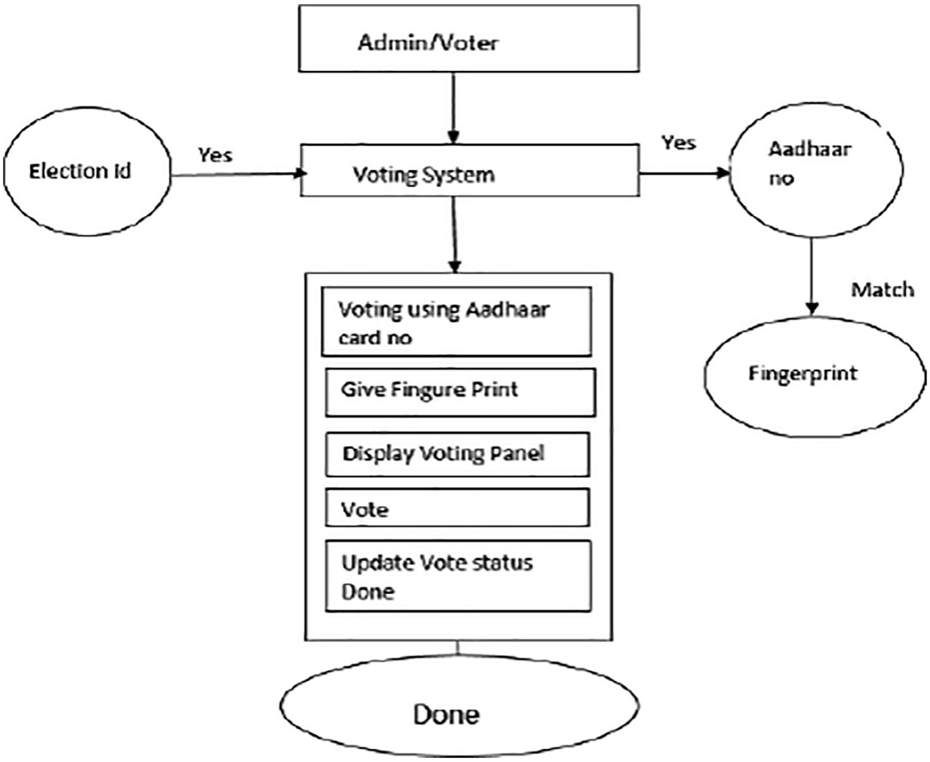

Fig. 1. Systen Architecture.

The paper's contributions can comprehend as follows:

1. The paper introduces a e-voting system based on blockchain that follows the fundamental e-voting properties while still being decentralized.
2. A review of the implementation issues and the drawbacks of the underlying platform promote the e-voting proposal.
3. The technique presented secures the e-voting process from the quantum type of attack in the network, for which quantum cryptography is being implemented.

1.1. Concept of blockchain

The main aim of the design of a timestamp for digital documents is to prevent influence. The first blockchain-based system is believed to have been created in 2008 by Satoshi Nakamoto [6]. It is similarly transparent that Bitcoin was the first massive usage of blockchain technology. In the field of cryptocurrencies, the blockchain theory can be compared to an open and safe globally distributed knowledge book. Blockchain is well-known, and it is not unreasonable to believe that its potential would outstrip that of digital currency. Blockchain experiments have also been launched by private companies and government agencies [7]. It is possible to identify Blockchain as a chain of blocks, time-engraved and connected cryptanalytic messages. The sequence is continuously increasing by inserting new partnerships so that each new block preserves the hash of the previous block information. In essence, the Blockchain aims to prevent modification and misuse of both private and public records. In a sense, the Blockchain is the public ledger with all transactions carried out directly between the system's users and providers. The nodes verify these transactions. The Blockchain, therefore, enables protection to be built without the need for a Central Authorization. Asymmetric cryptography, which is gentler than symmetrical cryptography, is the basis of blockchain techniques [8].

As described earlier for the structure and format of the blockchain the blocks are depictions having the hash of the previous block and also the information about the transactional data. As shown in the Fig. 2 above in respect to the voting system.

1.2. Types of blockchain network

In three different ways, the blockchain can be constructed. It can be configured as a public, private or association blockchain, depending on requirements [9]. The sorting of the centralization, agreement, and length of the operation to be considered in system design is shown in Table 1. Only specified peers with rights will provide to obstructing data, and the consent process will be authorization-based in the confidential blockchain. The network is not accessible to anyone in a private blockchain where written rights are reserved in one party centralized (Table 2).

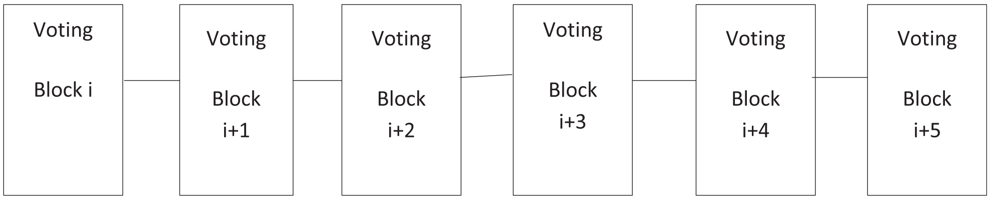

Fig. 2. The blockchain for e-voting.

Table 1
Blockchain Network Types.

Property	Public	Private	Consortium
Efficiency	Low	High	High
Participants Access	Permission not required	Permission to be taken	Permissioned
Duration of Transaction	Longer	Shorter	Shorter
Centralized	Not Centralized	Centralized	Partial Centralized
Determination of Consensus	All miners can determine	Organization Participating can only determine	Selected miners can determine
Blockchain network Management	No Centralized management	Single Organization	Multiple Organization

1.3. Block formation

Every block includes the vote, voter signature, blocks voting ID, timestamp and digest (hash), as shown in Fig. 3 [10]. The e-voting blockchain is represented successively as a set of voting blocks chained to each other. The initial block is called the genesis block.

- Voter's ID: Voter IDs are apportioned randomly to somebody who has the right to election.
- Vote: A voting poll is to declare an opinion poll for the candidate selected by the voter.
- Hash of the previous block: we utilize the SHA-256 algorithm to measure the last block's significance. Thus, non-repudiation is the blockchain-based e-voting method.
- Voter signature: the voting ball identified as a signature by the electors so that nobody else will figure out who a person is voting for. Voters use their secret key to sign the vote hash, which is managed to determine the election's authenticity.
- Block Timestamp: The timestamp is used for documenting the block's submission time. When they have a similar timestamp, the block with a more excellent signature value is chosen over others [11–14].

1.4. Requirements of a secure voting system

E-Voting Security Properties: High security is essential for elections to take place. The democratic System depends on widespread confidence in the authority of elections [15]. Due to the daunting need to instantaneously attain several contradictory properties, such as anonymity, audit ability, and correctness, there has been a measure of consideration to electronic voting by cryptographers. In e-voting, the most relevant standards are the following:

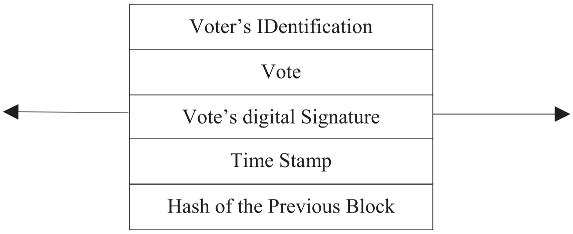

Fig. 3. Voting block.

1. In the final count, accessible voters will cast ballots that are counted.
2. It disfranchises non-authorized electors.
3. Suitable electors are incapable of delivered two votes, both of which are against the final count.
4. Voting is confidential and non-coercible. This contradicts accuracy since it is essential to categorize eligible voters to differentiate them from non-eligible voters.
5. Verifiers will check to see if the final tally was calculated correctly. This clause states that the correctness of voting may be checked by a group of dedicated auditors or an electoral committee.
6. The voting fallouts have to be confidential. No one, involving the calculating sergeants of the ballots, should distribute the last count proceeding to the representative time. Otherwise, the outcome of voting may impact the choices of voters.

Some researchers say that e-voting has more robust security properties, but then we distillate just on the significant assets that are clearly in line with standard voting requirements. One of the keys is the beginning goals of this effort because e-voting protection should be like that of conventional selection. While utilizing contemporary cryptographic techniques, we might achieve more. The properties mentioned above apply to practically all balloting procedures and are the base of our security assessment. Cryptographic methods are not the biggest challenge for safely introducing e-voting schemes in an actual-life ballot vote [16]. For such a security-critical mission, a much deeper issue is whether the workstations of' ordinary people' (where computer viruses are daily visitors) can be used (Fig. 4).

1.5. Objective of this research

- To study and evaluate the concept of block about e-voting,
- To design a novel process to effectively use the concept of blockchain for secure, authentic, easily available, and easy to validate the data generated in the e-voting process,
- To validate the designed process for the feasibility of the same over some pre-defined tool,
- To validate the efficiency of the proposed system over previous techniques considered for the e-voting using blockchain.

2. Related work

The framework raised in the issues and usefulness of digital voting blockchain technology reveals that the Blockchain is a technol-

Table 2
Comparison of E-voting System methodologies.

Scheme	Hard Problem	Evoting Requirements							
		Anonymity	Fairness	Uniqueness	Verifiability	Audit	Anti-Quantum	Tamper-Resistant	Scalability
[28]	ECDLP	YES	YES	YES	YES	–	–	–	–
[29]	RSA	YES	YES	YES	YES	YES	–	–	–
[30]	ECC	YES	YES	YES	YES	–	–	–	–
[31]	SD, ECC	YES	YES	YES	YES	YES	YES	YES	–
Our scheme	QKD	YES	YES	YES	YES	YES	YES	YES	YES

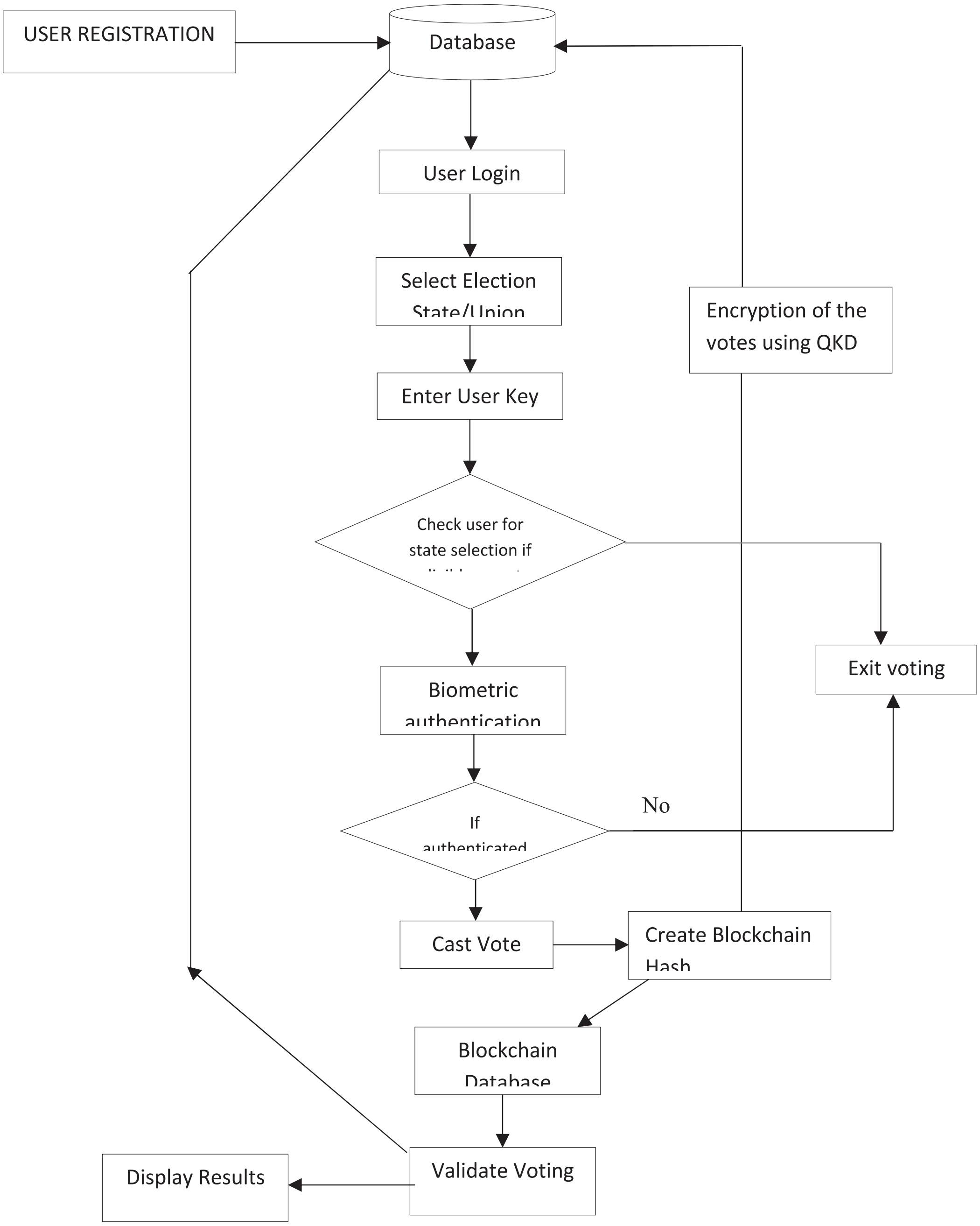

Fig. 4. Flow diagram for proposed methodology.

ogy that allocates digital coins or assets to be passed from one person to another. With the idea of the associated list in Data Structure, the Blockchain concept can be understood since the following critical report is stored in the previous key and linked. It was first conceptualized in 2008 as a central element of the digital currency bitcoin, which acts as a society record of all transactions, and was launched in the subsequent year.

There are some problems and efficiency with digital voting through blockchain technology, but their concern is to focus on how much scheme makes this technique more efficient. Here, their emphasis is on how the system in their everyday lives can apply this approach. India is highly interested in our country's potential usage, and a lot of efforts are being made to resolve security concerns as early as possible.

The method suggested in the Blockchain-based electronic voting machine and Aadhar verification notes that a nation with a lower percentage of votes will flunk to progress. It is essential to choose the correct leader for the nation. Their proposed framework was planned to provide the people of democracy with safe data and trustworthy elections. As the Aadhar card is the most required for a person's identity, it is also highly recommended to deploy an election mechanism. Blockchain will be publicly certifiable and distributed in a way that will be able to corrupt it [17]. Their proposed system is specifically built for our country based on Aadhar verification. As it had become mandatory in the current scenario, the information of over 18 years old is extracted from the Aadhar card database. Voting fingerprints are used as the primary authentication resource to ensure greater security. The device will allow t h e-voting through his fingerprint to vote. As soon as they cast their vote, blockchain technology embedded into EVM comes into existence. Database manipulation can be reduced essentially by implementing Blockchain in database delivery.

For e-voting to become more approachable, understandable, and individually auditable, the foundation for blockchain technology and its utility in the e-voting scheme that is then applied will be a possible solution. Electronic voting systems aim to be as simple to use and safe as conventional, ideal elections and remove the described human errors [18]. This isn't easy to accomplish since electronic voting systems require strong encryption to guarantee the vote's confidentiality, legitimacy, and anonymity. This must be assured and yet contribute to a user-friendly application, which is always difficult to accomplish. But it is also problematic to conclude that conventional elections are entirely safe and correct, as the method already is, and this is an excellent opportunity to think about reinventing elections with the help of computers and cryptography [19].

A Smart Pact proposed the first operation of regionalized and self-registering net polling procedure which has voter privacy called The Open Vote Network for Boardroom Electing Highest Voter Privacy (OVN) [20]. The OVN for the Ethereum blockchain is authored as a smart contract. OVN implements the Anonymous vote in its general concept through a two-round public debate we have previously addressed. After implementing the system, the OVN developers concluded that the operating cost of such a program on the Ethereum blockchain was $ 0.73 per voter. The reliable higher limit for electors was 50 voters, but the price could be deemed fair because it is publicly verifiable and offers complete privacy for voters. Due to the gas cap on the public Ethereum blockchain, this one proposed to limit the number of voters.

A Stable and Optimally Efficient Multi-Authority Election System proposed a multi-agency covert ballot election system to ensure confidentiality, standardized verification, and strength. Electors will participate using a PC with the effort needed by a voter being the critical consideration. In this model, by displaying ballots to a bulletin board, electors cast their votes. The degree that any political party can retrieve its substance, the statement panel acts as a broadcast network with remembrance, but no coalition can remove everything from the bulletin panel. The ballot does not disclose any information on the vote itself but is assured by accompanying proof that a correct ballot is included in the election. Any observer can then obtain and validate the final count, all options, which happens when the deadline is met, against all the ballots presented. This, due to the homomorphic properties of the encryption system used, would ensure universal verifiability [21].

In this model, by publishing ballots to a bulletin board, electors cast their votes. The degree that which party can retrieve its substance, the notice board, acts as a recording channel with memory, but no party can remove anything from the bulletin board. The ballot does not disclose any information on the vote itself but is assured by additional proof that a correct ballot is included in the poll. Any observer can then obtain and validate the final count, the total of all options, which happens when the deadline is met, against all the ballots presented. This, due to the homomorphic properties of the encryption system used, would ensure universal verifiability.

Although this plan will scale up improved than the prior ones to general elections, the suggestion does not have any forbearance to intimidation. The balloting takes a spot at home on PC, similar to the Ethereum shrewd agreement, and the coercer will stand for above the constituent's arm.

2.1. Literature review

Shah et al. [22] state that the Android application has been presented with improved security features to include authentication and acceptance. Using authentication is integrated, a unique identification key and permission is performed using fingerprints. One-time password authentication is also required of voters. A 128-bit AES encryption algorithm and SHA-256 is used here to provide protection. The vote is cast in the form of a contract, and a blockchain is built to keep track of the number of votes cast. The author has demonstrated that blockchain technology offers a new incentive for democratic countries to move away from the Pen and Paper Electoral Mechanism and the Paperless Direct Recording Electronic Voting Machine (DRE) to a more cost-effective and time-efficient electoral form, thereby enhancing current system security and providing new accessibility.

Haibo Yi [23] A blockchain-based electronic voting system has been proposed, which meets the basic requirements of the e-voting procedure. All votes on the Blockchain are cryptographically linked. When their timestamps are the same, the block with the higher signature score is chosen. The elector will vote for themselves or for someone else on the list of candidates. Since the vote is usually available to the public, the voting information is not encrypted. The blockchain-based e-voting method can be extended to a number of voting scenarios. Since ECC uses public-key encryption, which is in blockchain, it is not suitable for quantum computer attacks.

Koç et al. [24] proposed a Smart contract for Ethereum blockchain that uses wallets of Ethereum and the Solidity language, a sample e-voting framework was implemented and tested. It is also considered that the Android network enables people without an Ethereum wallet to vote. Ultimately, the Ethereum blockchain can keep the records of votes casted after an election is held. Users can send the polls directly from their Ethereum wallets or an Android device and, with the approval of any single Ethereum node, these transaction requests are managed. This consensus creates an unmistakable atmosphere of e-voting, in addition to the broad debate on the security and efficiency of e-voting systems based on Blockchain.

Hjalmarsson [25] build an online voting programme that meets legislation which has long been a challenge. In this work, Blockchain is explored as a strategy for implementing centralized electronic voting systems. The paper discusses and analyses the legal and technologically limited implementation of Blockchain to integrate electronic voting systems. The work begins with a summary of some of the conventional blockchain systems supplied by Blockchain. The authors proposed a new blockchain-focused online voting system that solves all the constraints found. More generally, through a case study overview, this work discusses the potential of distributed headline technologies, including the mechanism of choice and implementation of blockchain-centred applications, enhanced security and lowering the cost of holding national elections are two goals.

Hardwick et al. [26] has shown that technology has profound consequences in various areas of our everyday lives. Creating an interconnected global 24-hour set of sources and services can be efficiently accessed via the network. Technologies such as the Internet have, in turn, become a fertile source of creativity and imagination. The Blockchain is one such technological breakthrough, a central aspect of cryptocurrency. The blockchain network is seen as a game-changer for any of the new and evolving technology and facilities. Thanks to the attributes of its immutability and decentralized design, it stresses other markets as an equalizing factor in the existing equality between consumers and big corporate governments. In e-voting schemes, the Blockchain can be used. The purpose of this framework will be a decentralized infrastructure to operate and sustain an open, equal and autonomous voting scheme. The author proposes a possible new e-voting method, utilizing the Blockchain as just a clear voting box. The protocol is designed to encourage simple e-voting properties and to allow voters, by providing some degree of decentralization, to alter/adjust their votes (within the approved voting period). From a practical point of view, this paper explores the advantages and disadvantages required by Blockchain in terms of creation/implementation and use for such a project. The paper is a possible roadmap for different implementations of blockchain technology to be funded.

Dagher et al. [27] has developed a blockchain-based voting system called Bronco Vote protects voters' privacy and accountability while ensuring that the voting system is free, safe and cost-effective. To achieve election administration and auditable voting records through the Ethereum blockchain and smart contracts, Bronco Vote uses the University-scale Voters Platform. Also, to promote the protection of voters, Bronco Vote utilizes several holomorphic encryption methods. The implementation was considered over the Ethereum Test Net for usage capacity, scalability and reliability.

Hanifatunnisa & Rahardjo [26] Blockchain itself was used in the Bitcoin system known as the decentralized bank scheme. This concept investigates the study of voting data using blockchain algorithms from all kinds of polling areas. The method based on a pre-determined system switch for each node in the built-in Blockchain, as opposed to Bitcoin's work proof, this thesis implied. Researchers are proposing various protocols [32–37] for providing security in healthcare sector to maintain the confidentiality, integrity of the shared data among devices.

2.2. Research gaps

As per the descriptions available in the literature, most authors have considered the private type of network for the block execution just because of the security issues. The selection of the network's unique style is just because of the security paradigm attached to the private type of network. Significant work has presented the authentication of the users, way of votes validation, and somehow have left out the concept of data availability like decentralized system by the time the public type of network is considered. The network's work has considered Blockchain as a significant security concern while the Blockchain can also be attacked, and the concerned data can be compromised. It is quite easy to detect the alteration in the blockchain transactions and validate the same by following the back-tracking process. When the Blockchain is being attacked for the functions like voting processing, the altering is supposed to be secured from possible attacks.

- Use of the private network for public domain applications like e-voting,
- The improper security mechanism for attacks possible at blockchain level,
- Blockchain integrity,
- Data availability,
- Security from attacks like DoS for decentralized systems.

3. Contributions of the work

As far as the security concern for the Blockchain is concerned, then it is quite secure but can be compromised for situations like using specific algorithms like Grover's technique. The blocks can be further replaced using the search specification for hash in situ and keeping the block chain's integrity. And also, by speeding the nonce's creation, the complete list of chains can be recreated again and alters the hashes at a fast rate and compromises the integrity of the Blockchain. In the current work, the enhancement over the e-voting process using the Blockchain is authentication of the users, ensuring data availability, Security over the public network from DoS attacks, Speed optimization, and computational overhead. There have been some changes in the registration phase in the current work to ensure the authentication level for the users. The system also incorporates the clustered database, which provides data availability and reduces the computational overhead while verifying the transactional details over the Blockchain to detect the persistence of any attack.

3.1. Problem formulation

The voting process is a confidential process where they conducted votes should be considered an insecure process, and it should be authenticated for all sort of vulnerabilities. Several studies are available in the literature that considers several concepts to make the e-voting process prone to the voting process's security and authentication. In recent year's researchers have considered the concept of Blockchain, which is a chain of blocks having the transactional information and hash of the previous block. The blockchain technique ensures the security of the process and data. It is quite easy and convenient to detect the unwanted breaks in the data flow for unwanted processing just because of the technique's structure. In previous studies, the primary concern is about the Blockchain's applicability for secure e-voting process and the authentication of the system or actors in the process. In the current work, three different aspects are considered to secure the votes, authentication of the actors, and data availability and validation.

3.2. Materials and methods

E-voting is a digital medium for casting the votes and counting and validating the process as things are over the digital medium. The e-voting mechanism is a cost-effective and time-saving process, which reduces human efforts to a minimum. In the current years, the primary concern about the security of the process is under consideration. Several types of research have proven to be adequate to make the complete process secure from attacks. In the current era, Blockchain is being effectively used for the security of the voting process. Blockchain is a chain of blocks, with the current block having the previous one defined using the hash generated using the SHA 256.

The proposed system is prone to many attacks in the network layer and over the cloud at the time of data management. In the current system, the data is being stored in a distributed format, which ensures the data's availability anytime and quickly. The database is formatted in clusters, and information about the cluster and voting hash is made available into the block generated for every vote cast by the user. Majorly the system works for the performance-related parameters as data management, authentication of the ballots and user, data security, data integrity, data availability, validation of the process, authentication of the voting system, etc.

E-voting is a digital medium for casting the votes and counting and validating the process as things are over the digital medium. The e-voting mechanism is a cost-effective and time-saving process, which reduces human efforts to a minimum. In the current years, the primary concern about the security of the process is under consideration. Several types of research have proven to be adequate to make the complete process secure from attacks. In the current era, Blockchain is being effectively used for the security of the voting process. Blockchain is a chain of blocks, with the current block having the previous one defined using the hash generated using the SHA 256.

In the current technique, along with the level changes made for the authentication and data availability, the primary consideration is about the votes' security. Instead of encrypting the votes data available in every block's transactional messages, quantum cryptography is being used. In the field of cryptography, the most nurturing technology nowadays is QKD (Quantum Key Distribution). QKD is a protocol for the generation of the bitstreams randomly for two points of communication. The randomly generated bitstream is then used as the one-time pad to encrypt the message secretly. In the traditional process of required distribution, methods like Diffie-Hellman are considered, which is replaced by quantum physics concepts and laws in the case of quantum cryptography. For the required distribution in the case of quantum cryptography, the idea of the Quantum No-cloning theorem is being used as per the Heisenberg uncertainty principle ("signals comprise of individual quantum particles cannot be copied without the insertion of the nose into it"). As in the case when the message is encrypted using the key generated using the QKD protocol, and then the same can be unconditionally considered to be secured over the network.

The complete system is further represented into different phases as:

Registration Phase: User registration using the user id, name, Address. After making the required entries, the user is authenticated by the government body to authenticate the details provided by the user. At the same, a user key is generated for the user who is 32-bit key having the state code and last four digits of the user identity proof.

Voting Phase: The user is asked to make a login request using the credentials generated at the user registration time and must select the type of election like state/panchayat/union. After verifying the candidate for the election verifying the user key generated authentication, the user is considered using the biometric authentication system as figure print scanning, which can be quickly developed using the computer system or even from the mobile device the functionality of the scanning.

Data Management: After successfully considering the voting process, the vote is then hashed to be included into the blockchain, and at the same time vote is also stored into the dataset and encrypted using the hash key generated for the block of the option. The data generated is stored in clustered form into the database, and the information related to the cluster is provided to every block of the vote in encrypted form.

Validation of the process: The complete method can be further validated by randomly checking the blockchain and checking the cluster information available over the block by mining the defined cluster over the database. The outcomes are also validated in the same way.

3.3. Quantum based cryptography

Exploiting quantum characteristics in new technologies is another method for future crypto-systems. This division of quantum cryptography is very much different from post-quantum cryptography, which has reliability on classical methods. The current technologies require defending against hypothetical types of quantum attacks in the future. So Quantum cryptography is another discipline of quantum information science that looks into how quantum can effects and lead to generate fundamentally new cryptographic techniques for future.

Quantum key distribution is the most well-known and well-developed technique to emerge from quantum cryptography (QKD). A random bit stream can be generated between two parties using the QKD protocol. This random message is then used to encrypt a secret message using a one-time pad (OTP). This method of distributing a secret shared key is secured by quantum mechanics own principles rather than other mathematical complex cryptographic key distribution methods (e.g. Diffie– Hellman).

The Quantum No-cloning theorem is based on Heisenberg uncertainty principle which argues that a signal made up of individual quantum particles cannot be cloned without introducing noticeable defects, preventing any eavesdropper from escaping discovery. The encrypted message is considered cryptographically or unconditionally secure, once a random key has been established between two parties using the QKD protocol.

Within the subject of quantum information science, QKD is the most advanced technology. Commercial transmitters and receivers are available for purchase, and such systems have been deployed in both the commercial and public sectors. The technique is currently limited to city scale networks and requires private networks (e.g. black fibers). It also cannot be replicated or routed.

Despite the fact that these existing constraints severely limit QKD's applicability in most cases, the technology is currently evolving at a rapid pace and will most likely become more widely used in the near future. Aside from QKD, there are a slew of other concepts being investigated that could have a substantial impact on blockchain-based systems.

Information can be encoded and transferred directly into a quantum stream, for example (rather than just using a quantum channel to distribute a key). A proposal for a "Quantum Bitcoin" has also been made, which uses a traditional blockchain ledger but employs quantum technologies to mine and validate blocks. In a quantum system, there are other protocols for encoding and storing information, such as a ledger making the information tamper-proof.

Quantum bit commitment protocols are a form of digital signature system that can be used as an alternative. Many of these concepts are intriguing, but they are all still in the early stages of development, with many of them proving to be as challenging to execute as quantum computing.

4. Result and analysis

The proposed method has been implemented on the Linux platform in this section. Python programming language has been used as source code. Here Ubuntu which is the Linux distribution framework used for deployment. The blockchain formed has been formed by the chain of blocks which includes the voter's ID for identification of voter, voter's vote, digital signature, timestamp unique serial data and the previous block's hash.

Using Linux platforms a blockchain based e-voting system for multiple candidates has been developed. The result on implementation demonstrates a realistic and reliable e-voting system that addresses the issue of vote forgery during electronic voting. This kind of blockchain based e-voting system using QKD concept is more stable and anonymous than other e-voting systems.

(1) Anonymous: The implementation result demonstrates a realistic and reliable e-voting system that addresses the issue of vote forgery during electronic voting. The blockchain-based e-voting system is more stable and anonymous than other e-voting systems.
(2) Non-repudiation: To provide authentication and no repudiation, we develop a user credential model based on ECC. As a result, refusing a vote is exceedingly difficult.
(3) Withdrawable: We develop a model that allows voters to change their minds before casting a vote.
(4) Anonymity: In a blockchain-based e-voting system, each user uses an ID rather than his real name, and the system is decentralized without the involvement of a third party so protecting the privacy of voters.
(5) Security: To prevent vote forgery, we create a synchronized voting records model based on DLT. As a result, winning votes is exceedingly tricky.

The system designed works towards pruning the attacks like Stale block and Blockchain forks. A fork describes how network nodes have divergent beliefs for lengthy periods or even forever about the Blockchain state. Via protocol defects or instabilities in client programmed updates, these forks may be produced accidentally. Malicious attempts such as the implantation of ''Sybil nodes,'' which comply with conflicting validation laws, or ''selfish mining'' under race conditions may also trigger forks.

The study proposes a blockchain based e-voting system that adheres to the basic properties of e-voting while still maintaining a degree of decentralization and placing as much control of the process in the hands of the voters as possible.

- Discussion of the technology issues and drawbacks of the underlying framework (Blockchain and smart contracts) to help e-voting.
- The double-layered security system, ensuring security at the blockchain level and after considering the security of the process over the public network.
- The technique presented work towards the speed optimization process to avail the maximum transactions during the complete process.

5. Conclusion and future direction

This blockchain based e-voting scheme here tries to satisfy all the e-voting process's specifications and requirements. Block by block, all votes in the blockchain are cryptographically connected using our proposed method. When two blocks with the same timestamp have the same signature value, the partnership with the higher signature value is chosen.

In most cases, the vote is open to the public, but the vote's information is not encrypted. This kind of concept can be used for a variety of voting and other purposes. Despite being a secure technology, blockchain employs Quantum key cryptography, which can be tested to check vulnerability for the possibility of quantum computer attacks. As a result, blockchain with quantum computer countermeasures is a future research area.

CRediT authorship contribution statement

Sweta Gupta: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology. **Aparna Gupta:** Project administration, Resources, Software, Supervision. **Ishan Y. Pandya**: Validation, Visualization. **Abhishek Bhatt**: Writing - original draft. **Komal Mehta**: Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] D. Barry, Wilde's evenings: the rewards of citizen journalism, M/C J. 10 (6) (2008), https://doi.org/10.5204/mcj.2722.

[2] C. Michael, P. Nachiappan, S.V. Pradan, V. Kalyanaraman, BlockChain technology: beyond bitcoin, Int. J. Hyperconnectivity Internet Things (2016).

[3] R. Guhathakurta, Blockchain in automotive domain, IndraStra Glob. (2018).

[4] N. Kshetri, J. Voas, Blockchain-enabled E-voting, IEEE Softw. 35 (4) (2018) 95–99.

[5] M. Gibbins, S. McCracken, S.E. Salterio, The auditor's strategy selection for negotiation with management: flexibility of initial accounting position and nature of the relationship, Organ. Soc. Accounting (2010).

[6] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute, 2008.

[7] W. Nasri, Citizens' E-government services adoption: an extension of unified theory of acceptance and use of technology model, Int. J. Public Adm. Digit. Age, 2014.

[8] X.-H. Zhang, X.-Y. Yan, Y.-Q. Wang, L.-H. Gong, Tripartite layered quantum key distribution scheme with a symmetrical key structure, Int. J. Theor. Phys. 59 (2) (2020) 562–573.

[9] R. Lai, D. Lee Kuo Chuen, Blockchain-from public to private, in: Handbook of Blockchain, Digital Finance, and Inclusion, 2018.

[10] M. Walport, Distributed ledger technology: beyond block chain, Gov. Off. Sci. (2015).

[11] D. Korepanova, M. Nosyk, A. Ostrovsky, Y. Yanovich, Building a private currency service using exonum, in: 2019 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2019, 2019.

[12] J. Polge, J. Robert, Y. Le Traon, Permissioned blockchain frameworks in the industry: a comparison, ICT Express 7 (2) (2021) 229–233.

[13] S. Rouhani, R. Deters, Performance analysis of ethereum transactions in private blockchain, Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, 2018.

[14] W.J. Lai, J.L. Wu, An efficient and effective Decentralized Anonymous Voting System, arXiv. 2018.

[15] S. Khazaei, M. Rezaei-Aliabadi, A rigorous security analysis of a decentralized electronic voting protocol in the universal composability framework, J. Inf. Secur. Appl. 43 (2018) 99–109.

[16] J. Katz, Introduction to Modern Cryptography, 2007.

[17] G. Hileman, M. Rauchs, 2017 global blockchain benchmarking study, SSRN Electron. J. (2018).

[18] P.R. Santhias, R. Cabral, Electronic voting machine, in: Electronic Government, 2011.

[19] A. Montanaro, Quantum algorithms: an overview, npj Quantum Inf. 2 (1) (2016), https://doi.org/10.1038/npjqi.2015.23.

[20] P. McCorry, S.F. Shahandashti, F. Hao, A smart contract for boardroom voting with maximum voter privacy, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017.

[21] X. Yi, R. Paulet, E. Bertino, Homomorphic encryption, SpringerBriefs in Computer Science, 2014.

[22] A. Shah, N. Sodhia, S. Saha, S. Banerjee, M. Chavan, M.D. Patil, V.A. Vyawahare, Blockchain enabled online-voting system, ITM Web Conf. 32 (2020) 03018, https://doi.org/10.1051/itmconf/20203203018.

[23] H. Yi, Securing e-voting based on blockchain in P2P network, Eurasip J. Wirel Commun. Netw. 2019 (1) (2019), https://doi.org/10.1186/s13638-019-1473-6.

[24] A.K. Koç, E. Yavuz, U.C. Çabuk, G. Dalkiliç, Towards secure e-voting using ethereum blockchain, in: 6th International Symposium on Digital Forensic and Security, ISDFS 2018 – Proceeding, 2018.

[25] F.P. Hjalmarsson, G.K. Hreioarsson, M. Hamdaqa, G. Hjalmtysson, Blockchain-based E-voting system, IEEE International Conference on Cloud Computing, 2018.

[26] R. Hanifatunnisa, B. Rahardjo, Blockchain based e-voting recording system design, in: Proceeding of 2017 11th International Conference on Telecommunication Systems Services and Applications, TSSA 2017, 2018.

[27] G.G. Dagher, P.B. Marella, M. Milojkovic, J. Mohler, Broncovote: secure voting system using ethereum's blockchain, ICISSP 2018 – Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018.

[28] T.C. Hsiao et al., Electronic voting systems for defending free will and resisting bribery coercion based on ring anonymous signcryption scheme, Adv. Mech. Eng. 9 (1) (2017), 1687814016687194.

[29] Y. Wu, An e-Voting System Based on Blockchain and Ring Signature M.S. thesis, Dept. Computer Science., University of Birmingham, 2017.

[30] L. Wei-Jr, W. Ja-Ling, An efficient and effective Decentralized Anonymous Voting System, arXiv preprint, arXiv:1804.06674, 2018.

[31] Shiyao Gao, Dong Zheng, Rui Guo, Chunming Jing, Chencheng Hu, An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function" Volume 4, 2016, 10.1109/Access.2019.2935895, Ieee Access.

[32] Trupil Limbasiya, Mukesh Soni, Sajal Kumar Mishra, Advanced formal authentication protocol using smart cards for network applicants, Comp. Electr. Eng., 66, 2018, 50–63,ISSN 0045-7906.

[33] M. Soni, D. Kumar, Wavelet Based Digital Watermarking Scheme for Medical Images, in: 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 2020, pp. 403-407, doi: 10.1109/CICN49253.2020.9242626.

[34] Mukesh Soni, Dileep Kumar Singh, Privacy Preserving Authentication and Key management protocol for health information System, Data Protection and Privacy in Healthcare: Research and Innovations, Page-37, CRC Publication, 2021.

[35] Mukesh Soni, Dileep Kumar Singh, Blockchain-based security & privacy for biomedical and healthcare information exchange systems, Mater. Today: Proc., 2021, ISSN 2214-7853,https://doi.org/10.1016/j.matpr.2021.02.094.

[36] M. Soni, D.K. Singh, LAKA: lightweight authentication and key agreement protocol for internet of things based wireless body area network, Wireless Pers Commun (2021), https://doi.org/10.1007/s11277-021-08565-2.

[37] Mukesh Soni, Yash Barot, S. Gomathi, A review on privacy-preserving data preprocessing, J. Cybersecurity Inf. Manage., 4 (2), 16–30.