Untangling E-Voting Platform for Secure and Enhanced Voting Using Blockchain Technology

Muskan Malhotra, Amit Kumar, Suresh Kumar, and Vibhash Yadav

1 Introduction

The blockchain technology was introduced in 2008 by Satoshi Nakamoto [1], who created the first cryptocurrency called Bitcoin. Since technology has been emerging over the years, analysts believe that blockchain will have a wide and impactful scope in the near future. Most likely, people have heard about blockchain, but conceivably, most of them do not consider it, contemplating it a buzzword. But actually, blockchain is a breakthrough technology. The expectation with blockchain technology is so high that it is believed that it may reconstruct most industries in the upcoming years.

1.1 Blockchain Technology

This technology came into existence with bitcoin, a highly popular cryptocurrency. Blockchain can be integrated into several artificial intelligence technologies like neural networks, support vector machines and fuzzy logic. Bitcoin made us take

M. Malhotra · A. Kumar (✉)
Department of Computer Science and Engineering, HMR Institute of Technology
and Management, Delhi, India
e-mail: Amit.kumar@hmritm.ac.in

S. Kumar
Department of Computer Science and Engineering, School of Engineering
and Technology, Sharda University, Delhi, India
e-mail: sureshkumar@aiactr.ac.in

V. Yadav
Department of Information Technology, Rajkiya Engineering College,
Banda, Uttar Pradesh, India
e-mail: vibhashds10@recbanda.ac.in

F. Al-Turjman et al. (eds.), *Transforming Management with AI, Big-Data, and IoT*, https://doi.org/10.1007/978-3-030-86749-2_3

into account new technology, namely, Blockchain. Blockchain technologies offer to profit applications from sharing economies. When transactions were digitally linked and recorded, distributed ledger came into existence. It is highly shared. The blockchain structure is a type of append-only data structure. In this type of data structure, blocks that are new cannot be altered and eliminated. They can only be written. These blocks are chained in such a way that each block has a hash code. This block is a function of the previous block. This ensures immutability. These blocks ensure the entire history or provenance of an asset. Cryptographically, the chain is signed, duplicated and verified publicly at every transaction [2]. This ensures that none of the individuals can mitigate data that has been written onto a blockchain. A transaction is validated using a consensus protocol and only then added to the blockchain. The consensus protocol ensures that the transaction is the only version of the truth. Each record or transaction is efficiently encrypted.

Hence, Blockchain is nothing but a disseminated database that exists on multiple computers at one time. The technology has been growing since various sets of 'blocks' are added to it. These blocks contain a link to the previous block and a timestamp that forms a chain. The database is managed unanimously by the users as everyone gets a copy of the complete database. All blocks are encrypted, but a special key user will have access to add new records. Hence manipulation in transactions is near to negligible. Blockchain in itself is transparent, secure, and independent.

Blockchain technology is not just a backup mesh, rather it has a lot more to offer. Now, the question arises: What are those key elements that helped blockchain stand out from all other technologies? Why is this technology gaining so much popularity? Let us dive into its key elements to answer these questions.

1.2 Blockchain Working Principle

Blockchain has three pillars: blocks, nodes, and miners.

Blocks: A chain in blockchain consists of blocks which is made up of data, nonce, and hash. There can be multiple blocks in a chain. The data is the building block of any blockchain feature. A nonce is a whole number of 32 bits. The nonce is generated whenever a block is created. It is generated randomly. A 256-bit number wedded to the nonce is known as a hash [3]. Every time a block is generated, a nonce generates the cryptographic hash. Block data is tied to the hash and nonce unless it is mined. The data is also considered signed.

Miners: Mining is a process which helps the miners in creating a chain of new blocks. Every block in a blockchain has its own unique hash and nonce. Every hash also has a reference to the previous block inside the chain. Hence, mining a block is critical, especially when the chain is large. The miner uses special software to solve highly intricate maths problems. These math problems help to generate hash codes that are accepted, by finding nonce. This process is a bit complex as well as complicated because the hash is 256 bits and nonce is only 32 bits. There are approximately four billion possible combinations for hash-nonce that has to be mined before the right one is found. ‘Golden Nonce’ is the term used, if a miner finds an acceptable combination, and their block is added to the chain.

Making changes in a block requires re-mining of the current block that needs to be changed and all the blocks that come after. This is why it is said that it is notably challenging to manage chains of a blockchain. Finding the golden nonce is a tough job; it requires a tremendous amount of time and effort. A miner is rewarded when a block is mined successfully, and the change is accepted by all of the nodes on the network.

Nodes: Any kind of electronic device that maintains the copies of the blockchain and helps to keep the network functioning is acknowledged as a node. As not a single organization or computer can own the chain, hence it is a distributed ledger via the nodes connected to the chain. Every node has its own copy of the blockchain. The network has the power to permit any newly mined block (algorithmically) for the chain to be verified, updated and trusted. As the blockchain is transparent, hence each and every action is precisely taken into consideration. Each participant that is part of the entire transaction has a unique alphanumeric identification number. Public information is consolidated with balances and checks that create a sense of trust among the user. This maintains the integrity of blockchain.

Blockchain can be considered as the scalability of trust via technology.

1.3 Blockchain Key Elements

- *Distributed Ledger Technology*: Distributed ledger technologies have seen some astonishing technological advancement in the information technology world. Distributed Ledger is a digital system. It is used to record the transaction of assets. It records the transaction at the same time and the details are recorded at multiple positions. Each node processes and verifies each item as it generates a record for each item and creates consensus on each item’s veracity. This sort of architecture of computers represents a significant revolution. This significant revolution helps to keep records by changing how information is gathered and communicated.

Unlike traditional databases, these ledgers have no administration functionality or central data storage as it is visible in the centralised model shown in Fig. 1.

All the participants inside a network can access the immutable records of transactions and easily access the distributed ledger. This eliminates the duplicity of efforts present in the conventional business networks; hence, with this shared ledger transactions are recorded only once [4]. It also has the potential to diminish the cost of transactions. The technology makes it challenging to manipulate or attack the system as nodes of the network possess separate records. The information is shared across the network and witnessed, thereby making the system transparent and reliable.

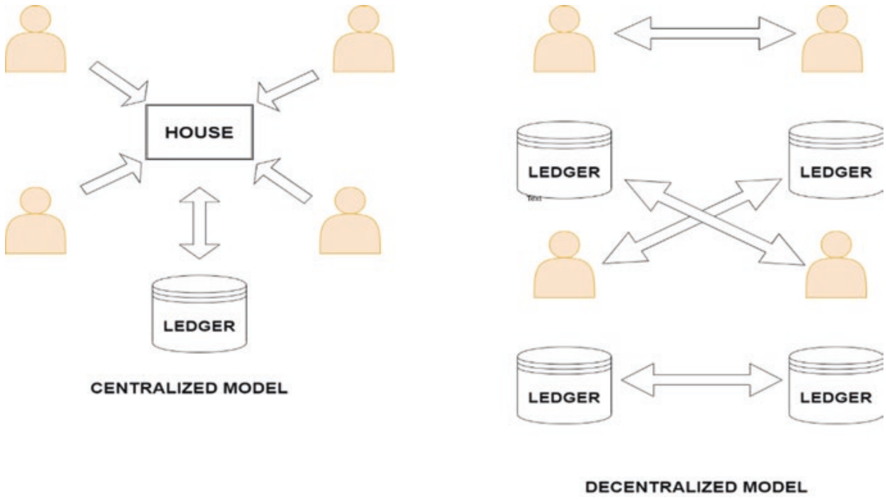

Fig. 1 Centralized vs decentralized ledger

Some aspects of decentralization are:

No malicious activities: Distributed ledger responds drastically to sceptical activity or tampering. Tracking is quite easy through the nodes.

Ownership of verification: This provides fair participation of the user, as on the ledger the nodes act as verifiers [5].

Managership: Every node that is active has to maintain the ledger and participate, so that the features of blockchain are workable.

Quick responses: Removing the intermediate accelerates the system response; thus, any change in the ledger is updated within minutes or even seconds.

- *Records Are Immutable*:

Immutability is the ability of the blockchain ledger to remain stable; this makes the blockchain to remain unaffected and indelible. Using hash values or cryptographic principles, each block of information can be processed efficiently. These blocks of information include facts and transaction details. The hash code value consists of an alphanumeric string generated by each block separately [6]. Each block contains digital signatures and hash values for itself and for the previous block. This makes the block unrelenting and makes them coupled together radioactively. These are the functionalities of blockchain that eliminate any kind of alteration by any intruder.

As we have discussed before, blockchain is distributed and decentralized in nature; therefore, a consensus is made among various nodes that store the replica of data. The originality of data is maintained by these consensuses only. Undoubtedly, immutability is a definite feature of technology. Immutability redefines the data auditing process and makes it cost-effective and efficient, and brings more trust and integrity to the data.

Once the transaction is recorded in the shared ledger, no participant can tamper with the transaction or change the transaction according to his will. Both the transaction records that constitutes an error and the new transaction record that has been added to reverse the error [7]. Even though immutability is beneficial in blockchain, we must remember that this technology has both positive and negative data privacy implications.

- *Smart Contracts*:

Lines of code that are stored on blockchain are known as Smart Contracts. They execute implicitly when deliberate terms and conditions are met. Smart contracts follow simple 'if…then…else' statements.

Smart contracts, also known as the set of rules for blockchain, are automatically executed and stored on the blockchain. These rules help to expedite the transaction. Smart contracts can define conditions for the corporate bond transaction and also include travel insurance terms and much more. Business collaborations are mostly benefited by smart contracts. They are used to enforce different types of agreements so that all participants have an intermediary's involvement [8]. They probably enforce some type of agreement and bring transparency, efficiency, and simplicity to every financial transaction. Smart contracts can be efficiently explained with the help of the supply chain example:

> Buyer B wants to buy something from Seller A, so she puts money in an escrow account. Seller A will use Shipper C to deliver the product to Buyer B. When Buyer B receives the item, the escrow money will be released to Seller A and Shipper C. If Buyer B doesn't receive the shipment by Date Z, the escrow money will be returned. When this transaction is executed, Manufacturer G is notified to create another item sold to increase supply. All this is done automatically.

- *Decentralized Technology*:

By de-centralization, we mean that it does not have an authority to govern and no certain person looks after its frameworks. Nodes group together to maintain the network, making it decentralized. This is the most important characteristic of blockchain technology that helps to work. Blockchain provides access to all the participants as the system is decentralized. Hence, the participants have access to the data which is linked with the web in order to store the assets. Participants can store any kind of information, for example, contracts, cryptocurrencies, important documents or any other valuable digital assets [9]. This is made possible only because the participants have direct control over their data, provided with their private key. Therefore, we can resolve that a decentralized structure gives power to the common people and rights on their assets.

Salient Features of Decentralized Technology

- *Fewer Chances of Failure*: As everything is well-organized in blockchain, it is highly fault-tolerant. Hence, its usual output does not have an accidental failure.
- *Transparency*: The profile of every participant is transparent. Changes are viewable on a blockchain making it more concrete.

- *Genuine by Nature*: This nature of the system makes it distinct and eliminates any kind of actions from hackers to break in.
- *No Third-Party Intervention*: No third-party interference results in no added risk. This nature of the technology removes its reliance on any third party, making it decentralized.
- *Less Prone to Breakdown*: The technology has developed survival techniques for any malicious attack. System attack is expensive and not a solution for hackers. So, it is likely to break down.
- *User Control*: Users have control over their properties. To maintain assets, third-party reliability is removed. All users can maintain and control their assets simultaneously by themselves.
- *No Scams*: There is no chance of scam as the system runs on algorithms. There is a big no for utilizing blockchain to gain personal profit.

Enhanced Security: As the blockchain technology gets relieved of the central authority's need, it does not allow any of its participants to transform any network characteristic for their gain. Another security layer for the system is encryption. This encryption is done with the help of cryptography. Cryptography provides another layer of protection for users, along with decentralization. Cryptography acts as a firewall for attacks having coded in obscure mathematical algorithms. It works on abstraction, that is, concealing the actual information on the chain and hiding the nature of the data [10]. The information undergoes a process that gets the data as input and processes it through various mathematical algorithms. The output that is produced has different values that are always of fixed length. You can think of it as a unique identity that is generated for the data that has been taken as input. Unique hash codes are provided to every block along with the previous block in the ledger. Therefore, tampering with any information on the block will lead to a change in the hash IDs, which is a kind of impossible task. The user is provided with a key which is public to make transactions and a private key to access the data.

- *Irreversible*:

Hashing being complex makes it impossible to alter or modify it. It is even more challenging to get a private key from a public key. If someone wants to forge the network, the hacker is made to modify every aspect of the information stored on every node in the network. All the participants of the node will have a similar copy of the ledger [11]. Accessing such a massive amount of data via hacking is nearly impracticable.

- *Consensus*:

The building block of every blockchain is consensus algorithms. Blockchain technology has efficiently designed architecture, and consensus algorithms are the core of this architecture. Consensus helps to make decisions.

By definition, a consensus makes decision for all the active nodes that are part of the network and makes a group of these nodes. With this feature, nodes instantly agree to the agreement which makes it relatively faster. The importance of consensus is even more when millions of nodes validate a transaction. At this time, a consensus is necessary to maintain the working and flow of transactions and data placidly. You can assume it to be a kind of voting system where the minority has to support the majority that wins.

This feature may lead to trustlessness within the system of nodes. Nodes might not trust other nodes but they can trust the running in core algorithms. Hence, making every decision that is present inside a network is a winning scenario for blockchain. There is a huge variety of consensus algorithms for blockchain around the globe [12]. Every algorithm has a unique way of making decisions along with improving previous mistakes. The architecture creates a realm of fair web. Hence to maintain decentralization, consensus algorithm is must for every blockchain, or else the core value will be lost.

- *Swift Settlement*:

Traditional transaction systems in the bank are quite slow. Processing a transaction takes an immense amount of time even after finalizing all settlements. There are quite a few chances of corruption as well. As compared to traditional baking systems, blockchain offers a faster settlement. With this, the user time is saved as the transfer of money is relatively faster.

1.4 Types of Blockchain

At present there are four types of blockchain networks: private blockchain, public blockchain, consortium blockchain and hybrid blockchain. The right to read or write a blockchain can be restricted or unrestricted to the participants.

1.4.1 Private Blockchains

A private blockchain is a permission-restricted blockchain. Private blockchains are access control-based that restrict the participation of users in the network. It not only limits access to read but the access to write as well. This specifies who can verify their transactions and who have to be provided with the read access only. On a private network, transactions are made more affordable since only a few nodes need to be verified. There is a verification of only trusted nodes that offer guaranteed high-processing power. One cannot be a participant in a private blockchain unless the network administrator invites the user [13]. Validators and participants are restricted to access information in this type of blockchain. There may be one or more administrators in a network, and they rely on third-party transactions. In this type of private blockchain, only the members of the transaction will know about the transaction, whereas any other participant or participants will not know about the transaction. For example, anyone can sell or buy bitcoins without having their identity revealed. Additionally, private blockchains do not allow anonymity, while some of the public blockchains allow. The most common examples of private blockchains are Hyperledger and Ripple (XRP).

1.4.2 Public Blockchains

A public blockchain has open network. Anyone can read, write, or participate in the network and even download the protocol. There is the availability of information in a public domain. The data is accessible to all, and any participant can view, read, and write data on the blockchain, due to its permissionless nature. In a public blockchain, no individual participant has control over the data. Public blockchains are decentralized and immutable [14]. This signifies that an entry cannot be modified or eliminated once it is approved. Another significant factor that distinguishes public blockchain with private blockchain is open reading and writing of data.

The most common examples of public blockchain are Ethereum (ETH) and Bitcoin (BTC). Both the cryptocurrencies can be viewed and used by anyone as they are created with open-source computing codes.

1.4.3 Hybrid Blockchain

A hybrid blockchain consolidates the benefits of both private and public blockchain. On a permissible blockchain, an application or service can be hosted independently for leveraging a public blockchain for security and settlement. To understand the hybrid blockchain model, one must first understand the difference between private and public blockchain. The feature of immutability and trust from a permissionless public network is best for application developers. It still retains the benefit of control and performance, which is provided by a permitted blockchain [15]. It does have use cases in organizations that neither want to deploy proper private blockchain nor do they want to implement a proper public blockchain. They simply want to deploy the best of both the chains. Hybrid blockchain is used in the hyperledger.

1.4.4 Consortium Blockchain

A consortium blockchain is also known as Federated blockchain. It is a creative approach in providing solutions for the demand of the organizations. In this type of technology, some of the aspects of an organization are public and the rest of the aspects remain private. There is no centralized outcome here, as the blockchain is managed by more than one organization.

A consortium blockchain is a partially decentralized blockchain. In this type of blockchain technology, a preselected set of nodes controls the consensus process. Consortium blockchains are often associated with their use in enterprises. Groups of companies collaborate to leverage blockchain technology for improving their business processes. Examples of consortium blockchain include Corda, Quorum, Hyperledger, etc.

1.5 How Secure Is Blockchain?

Blockchain can be secure, trusted, and robust – as long as the technology is appropriately executed. Blockchain technology is transforming the way we do business as it cuts-of-the-middleman – reducing cost, boosting efficiency in numerous vital services. In this way, it has the potential to lead the business efficiently.

But is it secure? Most importantly, can blockchain-based technologies offer privacy and trust to ensure temper-free and private records?

Blockchain is perhaps best understood as a decentralized ledger that reduces costs by removing intermediaries such as adequately decentralizing trust.

A private blockchain controls access to information given to the user making it less transparent than public blockchain. A public blockchain is a transparent ledger, as it is decentralized [16]. On multiple devices an information is stored in encrypted form. Another name for public blockchains is 'censor-free'. It is explicitly resistant to distributed denial-of-service (DDoS) attacks. On the other hand, private networks are more vulnerable to threats as a private blockchain network can be altered by its owner.

Blockchain can upgrade old systems. Voting with the help of blockchain will provide new dimensions to the democratic system. Blockchain will serve the voters as a digital ledger. The technology is known to draw its power from peers, or better known as 'nodes'. These nodes record, process, and verify all transactions across the system. Rather than being stored, a ledger exists on the 'chain' which is simultaneously supported by millions of nodes. Consensus between all auditing nodes on the network will help prevent computers from making undetectable changes to records. Each record is easily verifiable, and the database of transactions is incorruptible, making blockchain encrypted and decentralized [1]. As it does not exist in one place, the network cannot be influenced or taken down by an individual party. As no single authority has access to every feature of blockchain, hence anyone can be part of the network.

The main aim of blockchain is to make the voting process fair and without any third-party intrusion. Blockchain is an easily confirmable and inalterable system. It has capabilities to be an alternative to traditional voting processes. It has solutions that are smart alternatives, and central authority can take these solutions into consideration, in terms of blocks having data in the chain. Blockchain increases the security with which the data is stored in the blocks. It also minimizes the need for an official centre that provides secure elections. Various attempts have been made to tackle the issues of the traditional election. These attempts serve as a benefit to establish an online system and automate the whole process. Estonia became the first country to use electronic voting during its local elections that were held in October 2005. Moreover, Estonia became the first country that legally bounded general elections using the Internet facility to cast the vote. The option of voting over the Internet was available nationally in the local elections. Not only Estonia but also Switzerland and the Austrian Federation of Students in 2009 held their elections electronically. The world on the other hand is accepting this system gradually. Blockchain has impressive attributes to overcome the problems of voter privacy, data integrity and security.

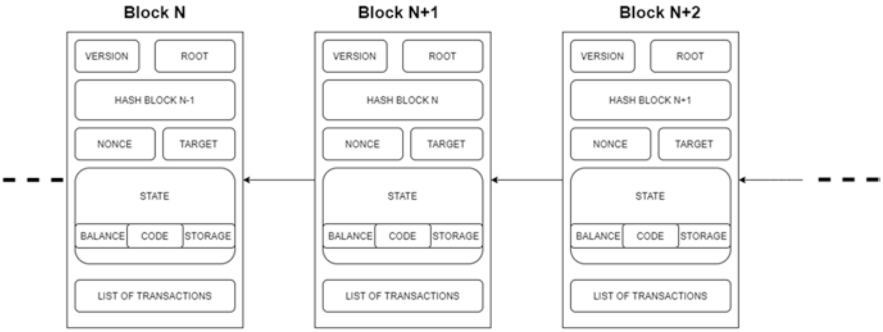

Fig. 2 Block diagram stating the structure of the blockchain

Mobile, as a computing platform, certainly is the future of the democratic voting system. It will provide all new facets to how humans interact with their world. Across the globe, smartphone penetration is expected to exceed 80% or even higher within a few years. Technological challenges and human factors are greater on a mobile device, but the time is propitious for this intersection. ‘Mobile voting’ can be defined as ‘remote voting’ and the form factors of ‘mobile’ will vary widely on different devices around the world [17]. The hurdles will be tough to tackle, and the citizens need to trust their election management bodies.

Sophisticated adversaries provide correlation attacks in the long run. They track the packet sender and receiver. This creates room for hard-to-trace-communication. Receiving messages from multiple senders, shuffling them, and sending them further to the next destination in an arbitrary order is part of such communications. To expedite a decentralized approach in decision-making securely, there is end-to-end encryption that exists within the network protocol of blockchain [18]. With blockchain, we can examine every vote in real time. Blockchain architecture is designed in such a way that it is hack-proof, with the highest security level from the ground up to mass. It renders the hackers’ mission virtually impossible making it an ideal platform for voting.

To tackle issues like availability, fairness, anonymity and reliability, various researches have been conducted in order to make the system secure and reliable. Election serves the entire public. Therefore, its design must be in such a way that minimal technical skills and training should be enough. Elections must be flexible enough to assist a large population. Each voter must be given exactly one chance to cast its vote. The system must be competent enough to verify its voters’ identity and the certitude of keeping the information secured. To encourage participation, the system must provide an ecosystem for decision-making where authority and resources are shared. E-voting has always remained a cause of discussion both politically as well individually. There is a fervent requirement of strong foundation rules along with mutual understanding among the people (Fig. 2).

2 Literature Survey

In their work, Kanika Garg et al. [19] explained that through the decentralized system, the voting process is made simple, secure and anonymous and hence the focus is constantly drifting. The paper presented a literature review on the techniques used to tackle the challenges of voting. In their article, Hsin-Te Wu et al. [20] have proposed a paper that presents views about the voting system that relies on blockchains to create a trustworthy voting system. To ensure the overall security of a voting procedure, the study also implements a bilinear pairing security mechanism in order to establish both a secret ballot and an open ballot system. According to Ashish Singh et al. [21], the paper focuses on digital e-voting system to solve the security issues and fulfils the system requirements in the blockchain technology. It stated opportunities for a secure e-voting system in any organization or country that needs to be deployed. In 2018, A. Singh et al. [22] explained that the Estonian electronic voting system which is a leading electronic voting system still suffers from universal verifiability issues and may need improvement of its availability. They proposed a blockchain-based electronic voting system in the paper to solve the problems of elections. In their paper, Wenbin Zhang et al. [23] proposed a receipt-free, perfectly verifiable and privacy-preserving peer-voting protocol that can help facilitate voting for peers existing on a blockchain network. Basit Shahzad et al. [24] suggested a framework by using effective hashing techniques to ensure the security of the data. The concept of block creation and block sealing was introduced in the paper. In Nir Kshetri et al. [25], the idea behind the paper was to make eligible voters cast a ballot anonymously using a computer or smartphone. BEV employs tamper-proof personal IDs and encrypted keys, and Friðrik Þ. Hjálmarsson et al. [26] aim to implement a distributed electronic voting system and the application of blockchain as service to implement the electronic voting system. Rumeysa Bulut et al. [27] have proposed a solution to eliminate disadvantages of conventional elections using blockchain.

3 Research Motivation

A voting system contains a set of rules that determine how referendums and elections are conducted and how the results are determined. Government bodies conduct these political electoral systems. These bodies govern every aspect of the election process. When the elections take place, the government bodies take account of different aspects like who can stand as a candidate, who are allowed to vote; every voter has its voter id, how ballots are marked, how the vote is counted, to set a limit on campaign spending and all the other factors are precisely taken into consideration, that can affect the outcome. Constitution and electoral laws define the political electoral system [28]. The election commission typically conducts them. Some electoral systems tend to elect individuals for specific positions such as the prime minister, president, governor, etc. Multiple candidates are also elected for positions such as members of parliament or members of the legislative assembly. Variations are visible at various steps of the electoral system. The most common systems are *first-past-the-post voting*, the *two-round system*, *proportional representation*, and *ranked voting*.

- *First-past-the-post voting*: In this type of electoral system, candidates are selected with the help of votes that are cast by eligible voters. The candidate having the maximum vote in his favour is elected. The voting system can be used for both the divisions, be it single or multi-member elections. The candidate with the highest number of votes is elected. In the multi-member election, each voter casts the same number of votes to fill positions. The candidates who are elected have the highest chances to be placed corresponding to the number of positions.
- *Two-round system*: This type of electoral system is used for electing candidates for the legislative bodies or where presidents are elected directly. In this system, voters cast a single vote for their chosen candidates. The one who gets the majority wins. This is a voting method that is used to elect individual winners. If no individual candidates get a clear majority, then the second round of the voting takes place with either the top two candidates or the candidates who have equal proportions of vote.
- *Proportional Representation*: This type of system's essence is that all votes contribute to result and not just a bare majority. The most prevalent forms of proportional representation require the use of multiple members' voting districts, as no single seat is filled in a proportional manner. Proportional representation categorizes the electoral system in which divisions in an electoral system are reflected proportionally in the elected body [29]. If a certain number of electorates support a particular political party, then a certain number of seats will be won.
- *Ranked Voting*: It is a type of voting system where voters are provided with a ranked ballot to rank their choices in a sequence on the ordinal scale: first, second, third, etc. There are multiple ways in which the ranking can be generated. In the same way, there are multiple ways to count and determine which candidate is (or are) elected. This type of voting system collects more information from the voters as compared to other voting systems. There are different types of ranked voting as well, provided the root process remains the same.

The soundness of election is a matter of national security, in every democracy. Various studies have been working on the possibilities of an electronic voting system, continuously. The goal is to fulfil the needs of the citizens while minimizing the cost of having national elections. With the rise of candidates being elected under democracy, the early voting system was based on a ballot paper system. Replacing the traditional ballot paper scheme with sound election techniques was critical to implement, making the voting process's verification and traceability prone to fraud. Electronic Voting Machines (EVMs) are considered to have flaws. There have been debates about the security and credibility of votes that have been cast through these electronic voting machines. Discussions have been rife on sabotaging the machines, thereby affecting the votes that have been cast on the aforementioned machine.

Satisfying the legal legislator requirements along with establishing an efficient electronic voting system has been a challenge from a long time.

There are numerous aspects of the implementation of blockchain. One such aspect is its implementation in the E-Voting System.

Elections being a huge organization is supposed to provide democracy and democratic rights to the citizens of the country. They play a very crucial role in the life of the citizens and the country. The future of a country lies in the hands of elections. Hence, it is much important for every individual that is part of the election. Even though the election is an organization, they have to be worthy of trust. They must ensure the privacy of votes and security of its voters. Accordingly, the counting of votes under an authorizing body should not be time-consuming. Delay in this counting and declaration of results increase concerns about result manipulation. In order to conduct elections in an efficient manner, we must take into consideration the roles that are involved in the agreement and the different components and transactions that are involved in the agreement process.

These processes include the following:

1. *Planning election in advance*: Structure and planning for elections commence months before the actual voting takes place. The foremost aspect that is taken into consideration is the total population of the district. Having a fair knowledge about the population index and listing down the newly eligible voters increase the expectancy of votes cast. The second factor is the expected turnout. The expected votes cast in the election is known as 'expected turnout'. There have been cases where eligible voters do not cast their votes. The trend can be determined by taking into account past elections. If there was a 25% turnout in the last city elections and no added factors changed the situation, one can figure out that 25% would vote in the elections this time. If due to voters' new eligibility, the turnout increases to be 35%, it further increases the expectancy of the vote cast this time.
2. *Electorate*: The next step is the electorate procedure. All the eligible voters who are allowed to vote is known as the electorate. The election governing body must verify all the eligible voters along with those who will cast their first vote. Providing voter-id cards on time and other aspects like verifying documents of voters, enrolling their names in the voter list and other such details must be precisely taken into consideration. If the factors are neglected, then it may lead to decreasing the expectancy of votes that have been cast. It will also provoke the rights of the voters to vote.
3. *The nomination of candidates*: The nomination of candidates is an important part of the election process. Candidates are nominated by public parties. However, the nominations are regulated by the legislature. To be able to get nominated by the party, the candidate has to provide details to the committee members before the deadline. A majority of selection committee members must support the nomination. The petition, certificate, and nomination application must be filed with the officer specified in the election statute. The nomination officer scrutinizes the papers [30]. If the officer is dissatisfied, he is refused from his candidature. A

candidate can withdraw his nominations even after being granted permission for candidacy. All these factors support the nomination of a candidate.

4. *Scheduling*: Different techniques are used by the parties and the candidates to spread their messages to the voters. Rallies and meetings are organized and processions are carried out. Party leaders, especially the crowd pullers, are assigned to address the public meetings as their task. The candidates do door-to-door canvassing along with the influential personalities in order to attract crowd. Slogans are coined to attract the audiences along with releasing the advertisements to the press before the campaign begins. To highlight the speeches of the leaders and panel discussions of the various party and party members, radio and television are pressed into services. Electronic media plays essential role in creating awareness about the political parties' programs among the people.
5. *Election campaign*: Parties tend to issue their Election Manifestos as a part of their campaign. A manifesto is considered as a statement of great significance. It is a kind of formal statement of the program that consists of a political party's objectives. Reconstructing Centre and State relations, social justice, fiscal reform, economic growth, health, nutrition, education, defence, and world peace are some of the issues that the manifesto deals in. The manifesto contains programs and promises, intending to attract a large number of voters. The party leaders go through a series of interviews to television and newspaper agencies. A wide coverage is given at regular intervals. The most important aspect to note down is that parties are made to stop their election campaign about 48 hours before the time of polling day. Supervision of the whole polling process is done under the guidance of the presiding officer. He ensures that all the electoral norms and practices are adhered.
6. *Declaration of results*: After the polling is done, the voting machines or the ballot boxes are sealed and carried under customs to the counting stations. The counting of the votes begins. It may take some time to announce the results of the elections. After the results are declared, the party that gets the maximum number of votes has to prove its majority. If there are chances that the winning party is unable to prove its majority, the party forms an alliance to prove its majority.

The features of blockchain that we discussed before in the introductory section get operated through advanced cryptography along with providing a level of security which is greater than or equal to any previous known database. Therefore, blockchain technology is considered to be an ideal tool that can be used to modernize the democratic voting process. The aim is to work on solutions in which voters have power, to review the method in which the vote has been cast and that too at any given moment. The method should also have the ability to review the way votes that have been cast for a bill or a particular legislative proposal. This will lead to overall better governance and better outcome of decisions. This will allow people with domain-specific knowledge to present their views liberally. They will have a better understanding of the process, provided the process is transparent, trustworthy, and reliable. Stating some inessentials that thwart the blooming bud of belief for the democratic voting system, these inessentials refrain the process of voting from conducting smoothly.

1. Persuading voters to vote for a particular party
2. Enabling traceability of votes and identifying credentials of voters
3. Inability to ensure trust among the voters that the vote has been counted accurately
4. The third-party intervening and controlling the course of votes being cast
5. Tampering votes and favouritism towards certain beliefs.
6. Single entity control over tally of votes and determining election results
7. Not allowing a certain group of individuals to cast a vote
8. Providing seats to unfit candidates

By overcoming these inessentials, the democratic structure can finally become trustworthy and reliable. Not only these but there have been various aspects of democratic rights that need to be highlighted. With the coming of age technology, the voting system will get a new dimension, thereby overcoming the system's backdrops.

There is another concept called the *Non-Interactive Zero-knowledge proof* [31]. Non-interactive zero-knowledge proof is indirectly related to blockchain. It can be seen as an essential component for satisfying the requirement of the e-voting system. Perhaps, it acts as a building block for conceptualizing blockchain in the electronic voting system. The concept of zero-knowledge proof is a cryptographical method. In this type of method, a party proves to another party that he knows a certain value, without revealing the value. The party that proves is known as 'the prover' and the other party that counters the prover is known as 'the verifier'. A simple example was first demonstrated live by Konstantinos Chalkias and Mike Hearn. Using the example of 'Two balls and the colour-blind friend', the ZKP works as follows: The prover has two balls, one red and one green, and otherwise identical. The verifier (the friend) is colour-blind. To prove that they are differently coloured, you give your friend the balls, who hides them behind his back. Your friend then decides whether to switch the balls between hands or not, and then reveals one of the balls. The prover declares if the balls were switched. By repeating this process, the prover can prove that he can correctly identify the balls, as the verifier confirms that the likelihood of repeated success is halved each time.

A non-interactive zero-knowledge proof is a variant of zero-knowledge proofs. In this type of non-interactive system, the prover and the verifier do not interact with each other. Researchers believe that to achieve computational zero-knowledge without any interaction, a common reference string can be shared between the prover and the verifier. Some studies have also stated that any voter can prove their message's identity and authenticity without a shared public key. This can be achieved with the help of the random oracle model, which in practice can be used as a cryptographic hash function. This scheme is ideally suitable for smart cards, remote control systems, or personal computers, basically in all the microprocessor-based devices [32].

A large aspect of the modern voting system is stuck in the last century. In order to submit paper ballots to local authorities, people have to leave their homes. Any kind of manual evaluation is prone to errors and mistakes. These mistakes may create conditions of distrust among citizens. Moreover, the situation in the current scenario has reached such a level that under conditions of the outbreak, the democratic system faces issues in a pandemic. The recent national elections that were held in South Korea with 44 million voters in the midst of the pandemic define the need for acceptance of e-voting. At times, there have been conditions where it is difficult to put faith in the results due to security gaps. Some of the main issues of the system constitute Trust, Intermediation, Accessibility, and Autonomy. A vote being a small piece of high-value data, systematic infrastructure is extremely valuable and the need of the hour.

A decisive and crucial part of any election is voting. Hence it shows individual rights power along with their concern for the topic. Voting challenges like privacy issues, resistance from fraud, viable and feasible approach, systematic and secure counting of votes must be taken into consideration. A vote is defined as a right to express opinion, choice or wish. It is the right to express one's opinion on how one would like to be governed, in the context of democracy [33]. If this is the primary goal of a vote, is the mechanism we use to capture the user's opinion serving our nation well? So, what is the problem that we need to fix in this? We will be taking into account the different scenarios that the voting process will go through with and without blockchain. This could lead to an affable approach towards the topic. With the help of these scenarios, we can forecast the outcome up to some extent.

1. *The framework of the voting system at present*

The voting system at present goes on too long. Due to which the enthusiasm of voters and elections is drained. The present framework of the voting system is vulnerable to hacking as well. In some parts of the world, electronic voting machines have been doubted to be corrupted. There are some beliefs that revolves around the tampering of voting machine; computer scientists have tampered with the machine to prove that it can actually take place. These facts demolish the faith of the voter on the governing bodies. The other factor that must be taken into consideration is that of the inaccuracy in capturing voters' intent. The touch screen sensors can be knocked out easily just by vibrations or shocks that may occur during machines' transportation. Unless the sensors are re-aligned or corrected at the time of its placement, it may mislead the voter or even misinterpret the voter's intent. For instance, a voter who wants to vote for candidate X, cast a vote for candidate X, but candidate Y would light up instead and then cast for candidate Y. This leads to fraud in the casting process. The machines have always been subject to scrutiny and distrust.

With the help of software programming and coding, any computer software can be generated. The software can easily be corrupted by any programmer who has or knows the source code. It is impossible to test the present voting system for security problems, especially if problems were intentionally introduced and concealed. If the hackers can insert malicious codes to the electronic voting machines' software, it can change the election results completely. They can be triggered by the obscure combinations of keystrokes and commands via the keyboard. If one talks about the physical security of the machines, then there are faults in that too. Many of the DRE (Direct Recording Electronic voting machine) models are under examination regarding the physical hardware controls. It has been surveyed that the EVMs contained loopholes in controls designed to protect the system. All these choices leave people hopeless and disenfranchised about being able to effect change through their votes. In fact, in the long run, these voting systems face much of the backlash. These systems reduce incentives for new candidates to participate, result in fewer parties, increase gerrymandering, give birth to spoiler candidates whose sole aim is to distract the front runners and privatize mass media on political outcomes, the degradation of rights and democracy. None of these are the desired results for a nation or even a political party or candidate's conspiracy. So, what can we do to improve conditions on the voting front? We can change the rules that govern them. We can design the voting process that makes it more expressive and efficient. While there are no perfect systems out there, we can adopt the 'more perfect union' spirit. We need to keep fixing the new problems and keep trying to find better solutions. We have to look ahead and work with new technologies. Walking with the pace of the changing time is the need of the hour. Even when there is much advancement in every field, then why do elections have to be stagnant? We can only make advancements in this by adopting the trends and giving way to new technologies.

2. *The framework of the voting system with blockchain*

There is a reason why one has to fill out ballots at polling place for our elections. This is because this is our right. The law has given equal opportunity to every eligible voter, to cast his vote. The right to vote is one of the pillars of democracy. So, how to have a better approach towards voting is discussed in this section.

To protect the vote's integrity and the privacy of the voter at the same time can be done with the help of anonymous ballots. Anonymous ballots are the way to go. Digital voting has always been challenging as the verification and validation of each ballot is tough, while keeping them anonymous. These problems of validation of ballots and keeping the voter's privacy into consideration, Blockchain is a step towards the digitalization of the voting process. The privacy issues can be solved with the help of cryptography which is an essential part of blockchain. Blockchain-based voting is already providing new dimensions to elections. At present, US military officials serving overseas are able to cast their votes in their home elections using their smartphones [34]. An amalgamation of blockchain registry and encryption tallies those votes. Countries like Switzerland, Denmark, Brazil and South Korea are already exploring voting techniques with the help of blockchain. Noticeably, Estonia is leading the way ahead, as they have already developed unique ID cards for their citizens to be able to vote. This allows them to cast their vote over blockchain quickly and securely.

There will be a huge and lasting impact on global governance if the essential part of democracy is digitized. Public referendum becomes a feasible option, and citizens can make decisions much more quickly. With the direct democracy by the people, representative democracy may get marginalized. But this is not all, another result is rigging elections; this could become more complex or nearly impossible.

Blockchain voting is similar to analogue voting. The same processes and concepts are applied. The citizen is bound to prove and register their citizenship in a particular jurisdiction to cast a vote. The identity and citizenship can be recorded on the blockchain associated with that user's key. The other most important thing is to cast a vote. This can be achieved in the form of a specially assigned voting token that would be deposited in the user's account. The token will have a time limit after which it gets destroyed via a smart contract or in short, becomes useless. Once the vote is cast, it gets registered on the blockchain where it is verifiable, transparent, and immutable. One can easily declare the results of the election by just counting up the votes [35]. So, now the question arises that if the voting process becomes easy with blockchain, why does voting by blockchain not be implemented everywhere? The reason is there are some complications in this too. One major issue is the verification of the voter's identity. Moreover, we also have to prevent the people who are not a citizens from casting their vote. This is a bit tricky as it depends on the central governing body to verify residency documents, eligibility, and citizenship. Even though this can be achieved with a biometric system's help, it increases the complexity of the model. Once the verification is done, the next step is to separate it from the ballot itself. Most importantly, the key part of democracy is the secret ballots. Nobody should be aware of the fact that to whom the voter has cast its vote. This way they would not be able to influence the vote in any way [36]. The secrecy of ballots can be achieved with the help of zero-knowledge proofs, ring transactions, or various encryption methods. Each method has its technical challenges, benefits, and drawbacks. Proving complete anonymity is still considered the biggest challenge of blockchain voting.

Experts of cybersecurity agree with the fact that blockchain is unhackable. However, the anonymity needed for voting is more difficult to secure, and one has to be very clear that it is not compromised at any cost.

4 Possible Implications

If the blockchain expands in usability as well as popularity for the common people, it has huge implications and is too better than the current voting procedure. It has the power to fundamentally change the way how democracy functions. The blockchain voting provides the benefit of improved transparency. As of now, a voter does not know what happens to the vote once the vote is cast. He has to trust the polling workers that his vote has been counted properly. However, there is no way to judge that the vote has been counted properly. With the help of blockchain, it is possible to track the vote [37]. A history of votes will be generated in the blockchain every time a vote is cast. The side effect of increased transparency is that it reduces fraud. Blockchain has the ability to raise the standard of voting at international platforms, with the communities of the world advocating for blockchain governance in all notions. Blockchain also allows real-time tallying of votes. This indicates that elections can now happen within a shorter time span. In addition to this, if the elections are conducted digitally, then it will lead to less investment in the polling infrastructure. This will completely change the voting procedure for voters. Any voter will be able to cast their vote from anywhere.

Blockchain is not only built specifically for elections but for initiatives within a company which require voting from employees and shareholders. With open vote from shareholders, it may be possible to imagine good decisions at earliest. Increased engagement of the voters will mark the biggest advantage of blockchain-based voting. Easy log in and casting a ballot will be done within minutes, if blockchain makes voting digitally possible from smartphones or computers [38]. It will result in more direct democracy as it would most probably increase the turnout of voters drastically.

Blockchain has tremendous abilities to overcome the problems of data integrity, voter security and privacy. It is impossible to alter any information of a block as it is discerned by other blocks which have the complete set of data.

Blockchain proves to provide an effective and systematic approach that the democratic system requires. A blockchain-based application is not concerned about the security of its Internet connection, because any hacker will not be able to access terminal and hence will not affect other nodes. Independent nodes cryptographically validate every vote, writing it to the ballot box permanently. This makes the system immune to malicious attacks. Counting of votes can be done with absolute certainty, as each ID is attributed to one vote giving zero scopes for tempering the results. Effective submission of votes without revealing the voters' true identity and their political preferences can be considered an auspicious aspect of blockchain. By providing an efficient and irrefutable way to vote from one's phone will encourage participation. Blockchain is paving for a democracy where people will decide the course of policies themselves rather than relying on representatives. A major advancement in rules of the elections will help make such a transparent system. Online voting has its benefits like:

- Ability to vote remotely
- Automatic calculation of results
- Ease in logistical challenges
- Centralized management

Not only elections but also polling, census, and even guided general meetings can be secured with the help of this technology. Blockchain voting software has diverse use cases. Its ability to manage constituencies and engage people is important for the future of society [39]. At present, the technology is in its infancy, but as it matures along with the young voters, it will play the most crucial role in many lives.

Blockchain voting is still not ready or perfect for prime time yet. However, once it gets legitimacy, it is expected to bring an enormous change to the democratic setup [40]. Making voting more transparent and easier will create a more engaged electorate. Several organizations are currently working and exploring voting on the blockchain. More accessible voting would mean more ongoing referendums on leadership or more frequent representative elections. All these features of blockchain will drastically change the procedure of elections.

5 Future Scope

E-voting using blockchain has a vast scope in the near future. As the technology is constantly advancing, the acceptance of blockchain will soon become much smoother. It will affect the complete outlook of the present scenario of conducting elections. The elections are more transparent, reliable and secure with the use of blockchain technology [41]. Many times elections require the voters to be physically present at the polling booth. This condition results in the reduction of the number of voters who are eligible to vote. It will increase the accessibility of the voters. Blockchain will tackle the convention of reaching out to booths to cast one's vote. Blockchain will help in solve the biggest challenge of Decentralized Voting System as it will pay close attention towards fraud voters. The techniques currently in use in the cryptocurrency systems such as decentralization, anonymity, high security, yet an auditable chain of records, provides wider scope to the use of the blockchain technology in E-voting [42]. Blockchain is not only limited to securing the financial transactions and any type of data transactions as well [43]. The kind of system infrastructure that blockchain will provide is extremely useful for voting. It has been rightly said that "A vote is a small piece of high-valued data," and thus it needs to be supervised with the utmost responsibility.

6 Conclusion

The requirement is to make the entire election process reliable and secure. Voters look up to elections as a medium of expression. The process has to come out clean and valid. The very foundation of an election is shaken even with a small tragic incident, as the voters doubt the creditability of elections. Blockchain will surely be the remedy for the problems prevalent in the present voting systems. The hurdles that make elections a less transparent and secure process will be resolved.

Most importantly, people will have more access to cast their vote, which will further increase the voting process's efficiency. The technology of blockchain is designed in such a way that it provides a refreshing vision to present scenarios. The adaptability of the system, that is, e-voting with blockchain is the biggest concern. Various governance practices of the world will need to come up with solutions to make the blockchain technology more adaptable in terms of voting. "The only thing that remains constant is change" and hence the voting system of the world needs a complete transition of ideas and approach. This will be the required dawn in the world of voting.

References

1. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Working Paper. [Online] Available: https://bitcoin.org/bitcoin.pdf
2. Hafid, A., Hafid, A. S., & Samih, M. (2019). A methodology for a probabilistic security analysis of sharding-based blockchain protocols. In *Proceedings of the international congress on blockchain and applications* (pp. 101–109). Springer.

3. Hafid, A., Hafid, A. S., & Samih, M. (2019). New mathematical model to analyze security of Sharding-based blockchain protocols. *IEEE Access, 7*, 185447–185457.
4. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxana, P. (2016). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 17–30). ACM.
5. Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2018). Omniledger: A secure, scale-out, decentralized ledger via sharding. In *Proceedings of the 2018 IEEE symposium on security and privacy (SP)* (pp. 583–598). IEEE.
6. Zamani, M., Movhedi, M., & Raykova, M. (2018). Rapidchain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security* (pp. 931–948). ACM.
7. ZILLIQA Team and Others. (2017, 2019). *The ZILLIQA technical whitepaper*. Retrieved September (vol. 16).
8. Harmony Team. *Harmony*. Technical whitepaper. [Online] Available: https://harmony.one/whitepaper.pdf.
9. Manuskin, A., Mirkin, M., & Eyal, I. (2019). *Ostraka: Secure blockchain scaling by node sharding*. arXiv preprint: arXiv:1907.03331.
10. Zochowski, M. (2018). *A highly scalable decentralized transaction system*. Version 1.0. [Online] Available: https://logos.network/whitepaper.pdf
11. Ethereum 2.0. *Ethereum roadmap*. [Online] Available: https://docs.ethhub.io/. Accessed 28 Jan 2020.
12. Buterin, V. *Ethereum sharding FAQ*. [Online] Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ. Accessed 28 Jan 2020.
13. Madaan, L., Kumar, A., & Bhushan, B. (2020). Working principle, application areas and challenges for blockchain technology. In *2020 IEEE 9th international conference on communication systems and network technologies (CSNT), Gwalior, India* (pp. 254–259). https://doi.org/10.1109/CSNT48778.2020.9115794
14. Dang, H., Dinh, T. T. A., Loghin, D., Chang, E., Lin, Q., & Ooi, B. C. (2019). Towards scaling blockchain systems via sharding. In *Proceedings of the 2019 international conference on Management of Data* (pp. 123–140). ACM.
15. Stegos AG. (2019). *A platform for privacy applications*. White paper version 1.0. [Online] Available: https://stegos.com/docs/whitepaper
16. Al-Bassam, M., Sonnino, A., Bano, S., Hrycyszyn, D., & Danezis, G. (2017). Chainspace: A sharded smart contracts platform. arXiv preprint: arXiv:1708.03778.
17. Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger*. Ethereum project yellow paper (vol. 151, pp. 1–32). [Online] Available: https://gavwood.com/paper.pdf
18. Kim, S., Kwon, Y., & Cho, S. (2018). A survey of scalability solutions on blockchain. In *Proceedings of the 2018 international conference on information and communication technology convergence (ICTC)* (pp. 1204–1207). IEEE.
19. Garg, K., Saraswat, P., Bisht, S., Aggarwal, S. K., Kothuri, S. K., & Gupta, S. (2019). A comparitive analysis on E-voting system using blockchain. In *4th international conference on internet of things: Smart innovation and usages (IoT-SIU), Ghaziabad, India* (pp. 1–4). https://doi.org/10.1109/IoT-SIU.2019.8777471
20. Wu, H., & Yang, C. (2018). A blockchain-based network security mechanism for voting systems. In *1st international cognitive cities conference (IC3)* (pp. 227–230). Okinawa. https://doi.org/10.1109/IC3.2018.00-15
21. Singh, A., & Chatterjee, K. (2018). SecEVS: Secure electronic voting system using blockchain technology. In *International conference on computing, power and communication technologies (GUCON), Greater Noida, Uttar Pradesh, India* (pp. 863–867). https://doi.org/10.1109/GUCON.2018.8675008
22. Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. *IEEE Access, 7*, 10127–10149.

23. Zhang, W., et al. (2018). A privacy-preserving voting protocol on blockchain. In *IEEE 11th international conference on cloud computing (CLOUD), San Francisco, CA* (pp. 401–408). https://doi.org/10.1109/CLOUD.2018.00057
24. Shahzad, B., & Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access, 7*, 24477–24488. https://doi.org/10.1109/ACCESS.2019.2895670
25. Kshetri, N., & Voas, J. (2018). Blockchain-enabled E-voting. *IEEE Software, 35*(4), 95–99. https://doi.org/10.1109/MS.2018.2801546
26. Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018). Blockchain-based E-voting system. In *IEEE 11th international conference on cloud computing (CLOUD), San Francisco, CA* (pp. 983–986). https://doi.org/10.1109/CLOUD.2018.00151
27. Bulut, R., Kantarcı, A., Keskin, S., & Bahtiyar, Ş. (2019). Blockchain-based electronic voting system for elections in Turkey. In *4th international conference on computer science and engineering (UBMK), Samsun, Turkey* (pp. 183–188). https://doi.org/10.1109/UBMK.2019.8907102
28. Yadav, S. P., Mahato, D. P., & Linh, N. T. D. (Eds.). (2020). *Distributed artificial intelligence: A modern approach*. CRC Press.
29. Shen, C., & Pena-Mora, F. (2018). Blockchain for cities—A systematic literature review. *IEEE Access, 6*, 76787–76819.
30. Jaoude, J. A., & Saade, R. G. (2019). Blockchain applications–usage in different domains. *IEEE Access, 7*, 45360–45381.
31. Qiheng, Z., Huawei, H., Zibin, Z., & Jing, B. (2020). Solutions to scalability of blockchain: A survey. *IEEE Access, 8*, 16440–16455.
32. Wang, J., & Wang, H. (2019). Monoxide: Scale out blockchains with asynchronous consensus zones. In *Proceedings of the 16th fUSENIXg symposium on networked systems design and implementation (fNSDIg 19)* (pp. 95–112). USENIX.
33. Rawat, D., Rana, G., Bindra, J., & Kumar, A. (2020). Implementation of blockchain in current transaction systems. *International Journal of Data Structures, 6*(1), 31–59. https://doi.org/10.37628/ijods.v6i1.590
34. Nordrum, A. (2017). Govern by blockchain Dubai wants one platform to rule them all, while Illinois will try anything. *IEEE Spectrum, 54*(10), 54–55.
35. Guangsheng, Y., Xu, W., Kan, Y., Wei, N., Andrew, Z. J., & Ren, L. P. (2020). Survey: Sharding in blockchains. *IEEE Access, 8*, 14155–14181.
36. Wang, G., Shi, Z. J., Nixon, M., & Han, S. (2019). Sok: Sharding on blockchain. In *Proceedings of the 1st ACM conference on advances in financial technologies* (pp. 41–61). ACM.
37. Bansal, P., Panchal, R., Bassi, S., & Kumar, A. (2020). Blockchain for cybersecurity: A comprehensive survey. In *IEEE 9th international conference on communication systems and network technologies (CSNT), Gwalior, India* (pp. 260–265). https://doi.org/10.1109/CSNT48778.2020.9115738
38. Huang, K., Zhang, X., Mu, Y., Rezaeibagha, F., Du, X., & Guizani, N. (2020). Achieving intelligent trust-layer for internet-of-things via SelfRedactable blockchain. *IEEE Transactions on Industrial Informatics, 16*(4), 2677–2686.
39. Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE Access, 7*, 147782–147795.
40. Mertz, L. (2018). (Block) chain reaction: A blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution. *IEEE Pulse, 9*(3), 4–7.
41. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019). Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal, 6*(2), 2188–2204.
42. Shankar, A., Pandiaraja, P., Sumathi, K., Stephan, T., & Sharma, P. (2020). Privacy preserving E-voting cloud system based on ID based encryption. *Peer-To-Peer Networking and Applications*. https://doi.org/10.1007/s12083-020-00977-4
43. Yao, H., Mai, T., Wang, J., Ji, Z., Jiang, C., & Qian, Y. (2019). Resource trading in blockchain-based industrial internet of things. *IEEE Transactions on Industrial Informatics, 15*(6), 3602–3609.