Leveraging Secured E-Voting Using Decentralized Blockchain Technology

Anushka Chaubey, Anubhav Kumar, Vikalp Pandey, Bharat Bhushan, and Priyambada Purohit

1 Introduction

Poor electoral systems have always been a major issue leading to election violence in many democratic countries, including India. Electronic voting was postulated as a potential replacement for the paper and ballot system. Over the years, e-voting has evolved as a viable alternative for many non-governmental elections. Various nations are now conducting a number of e-voting trials in the political sphere despite the numerous debates, disputes, and anomalies that have been brought up in relation to them. One of the well-known instances that sparked numerous concerns regarding vote tampering and miscounting was the Ohio e-voting incident in 2004 [1]. As a result, it is difficult to ensure that e-voting can be a precise and error-free practical approach for governmental elections yet. In this scenario, blockchain technology comes to the rescue.

Satoshi Nakamoto originally proposed the idea of blockchain [2]. It was the first time that a distributed system of network and cryptology were combined in order to execute peer-to-peer transactions of the cryptocurrency known as bitcoin in a secure and open fashion. Due to its intricacy and unpredictable nature, blockchain was initially used sparingly, but over time it has drawn attention on a global scale. A blockchain, which is a chain of blocks made up of cryptographically linked blocks, is essentially a data structure utilized throughout transactions that maintains data or information in the structure of blocks. Each block includes a unique hash value in addition to the preceding block's hash, which aids in creating the links between the

A. Chaubey (✉) · A. Kumar · V. Pandey · B. Bhushan · P. Purohit
School of Engineering and Technology, Sharda University, Greater Noida, UP, India

Faculty of Management Studies, SRM IST, Ghaziabad, UP, India
e-mail: 2019004401.anushka@ug.sharda.ac.in; 2019549001.anubhav@ug.sharda.ac.in; 2019641513.vikalp@ug.sharda.ac.in; bharat.bhushan@sharda.ac.in; priyambv@srmist.edu.in

R. Sharma et al. (eds.), *Data Analytics for Internet of Things Infrastructure*,
Internet of Things, https://doi.org/10.1007/978-3-031-33808-3_15

blocks. It is the responsibility of the nodes within the network to interconnect these blocks. To ensure the integrity and safety of the data, the blocks are encrypted, and the network itself validates the blocks. Basically, blockchain technology is a concept that makes use of a number of technologies, including decentralized networks, peer-to-peer transactions, smart contracts, and cryptographic algorithms.

Recently, blockchain has become a tool for boosting the effectiveness of technologies used in several industries. In order to get around some potential problems with e-voting, the voting systems that are based on blockchain technology have recently grown more and more significant. The immutable property of blockchain technology has rendered it a decentralized and distributed ballot box, leading to the proposal of blockchain-based voting systems as the forthcoming generation of contemporary electronic voting systems [3]. Governments are encouraged by blockchain technology to adopt intelligent sustainable voting machines and incorporate sustainability reports into voting systems. It guarantees that all parties have access to trustworthy information on sustainable assets. In spite of the fact that blockchain technology is rapidly being used to strengthen the security of the e-voting system, a number of problems still exist.

So as to address as many issues as possible that might emerge while implementing a blockchain-enabled e-voting system, it is very important to understand the concept of blockchain technology from its core. For this purpose, this chapter provides a very detailed understanding of blockchain technology and its integration and implementation with e-voting systems. The following contributions are made by this chapter: providing detailed information on the blockchain technology, its working and, integration with the e-voting system including the Elliptical Curve Digital Signature Algorithm; understanding how different types and features of blockchain technology help in improving the electronic voting mechanism; providing an overview on different consensus algorithms; and identifying a set of the previous paper and ballot and e-voting system's unfilled gaps. This chapter shows how blockchain technology, if integrated, can help overcome most of the major issues of an electronic voting system.

Further, this chapter has been organized in the following manner. Section 2 defines blockchain technology, its working, and, its features. Section 3 discusses the different types of blockchains and the associated consensus protocols. This section further outlines the unfilled gaps in the existing voting systems. Section 4 presents a literature survey on the various electronic voting systems in existence. Finally, this chapter concludes in Sect. 5 highlighting some open research directions to guide further research in the area.

2 Blockchain

Let us begin by understanding the meaning and significance of blockchain technology and how is it useful. Haber and Stornetta first put forth the idea of the blockchain in 1991. The major goal was to create a digital document timestamp that could

not be altered. Satoshi Nakamoto is thought to have created the first blockchain-based system in 2008. It is also obvious that Bitcoin was the first widely used blockchain technology. The idea of a blockchain can be compared to a distributed, open, and secure data book. Most people believe that the idea will be a crucial part of industry 5.0 applications in the next years. While blockchain is well recognized in the cryptocurrency industry, one could easily make the case that its potential goes much beyond digital currency. Government agencies as well as private businesses have started experimenting with blockchain. In further sections, the definition of the blockchain (Sect. 2.1), its working (Sect. 2.2), and the features of the blockchain (Sect. 2.3) have been discussed.

2.1 What Is Blockchain?

Blockchain is defined as a digital database or a ledger that is shared among the nodes of a peer-to-peer system of a network. It is a database that electronically saves data or information in digital form [4–7]. It is a sort of distributed ledger technology (DLT) made up of an expanding list of data, known as blocks, that are safely connected to one another using cryptography. Every block includes the timestamp, a cryptographic hash value of the preceding block, and transaction information. The timestamp establishes the existence of the transaction data at the time the block was produced. They basically create a chain (same as the linked list), with each new block linked to the previous ones since each block carries information about the prior block [8]. Blockchain transactions are therefore irreversible in the sense that, once they have been stored, the contents of any specific block cannot be changed subsequently without changing all succeeding blocks.

The blockchain is a series of blocks that, like a traditional public ledger, contain an exhaustive list of transactional data [9]. Each block has a reference, known as the parent block, which is effectively a hash value of the block preceding it and points to it. The genesis block is the first block in a blockchain and is the only block without a parent block [10].

Blocks are made up of the block body and the block header. The block header consists of the following:

- The block version specifies the set of block verification guidelines that are to be followed.
- A 256-bit, cryptographic hash value called the parent block hash points to the block previous to it.
- The hash value of each transaction stored within the block is represented by the Merkle tree root hash.
- The timestamp is the demonstration of the current time in seconds since January 1, 1970, at 0:00 UTC.
- nBits is the shorthand for the current hashing goal.

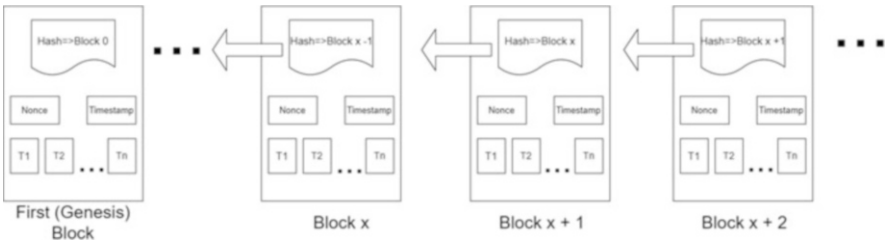

Fig. 1 Representation of a blockchain consisting of a sequence of blocks

- A 4-byte field known as a nonce is typically initialized with 0 and rises with each hash calculation.

Transactions and a transaction counter constitute the block body. A block's maximum capacity for transactions is determined by the size of every transaction and the block size. Asymmetric cryptography is used by blockchain to verify transaction authentication. The utilization of an asymmetric cryptographic digital signature in an unreliable environment is applied. Figure 1 represents an example of a blockchain consisting of a sequence of blocks.

Utilizing a peer-to-peer system of network and a decentralized timestamping server, a blockchain database can be unilaterally controlled. Via widespread cooperation driven by unit self-interest, they are verified. Since participants are minimally concerned about the security of the data, a design like this promotes a strong workflow. A digital asset loses its ability to be replicated indefinitely when a blockchain is used. The long-standing issue of double spending is resolved since it demonstrates that each unit of currency was transferred just once. A value-exchange protocol has been used to characterize a blockchain [11]. Since it produces a record that enforced offer and acceptance when the exchange agreement was correctly set up to document it, a blockchain can preserve title rights.

2.2 Working of a Blockchain

A blockchain can be defined as typically a continuous series of blocks of information that are cryptographically linked to each other and shared among the nodes of a network. Let us now understand how exactly this technology works.

By employing a digital signature that utilizes private key cryptography, a node begins a transaction among a decentralized blockchain network. On the blockchain platform, a transaction could be viewed as a data structure that reflects the exchange of digital assets among peers. Each transaction is kept in a pool of unconfirmed transactions, and the Gossip protocol, a flooding mechanism, is used to spread it throughout the network. Peers then need to select and authenticate these transactions in accordance with a set of predefined criteria. For instance, the nodes attempt

to authenticate and confirm these transactions by determining if the initiator has enough balance to initiate a transaction or just by enforcing double spending in an attempt to deceive the system. Double spending is when you make a number of distinct transactions utilizing the very same amount of money as your input [12].

The miners confirm and validate the transaction, and then it is added to a block [13]. Peers who mine for blocks employing their computing resources are referred to as miners [14]. To publish a block, miner nodes must utilize enough of their computing power and resolve a computational problem. The miner who is able to figure out the riddle first wins and earns the opportunity to add a new block. Upon successfully establishing a new block, a tiny bonus is granted. The new block is then verified by every peer in the network using a consensus algorithm, which is a mechanism used in distributed systems to achieve consensus. A localized copy of every peer's immutable ledger is then created, and the new data block is added to the already existing chain. The transaction is finalized at this stage. A cryptographic hash reference is used by the following block to connect itself to the freshly formed block. The block now receives its first confirmation, and the transaction now receives its second confirmation. The transaction will also be reaffirmed every time a fresh block is incorporated into the chain. Typically, a transaction takes 6 network confirmations to be deemed complete [15]. A complete diagrammatic representation of the working of a blockchain is portrayed in Fig. 2.

A detailed overview of the process of transactions has been described further. Verifying the sender's identity is the initial stage in the transaction process, indicating that only the sender and not anybody else is requesting the transaction between both the sender and the recipient. Let us use a simple transaction between Robin and

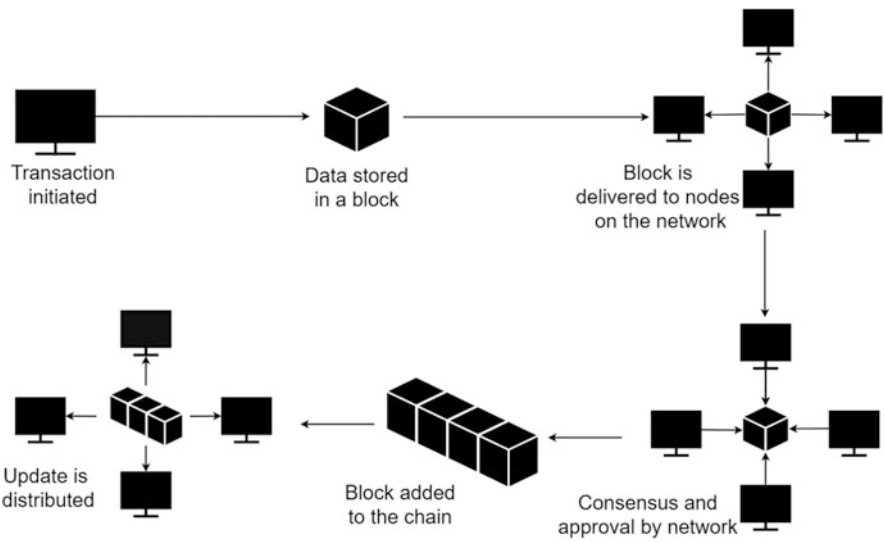

Fig. 2 Working of a blockchain

Ana as an example. Assume that Robin and Ana each have a balance in bitcoins and that Ana wants to send Robin 10 bitcoins. Ana will now broadcast a message in the blockchain network with the details of the transaction in order to send the money. Blockchain utilizes digital signatures (private and public keys) to accomplish this [16]. Robin's details, including his public address and the amount of transaction, as well as Ana's public key and digital signature, are provided for the broadcast. Ana created that digital signature using her private key. All miners individually perform transaction validation based on several standards. Blockchain employs the Elliptic Curve Digital Signature Technique (ECDSA) [17]. This algorithm makes sure that the funds can only be used by the people who actually own them.

2.2.1 Elliptic Curve Digital Signature Technique (ECDSA)

It is among the most challenging public key encryption techniques. Elliptic curve cryptography produces keys that are generally smaller than those produced by digital signing techniques. It is a type of public key cryptography that is based on the algebraic nature of elliptic curves on finite fields. Elliptic curve cryptography is mostly used to generate digital signatures and pseudo-random numbers, among other things [18]. Bitcoin uses the encryption technique ECDSA to make sure that only the rightful owners of currency may use it. It depends on the hash function and curve order chosen. These are, respectively, Secp256k1 and SHA256 (SHA256()) for bitcoin [19]. Some of the terms that describe the procedure of ECDSA are as follows:

Private key: A code that is only known to the person who created it. In essence, a private key can be described as a numeric code that was chosen at random. In Bitcoin, the funds can only be spent by someone who has a private key associated with them. A private key in Bitcoin is a unique 256-bit and 32 bytes unsigned integer.

Public key: It is a numeric value that is equivalent to a private key although it doesn't have to be hidden. A private key is used to calculate a public key, but not the other way around. Without disclosing the private key, a public key is utilized to check whether a signature can be deemed authentic. Public keys in Bitcoin are either compressed or not. A 256-bit integer, say x, and a prefix of either (0x03) or (0x02) constitute the 33 bytes compressed public keys. The earlier uncompressed keys include a prefix that is a constant (0x04), and two 256-bit integers that are known as x and y (2×32 bytes) and are 65 bytes long. A compressed key's prefix enables its y value to get calculated from its x value.

Signature: It is a code that demonstrates the completion of a signing process. The hash of the object that is to be signed and the private key are mathematically combined to create a signature. The signature is made up of the two integers r and s. Without requiring access to the private key, a mathematical procedure using the public key on the signature can be used to establish that it has been initially formed using the hash combined with the private key. The resulting

signatures are 73, 72, or 71 bytes long, with probabilities of approximately 25%, 50%, and 25%, respectively. However, proportions that are considerably smaller are feasible along exponentially diminishing probabilities.

Let us take a look at some of the primitives used by ECDSA for obtaining a signature of a message and for its vice versa.

- s and r: Both these values together form the signature.
- z: It is the message's hash that is required to be signed.
- k: The nonce value used to determine the values of s and r.
- Q_{A} and d_{A}: They represent the public key point and private key number of the message, respectively. When an address inside the wallet is provided, a copy of this can be derived.

Signature Algorithm
The pair s and r (also known as the signature pair) are calculated using the signing algorithm from d_A to z.

- Identify the curve's group order n.
- Follow by generating a cryptographically secure value k (a random number) that ranges between 1 and $n - 1$.
- Calculate $(x, y) = k * G$, where G can be defined as secp256k1 curve's generator point.
- Determine $r = x \bmod n$. Create a new random k and restart if $r = 0$.
- Calculate $s = k^{-1}(z + r * d_{\mathrm{A}}) \bmod n$. Generate a new random k and restart if $s = 0$.

Note: Reusing k after a signature has been created with it is not advised because of the defects that allow a perpetrator to obtain signed messages' private key if they are aware of k (the shared nonce) that was utilized in them.

Verification Algorithm
- The verification algorithm checks the consistency of the signature pairs z and Q_{A},s and r.
- Make sure that r and s are both between 1 and $n - 1$.
- Calculate $u_1 = z * s^{-1} \bmod n$ and $u_2 = r * s^{-1} \bmod n$.
- Make sure (x, y) is not the same as the infinitesimal point when you compute $(x, y) = u_1 * G + u_2 * Q_{\mathrm{A}}$. When two points are added together that would not otherwise result in a point on the curve, for instance, two points with identical X values but reversed Y values, a peculiar point known as the point at infinity is created.
- The signature is valid if $r = x \bmod n$, it is invalid whenever a test fails or if anything else goes wrong.
  The complete process of ECDSA is represented in Fig. 3.

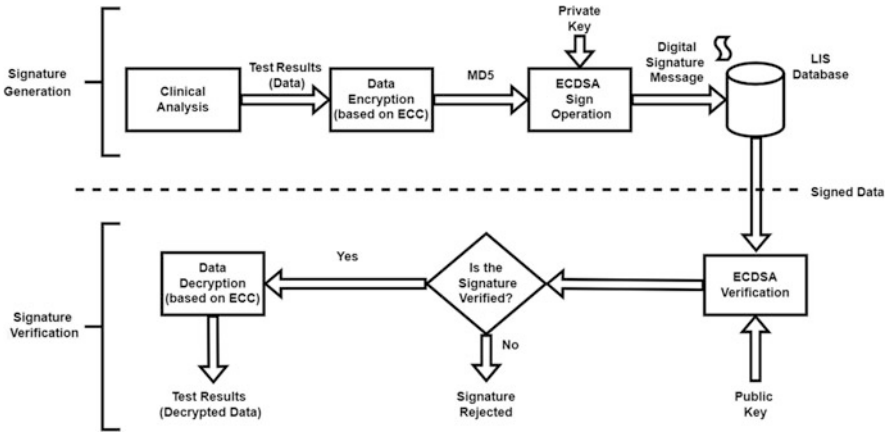

Fig. 3 Working of an elliptical curve digital signature technique

2.3 Features of Blockchain Technology

Blockchain is among the most exciting and popular technologies in today's era. Now that we already have a basic understanding of this technology, let us take a look at some of its primary features.

2.3.1 Immutability

The attribute of immutability is the inability to change or modify. One of the main characteristics of a blockchain that guarantees the network's permanence and immutability would be this. Since centralized information depends on the third-party gateway for its security, it is susceptible to theft and hacking. Blockchain systems are secure because of their decentralized organization; however, because of their immutability, it is almost impossible to alter or manipulate the data. These problems are easily resolved by enterprise blockchains [20]. Data can be easily modified with everyone's consent because they are little in size and connected as they have a common structure and purpose.

2.3.2 Auditability

A digital timestamp and distributed ledger are used as the verification and record, respectively, of every transaction that takes place within a blockchain system or network. As a consequence of this, through gaining authorization for any network node, it is probable to review and trace earlier records [21]. For instance, Bitcoin allows for the iterative tracing of all transactions, supporting the transparency and

auditability of the data state of the blockchain. However, it becomes exceedingly challenging to track down the source of the money when it is spread across numerous accounts.

2.3.3 Persistency

Blockchain enables both producers and consumers to demonstrate that their data is true and undamaged by providing the framework by which veracity can be evaluated [22]. For instance, if a Blockchain has 10 blocks, block number 10 would have the prior block's hash, and the current block's information would be employed to build a new block. The result is, every block in the chain that already exists is linked and connected to every other block. Even transactions have connections to earlier transactions. Thus, a simple change to any transaction will drastically alter the block's hash. Anyone who wishes to edit any information must alter all the hash data from prior blocks, which is thought to be an enormously challenging task given the amount of effort required. Additionally, the block is validated by other members of the network once it is produced by a miner. Therefore, the network is able to identify any data tampering or fabrication. Due to this, blockchain is almost impervious to manipulation and is viewed as a distributed ledger that cannot be altered.

2.3.4 Decentralization

In conventional centralized transaction systems, the trusted centralized agency must verify every transaction (e.g., a bank). A wiser approach would be a distributed peer-to-peer blockchain structure to address the key issue of lift resilience, availability, and failover that decentralization requires, which is trust. In contrast to centralized systems, any two peers (P2P) can perform a transaction within the blockchain network without the need for central authentication. By utilizing several consensus techniques, blockchain can in this way lessen the trust issue. Additionally, it can alleviate performance bottlenecks at the central server and lower server expenditures (including development and operation costs).

2.3.5 Anonymity

A participant's genuine identity is concealed on a blockchain platform. Every member of the dispersed network is assigned an address. Instead of an actual identity, this address serves as that entity's identification. On the network, the addresses maintain the user's privacy [23]. An element of anonymity is provided by the trustless environment provided by blockchain technology.

3 Types, Consensus Protocols, and Unfilled Gaps

The meaning of blockchain, its working, and its different features and characteristics that make this technology a better alternative as compared to the traditional central ledger systems have been described so far. To get a deeper understanding of blockchain technology, understanding the different types that blockchain technology has been divided into, based on its characteristics and applications, is crucial. Blockchain is a technological mechanism that employs its own decentralized nodes to record, validate, transact, and exchange network data without the aid of a third party. Blockchain is based on intelligent distributed cryptographic and mathematical techniques. The participants come to an agreement and resolve the issue of cost-effective and dependable trust and value transmission. Blockchain networks could be utilized to adapt their functioning to the specific needs that an enterprise may have. Although the technology can initially seem perplexing, blockchain can be broadly divided into two broad categories and four different kinds of networks.

The different types of blockchains available have been described in Sect. 3.1. Further, in Sect. 3.2, the significance of the consensus protocol in creating a secure and reliable blockchain network and the different types of consensus protocols available for use have been studied. Following this, the various challenges faced by the existing voting systems and their unfilled gaps have been discussed later in Sect. 3.3.

3.1 Types of Blockchain

Permissioned networks and permissionless networks are the two primary forms of blockchain networks. Either of these sections can be used to group the four different types although some might use both. A permissionless or permissioned chain might depend on the needs of the company considering using blockchain technology [24]. Both the advantages and disadvantages of the networks within these two bigger divisions are distinct.

A deeper understanding of the four different forms of blockchains has been provided below.

3.1.1 Public Blockchain

Any system or node can participate in a public blockchain, making it a particularly inclusive sort of blockchain system. Anyone with access to a public blockchain can try to decrypt a block of data's hash and include it in the chain. A public blockchain network is still safe as an attack would take a lot of time and effort. Any potential attacker would be required to possess control over 51% of the chain's nodes. Permissionless blockchain networks are another name for

this kind of blockchain technology. It should be no surprise that the exchanging and tracking of cryptocurrency transactions is the most popular use of public blockchain technology provided that the primary public blockchain was utilized for cryptocurrency. Although Bitcoin was the initial cryptocurrency, Litecoin, and several other cryptocurrencies soon followed, each running on its own blockchain. Notarizing papers and keeping a record of public property ownership data are two other potential uses of a public blockchain. The important thing to remember is that any information that requires to be both public and secure is best served by a public blockchain.

3.1.2 Private Blockchain

A private blockchain network is one that is either administered in kind of a closed environment or is managed by a single organization, like a company. In other terms, it often has a smaller size as compared to a public blockchain. The controlling entity among a private blockchain (also known as an enterprise/permissioned network of blockchain) determines who is allowed access to the chain and who shall validate all data before it is incorporated. Private blockchains can be used for a variety of tasks, including supply chain management, private voting, and safeguarding trade secrets. There are restrictions regarding who can obtain the information and incorporate information into the chain in a permissioned blockchain. The data is not accessible to outside parties. Due to the fact that there are lesser nodes, they are typically quicker as compared to public blockchains since data can be authenticated and uploaded to the blockchain much more quickly.

3.1.3 Consortium Blockchain

A consortium or federated blockchain is a partly private blockchain that is run by numerous entities rather than just one. Participants of a verified group can only access the blockchain, removing some of the hazards associated with letting a centralized authority supervise the network, as would be the case in one private blockchain. In contrast to a public blockchain, where any node wishing to join could reach consensus, a consortium blockchain's consensus process is managed by predetermined nodes, along with a validator station that can send, accept, and verify any transaction. Transactions can also be transmitted and received by member nodes; however, they would not be able to validate them. A consortium blockchain is mostly used in the payments and banking industries. Theoretically, banks might organize a consortium and choose which node should be in charge of authenticating all transactions. The technique could also be helpful for supply chain processes and research. The benefit of developing a consortium network is the fact that it provides access control similar to a private blockchain while being more robust and flexible than that of a public blockchain.

3.1.4 Hybrid Blockchain

A hybrid blockchain provides its developers with all of the features and benefits of both private and public blockchains. A hybrid blockchain often consists of a private, permission-based network alongside a public, permissionless network. The corporation has control over who may obtain and add information to the blockchain. The hybrid blockchain is owned by a private organization, but it cannot modify transactions. Given that it is more challenging to manipulate or influence 51% of the total nodes, it is more robust than from a private blockchain. In contrast to a public blockchain, a hybrid blockchain does not make the data and transactions it adds publicly available. They may, nevertheless, be publicly validated if necessary. A smart contract, which comprises a code fragment contained in a block and can start a consented event whenever an agreement milestone is achieved, is one example. Every participant's identity is hidden from other participants until they conduct a transaction, which is another essential feature of a hybrid blockchain. Hybrid blockchains can be used for a variety of purposes. Real estate, where only certain details should be kept hidden however listings and sales should be publicly disclosed, is among the areas on which there is a significant focus. It might also be used in the retail and financial sectors. In Table 1, all four types of blockchains have been compared.

3.2 Consensus Protocols

Blockchain is a distributed system of a network that attempts to provide data security and data integrity. Every transaction on a blockchain platform is regarded as being quite secure and authenticated because there is no central body to check and audit the transactions. The intricacy of the truth may exist because blockchain operates in

Table 1 Comparison between various blockchain networks

Public blockchain	Private blockchain	Consortium blockchain	Hybrid blockchain
Anyone is free to sign up and take part in the network	This system of the network is governed by a single corporation	The blockchain network is influenced by numerous organizations	Authenticated access; just a few components are private
Immutable, fully decentralized, and secure ledger system	Faster production, better energy efficiency, and privacy	A system that is scalable, decentralized, and lightning-fast	Flexible management of which data is made public and which is private
Transactions are transparent to all parties but remain anonymous	Data processing has been made simpler but is not accessible to everyone	Network security and privacy are maintained	A highly scalable, decentralized, and controlled system

a decentralized fashion and stores high-frequency transactions at the same time. In order to avoid harmful events like double-spending assaults, it is crucial to reach a consensus [25]. The consensus protocol enters the picture here. A consensus protocol is a technique used in computer science to achieve unanimity among distributed systems or components over a particular data item. A consensus protocol is a procedure that enables all participants throughout a decentralized computing system to reach a consensus about the ledger's current data state and also be capable of trusting unknown participants. Several consensus algorithms have been discussed below.

3.2.1 Proof of Work

A "Proof of Work" is really a fragment of information that is complex to produce (expensive, time-taking), yet simple to be authenticated by other participants. Blockchains that use the PoW algorithm make use of specialist nodes, or "miners," which use energy resources to provide security and accounting functions for the platform. Freshly minted coins are used to pay miners for their work. PoW aims to make it ridiculously expensive to hack the network. Since authentic resources must be employed to modify the ledger, it is impossible to "fake the work." From the viewpoint of behavioral economics, Bitcoin's PoW design strikes a very fine balance between incentives. Miners are motivated by rewards.

3.2.2 Proof of Burn

Iain Stewart's Proof of Burn algorithm attempts to address the problems with the proof-of-work approach. PoB protocol makes use of the concept of obliterating or burning the currencies, which reduces the requirement for high-energy resources during mining. It lessens the PoW's reliance on robust computational gear as a result. By transmitting the coins to a publicly recognized, untraceable, and authenticated address, they are burnt. The transmitted coins then lose their ability to be spent. Instead of having to wait months after burning the coins, the miner instantly gains the ability to contest for the generation of fresh blocks. The node has a greater likelihood of producing the subsequent block and earning rewards the more coins it burns. However, this approach does not guarantee that the node would be permitted to mine after burning a specific number of coins. Therefore, the node can experience significant financial loss before receiving its reward. Additionally, the likelihood of being awarded decreases as the count of miners rises [26].

3.2.3 Proof of Stake

The Proof of Stake-based database keeps a record of each validator (PoW's counterpart of a miner) and each party's individual investment in the blockchain

network. In a PoS system, each validator makes an investment to increase their odds of mining the following block. The chances increase with increasing stakes. It does not, however, ensure that the validator having the biggest stake would be chosen. Comparable to a lottery, this mechanism selects the node for the role of a validator at random for block creation. Any person who tries to game the system forfeits his stake. Block construction is simple and does not require a lot of computer power, unlike PoW.

3.2.4 Delegated Proof of Stake

According to DPoS principle, only the nodes with stakes can elect block verifiers (also known as block producers) [27]. By using this voting method, the stakeholders grant the delegates they support the right to create blocks rather than doing so themselves, resulting in a computational power consumption of 0. The stakeholders will choose other nodes to take their place if the delegates are not able to produce blocks during their rounds. To arrive at a conclusion in a fair and democratic way, DPoS makes the best use of the shareholders' votes. DPoS is a low-cost and very efficient consensus protocol when compared to PoW and PoS. Other cryptocurrencies, including BitShares, EOS, are implementing DPoS.

3.2.5 Proof of Elapsed Time

While the Proof of Elapsed Time (PoET), a jackpot-based consensus technique of the blockchain network, has an equivalent activity flow to the PoW protocol, it uses significantly less computation power because it does away with the requirement for mining-intensive mechanisms, which reduces energy use and resource utilization [28]. In PoET, each node of the shared ledger has its own independent random timing that dictates whether or not it will incorporate a fresh block to the network and receive a reward. As a result, it primarily prioritizes efficiency and makes sure that every node is given an equal opportunity of becoming the following block generator.

3.2.6 Proof of Participation

Proof of Participation merges aspects from PoS and Federated consensus techniques to a novel algorithm aimed to demonstrate that a node is contributing valuable network work. The "Node Registry" is a consortium of nodes maintained by the PoP protocol. Anyone may submit a request to join the network, and the distributed protocol shall select who is accepted. This is a significant improvement above federated chains, such as Ripple, in which a central authority chooses who can join the network. Only nodes within that Node Registry are authorized to produce blocks, and every node has approximately the same probability of generating the subsequent

block within the chain. To participate, nodes should wager tokens, and this technique serves to combat Sybil assaults. PoP is intended to compensate a broader range of participants with fresh issuance, hence reducing the centralizing effects of PoW and PoS.

3.2.7 Proof of Authority

Proof of Authority can be described as an image-based technique for consensus that capitalizes on the reputation and identification of block auditors. An organization of Ethereum engineers headed by Gavin Wood presented PoA as a response to spamming assaults against Ropstein Ethereum test net in March of 2017. PoA is comparable to PoS; however, auditors wager their reputation rather than coins. PoA is really only suitable for private blockchain systems due to the fact that network leaders choose trustworthy nodes/validators [29]. PoA networks typically depend on a limited group of validators, thus resulting in greater performance per layer. PoA is commonly regarded as a viable alternative for semi-trusted management of supply chain settings. Ideally, diverse businesses in such a supply network would be able to protect the confidentiality of their data while yet taking advantage of a shared network.

3.2.8 Proof of Importance

Proof of Importance, first established by NEM (XEM), chooses its miners based on specific criteria in a procedure known as "harvesting." The volume and quantity of transactions over the previous 30 days, the amount of invested currency, and network activity are typical determinants. These elements form the basis of the importance score given to nodes. The likelihood of being selected for harvesting a block and collecting the associated transaction fee increases with the score. Although comparable to PoS, PoI avoids the latter's propensity to automatically reward the wealthy by taking into consideration participants' total network support. As a result, simply placing a big POI bet does not ensure that you will win the block.

3.2.9 Proof of Capacity

Proof of Capacity, sometimes recognized as the proof of space, is a mining algorithm that bases mining rights on the amount of accessible space on a miner's hard drive, in contrast to the majority of its predecessors, which awards mining rights based on the computation power or coins staked [30]. In PoC, the process of "plotting" is used by miners to create a list of all feasible hashes beforehand. Then, a hard disc is used to store these plots. There are more potential solutions for the more storage space a miner has. The likelihood of having the right hash combination and receiving the reward rises as the proportion of solutions rises. PoC makes it possible for the

common person to take part in the network because it does not call for expensive or specialized equipment. As a result, it is a more decentralized and less energy-intensive alternative to some of the more widely used consensus mechanisms. The system has not yet been adopted by many developers, and there are worries that it could fall victim to virus assaults.

3.2.10 Proof of History

Proof of History (PoH) offers evidence of historical occurrences, as the term implies. PoH technology enables "timestamps" to be incorporated directly into the blockchain, independently confirming the interval between transactions. This timestamping technique is made possible by a sequential-hashing verifiable delay function (VDF), like SHA-256. It functions by using the outcome of a transaction as the input for the subsequent hash, allowing everyone to plainly understand which event occurred in a specific order. PoH significantly minimizes the processing weight of the blockchain because the VDFs can only be solved by a single CPU score, making it faster and more energy-efficient than many of its peers. PoH has not yet undergone extensive testing because Solana is the only company that uses it [31].

Protocol architecture is replete with choices. Every architecture has its own advantages, disadvantages, and potential applications. From this perspective, it is logical to conclude that they are not genuinely in competition with one another. Bitcoin's application of PoW, for example, is really safe and open. PoW is an excellent consensus protocol for cryptocurrencies. On the other hand, it would have been a horrible option for blockchain-based social media. With blockchain being such a new sector, it is imperative that we maintain our research in order to find new blockchain architectures. New consensus techniques will enable further blockchain applications.

3.3 Challenges Faced by Existing Systems

Elections have always been a contentious issue. Paper ballots and electronic voting machines (EVMs) both have their share of issues and challenges. When elections were still decided by paper ballots, a party's victory was attributed to booth capturing; in modern times, it is linked to EVM tampering. EVMs were proposed as a better alternative to paper and ballot systems as they are time efficient and do not require huge manual labor for the counting of votes but due to their centralized nature, they are vulnerable to security threats. In the below-mentioned sub-sections, we will look at the several challenges faced by both the paper and ballot and digital e-voting systems.

3.3.1 Paper and Ballot Systems

The major issues of using the paper and ballot system for elections are as follows:

Wastage of Paper
It would be equivalent to going back to eating raw meat in the Stone Age after the discovery of fire to switch back to the paper from technological devices. Even the most polluting businesses are working to lower their carbon footprints, so using paper on such a large scale when there are other, more environmentally friendly solutions is a clear disregard for the environment.

Manual Ballot Counting Takes a Lot of Time
The manual counting of votes is laborious and prone to mistakes. It is quite tough to manually count crores of votes, and it takes far more man-days to tally the votes and determine the outcome. As a result, the votes are counted incorrectly, extending the already lengthy counting process.

Booth Capturing
Political parties have used force as a weapon to influence election results in their favor. In the media, a booth capture video became viral during the 2017 Odisha elections. In addition, CPM party booth capture incidents in West Bengal are public knowledge. The Chief Election Commissioner, Sunil Arora, stated about the return to paper ballots in an interview on February 1, 2019, "Political parties have a right to make their thoughts and concerns known because they're the biggest stakeholders after the voters. But we won't return to the era of paper ballots. We're not going back to the days when ballots were seized, force was employed to accomplish the task, and counting took an abnormally long time" [32].

Ballot Paper Manipulation Techniques
Other techniques of vote manipulation, besides booth capturing, have been used in previous elections. This includes the variations in the ink used when casting a ballot. A video from the Rajya Sabha elections in Haryana demonstrated how the voting periods for BJP and Congress MLAs differed, and how later, the votes made by Congress MLAs were disregarded due to a change in the voting pen. Even some voting papers may occasionally be altered voluntarily or forcibly, making the voting process dangerous for both voters and electoral commission members.

3.3.2 Digital E-Voting Systems

E-voting has improved the voting process's performance and credibility in contrast to traditional voting techniques. Electronic voting is frequently deployed in a variety of methods throughout elections due to its adaptability, ease of use, and competitive pricing as compared to traditional elections [33].

Despite these benefits, conventional electronic voting techniques have the danger of encountering excessive authority and manipulated data, so reducing the voting process' essential impartiality, confidentiality, opacity, untraceability, and verifia-

bility [3]. Due to the fact that e-voting techniques are consolidated and licensed by the crucial organization that regulates, analyzes, and supervises the procedure of an e-voting platform, this is a potential obstacle to a fair voting procedure. Recent issues in democratic countries like the United States and India bolster this thesis and demonstrate its validity. It is crucial to prevent the erosion of voter confidence [34].

It is recommended that e-voting systems have the following qualities:

- Receipt-freeness prohibits the production of any receipts as evidence of a voter's support for a certain candidate [35].
- Fairness, preliminary outcomes that could have an impact on other voters' choices are not acceptable [36, 37].
- Data integrity guarantees that every vote is recorded accurately and that it cannot be altered in any way after it has been logged [38].
- Voter anonymity and privacy: Voters' names and the candidates they support should not be made public [39]. Only eligible democrats should be allowed to cast ballots [40].
- Dependability and robustness; voting platforms must function error-free. Software and procedures ought to be created without any malicious code or mistakes [41].
- Individuality should not let voters cast multiple ballots [42].
- Verifiability: Voters should be able to ascertain that their ballots were appropriately counted [43].

4 Recent Advances

Habib et al. [44] discussed applications of an electronic voting platform utilizing the Ethereum technology and smart contract technology. Their describes the old approaches and the drawbacks of using them and how untrustworthy it is in a democratic country so it suggests an alternative approach using the technologies of this new era to move to a technique that is cheaper, faster, and easier to implement as compared to old approaches which are costly, easy to manipulate, and always questionable. New approaches ensure data integrity, increased voter count, and transparency. The proposed system in the forehand mentioned work ensures the security measures using fingerprint authentication and artificial intelligence used for face recognition. Zhang et al. [45] proposed a message authentication and transmission system that verifies authority while hiding the identity. The work suggests that this system can be used in various scenarios like complaint boxes, questionnaires, outcome assessments, opinion collection, and many more. This verifies the organizer and the voters with a design that implies that authentication can be carried out while preserving anonymity which is implemented using the blind signature. It solves the problem of trust between the organizer and the voter and defines the true meaning of democratic voting.

Sayyad et al. [46] described blockchain to be a "cryptographically secure transactional singleton machine with shared-state." This work explains the working based on a network that is decentralized and records transaction history and no single machine can alter the record on the decentralized network. Further, the work explains that the data is recorded in the blocks and every block is associated with two blocks, the previous and the subsequent one, through the hash algorithm. In case someone attempts to manipulate the information in any of the blocks, the chain becomes invalid. Thus, the data once stored, becomes immutable. The employed hash algorithm is SHA-256 which is a function that converts the raw data into hash data using a mathematical expression. It explains some limitations including that 51% of computational power can modify the transaction data. Another limitation specifies that on updating the system divides the network nodes into two types: new nodes, and old nodes, and after the change of version, old nodes cannot connect with the new nodes. Mohammedali et al. [47] presented a framework that is effective and stronger; it has a wallet that is used for the creation of a key pair. An administrator first adds the voter data to the voting system after checking its private key with the parent pair and, therefore, confirms that information. All blocks are associated to one another via the previous hash field. All the blocks are arranged chronologically. This makes it immutable. The framework has an administrator who verifies the outcome with the previously stored data. Authorities can see the results but still cannot change them. The framework is created using the Java programming language to make a portable application, therefore, motivating the voters and increasing the voter count and hence, making the framework less expensive and more secure. SHA 512 increases security even more as compared to SHA 256.

Rezvani et al. [48] proposed security policies of CIA (Confidentiality, Integrity, and Availability) model and their parameters which are relevant to the application of the E-voting system. It explains the CIA model into four categorical Voting Governmental Policies such as pre-registration, multi-candidate, and multi-casting. Confidentiality is a set of rules which stops unauthorized access to the data. Some majors of confidentiality are eligibility, no impersonation, ballot secrecy, vote casting secrecy, voting data secrecy, and privacy. Integrity ensures the trustworthiness of data without any forgery and it constitutes No Double voting, Ballot Immutability, self-tallying, and no ballot forging. Availability means the security of hardware, software, and database. It should resist online hacking attacks like DoS attacks, keys should be kept secret, and prevent loss of voting keys. Sukheja et al. [49] pointed out the issue that software developers who built the web application can manipulate the data, or can add extra voters and remove voters which grants them authorization that can be misused. Therefore, he suggested that a different committee should be appointed (except software developers who built it) which should ensure DAOs contracts. The committee should be able to add or remove members and grant the member the type of authorization according to the system or it should be autonomous. An institution should be answerable for any type of fraud or theft that takes place. This would help in the transparency of blockchain and make it more secure.

Rathee et al. [50] discussed that the e-voting system's privacy and security threats create a significant issue that could result in hackers committing a variety of scams to rig the election. Therefore, a possible challenge is establishing a trustworthy channel of communication by separating genuine devices from untrustworthy ones by calculating their level of trust using an optimizer. In order to identify and address the numerous hazards brought on by an intrusion at multiple levels, they developed a safe method using IoT devices utilizing blockchain. Benabdallah et al. [51] presented that due to its ability to eliminate TTP, decentralize transactions, provide transparency, and completely secure data storage. Blockchain is already being offered as a new technological foundation for a variety of applications. Additionally, it enables the usage of smart contract that automates and executes licensing terms, inside their context. Li et al. [52] proposed that the e-voting protocol allows multiple options and self-tallying options. The work demonstrates that these protocols fulfill complete tracing, likability, privacy, and secrecy. Furthermore, the work suggests that e-voting is realistic and can be used for practical applications after examining the time and gas expense of activities.

Gao et al. [53] discussed an e-voting mechanism based on blockchain that offers a transparent process. By utilizing certificate-less and software encryption, this approach can also audit voters who practice malfunctioning and withstand quantum assaults. Following an evaluation of the performance, it was determined that the proposed work is appropriate for local elections and offers certain benefits in regard to effectiveness and safety when there are few voters. Farooq et al. [54] presented that without using actual polling sites, their proposed technology offers an architecture that could be used to perform voting activities online. They suggested a design that uses adaptive consensus algorithms. Voting is safer because of the chain security methodology used in the electoral platform. When a transaction is being carried out, smart contracts could offer a safe link connecting the network and the client. Shahzad et al. [55] proposed that the architecture outlined in the proposed study considers the utility of hashing methods, the building and securing of blocks, the collection of information, and declaring outcomes by utilizing a flexible blockchain strategy. This work makes the argument that the proposed framework understands data and security management issues with blockchain technology and offers a better representation of e-voting. Huang et al. [56] aimed to make data anonymous and verifiable, and hence they used proof of knowledge encryption which is homomorphic. The result of evaluation and testing and the result of evaluation and checking, as well as compared with comparable ideas, demonstrate that our work has benefits in terms of robustness and security, which demonstrates that our plan is both scalable and practical.

Tran et al. [57] discussed that considering the developments in the field of blockchain, it will soon open new possibilities for applications such as smart contract systems, agriculture, smart cities, and e-voting. As a consequence, there will be a growing need for enhanced security that preserves transparent and decentralized technology that is expected to support blockchain developments. Zaghloul et al. [58] presented an idea that is safe and protects voter's anonymity by using secure multiparty calculations that are carried out by parties with various

allegiances. Additionally, the presented work uses a blockchain powered by smart contracts as a tamper-proof bulletin board that is open to the public to save votes forever and avoid duplicate voting. Their examination of confidentiality and safety demonstrates that the suggested system offers voter identification and is safe against vulnerability management threats. In this suggested approach, the findings of the research study and cell phone modeling demonstrate the viability of the suggested strategy for large-scale elections. Li et al. [59] aimed for a system that meets all the security criteria, maximum voting secrecy, conflict-free, and fair voting system. This work examines the processing time and assesses the running expenditure of every method on the blockchain platform by simulating them on a computer, Raspberry Pi, and a smartphone. The outcome of this experiment shows how useful it is.

Panja et al. [60] presented security evidence to demonstrate that their proposed system gives the highest level of ballot data secrecy. They put their concept into practice by leveraging Ethereum blockchain as an open forum to register election processes as openly auditable transactions. The testing results and their studies demonstrate the protocol's capability to be used in real-life applications. Zaghloul et al. [61] presented a comprehensive assessment and study of the main difficulties, possibilities, confidentiality, and safety concerns relating to Cryptocurrency and blockchain-based technology. Their discussion on confidentiality and security characteristics concludes with a summary of the most recent technological developments. Their findings could help miners create effective tactics for engaging in mining and maximizing income. Gao et al. [62] presented the results of their tests that demonstrate the effectiveness of the suggested MASE-based classification and method in achieving the best possible exchange between computing performance and interactions. The result of this escapes the FHE-based paradigm's inefficiencies. Table 2 summarizes the literature survey of the abovementioned papers.

5 Conclusion

In this chapter, the importance and advantages of an e-voting platform based on blockchain are highlighted. This chapter uses blockchain technology to present a systematic analysis that compiles the most recent e-voting research. The concept of blockchain and its characteristics and working are presented prior to details on existing electronic voting techniques. Following this, a number of flaws in the current electronic voting architecture, opportunities presented by the blockchain framework to enhance electronic voting, and existing e-voting system solutions integrated with blockchain are noted and explored.

The blockchain can serve as an appropriate arrangement for decentralized electronic voting, according to many researchers. Moreover, all electors and outside spectators can view the electoral records stored in the above-proposed systems. This chapter focuses on the five major features and different consensus algorithms of blockchain that make this technology highly suitable to be incorporated in

Table 2 A brief summary of literature survey

References	Year	Contribution
Habib et al. [44]	2021	Highlighted the applications of an electronic voting platform using Ethereum technology and smart contract technology
Zhang et al. [45]	2019	Proposed a message authentication and transmission system that verifies authority while hiding the identity
Sayyad et al. [46]	2019	Explained the working of a decentralized network and recording transaction history on the decentralized network
Mohammedali et al. [47]	2019	Presented a framework with an administrator verifying the outcome of stored data
Rezvani et al. [48]	2019	Proposed a security policy of confidentiality, integrity, and availability
Sukheja et al. [49]	2019	Pointed out the possibility of data manipulation without any authorization
Rathee et al. [50]	2021	Discussed the challenges in establishing a trustworthy channel of communication
Benabdallah et al. [51]	2022	Presented the ability to eliminate TTP and provide transparent and secure data
Li et al. [52]	2021	Proposed the protocols of e-voting which allows multiple options
Gao et al. [53]	2019	Discussed a mechanism that offers a transparent process of blockchain-based e-voting
Farooq et al. [54]	2022	Presented an adaptive framework that can be used for e-voting purposes
Shahzad et al. [55]	2019	Proposed the use of hashing algorithms, construction, and sealing of blocks
Huang et al. [56]	2022	Demonstrated the use of proof of knowledge for better security and efficiency
Tran et al. [57]	2021	Discussed the possibility of applications of smart contract systems and e-voting
Zaghloul et al. [58]	2021	Presented an idea that is safe and protects voters' anonymity
Li et al. [59]	2022	Proposed a system that meets all the security criteria, including maximum voting secrecy
Pania et al. [60]	2020	Presented evidence that their system gives the highest level of ballot data secrecy
Zaghloul et al. [61]	2020	Examined all the difficulties, possibilities, confidentiality, and safety concerns
Gao et al. [62]	2022	Demonstrated the effectiveness of MASE-based classification in achieving the best computing performance and interaction

e-voting systems making them completely immutable, secure, highly persistent, and maintaining user anonymity.

A decentralized voting system using blockchain could be the future of electronic voting. This framework would be capable of overcoming most of the significant flaws of the conventional electoral systems. Although blockchain technology holds out a lot of promise, its existing limitations may prevent it from realizing its full

potential. Research on the fundamentals of blockchain technology needs to be intensified in order to enhance its features and support for complicated apps that can operate on the blockchain architecture.

References

1. Cetinkaya, O., & Cetinkaya, D. (2007). Verification and validation issues in electronic voting. *Electronic Journal of e-Government, 5*(2).
2. Idrees, S. M., Aijaz, I., Jameel, R., & Nowostawski, M. (2021). Exploring the blockchain technology: Issues, applications and research potential. *International Journal of Online & Biomedical Engineering, 17*(7).
3. Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. *Symmetry, 12*(8), 1328.
4. Bhushan, B., Sinha, P., Sagayam, K. M., & J, A. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering, 90*, 106897. https://doi.org/10.1016/j.compeleceng.2020.106897
5. Goyal, S., Sharma, N., Kaushik, I., & Bhushan, B. (2021). Blockchain as a solution for security attacks in named data networking of things. *Security and Privacy Issues in IoT Devices and Sensor Networks*, 211–243. https://doi.org/10.1016/b978-0-12-821255-4.00010-9
6. Staff, E. (2016). Blockchains: The great chain of being sure about things. *The Economist, 18*(7).
7. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
8. Haque, A. K. M. B., Bhushan, B., Hasan, M., & Zihad, M. M. (2022). Revolutionizing the industrial internet of things using blockchain: An unified approach. In V. E. Balas, V. K. Solanki, & R. Kumar (Eds.), *Recent advances in internet of things and machine learning. Intelligent systems reference library* (Vol. 215). Springer. https://doi.org/10.1007/978-3-030-90119-6_5
9. Saxena, S., Bhushan, B., & Ahad, M. A. (2021). Blockchain based solutions to secure Iot: Background, integration trends and a way forward. *Journal of Network and Computer Applications*, 103050. https://doi.org/10.1016/j.jnca.2021.103050
10. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375.
11. Bheemaiah, K. (2015). Block chain 2.0: The renaissance of money. *Wired*. Wired.com. Accessed 10 Apr.
12. Karame, G. O., Androulaki, E., & Capkun, S. (2012). Two bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin. *Cryptology EPrint Archive*.
13. Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access, 7*, 117134–117151.
14. Kroll, J. A., Davey, I. C., & Felten, E. W. (2013, June). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS* (Vol. 2013, No. 11).
15. del Castillo, M. (2017). *Chain is now working on six 'Citi-Sized' blockchain networks*.
16. Karame, G. O., & Androulaki, E. (2016). *Bitcoin and blockchain security*. Artech House.
17. Yuan, Y., & Wang, F. Y. (2018). Blockchain and cryptocurrencies: Model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48*(9), 1421–1428.
18. Soni, D. K., Sharma, H., Bhushan, B., Sharma, N., & Kaushik, I. (2020). Security issues & seclusion in bitcoin system. In *2020 IEEE 9th international conference on communication systems and network technologies (CSNT)*. https://doi.org/10.1109/csnt48778.2020.9115744

19. https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm. Accessed on 24 Sept 2022.
20. https://data-flair.training/blogs/features-of-blockchain/. Accessed on 26 Sept 2022.
21. Yu, H., Yang, Z., & Sinnott, R. O. (2018). Decentralized big data auditing for smart city environments leveraging blockchain technology. *IEEE Access, 7*, 6288–6296.
22. Shrier, D., Wu, W., & Pentland, A. (2016). Blockchain & infrastructure (identity, data security). *Massachusetts Institute of Technology-Connection Science, 1*(3), 1–19.
23. Wang, Q., Li, X., & Yu, Y. (2017). Anonymity for bitcoin from secure escrow address. *IEEE Access, 6*, 12336–12341.
24. https://data-flair.training/blogs/types-of-blockchain/. Accessed on 7 Nov 2022.
25. Bhushan, B., Sahoo, C., Sinha, P., & Khamparia, A. (2020). Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions. *Wireless Networks*. https://doi.org/10.1007/s11276-020-02445-6
26. Bansal, N., Singhal, M., Rastogi, M., & Arora, L. (2021). Understanding and analyzing consensus algorithms for blockchain. *NVEO-Natural Volatiles & Essential Oils Journal | NVEO*, 1794–1812.
27. Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT Express, 6*(2), 93–97.
28. Xiao, Y., Zhang, N., Li, J., Lou, W., & Hou, Y. T. (2019). Distributed consensus protocols and algorithms. *Blockchain for Distributed Systems Security, 25*, 40.
29. Kaur, S., Chaturvedi, S., Sharma, A., & Kar, J. (2021). A research survey on applications of consensus protocols in blockchain. *Security and Communication Networks, 2021*.
30. Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017, January). Survey of consensus protocols on blockchain applications. In *2017 4th international conference on advanced computing and communication systems (ICACCS)* (pp. 1–5). IEEE.
31. https://101blockchains.com/what-is-consensus-algorithm/. Accessed on 12 Nov 2022.
32. https://en.wikipedia.org/wiki/Electronic_voting_in_India#:~:text=EVMs%20are%20easier%20to%20transport,easier%20than%20ballot%20paper%20system. Accessed on 18 Nov 2022.
33. Jardí-Cedó, R., Pujol-Ahulló, J., Castella-Roca, J., & Viejo, A. (2012). Study on poll-site voting and verification systems. *Computers & Security, 31*(8), 989–1010.
34. Sharma, R., Gupta, D., Maseleno, A., & Peng, S.-L. (2022). Introduction to the special issue on big data analytics with internet of things-oriented infrastructures for future smart cities. *Expert Systems, 39*, e12969. https://doi.org/10.1111/exsy.12969
35. Sharma, R., Gavalas, D., & Peng, S.-L. (2022). Smart and future applications of internet of multimedia things (IoMT) using big data analytics. *Sensors, 22*, 4146. https://doi.org/10.3390/s22114146
36. Sharma, R., & Arya, R. (2022). Security threats and measures in the internet of things for smart city infrastructure: A state of art. *Transactions on Emerging Telecommunications Technologies*, e4571. https://doi.org/10.1002/ett.4571
37. Zheng, J., Wu, Z., Sharma, R., & Lv, H. (2022). Adaptive decision model of product team organization pattern for extracting new energy from agricultural waste, 102352. *Sustainable Energy Technologies and Assessments, 53*(Part A). https://doi.org/10.1016/j.seta.2022.102352. ISSN 2213-1388.
38. Mou, J., Gao, K., Duan, P., Li, J., Garg, A., & Sharma, R. (2022). A machine learning approach for energy-efficient intelligent transportation scheduling problem in a real-world dynamic circumstances. *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2022.3183215
39. Priyadarshini, I., Sharma, R., Bhatt, D., et al. (2022). Human activity recognition in cyber-physical systems using optimized machine learning techniques. *Cluster Computing*. https://doi.org/10.1007/s10586-022-03662-8

40. Priyadarshini, I., Alkhayyat, A., Obaid, A. J., & Sharma, R. (2022). Water pollution reduction for sustainable urban development using machine learning techniques. *Cities, 130*, 103970., ISSN 0264-2751. https://doi.org/10.1016/j.cities.2022.103970
41. Pandya, S., Gadekallu, T. R., Maddikunta, P. K. R., & Sharma, R. (2022). A study of the impacts of air pollution on the agricultural community and yield crops (Indian context). *Sustainability, 14*, 13098. https://doi.org/10.3390/su142013098
42. Bhola, B., Kumar, R., Rani, P., Sharma, R., Mohammed, M. A., Yadav, K., Alotaibi, S. D., & Alkwai, L. M. (2022). Quality-enabled decentralized dynamic IoT platform with scalable resources integration. *IET Communications, 00*, 1–10. https://doi.org/10.1049/cmu2.12514
43. Deepanshi, I. B., Garg, D., Kumar, N., & Sharma, R. (2022). A comprehensive review on variants of SARS-CoVs-2: Challenges, solutions and open issues. *Computer Communications*. https://doi.org/10.1016/j.comcom.2022.10.013. ISSN 0140-3664.
44. Ahasan Habib, A. K. M., Hasan, M. K., Islam, S., Sharma, R., Hassan, R., Nafi, N., Yadav, K., & Alotaibi, S. D. (2022). Energy-efficient system and charge balancing topology for electric vehicle application. *Sustainable Energy Technologies and Assessments, 53*(Part B), 102516. https://doi.org/10.1016/j.seta.2022.102516. ISSN 2213-1388.
45. Zhang, Q., Xu, B., Jing, H., & Zheng, Z. (2019). Ques-chain: An ethereum based e-voting system. *arXiv preprint arXiv:1905.05041*.
46. Sayyad, S. F., Pawar, M., Patil, A., Pathare, V., Poduval, P., Sayyad, S., et al. (2019). Features of blockchain voting: A survey. *International Journal, 5*, 12–14.
47. Mohammedali, N., & Al-Sherbaz, A. (2019). Election system based on Blockchain technology. *International Journal of Computer Science and Information Technology (IJCSIT), 11*(5), 13–31.
48. Rezvani, M., & Khani, H. (2019). E-voting over blockchain platforms: A survey. *Journal of Network Security and Data Mining, 2*(3), 1–14.
49. Sukheja, D., Indira, L., Sharma, P., & Chirgaiya, S. (2019). Blockchain technology: A comprehensive survey. *Journal of Advanced Research in Dynamical and Control Systems, 11*(9), 1187–1203.
50. Rathee, G., Iqbal, R., Waqar, O., & Bashir, A. K. (2021). On the design and implementation of a blockchain enabled e-voting application within IoT-oriented smart cities. *IEEE Access, 9*, 34165–34176.
51. Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for E-voting: A systematic literature review. *IEEE Access*.
52. Li, H., Li, Y., Yu, Y., Wang, B., & Chen, K. (2020). A blockchain-based traceable self-tallying E-voting protocol in AI era. *IEEE Transactions on Network Science and Engineering, 8*(2), 1019–1032.
53. Gao, S., Zheng, D., Guo, R., Jing, C., & Hu, C. (2019). An anti-quantum e-voting protocol in blockchain with audit function. *IEEE Access, 7*, 115304–115316.
54. Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022). A framework to make voting system transparent using blockchain technology. *IEEE Access, 10*, 59959–59969.
55. Shahzad, B., & Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access, 7*, 24477–24488.
56. Huang, J., He, D., Chen, Y., Khan, M. K., & Luo, M. (2022). A blockchain-based self-tallying voting protocol with maximum voter privacy. *IEEE Transactions on Network Science and Engineering, 9*(5), 3808–3820.
57. Tran, Q. N., Turnbull, B. P., Wu, H. T., De Silva, A. J. S., Kormusheva, K., & Hu, J. (2021). A survey on privacy-preserving blockchain systems (PPBS) and a novel PPBS-based framework for smart agriculture. *IEEE Open Journal of the Computer Society, 2*, 72–84.
58. Zaghloul, E., Li, T., & Ren, J. (2021). d-BAME: Distributed blockchain-based anonymous mobile electronic voting. *IEEE Internet of Things Journal, 8*(22), 16585–16597.
59. Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M. (2020). A blockchain-based self-tallying voting protocol in decentralized IoT. *IEEE Transactions on Dependable and Secure Computing, 19*(1), 119–130.

60. Panja, S., Bag, S., Hao, F., & Roy, B. (2020). A smart contract system for decentralized borda count voting. *IEEE Transactions on Engineering Management, 67*(4), 1323–1339.
61. Zaghloul, E., Li, T., Mutka, M. W., & Ren, J. (2020). Bitcoin and blockchain: Security and privacy. *IEEE Internet of Things Journal, 7*(10), 10288–10313.
62. Gao, C., Li, J., Xia, S., Choo, K. K. R., Lou, W., & Dong, C. (2020). Mas-encryption and its applications in privacy-preserving classifiers. *IEEE Transactions on Knowledge and Data Engineering, 34*(5), 2306–2323.