ISSN: 0067-2904

Review Study of E-Voting System Based on Smart Contracts Using Blockchain Technology

Maral Hassan Jumaa[1]*, Ahmed Chalak Shakir[2]
[1]*Department of Computer Science, College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq.*
[2]*Department of Network, College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq*

Received: 7/2/2022 Accepted: 16/7/2022 Published: 30/4/2023

Abstract:
Voting is an important procedure in democratic societies in different countries, including Iraq. Electronic voting (E-voting) is becoming more prevalent due to reducing administrative costs and burdens. E-voting systems have many restrictions that affect the electoral process. For example, fraud, tampering with ballot boxes, taking many hours to announce results, and the difficulty of reaching polling stations. Over the last decade, blockchain and smart contract technologies have gained widespread adoption in various sectors, such as cryptocurrencies, finance, banking, and most notably in e-voting systems. If utilized properly, the developer demonstrates properties that are promising for their properties, such as security, privacy, transparency, and decentralization. Moreover, these technologies allow citizens to vote wherever they are via digital technology (computers, smartphones). This paper explains the nature of blockchain and smart contracts and systematically reviews several important e-voting studies. Comparative analysis is conducted on recent related papers in the last five years (published in highly ranked journals and international conferences) regarding blockchain types, frameworks, security requirements, and the implemented algorithms.

Keywords: Blockchain, Smart Contract, E-Voting, Ethereum, Merkle Tree.

دراسة مراجعة في نظام التصويت الإلكتروني القائم على العقد الذكي باستخدام تقنية البلوكجين

مرال حسن جمعه[1]*، أحمد جالاك شاكر[2]
[1]قسم الحاسوب، كلية علوم الحاسوب وتكنلوجيا المعلومات، جامعة كركوك، كركوك، العراق.
[2]قسم الشبكات، كلية علوم الحاسوب وتكنلوجيا المعلومات، جامعة كركوك، كركوك، العراق.

الخلاصة
يعتبر التصويت إجراءاً مهماً في مختلف البلدان التي تؤمن بمفهوم الديمقراطية ومنها العراق. حيث أصبح التصويت الالكتروني أكثر إنتشاراً من نظيره بسبب تقليل التكاليف والاعباء الإدارية. الانظمة الانتخابية

*Email: stcha018@uokirkuk.edu.iq

المتعارف عليها الان لها العديد من القيود التي تؤثر على العملية الانتخابية منها: التزوير، التلاعب بصناديق الاقتراع، صعوبة الوصول الى مراكز الاقتراع في المناطق النائية، وتأخير إعلان النتائج بعد التصويت. في الاونة الاخيرة إكتسبت تقنيات البلوكجين والعقود الذكية إعتماداً واسع النطاق في مختلف القطاعات مثل العملات الالكترونية المشفرة، التمويل، الخدمات المصرفية، وعلى وجه الخصوص إنظمة التصويت الالكتروني. عند برمجة منصة البلوكجين بطريقة صحيحة سوف يجعل نظام التصويت الالكتروني يتمتع بخصائص الامان، الخصوصية، الشفافية واللامركزية. بإضافة الى ذلك تسمح هذه التقنية للمواطنين بإجراء التصويت اينما كانوا عبر الاجهزة الرقمية (الهواتف الذكية). في هذه الورقة تم شرح طبيعة البلوكجين والعقود الذكية وتم دراسة العديد من الابحاث الخاصة بالتصويت الالكتروني ومن ثم تم إجراء المقارنة بين هذه الابحاث ذات الصلة وتحليل البيانات من حيث هيكلية العمل، الخوارزميات المطبقة، المنصات المستعملة ومتطلبات الامان التي يجب تحقيقه في نظام التصويت الالكتروني.

1. Introduction

Blockchain is considered the next generation of the internet (great innovation), as it is reshaping the way we live and work [1]. In the past decade, blockchain technology has become a mainstream research topic due to the technique of record-keeping and validating documents that are distributed transparently among the users of a specific network [2]. The blockchain ledger is a transaction with a list of chain blocks as illustrated in Figure 1.

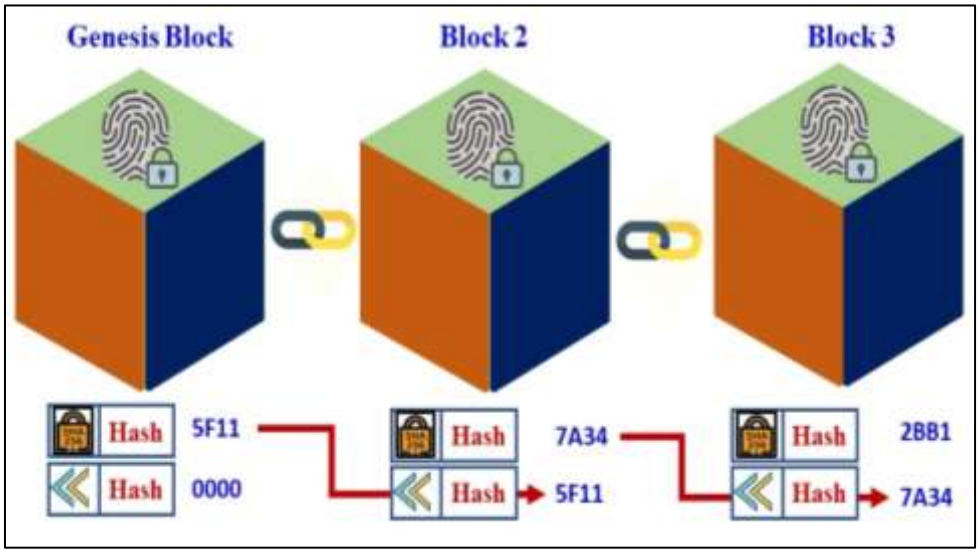

Figure 1: Blockchain Technology [3]

The blocks are linked together by the hash in sequential order of the previous blocks. This ensures the security and integrity of its data from any penetration, side by side of the cryptographic process [4]. Each node in the network receives a copy of all valid transactions made on the network [5]. Blockchain technology was introduced as a support for the trust needed between transactions in electronic information systems. The data in the blockchain is immutable in a secure and encrypted manner, ensuring that it is not altered or tampered with by hackers and vandals [6]. The blockchain technology contains miners that adhere to the consensus protocol to choose which miner will be able to add the next block [5]. It is defined as a new model of decentralized computing for enabling smart contracts. A smart contract is an assortment of codes that build on the properties of blockchain technology, which are self-verifying, self-executing, and tinker-resistant. Smart contracts with the integration of blockchain technology can perform a task in real-time with less cost and supply a better degree of safety [7]. Smart contracts could be implemented on distributed ledger platforms

such as Ethereum, Hyper-ledger Fabric, AxCore, Corda, and Digital Asset Platform [8]. Blockchain-based smart contracts can transform the working architecture of almost all industries towards high service standards because it has many benefits, as illustrated in Figure 2.

Figure 2: Smart contract benefit [9]

The widespread use of blockchain technology in various fields has been represented in the results of scientific research and real-life: real estate [6], healthcare supply chain [5], vaccine supply management of COVID-19 [10], distribution and delivery of COVID-19 vaccines [11], Internet of things [12], online examination [13], e-vehicle power trading mechanism [14], enhancing vendor managed inventory supply chain operations [15], and e-voting [16].

An effective e-voting system must balance critical elements. Security and privacy concerns are clearly among the most important considerations if malicious actors are to be prevented from being able to influence outcomes and protect election integrity. This study can make a valuable contribution because it clarifies the most important requirements for a fair e-voting system (see Figure 3), which guarantees the human rights of the citizens and guides them to the appropriate choice.

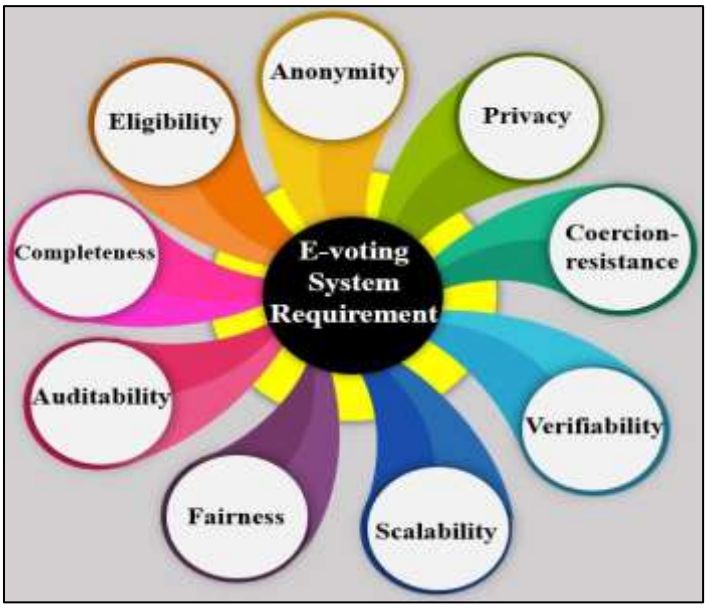

Figure 3: E-voting system's requirement [17]

In this paper, various aspects of e-voting systems using smart contracts based on the blockchain in prior studies were reviewed. The remainder of this paper is organized as follows: Section II provides a background of the blockchain smart contracts and e-voting. Section III is a review of previous electronic voting systems. Section IV presents a comparison between the e-voting systems used in previous studies, the security requirements they achieved, and the algorithms they used. In section V, the conclusion will be introduced.

2. Background

2.1 Blockchain

The concept of blockchain was first developed in 2008 by a researcher who implemented it on the digital currency bitcoin. Blockchain technology is known as the foundation of cryptocurrencies, such as the bitcoin system. Bitcoin is considered to be the initial cryptocurrency system that was presented, and it's presently the most important cryptocurrency in terms of capitalization [2]. Since then, a bundle of cryptocurrencies with far more complex features has emerged, like Ethereum, which includes smart contracts. Blockchain was renowned for being a decentralized peer-to-peer network (P2P), it is the aim of using blockchain is to eliminate centralized control and middleman from procedure [18]. This is achieved by adopting an incorruptible, unchangeable, and decentralized public record. The blockchain eliminates the need for any central authority amongst numerous parties conducting financial and administrative transactions [1], which is a digital platform for digital properties. It contains a continuously increasing list of records, called blocks, that are connected and secured using cryptography. The major usage of blockchain has been in cryptocurrency transactions. However, they are increasingly being used in several other applications due to their inherent resistance to the alteration of the whole distributed ledger [19].

On the other hand, a blockchain is a distributed database or a public ledger of all transactions or digital events that happened as well as shared among participating parties linked inside transactions [20]. It's a secure and irreversible encrypted record of all transactions. Once the data has been confirmed and added to the blockchain, it cannot be erased or amended, making the blockchain unchangeable. Without any affirmation or verification by a central authority, each transaction is confirmed by the participants using pre-

defined validation and consensus processes. Figure 4 shows the characteristics of the blockchain.

Figure 4: Blockchain Characteristics [1]

The ledger copies are synchronized among all participants. This does not only lower the cost but also removes the risk of information loss due to a single point of failure [1]. In the subsections below, the basic components of blockchain networks will be described as illustrated in Figure 5:

- **Peer-to-Peer Network (P2P):** This term is frequently used to describe how blockchain works. This means that transferring the values or the assets on blockchain networks is enabled without the requirement for a trusted third party. The blockchain is spread out across a broad network due to the presence of the P2P network [21].
- **Transactions**: Are defined as the exchange of value between two or more people. A blockchain transaction is a specific sort of transaction that is recorded on the blockchain. A private key and a public key are used with the SHA-256 algorithm to improve transaction security [22].
- **Hashing**: In blockchain, Hashing refers to the transformation of a string of a fixed size of input data of any length that is carried out by a particular algorithm. For example, this algorithm is 256 bits of SHA-256. The implementation of a cryptographic hash function is useful in preventing fraudulent transactions, double blockchain spending, and storing passwords. To put it in context, its hash would also change automatically when there is a change in a hashed file. And each subsequent hash is bound to the previous hash, thereby ensuring that all blocks are consistent [23].
- **Mining:** The new block in the blockchain system is formed by a process known as mining, which lends legitimacy to the transactions by adding them to the former block. When mining, nodes examine past transactions to determine if a subject is authorized to spend a specific amount of bitcoin and, each time a block must be added to the chain, solve a complex and computationally intensive mathematical puzzle. This issue was created particularly to minimize the ability of a malevolent actor to influence the blockchain by fabricating transactions. Attacks are exceedingly unlikely to add a new (malicious) block or modify previously added transactions to the blockchain because they would need to control the majority of nodes in the network [24].
- **Consensus Mechanisms**: The hash will change if someone attempts to modify the block. This leads to the following: all following blocks will be invalid because they have a hash that differs from the freshly produced hash. To address such an issue, there is a piece of the

process known as "proof of work" (PoW) that inhibits the creation of new blocks. This goal is achieved by choosing a difficult encryption challenge for the two metals to be solved. Blockchains can utilize a variety of consensus algorithms, including proof of stake (PoS), which is based on the idea that only those with assets in the system can join in the consensus mechanism to grow the blockchain [25].

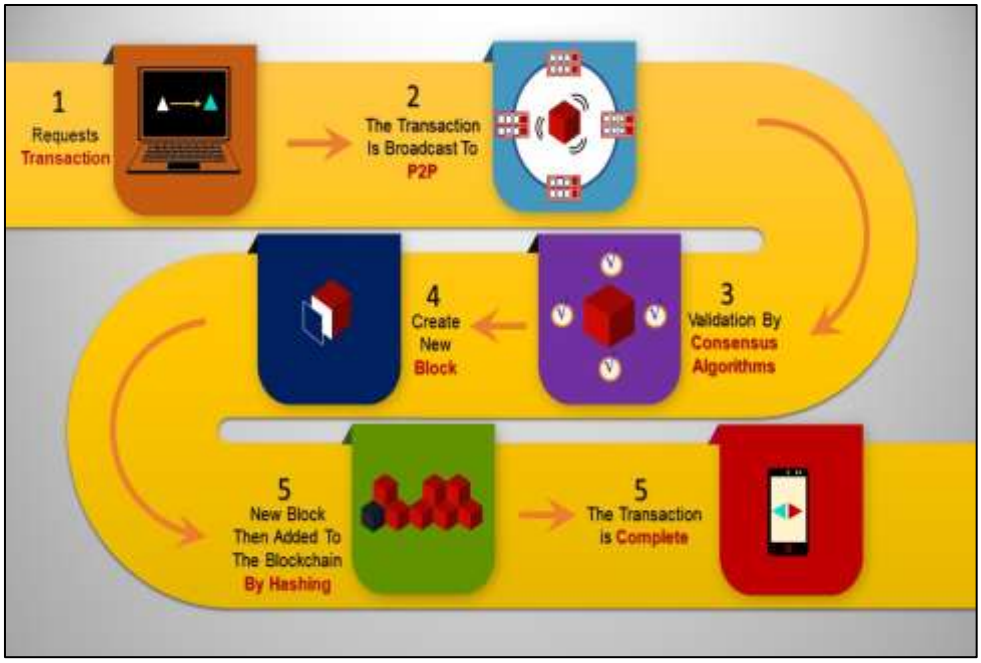

Figure 5: How Blockchain Works? [26]

- **Merkle Tree (binary tree):** Is a key component of blockchain technology. Since the blockchain is a distributed network, a safe and fast algorithm is required to ensure that all nodes have the same ledger and to verify data integrity. Fundamentally, within each block, there is data. This data creates a Merkle tree that has a hash function at the root. A Merkel tree is usually a binary tree. As a result, any fabrication of the transactions will result in a new hash value in the top layer, which leads to a faked root hash. Therefore, any forgery is quickly spotted. Figure 6 shows a simple, commonly used structure to comprehend Merkle Tree [27].

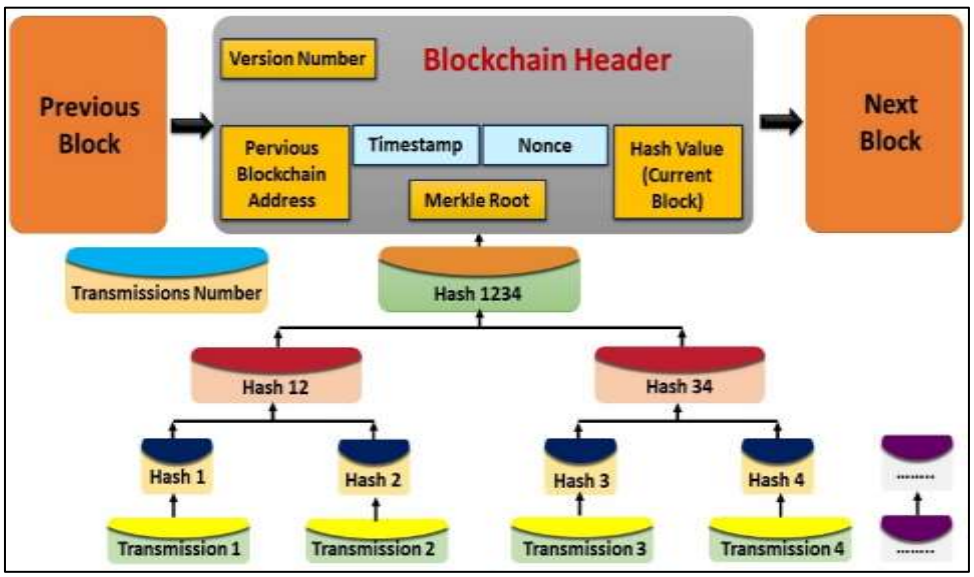

Figure 6: Blockchain Body and Merkle Tree [28]

2.2 Smart Contract

In 1994, Nick Szabo came up with the idea of using computer protocols to support the execution of contracts over computer networks. He wrote in a blog article: "The contract is the conventional approach to establishing a partnership". Smart contracts are a collection of commitments agreed upon at a "meeting of the minds" to formalize and safeguard connections across public networks. Smart contracts integrate protocols, user interfaces, and commitments stated via those interfaces. It decreases transaction costs imposed by principals, third parties, or their instruments in terms of both mental and computer processing [29]. With smart contracts, no middleman will be needed. Smart contracts are becoming enabled by blockchain, which is fundamentally built on blockchains. The accepted contractual provisions are transformed into computer programs that may be executed. The logical relationships between contractual provisions have also been kept in programs as logical flows (e.g., if-else-if statements) [30]. The scope of smart contracts is broad: First, this technology can be used for anything, such as breaching contracts, credit enforcement, or insurance premiums. Secondly, it can be used in financial and banking services, such as payments, settlements, and mortgages. Other potential use cases include applications that have predictions and guarantees, such as spending money if certain conditions are met. In addition, it can be used for insurance and real estate claims, in elections and vote counting, property law, and many more facilitating procedures and no longer requires an intermediary [31], as shown in Figure 7.

Figure 7: Smart Contract Use Case [31]

2.3 E-Voting

Currently, voting is viewed as a necessary democratic activity in life. It has been separated into two groups throughout time: conventional voting and e-voting [32]. Conventional current voting systems are slow due to the complicated process of ballot results that must be collected first from different areas and then calculated by a single central institution. The results collected from such a process are not verifiable. Voters have no way of assuring that their votes are included in the results or not.

Since the 1960s, voting systems have been first utilized in the form of punched cards. They were originally widely used in the United States [33]. Internet voting systems have increased in popularity with elections and referendums performed in the United Kingdom, Estonia, and Switzerland, as well as elections in Canada and party primary elections in the United States and France. E-voting is becoming widely popular around the world. The United States, Brazil, Australia, Canada, Germany, France, the European Union, Switzerland, Italy, and Norway are among the nations that utilize e-voting and voting over the internet. Voting machines were developed for the first time in the mid-nineteenth century [34]. This expansion in e-voting methods, often known as e-voting, has many more advantages than traditional voting systems [35].

In 1981, Chaum [36] proposed the e-voting system, which removes these problems. As a result, numerous e-voting solutions continued to emerge. Cloud and blockchain technologies have recently been widely employed in e-voting to create safe e-voting. Shankar et al. [37] presented a secure e-voting protocol for cloud technology, which successfully enables safe data transfer. Certain blockchain-related e-voting research is progressively increasing, such as decreasing voter fraud and reducing ballot content threats.

Despite this, the greatest challenge of e-voting is to broaden and deepen constitutional democracy while also reinforcing processes aimed at empowering citizens. Any election includes many phases, each of which has its own set of risks. These risks can include spoofing votes and voters, denial of service attacks, voting phishing sites, fraud, intercepting votes, and attacks on data centers. As a result, it is essential for government agencies and security professionals to collaborate to develop regulations and security standards that will be applied in the future [38], as shown in Figure 8.

Figure 8: Challenges of E-voting [38]

Blockchain has become an e-voting solution. Therefore, the voter needs to enter his/her credentials to vote in an e-voting system based on Blockchain technology. All data is then encrypted and stored as a transaction. This transaction is then broadcast to every node in the network and verified. If the network approves a transaction, it is stored in a block and added to the chain. Note that once a block is added to the chain, it stays there forever and can not be altered [10], as shown in Figure 9.

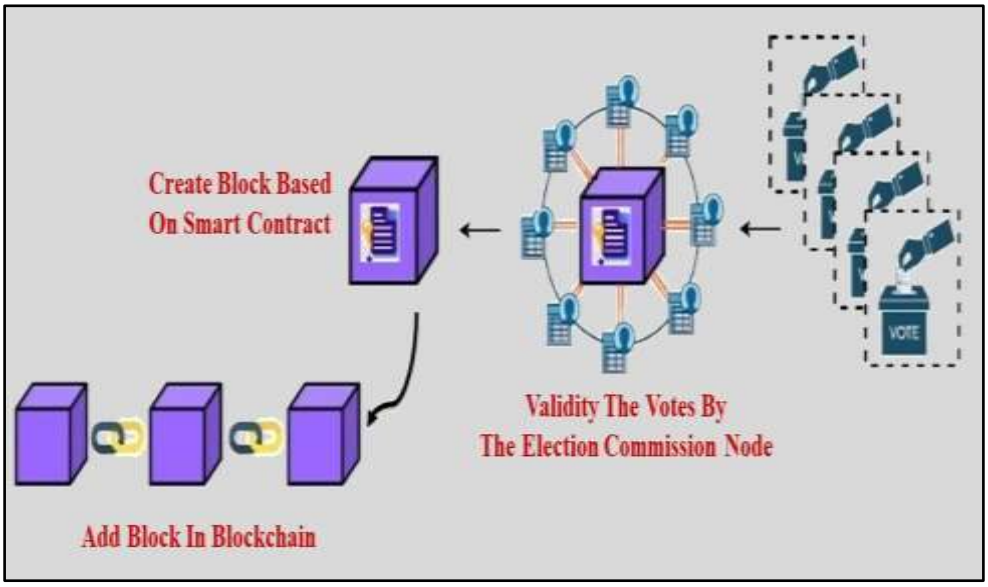

Figure 9: added vote in blockchain

3. Literature Survey

3.1 public blockchain

- Hsiao et al. [39] offered a decentralized e-voting system. The fundamental concept is to use blockchain technology in conjunction with a secret sharing system and homomorphic encryption to create a decentralized e-voting application that does not rely on a trusted third party. This approach utilizes the transparency of smart contracts to enable every voter to contribute to both castings and verify their ballots. It boosts voter trust while reducing voting wastage of resources and ensures a public and transparent voting process while safeguarding voter confidentiality, data transmission privacy, and ballot verifiability throughout the billing phase. To preserve privacy, the initial phase used RSA and the oblivious transport protocol. Fairness is the main problem in this scheme.
- Wei-Jr Lai et al. [40], a decentralized anonymous transparent e-voting system (DATE) with a low level of trust between participants was proposed. They also employ (Proof of Work) consensus, which has substantial limitations like power consumption: miners' "supercomputers" check a thousand operations per second, which occurs globally. This design necessitates a large amount of processing power, making it both costly and energy-intensive. It is believed that the existing DATE voting mechanism is appropriate for large-scale electronic elections. Unfortunately, because there was no third-party authority on the scheme accountable for auditing the vote after the election process, their suggested method is not powerful enough to withstand the (Denial of Service) attack. Due to the limitations of the platform, only small scale is used as a solution.
- Patidar et al. [18] presented an e-voting system supported by blockchain that removes a number of the issues in existing voting systems. It is convenient for small-scale elections and uses the Truffle framework for development, testing, and deploying good contracts. Ganache is employed as an Ethereum client for testing. The Meta-mask is used as a browser wallet and provides additional security and integrity used to connect with the Ethereum nodes. The aim behind Ethereum would be to make it easy for designers to create a platform, whether that's a public or private network.
- Tso Raylin et al. [41], the first decentralized e-voting system based on a blockchain and smart contracts was introduced. Changing the third party with an Ethereum blockchain-based smart contract is a viable technique for fulfilling the aim of cheaper costs and greater data verifiability, which results in safer and more efficient systems. The system employs

cryptographic approaches like oblivious transfer and homomorphic encryption to strengthen privacy protection, eligibility, non-repeatability, rationality, completeness, fairness, and anonymity. However, coercion is not resisted in this system and is used on a small scale for voting.

- Kazi Sadia et al. [42], a completely decentralized e-voting system is presented using blockchain technology. Smart contracts are used in this protocol to deal with security, accuracy, and voter privacy during the voting process. The protocol produces a method that is transparent, non-editable, and independently verifiable. The procedure eliminates any planned fraudulent acts from occurring throughout the election process by removing the smallest third-party engagement. At the same time, the protocol produces a method that is auditable, the privacy of voters, confidentiality, and anonymity, which are all features of the system.
- Syada Tasmia Alvi et al. [43] integrated digitalization and blockchain technology to create a voting system. This system employs three forms of storage: the database of the Election Commission; Blockchain Storage (a hash value derived from the voter's information will be kept in the genesis block as a list of voters; and each vote will be saved in the chain as a block). Another sort of blockchain is utilized to keep the metadata of the Voting Commission's database and cloud (before and after the election, a copy of the Election Commission's database and vote information will be maintained on the cloud). These voting systems are designed to offer voters integrity, anonymity, privacy, and security. This has all been achieved in our proposed digital voting systems thanks to the employment of the Markle tree and fingerprint hash. Future work will focus on developing an encryption approach to improve the security of our system.
- Vairam T. et al. [44] a voting system was introduced that provided transparency and confidentiality using Blockchain. The design of the election system is organized into four major activities: registration, authentication, voting, and results. The online voting system allows voters to cast their vote from any place at any time, which leads to an increase in the voter participation count. Using Ganache provides 10 accounts with 100 fake ethers which can be used to test the working of the developed application. The Truffle framework is used for deploying smart contracts. JavaScript has used migration for smart contracts as well as a proof of work algorithm for validation. To prevent multiple voting, each voter is granted only one vote, and only qualified voters are allowed to vote after their identification is verified.
- Valentin Sliusar et al. [45] provided a system user that needed to have a mobile-specific address space. The mobile device identification is saved on the Blockchain as a wallet address linked to the user's token. The token's usability for voting will be restricted in time. A vote is cast by sending a marker (token) to a specified candidate’s address. Votes are securely saved on the Blockchain. It offers transparency, anonymity, improving reliability, security, fault-tolerance, increased voter turnout, increased efficiency, and increased processing speed.
- Ehab Zaghloul et al. [46] suggested (d-BAME) a novel remote e-voting model for large-scale elections by offering the participation of two conflicting parties to ensure election integrity and accountability. It can be implemented in IoT devices such as smartphones. It was implemented in two versions. First, a desktop application, which was implemented using a MacBook Air utilizing Meta-Mask2, and a browser plug-in. Second, the smartphone application is iPhone XR, which incorporates the web3 swift library3. AES encryption is also used to encrypt the voter's vote; the El Gamal signature scheme to sign the election ID; and double encrypt the vote.
- Ali Mansour Al-Madani et al. [47] provided a high-security e-voting system by utilizing the Ethereum blockchain in the local network as the decentralized database used for storing voters’ accounts. It provides a decentralized paradigm that makes the network reliable, safe, versatile, and capable of supporting real-time services. Then, for this application, a 180 smart contract was uploaded on the local blockchain. and the application does not allow for

duplicate votes. To create a decentralized application (DAP), the following tools are required: node package management, truffle framework, and Ganache Meta Mask as a wallet.

- Awsan A. H. Othman et al. [48] utilized the Internet of Things (IoT) and Blockchain in their system to safeguard data from theft and prevent eavesdropping or vote manipulation. To preserve the integrity of the voting, the blockchain encrypts votes to secure each vote from forging. Using a smart contract (solidity language). The hardware used in a system (Arduino, ESP8266, Keypad board, Fingerprint sensor, LCD). The software that is required in the system (front end: HTML5, CSS3, JavaScript, and Bootstrap) Back end: (PHP to deal with DB, Node JS, and Web3).
- Wenjun Fan et al. [49] suggested a web application be applied to a blockchain-based electronic-voting system. To guarantee the fairness of e-voting and retrieve people's trust while protecting the voters' privacy to authenticate voters, face detection technology is used, which is applied by using an external webcam after extracting feature sets from images. This system secures voter information during the voting operation designed by a smart contract (Ethereum) coded using solidity. It is used with the OpenCV Haar Cascade detection algorithm of face recognition classifiers for the Implement approach.
- Abhishek Parmar et al. [16] Based on blockchain technology, they proposed a decentralized national e-voting system. It contains an admin panel for scheduling voting, managing candidates, and declaring results. At the time of the election, the web application will offer users an interface to input their Aadhaar card ID and a picture of themselves. When they enter their Aadhaar card, the voter's eligibility can be verified. The mobile numbers of eligible voters will be verified using an OTP. The voters will be monitored using a webcam/front camera during the election operation. Any tampering or misusing of the system will be easily detected because the votes will be stored in a blockchain.
- Vehbi Neziri et al. [50] discussed current Blockchain systems and provided a novel technique for achieving privacy and anonymity by combining two separate Blockchains. The first is for managing keys and the second is for storing voting data. Using Blockchain technology to implement this strategy would dramatically improve the present voting process by ensuring anonymity and privacy. The proposed system will encrypt the nonce and the voter's hash to investigate the anonymity and privacy features of the system.

3.2 Private blockchain

- In a paper by Francesco Fusco et al. [2], a new e-voting method was introduced called Crypto-voting. This solution is based on Shamir's secret sharing approach, which is implemented using permissioned blockchain technology. The suggestion highlights the potential of sidechain technology. Sidechains expand the blockchain and enable the development of new features by eliminating both the requirement to write on the primary blockchain (which reduces costs and failure risks) and the need to establish a new cryptocurrency. The sidechain is built on the ability to build a system that uses both the primary blockchain and a secondary blockchain to be connected depending on certain synchronization standards. The innovative concept of Crypto-voting is based on the use of two connected blockchains, one-way linked sidechain. The first sidechain keeps track of who is qualified to vote and how they vote. The second sidechain totals the votes cast for each contender (result). Smart contracts will be used to manage voting processes and outcomes. The use of a cloud system to identify a virtual voting box leads to the incorporation of cybersecurity and privacy tools. Ensuring voter privacy and anonymity without an intermediary increases traceability and auditing mechanisms for voting processes. This system does not support large companies and is only used in small and medium-sized companies. It didn't provide resistance to coercion and completeness.
- Freya Sheer Hardwick et al. [32] proposed an e-voting scheme based on blockchain technology that meets the basic characteristics of e-voting but at the same time provides some

degree of decentralization and provides voters with the fundamentals of processes. The protocol's single centralization point is the central authority (CA), which is presumed to be trustworthy. However, if the CA violates that confidence in the current configuration, it may cast votes for people who have not voted. This is why all people should exercise their right to vote. Due to the protocol is built on the blockchain, it will be implemented as a peer-to-peer network. Each voter will be considered a peer, or a node in a network of equals. Every voter will be held accountable for ensuring that fraudulent votes are rejected and that consensus is preserved by following the voting rules. To support the control of restrictions as much as possible (blockchains and smart contracts). The proposed protocol meets special characteristics such as eligibility, privacy, fairness, and verifiability. The system allows voters to change or update their votes (within the permitted period).

- Gaby G. Dagher et al. [25] presented a blockchain-based voting system that overcomes security and privacy concerns. For privacy, the new system relies heavily on Ethereum's blockchain, smart contracts, and homomorphic encryption. This is because the system is dealing with smart contracts. It is made up of three smart contracts coded in Ethereum's Solidity language, two JavaScript scripts, and one HTML page. Each component has a distinct function in keeping the process under control and trustworthy. They demonstrated that the new framework is simple to set up and deploy, but it is a university-scale voting system that wasn't used on a large scale and their encryption methods should be improved.
- Michal Pawlak et al. [33] introduced the Auditable Blockchain Voting System (ABVS), which defines the e-voting procedures and components of an auditable and verifiable internet voting system. ABVS does this by combining blockchain technology with a voter-verified paper audit trail. Voter identification tokens (VITs) are alphanumeric symbols that are being used to validate and authorize voters inside the system. The ABVS system's voting procedure is separated into three stages: election preparation, voting, and tallying and verification. To show ballot integrity and vote accuracy, blockchain technology was used to store cast votes and provide comprehensive audit and verification capabilities to voters. It is necessary to have solid capabilities to use this system and link it with the necessary nodes.
- Albin Benny et al. [19] used a blockchain-based e-voting system instead of completely replacing the current electoral system. It was integrated with it. The entire system is separated into two sub-systems: registration and voting. A registration system can be considered as an Aadhar database that would be used for the validation purposes of voters. The voting system can be considered as an E-Voting Machine (EVM). It is a decentralized application built with an interface in Bootstrap or HTML and uses a blockchain in the back-end. It enables safe and cheap elections using smart contracts (private Ethereum) while ensuring the privacy of voters and overcoming restrictions. It allows the sending hundreds of transactions per second to the blockchain.
- Vijayalakshmi V. et al. [52] A web application was developed based on the Ethereum blockchain to keep the voting data secure by encrypting the data and putting it on the blockchain. The concept behind a blockchain-enabled balloting method is to combine individuals' Aadhaar cards and mobile numbers to produce an OTP, which the voter may then use to cast their vote. The user can vote from any location (nearby booth), and the users are alerted to the matching contestants based on their constituency and candidate pledges. If the number of NOTA votes exceeds 50%, all the candidates are disqualified and allowed to run in the following election. If any citizen fails to poll their vote, a warning message will be delivered to that individual. They must present a good explanation for not voting within six months; if the rationale is invalid, the government will take appropriate action. If a citizen wishes to check his or her voting status, they may do so by inputting their Aadhaar number and the block number supplied to them via the mobile application. The installation of this

technique overcomes the majority of the concerns encountered in the balloting scheme, as well as reaching a vote percentage of greater than 95%.

- Abayomi-Zannu et al. [53] proposed a mobile-voting framework that uses blockchain technology. It securely stores cast votes while avoiding any pattern of tampering. It applies multifactor authentication to check eligibility while authorizing voters to cast their votes. It offers an easy, available, secure, and transparent mobile-voting system, thereby increasing voters' trust in the voting process and providing better transparency during the election process. Voters will not be required to leave their homes to vote. Several methods of validation will be employed to allow qualified voters to vote, and the elderly and disabled will benefit. The methods of coding and resisting coercion in voting should be improved, and the voting range should be expanded.
- Sathya V. et al. [54]: a blockchain-based solution was provided that includes a secure data storage technique. It collects the EVM's votes and submits them to the blockchain generator. The blockchain-generator creates blocks of (hashes and data) and ties them to the preceding hash. The hash value is transmitted to the cloud storage service for remote transmission via low-bandwidth internet. The data is received as a Publish-Subscribe pattern by the receiver station and stored in a hash table. The hash of the blocks is checked against the hash table; if there are any inconsistencies, the block is rejected and designated as NOTA. Polling data obtained using cloud-based technologies and blockchain is being used to improve security.
- Jiazhuo Lyu et al. [55] created a smart contract-based decentralized trustless e-voting system. The smart contract on the blockchain is utilized to offer a trustworthy public bulletin board and a trusted computing environment to ensure the accuracy of the vote results. A linkable ring signature is used for each voter to group a signature ring to obscure each voter's identity and avoid duplicate voting. Furthermore, threshold encryption without a trusted third party is used to make a secret key before the tally stage to ensure that all voters see the voting result at the same time or that no one can access it. Moreover, truffle and remix ID have put the smart contract on the Ethereum private network, and the smart contract is responsible for the tallying task. Correctness, robustness, privacy, double voting avoidance, fairness, and verifiability are all features of the protocol alongside avoiding the Dos attack and the Man in the Middle attack. But it is used on a small scale.
- C. H. Roh and Im Yeong Lee [56] proposed an e-voting system that assures dependability by incorporating Hyperledger private blockchain technology into e-voting. It provides secret voting and high integrity in voting. It provides the voter's privacy by using randomly generated keys for every voter. It is offering fairness by encrypting the contents of the ballot. The proposed system provides security by utilizing the PBFT algorithm and offering eligibility by voter list. It also achieves completeness, verifiability, and time savings. However, coercion is not resisted in this system and is used on a small scale for voting.
- Lakshmi Priya k. et al. [57] proposed a blockchain-based system that prevents voters from voting more than once, and votes can be effectively verified by controllers or reviewers at any time and from any location. The process includes decoding data using (symmetric key crypto) and using a Hyperledger private blockchain. It makes use of a calculation that conveys equally swift swaps through an agreement instrument based on the manner of life at stake, which can send many exchanges per second onto the blockchain, providing security and transparency. Some more steps would be expected to aid greater throughput of exchanges per second for nations of greater size.
- F′aber D. Giraldo et al. [58] demonstrated a proof of concept of how Blockchain and other technologies may be used to create an e-voting system for the election of one-of-a-kind candidates. This has been accomplished by specifying an architecture developed specifically for electoral processes. In this suggestion, just the candidate's addresses are utilized to perform token transfers rather than currency. The voter has the option of spending a single

token (vote), which he may then transmit to the candidate's wallet as a token (vote). It provides for voter anonymity because it only contains the voting station with the candidate's vote. A simulation is run to acquire data that is useful when assessing Blockchain technology as a replacement for present voting systems. The final result is a system in which the voter interacts with the candidate and votes for him or her. The voter may keep track of his vote and where he went after the voting session ends, and there is no fraud in this case.

3.3 Consortium blockchain

- Basit Shahzad and Jon Crowcroft [27] the BSJC proof of completion was presented as a very reliable e-voting technique. This research proposes a system for ensuring data security by utilizing effective hashing algorithms. This article introduces the concepts of block formation and block sealing. The implementation of a block sealing idea aids in the adaptation of the blockchain to fit the needs of the election process. It aimed to solve issues of anonymity, privacy, and security in the election. However, several other issues have been raised. Proof of work, for example, is a mathematically large and difficult task that needs a significant amount of energy to perform, and it is used on a small scale. Another issue is the involvement of a third party because there is a considerable possibility of data manipulation, leakage, and unfair tabulated results, all of which may influence end-to-end verification.

3.4 Hybrid blockchain

- Majd Soud et al. [59] provided a blockchain-based e-voting system (TrustVote) that was realized using public (Ethereum) and permissioned (Hyperledger) blockchains to facilitate managing electronic elections and to minimize human errors. It depends on the government's identity identification service to authenticate voters. It created Two Election Creation Smart Contracts (ECSC) and (PSC). The study showed that utilizing private permissioned blockchain for implementing e-voting systems can address many of the challenges and satisfy many of the requirements of e-voting systems. In particular, private and permissioned blockchain solutions have the advantage of better performance in terms of the number and execution time of transactions and adhere better to privacy and governance constraints.
- Praful M. Kukwase et al. [51] evaluated the popular frameworks for supplying blockchain as a service (BaaS) and provided a special e-voting method that considered all the cons of the current frameworks. The system employed smart contracts in all voting operations, including election organization, voter registration, and considered each vote as a smart contract that was then stored in the blockchain.

4. Comparative Analysis of Blockchain-Based E-voting System

Several requirements are mentioned below which must exist in any system, such as classic paper voting, digital voting machines, or online voting systems. The security and privacy requirements are analyzed to meet the goals of a successful e-voting system.

- ✓ **Eligibility**: Means that only legitimate voters should be allowed to vote. Voters must use a recognized registration mechanism to identify themselves. All valid voters' identities must be included in the participants. However, there are dangers: To begin, any changes to the participation list must be reviewed to ensure that no illegal voters are added, and the identification mechanism must be both trustworthy and secure so that a voter's account cannot be stolen or exploited by an intruder [60].
- ✓ **Anonymity**: Means that the turnout of the vote must be protected from outsider interpretation during the polling procedure. There should be no link between recorded votes and voter IDs inside the electoral framework [61].
- ✓ **Privacy:** In the case of online voting, privacy means that no one other than the voter has access to information regarding the voter's choice. Obtaining this attribute is mostly dependent on one (or even more) of the following methods: Homomorphic encryption, blind signatures, and mix-networks are all examples of cryptographic techniques [62].

✓ **Completeness:** This means that invalid ballots should be discovered and not counted while counting. Although the completeness and soundness characteristics appear to be simple, implementing them might be difficult depending on the protocol. When votes are decrypted one at a time, it is simple to discern between valid and incorrect ones, but things grow more difficult when homomorphic encryption is used. As a result, we must demonstrate that the encrypted data satisfies the requirements of a legitimate ballot without jeopardizing any information that may aid in determining how the vote was cast. A zero-knowledge proof is used to complete this assignment [17].

✓ **Fairness:** Means that no one receiving intermediate outcomes is easily achieved: voters encrypt their choices before delivering them, and those choices are decoded after the voting process. The crucial point to remember here is that anyone with a decryption key and access to encrypted choices may receive intermediate results. This issue is handled by sharing the key among many keyholders [63] (for example, Shamir's Secret Sharing technique).

✓ **Auditability:** Known as accuracy, requires that the stated results accurately correspond to the voting results. It means that no one may influence the votes of other voters and that the final total includes all valid votes [42].

✓ **Coercion-resistance:** Means that an election system should prevent coerced voting. Issues related to coercion and vote-buying are exacerbated by online voting. Coercers and vote purchasers can operate on a massive scale since ballots are cast remotely in an unregulated environment. That is why coercion resistance is one of the desirable qualities of an online voting system. Nothing can prevent the coercer from standing behind the voter and directing its actions, which is why it is termed "resistance" [64].

✓ **Scalability:** This means that an e-voting system must be scalable and contain the largest possible number of voters. When the network is used for large-scale elections, the number of users grows, resulting in greater transaction costs and time consumption. The increasing number of nodes in the blockchain network exacerbates scalability issues. The scalability of the system is already a serious concern in the election context [65].

✓ **Verifiability**: Known as implied that methods for election audits exist to guarantee that they are carried out accurately. The terms "universal verification" or "public verification" suggest that anybody, including voters, governments, and external auditors, can test the election once the tally is declared [66].

Blockchain depends on the above requirements to enhance its security and privacy. However, there is still potential for developing their performance by including other requirements in a blockchain-based e-voting system (see Figure 10).

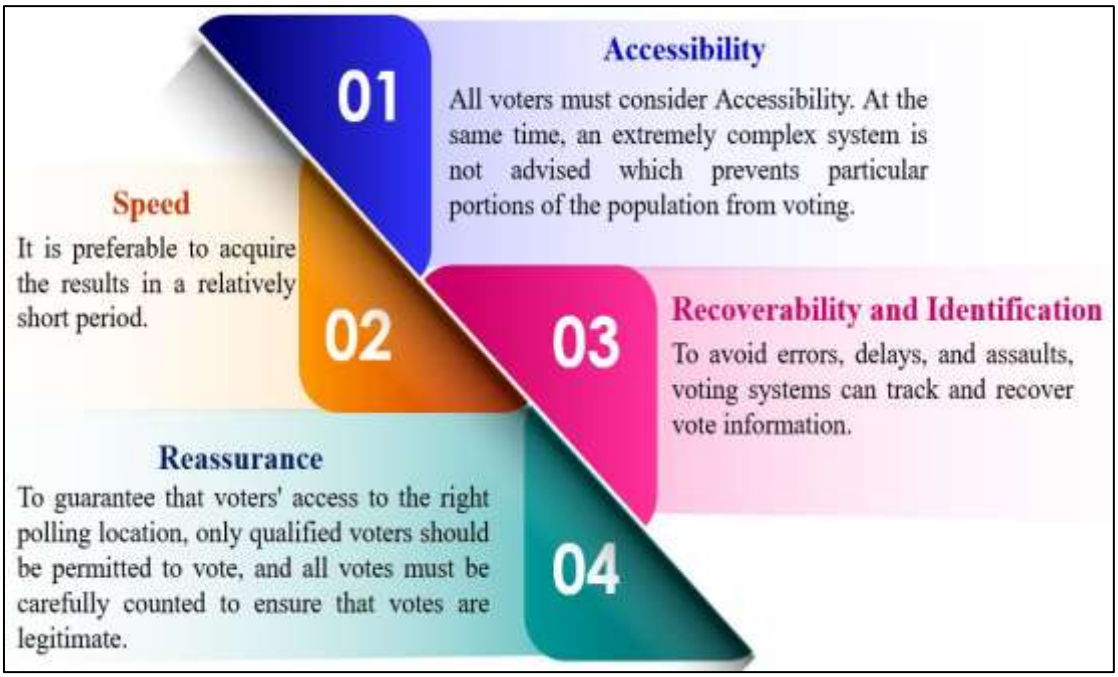

Figure 10: Other requirements for blockchain-based e-voting systems

Over the past few years, many studies have been released, discussing the most important requirements related to blockchain-based e-voting systems. Table 1 shows a comparison between the different references, showing the type of blockchain used, the type of framework used, the algorithms used, and the requirements that must be met in the electoral system.

Table 1: A comparison of e-voting systems based blockchain

Reference	Schema name	Publication year	Block chain Type	Frame work	The algorithm used	Security requirement								
						Eligibility	Anonymity	Privacy	Completeness	Fairness	Auditability	Coercion Resistance	Scalability	Verifiability
[2]	Crypto-voting	2018	Private	sidechain	Shamir's Secret Sharing	✓	✓	✓	×	✓	×	×	×	✓
[32]	E-Voting with Blockchain	2018	Private	Ethereum	Blind signatures & digital commitment	✓	✓	✓	×	✓	✓	✓	×	✓
[39]	Decentralized E-Voting Systems Based on the Blockchain Technology	2018	Public	blockchain	secret-sharing & homomorphic & RSA	✓	✓	✓	×	✓	✓	×	×	✓
[25]	BroncoVote	2018	Private	Ethereum	Paillier homomorphic encryption	✓	✓	✓	×	×	✓	×	✓	×
[40]	DATE voting system	2018	Public	Ethereum	ring signature & elliptic curve	✓	✓	✓	×	×	×	×	×	✓
[33]	ABVS	2018	Private	Blockchain	Vote Identification Token	✓	✓	✓	×	×	✓	×	×	✓

[27]	BSJC	2019	Consortium	Adjusted blockchain	SHA-256 & Merkle Tree	✓	✓	✓	×	×	✓	×	×	×
[18]	Decentralized E-Voting Portal	2019	Public	Ethereum	RSA algorithms	✓	✓	✓	×	×	✓	×	×	✓
[19]	Blockchain-based E-voting	2019	Private	Ethereum	unique hash code	✓	✓	✓	×	×	✓	×	×	✓
[52]	Novel P2P	2019	Private	Ethereum	RSA & AES &OTP	✓	✓	✓	×	✓	×	×	✓	✓
[53]	Mobile Voting	2019	Private	Blockchain	OTP & multi-factor authentication	✓	✓	✓	×	✓	×	×	×	✓
[54]	BC Based Cloud Computing Model on EVM for Secure Voting	2019	Private	Blockchain	UIDAI biometric & SAAS & hash table	✓	✓	✓	×	✓	×	×	×	×
[55]	Secure Decentralized Trustless E-Voting System	2019	Private	Ethereum	ring signature & threshold encrypt	✓	✓	✓	✓	✓	✓	×	×	✓
[41]	Distributed E-voting and E-bidding systems based on smart contract	2019	Public	Blockchain	secret sharing and homomorphic	✓	✓	✓	×	✓	×	×	×	✓
[56]	E-voting System Using Private Blockchain	2020	Private	Hyperledger	PBFT & encryption	✓	✓	✓	✓	✓	✓	×	×	✓
Reference	**Schema name**	**Publication year**	**Block chain Type**	**Frame work**	**The algorithm used**	**Security requirement**								
						Eligibility	**Anonymity**	**Privacy**	**Completeness**	**Fairness**	**Auditability**	**Coercion Resistance**	**Scalability**	**Verifiability**
[57]	Integrated and Robust E-voting App. Using Private Blockchain	2020	Private	Hyperledger	Symmetric key crypto	✓	✓	✓	✓	×	×	×	✓	✓
[42]	BC-Based Secure E-Voting with the Assistance of SC	2020	Public	Ethereum	POW & hashing	✓	✓	✓	×	✓	✓	×	×	✓
[43]	Digital Voting	2020	Public	Ethereum	POW & merkletree& hash	✓	✓	✓	×	×	✓	×	×	✓
[58]	E-Voting Using BC And Smart Contracts: Proof of Concept	2020	Private	Ethereum	Proof of concept	✓	✓	✓	×	✓	×	✓	×	✓
[59]	TrustVote	2020	Public & Private	Ethereum & Hyperledger	Ecsc & bsc & otp	✓	✓	✓	×	✓	✓	✓	×	✓
[44]	The blockchain-based Voting system in Local Network	2021	Public	Ethereum	POW & hashing	✓	✓	✓	×	×	✓	×	×	✓

[45]	Blockchain Technology App. for E-voting Systems	2021	Public	mobile app.	QR code as a wallet	✓	✓	✓	×	×	✓	✓	×	✓
[46]	d-BAME	2021	Public	Ethereum	AES& elgamal ring signature	✓	✓	✓	×	×	✓	✓	✓	✓
[47]	Decentralized E-voting system based on SC by using BC	2021	Public	Ethereum	Proof of Authority	✓	×	✓	✓	×	✓	×	×	✓
[48]	Online Voting System Based on IoT and Ethereum Blockchain	2021	Public	Ethereum	Otp & odp	✓	✓	✓	×	✓	✓	×	✓	✓
[49]	A Privacy-Preserving E-voting System based on Blockchain	2021	Public	Ethereum	Face recognition& hashing	×	✓	✓	×	✓	×	×	×	✓
[16]	Secure E-Voting System using BCT via Face recognition and OTP	2021	Public	Ethereum	OTP & Face Net algorithm	✓	✓	✓	×	×	×	×	✓	✓
[50]	"Assuring anonymity and privacy in e-voting with distributed technologies based on Blockchain"	2022	Public & Private	Ethereum & Hyperledger	Consensus algorithms and Smart Contract	✓	✓	✓	✓	×	×	×	✓	✓
[51]	"Blockchain Based E-Voting System"	2022	Public	Ethereum	NIZKP algorithm	✓	✓	×	×	×	×	×	×	✓

5. Conclusion and Future Work

One of the numerous applications of blockchain technology is the blockchain-based e-voting system. Without blockchain, e-voting must be implemented by a centralized organization to oversee the process. However, blockchain technology and its decentralized ledger eliminate the need for a potentially unreliable or corruptible central entity. This article evaluated several research papers on blockchain-based e-voting systems. The blockchain and smart contract concepts and their uses were first presented, followed by an examination of existing e-voting methods.

Several research gaps in an e-voting system must be considered in future studies. For example, attacks on scalability, a lack of transparency, the blockchain's transaction throughput must be improved, dependency on unreliable systems, and resistance to coercion are all possible downsides that must be handled. As a consequence of this study, it was discovered that the blockchain platforms that are utilized in the e-voting system may need to be improved by an experienced developer to avoid unanticipated security risks and weaknesses. Previous experience and the critical issues mentioned above must be discussed in more depth throughout the actual voting procedures.

References:

[1] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a Decentralized Security Framework [Future Directions]," IEEE Consumer Electronics Magazine, vol. 7, no. 2, pp. 18–21, Mar. 2018.

[2] F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, "Crypto-voting, a blockchain based e-voting system," in IC3K 2018 - Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, 2018, vol. 3, pp. 223–227.

[3] S. Johar, N. Ahmad, W. Asher, H. Cruickshank, and A. Durrani, "Research and applied perspective to blockchain technology: A comprehensive survey," Applied Sciences (Switzerland), vol. 11, no. 14, Jul. 2021, doi: 10.3390/APP11146252.

[4] E. Leka, B. Selimi and L. Lamani, "Systematic Literature Review of Blockchain Applications: Smart Contracts," 2019 International Conference on Information Technologies (InfoTech), 2019, pp. 1-3, doi: 10.1109/InfoTech.2019.8860872.

[5] I. A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob, and M. Omar, "Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts," IEEE Access, vol. 9, pp. 37397–37409, 2021, doi: 10.1109/ACCESS.2021.3062471.

[6] A. A. Varfolomeev, L. H. Alfarhani, and Z. C. Oleiwi, "Secure-reliable smart contract applications based blockchain technology in smart cities environment," in Procedia Computer Science, 2021, vol. 186, pp. 669–676.

[7] Mohanta, Bhabendu Kumar et al., "An Overview of Smart Contract and Use Cases in Blockchain Technology," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (2018): 1-4.

[8] Clack, Christopher D. et al., "Smart Contract Templates: foundations, design landscape and research directions," ArXiv abs/1608.00771 (2016): n. pag.

[9] S. Nzuva, "Smart Contracts Implementation, Applications, Benefits, and Limitations," Journal of Information Engineering and Applications, vol. 9, no. 5, 2019, doi: 10.7176/JIEA.

[10] C. Antal, T. Cioara, M. Antal, and I. Anghel, "Blockchain Platform For COVID-19 Vaccine Supply Management," IEEE Open Journal of the Computer Society, vol. 2, pp. 164–178, Mar. 2021.

[11] A. Musamih, R. Jayaraman, K. Salah, H. R. Hasan, I. Yaqoob, and Y. Al-Hammadi, "Blockchain-Based Solution for Distribution and Delivery of COVID-19 Vaccines," IEEE Access, vol. 9, pp. 71372–71387, 2021.

[12] K. Peng, M. Li, H. Huang, C. Wang, S. Wan, and K. K. R. Choo, "Security Challenges and Opportunities for Smart Contracts in Internet of Things: A Survey," IEEE Internet of Things Journal, vol. 8, no. 15. Institute of Electrical and Electronics Engineers Inc., pp. 12004–12020, Aug. 01, 2021.

[13] A. Jain, A. Kumar Tripathi, N. Chandra, and P. Chinnasamy, "Smart Contract enabled Online Examination System Based in Blockchain Network.," in 2021 International Conference on Computer Communication and Informatics (ICCCI), Jan. 2021, pp. 1–7.

[14] H. Liu, Y. Zhang, S. Zheng, and Y. Li, "Electric Vehicle Power Trading Mechanism Based on Blockchain and Smart Contract in V2G Network," IEEE Access, vol. 7, pp. 160546–160558, 2019.

[15] I. A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob, and M. Omar, "Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts," IEEE Access, vol. 9, pp. 37397–37409, 2021.

[16] A. Parmar, S. Gada, T. Loke, Y. Jain, S. Pathak, and S. Patil, "Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP," in 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Jul. 2021, pp. 1–5. doi: 10.1109/ICCCNT51525.2021.9580147.

[17] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," Sensors /MDPI, vol. 21, no. 17, Sep. 2021.

[18] Patidar, Kriti, and Swapnil Jain, "Decentralized e-voting portal using blockchain," in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1–4.

[19] Albin Benny, A. A. Kumar, A. Basit, B. Cherian, and A. Kharat, Benny, Albin, "Blockchain based e-voting system," Available at SSRN 3648870, 2019.
[20] K. Sadia, Md. Masuduzzaman, R. K. Paul, and A. Islam, "Blockchain-Based Secure E-Voting with the Assistance of Smart Contract," in IC-BCT 2019, 2020, pp. 161–176.
[21] S. K. Geetha, S. Sathya, and S. T. Sakthi, "A Secure Digital E-Voting Using Blockchain Technology," Journal of Physics: Conference Series, vol. 1916, no. 1, May 2021.
[22] Teja, K. Saikrishna et al., "Secured voting through Blockchain technology," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (2019): 1416-1419.
[23] S. Xiao, X. A. Wang, W. Wang, and H. Wang, "Survey on blockchain-based electronic voting," in Advances in Intelligent Systems and Computing, 2020, vol. 1035, pp. 559–567.
[24] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: Is the technology mature enough?," Future Internet, vol. 10, no. 2, Feb. 2018.
[25] G. G. Dagher, P. B. Marella, M. Milojkovic, and J. Mohler, "BroncoVote: Secure voting system using ethereum's blockchain," in ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018, vol. 2018-January, pp. 96–107.
[26] N. al Goni, S. S. Ahmed, and A. Ibrahim, "A P2P Optimistic Fair-Exchange (OFE) Scheme for Personal Health Records Using Blockchain Technology," in Lecture Notes on Data Engineering and Communications Technologies, vol. 51, Springer Science and Business Media Deutschland GmbH, 2020, pp. 1–21. doi: 10.1007/978-3-030-44372-6_1.
[27] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," IEEE Access, vol. 7, pp. 24477–24488, 2019.
[28] S. J. Hsiao and W. T. Sung, "Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks," IEEE Access, vol. 9, pp. 72326–72341, 2021, doi: 10.1109/ACCESS.2021.3079708.
[29] N. Szabo, "Formalizing and Securing Relationships on Public Networks", FM, vol. 2, no. 9, Sep. 1997.
[30] H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A Survey," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
[31] S. Xiao, X. A. Wang, W. Wang, and H. Wang, "Survey on blockchain-based electronic voting," in Advances in Intelligent Systems and Computing, 2020, vol. 1035, pp. 559–567. doi: 10.1007/978-3-030-29035-1_54.
[32] Hardwick, Freya Sheer, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, "E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy.," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), May 2018, pp. 1561–1567.
[33] Pawlak, Michał, Jakub Guziur, and Aneta Poniszewska-Marańda, "Voting process with blockchain technology: auditable blockchain voting system.," in In International Conference on Intelligent Networking and Collaborative Systems, 2018, vol. 23, pp. 233–244.
[34] F. Ahmad, M. Rafay, and K. Haider, "MOBILE VOTING SYSTEM," International Journal of Computer Science and Mobile Computing, Vol. 7, Issue. 1, January 2018, pg.13 – 17
[35] N. A. J. Al-Habeeb, N. Goga, H. A. Ali and S. M. S. Al-Gayar, "A New M-voting System for COVID-19 Special Situation in Iraq," 2020 International Conference on e-Health and Bioengineering (EHB), 2020, pp. 1-4, doi: 10.1109/EHB50910.2020.9280275.
[36] D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Commun ACM, vol. 24, no. 2, pp. 84–90, 1981.
[37] A. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, and P. Sharma, "Privacy preserving E-voting cloud system based on ID based encryption," Peer-to-Peer Networking and Applications, pp. 1–11, 2020.
[38] Y. Abuidris, R. Kumar, and W. Wenyong, "A survey of blockchain based on e-voting systems.," in PervasiveHealth: Pervasive Computing Technologies for Healthcare, Dec. 2019, pp. 99–104.
[39] Hsiao, Jen Ho, Raylin Tso, Chien-Ming Chen, and Mu En Wu, "Decentralized E-voting systems based on the blockchain technology.," in Advances in Computer Science and Ubiquitous Computing, Springer, Singapore, 2018, vol. 474, pp. 305-309.

[40] W. Jr. Lai, Yung-ChenHsieh, Chih-Wen Hsueh, and Ja-Ling Wu, "DATE: a decentralized, anonymous, and transparent e-voting system.," in 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Jan. 2018, pp. 24–29.

[41] Tso Raylin, Zi Yuan Liu, and Jen-Ho Hsiao, "Distributed E-voting and E-bidding systems based on smart contract.," Electronics (Basel), vol. 8, no. 4, p. 422, Apr. 2019, doi: 10.3390/electronics8040422.

[42] K. Sadia, Md. Masuduzzaman, R. K. Paul, and A. Islam, "Blockchain-based secure e-voting with the assistance of smart contract.," IC-BCT ; Springer: Berlin/Heidelberg, Germany, pp. 161–176, 2020, doi: 10.1007/978-981-15-4542-9_14.

[43] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital voting: A blockchain-based E-voting system using biohash and smart contract," in Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020, Aug. 2020, pp. 228–233.

[44] T. Vairam, S. Sarathambekai, and R. Balaji, "Blockchain based Voting system in Local Network," in 2021 7th International Conference on Advanced Computing and Communication Systems, ICACCS 2021, Mar. 2021, pp. 363–366.

[45] V. Sliusar, Aleksei Fyodorov, Aleksandr Volkov, Pyotr Fyodorov, and Vladislav Pascari, "Blockchain Technology Application for Electronic Voting Systems.," in 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), Jan. 2021, pp. 2257–2261.

[46] E. Zaghloul, T. Li, and J. Ren, "d-BAME: Distributed Blockchain-based Anonymous Mobile Electronic Voting.," IEEE Internet of Things Journal, vol. 8, no. 22, p. p.16585-16597, 2021.

[47] A. M. Al-Madani, A. T. Gaikwad, V. Mahale, and Z. A. T. Ahmed, "Decentralized E-voting system based on Smart Contract by using Blockchain Technology.," in 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), Oct. 2020, pp. 176–180.

[48] A. AH. Othman, Muhammed Emarn A.A., H. K. M. Mujahid, H. A. A. Muhammed, and M. A. A. Mosleh, "Online Voting System Based on IoT and Ethereum Blockchain.," in 2021 International Conference of Technology, Science and Administration (ICTSA), Mar. 2021, pp. 1–6.

[49] W. Fan, Shubham Kumar, Vrushali Jadhav, Sang-Yoon Chang, and Younghee Park, "A Privacy Preserving E-Voting System Based on Blockchain.," in Silicon Valley Cybersecurity Conference: First Conference, SVCC 2020, San Jose, CA, USA, December 17-19, 2020, Revised Selected Papers, 2020, vol. 1383, pp. 148-159.

[50] V. Neziri, I. Shabani, R. Dervishi, and B. Rexha, "Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain," Applied Sciences, vol. 12, no. 11, p. 5477, May 2022, doi: 10.3390/app12115477.

[51] P. M. Kukwase, G. P. Kolte, A. D. Sawarkar, C. K. Rajput, and J. Dehankar, "Blockchain Based E-Voting System," International Journal of Research in Engineering and Science (IJRES) ISSN, vol. 10, no. 5, pp. 74–76, 2022, [Online]. Available: www.ijres.org

[52] Vijayalakshmi V. and S. Vimal, "A Novel P2P Based System with Blockchain for Secured Voting Scheme.," in 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), 2019, vol. 5, pp. 153–156.

[53] Abayomi-Zannu T. P., I. A.Odun-Ayo, and T. F. Barka, "A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication," in Journal of Physics: Conference Series, Dec. 2019, vol. 1378, no. 3, p. p.032104.

[54] Sathya V, Sarkar Arpan, Aritra Paul, and Sanchay Mishra, "Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting.," in 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 2019, p. P. 1075-1079.

[55] Lyu Jiazhuo, Zoe L.Jiang, Xuan Wang, Zhenhao Nong, Man Ho Au, and Junbin Fang, "A secure decentralized trustless E-voting system based on smart contract.," in 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Aug. 2019, p. pp 570-577.

[56] C. H. Roh and I.-Y. Lee, "A study on electronic voting system using private blockchain," Journal of Information Processing Systems, vol. 16, no. 2, pp. 421–434, Apr. 2020.

[57] M. N. K. Reddy, L. Maruthi Manohar Reddy, and Priya k. Lakshmi, "An Integrated and Robust Evoting Application Using Private Blockchain," in 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI), 2020, pp. 842-846.

[58] F. D. Giraldo, Barbosa Milton C., and Carlos E. Gamboa, "Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept," IEEE Latin America Transactions, vol. 18, no. 10, pp. 1743-1751., 2020.

[59] M. Soud, Sigurður Helgason, Gísli Hjálmtýsson, and Mohammad Hamdaqa, "TrustVote: On Elections We Trust with Distributed Ledgers and Smart Contracts," in 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2020, pp. 176–183.

[60] J. E. Oliver, "The effects of eligibility restrictions and party activity on absentee voting and overall turnout," American Journal of Political Science, vol. 40, no. 2, pp. 498–513, 1996.

[61] Y. Zhou, Yining Liu, Chengshun Jiang, and Shulan Wang, "An improved FOO voting scheme using blockchain," International Journal of Information Security, vol. 19, no. 3, pp. 303–310, Jun. 2020.

[62] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices," IEEE Transactions on Industrial Informatics, IEEE, p. p.1-1, 2021.

[63] Fujioka Atsushi, Tatsuaki Okamoto, and Kazuo Ohta, "A practical secret voting scheme for large scale elections," in International Workshop on the Theory and Application of Cryptographic Techniques, Dec. 1992, pp. 244-251.

[64] D. B. Rawat, V. Chaudhary, and R. Doku, "Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems," Journal of Cybersecurity and Privacy, vol. 1, no. 1, pp. 4–18, Nov. 2020.

[65] J. G. Song, S. J. Moon, and J. W. Jang, "A scalable implementation of anonymous voting over ethereum blockchain," Sensors, vol. 21, no. 12, Jun. 2021.

[66] T. U. Sree, N. Yerukala, A. N. Tentu, and A. A. Rao, "Secret Sharing Scheme Using Identity Based Signatures," in Proceedings of the2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), , Feb. 2019, pp. 20–22.