IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 February 2023, accepted 26 February 2023, date of publication 6 March 2023, date of current version 13 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3253682

SURVEY

E-Voting Meets Blockchain: A Survey

MARIA-VICTORIA VLADUCU[1], (Student Member, IEEE), ZIQIAN DONG[2], (Senior Member, IEEE), JORGE MEDINA[3], (Student Member, IEEE), AND ROBERTO ROJAS-CESSA[3], (Senior Member, IEEE)

[1]Network and Innovation Laboratory, Department of Computer Science, College of Engineering and Computing Sciences, New York Institute of Technology, New York, NY 10023, USA

[2]Network and Innovation Laboratory, Department of Electrical and Computer Engineering, College of Engineering and Computing Sciences, New York Institute of Technology, New York, NY 10023, USA

[3]Networking Research Laboratory, Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, USA

Corresponding author: Ziqian Dong (ziqian.dong@nyit.edu)

This work was supported in part by the U.S. National Science Foundation under Grant 1830718 and Grant 1856032.

ABSTRACT The utilization of electronic voting systems for the election of public offices is becoming widespread globally. This trend can be attributed to the benefits provided by these systems, including remote voting capabilities and accelerated vote counting. Furthermore, electronic voting systems offer improved privacy and enhanced protection against voting bias. Blockchain technology enhances the robustness of the voting process through its immutable vote storage mechanism, thereby reducing the threat of vote tampering and safeguarding the legitimacy of elections. This technology has been adopted by countries such as Germany, Russia, Estonia, and Switzerland for use in their e-voting systems. This study provides a comprehensive overview of the blockchain-based e-voting systems currently being implemented by various countries and companies and proposed for academic research. Additionally, this study analyzes the challenges faced by blockchain e-voting systems and identifies areas for future research to enhance the trustworthiness of such systems.

INDEX TERMS Blockchain, consensus, e-voting, government, industry, security, survey, transparency.

I. INTRODUCTION

The implementation of electronic voting (e-voting) has the potential to transform the traditional paper ballot-based voting process into a more inclusive and accessible platform. This shift would allow a larger portion of the population to participate in the exercise of their civil rights during elections [1], [2], [3], [4]. While e-voting has been implemented in various elections as a supplement or alternative to in-person voting, concerns over its legitimacy and authenticity remain a hindrance to its wider adoption.

In a conventional paper ballot-based voting system, eligible voters are required to register with the election commission prior to casting their vote, as Fig. 1 shows. Voting can occur on election day through in-person voting or through mail-in ballots, with the latter requiring submission prior to a designated deadline for vote counting. The familiarity of in-person voting has made it more widely accepted than electronic voting. However, this approach has been criticized for its potential susceptibility to disruptions, such as adverse weather conditions, natural disasters, lockdowns, or lengthy lines at polling stations [5]. Furthermore, the logistics of in-person voting systems can be costly, requiring measures to verify voter identity, staff polling stations, and securely handle and store paper ballots to ensure the integrity of marked ballots and vote counting. In some instances, large crowds at polling stations on election day may pose safety concerns and increase the risk of terrorist attacks [1] or voter intimidation [6].

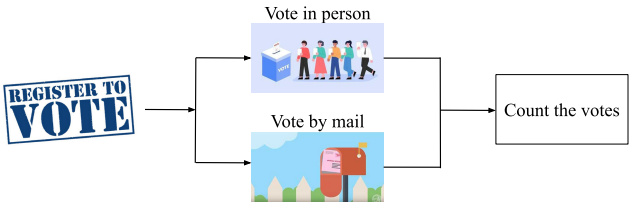

FIGURE 1. Traditional voting process.

The associate editor coordinating the review of this manuscript and approving it for publication was Santosh Kumar.

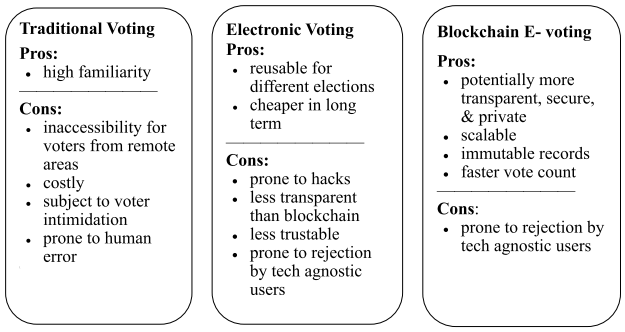

FIGURE 2. Comparison of traditional, electronic, and blockchain e-voting.

Citizens have expressed concerns over the security, privacy, authenticity of votes, and voter identification in the context of e-voting. For instance, the storage of voter information in a database can make it vulnerable to hacking attacks and manipulation by unauthorized parties [6]. The perceived lack of transparency in e-voting systems, due to the privacy measures implemented and the less visible process for vote processing compared to paper-ballot voting, also raises concerns [1].

Cryptography and biometric authentication have been proposed as potential solutions to address these security and transparency concerns [2], [7], [8], [9], [10], [11]. However, a more comprehensive approach is necessary to ensure the protection of voter registration and the voting process while preserving voter privacy and maintaining transparency in the voting process.

Blockchain is a distributed ledger that operates on a peer-to-peer (P2P) network [12]. Its decentralized structure, combined with the use of consensus algorithms for block recording and encrypted ledgers, makes it a potential solution for enhancing the security and transparency of e-voting systems. This technology holds great promise in resolving many of the security and transparency challenges faced by e-voting systems.

Therefore, it is no surprise to witness an increasingly broad interest in adopting blockchain-based e-voting systems by various countries to enhance election processes. This demand has also motivated many companies to develop products and academia to identify issues and develop algorithms that make such e-voting systems more equitable and resilient to various election threats. While much of the literature has focused on developing blockchain-based systems for several years, the most significant progress on e-voting has occurred recently and through the development of a significant body of work. Yet, such developments have not been highlighted by previous surveys on e-voting systems. As a response to this gap, this survey aims to identify and present important recent updates and to include a discussion of voter registration methods in the proposed blockchain e-voting systems.

The contributions of this survey are: it a) provides an extensive up-to-date review of more than 60 blockchain e-voting systems, including proposals adopted by governments and provided by companies, besides those developed by academia, b) introduces the terminology used in the description of recent and widespread blockchain-based e-voting systems; c) presents recent blockchain e-voting systems and categorizes them based on the challenges they address, and d) discusses the outstanding challenges in enhancing the adaptability and fostering public confidence in e-voting systems. This survey also identifies blockchain e-voting systems that have been adopted by various countries and used in elections, with an emphasis on the used registration method. Depending on the electoral structure of a country, the blockchain e-voting system might be customized to accommodate the needs of that process while providing the measures that give confidence to voters to exercise their voting rights.

Table 1 compares the scope of existing surveys and indicates the number of e-voting systems considered in each work. The table also shows the focus of each survey [6], [13], [14], [15], [16], [17], [18], [19], [20], their limitations, and characteristics [3], [21], [22], [23], [24], [25], [26], [27], [28], [29]. An overview of the blockchain e-voting systems covered in this survey is outlined in Table 2.

The remainder of this survey is organized as follows: Section II defines the terminology used in blockchain e-voting systems including consensus algorithms, cryptography, and characteristics of a trustworthy system. Section III presents the blockchain e-voting systems proposed by academia. Section IV presents the blockchain e-voting systems already used by governments and companies. Section V discusses challenges and future work. Section VI concludes this survey.

II. TERMINOLOGY

We introduce the terminology used in blockchain-based e-voting systems in this section. They are categorized based on the consensus algorithms, blockchain framework, cryptography, characteristics of a successful system, and the development tools used to implement blockchain e-voting systems. These terminologies are outlined in Table 3.

A. BLOCKCHAIN

Blockchain is a distributed ledger of transactions implemented on a P2P network [12]. It comprises a sequence of blocks, each with a set of records of verified transactions. These blocks are sorted in the order they are committed into the blockchain [89], [90]. Each participating peer, or node of a P2P network, verifies the received block and appends the validated block to the chain after the majority of nodes reach a consensus [91]. No entity can add or modify a block in the ledger without majority approval [92]. Moreover, the records in the blockchain are irreversible and cannot be changed or deleted by any node in the network [12], [93], [94]. Blockchain combines the advantages of consensus algorithms and cryptographic algorithms to ensure the validity of the system [95]. The immutability feature of blockchain where no

TABLE 1. Overview of literature review on blockchain E-voting systems.

Surveys	Main Feature	Number of reviewed systems
Cabuk et al. [1]	Strengths, Weaknesses, Opportunities, and Threats analysis on voting types	0
Ceinkaya et al. [30]	Differences between verification vs. validation in blockchain e-voting systems	0
Kshetri et. al [31]	Overview of the first countries & companies that adopted blockchain e-voting	6
Vivek et al. [3]	Requirements of a successful system	8
Jafar et al. [14]	Limitations and past solutions	12
Benabdallah et al. [32]	Comparison based on implementation stages	15
Tas et al. [6]	Large collection of works commented	39
This survey	Basic concepts of blockchain e-voting, analysis of academic proposals and commercial implementations and adoptions by different countries	64

TABLE 2. Overview of blockchain E-voting systems.

Use	Description	Blockchain Framework
Academia	Systems for student associations, churches, and non-governmental organizations (NGOs)	Ethereum [33]–[41]
		Not mentioned [42], [43]
	Systems for small-scale elections: student associations, church, and NGO voting	Auditable Blockchain Voting System [44]
		Biometrics [45], [46]
		Bitcoin [47], [48]
		Crypto [49]
		Ethereum [13], [50]–[53]
		Hyperledger Fabric [54]
		Quantum Blockchain [55], [56]
		Not mentioned [57]–[62]
		Permissioned Blockchain [63]
		Permission-free Blockchain [64]
		Blockchain Waves [65]
		ZCash [66]
Governmental	Systems for presidential or government elections	Proprietary Systems [31], [67]–[70]
		Adopt systems by other companies [16], [58], [58], [71]–[75]
Commercial	Systems for small- & large-scale elections	Bitcoin [76]–[78]
		Ethereum [73], [79]–[83]
		Hyperledger Fabric [84], [85]
		Proprietary blockchain [71], [86], [87]
		Permission blockchain [88]

TABLE 3. Terminology classification.

Type	Name
Consensus Algorithms	Proof of Work (PoW) | Proof of Stake (PoS) | Delegated Proof of Stake (DPoS) Proof of Activity (PoA) | Proof of Burn (PoB) Proof of Vote (PoV) | Parallel Proof of Vote (PPoV) Practical Byzantine Fault Tolerance (PBFT)
Framework	Bitcoin | Ethereum | Exorum Go-Ethereum/Geth | Hyperledger Fabric | Quorum | ZCash
Cryptography	Blind signature | Hashing | Merkle Tree Secure Hashing Algorithm | Zero-Knowledge Proof
Characteristics of a successful system	Accuracy | Anonymity | Audibility | Eligibility Integrity | Privacy | Reliability Security | Transparency | Verifiability
Tools	Ganache | Metamask | Truffle

individual is able to alter the recorded transactions improves the trust in the system [96].

There are three types of blockchains: public, private, or hybrid. A **public blockchain** allows pseudo-anonymous

users to join the network, read the content of the blockchain, submit new transactions, or verify the correctness of the blocks, and participate in the consensus process that results in the addition of new blocks. Examples of public blockchains are Bitcoin, NXT [97], and Ethereum [24]. A public blockchain is decentralized and with tamper-proof features [35], [98]. A **private blockchain** uses an entity as the sole responsible party for granting users permission to join the network and write or send transactions to the blockchain. Well-known examples of private blockchains are Ripple and Eris [6], [90], [99], [100]. While decentralization is the key feature of a blockchain, a private blockchain may adopt a different level of centralized structure where an authorized authority controls the data and network function to ensure efficiencies of the system such as throughput and transaction confirmation delay [101], [102], [103]. A **hybrid blockchain** is a combination of public and private blockchains where permission-based and permissionless systems are used. Users can access information via smart contracts and even if a primary entity owns a hybrid blockchain the transactions cannot be altered [98].

A blockchain can be classified as permissionless or permissioned. A **permissionless blockchain**, or a public blockchain, is available for everyone to participate in the blockchain validation process. It does not have a central authority and provides high transparency. However, privacy preservation in this type of blockchain may be limited as many of its components are available to the public [104]. A **permissioned blockchain** allows only a set of groups of miners to validate transactions in a blockchain network. Consortium blockchains and private blockchains are considered permissioned blockchains because a node must be certified by the majority of miners to join the consensus process [98]. A **consortium blockchain** is controlled by a group where multiple organizations can participate and decisions are made by the group on a decentralized architecture [12]. A well-known example of a consortium blockchain is Hyperledger Fabric. Permissioned blockchain provides more privacy compared to permissionless blockchain and is more scalable due to the limited number of nodes in the network. A permissioned blockchain is partially decentralized because different members may have different levels of control authorizations [105].

B. CONSENSUS ALGORITHMS

Consensus Algorithms are protocols employed by blockchain to ensure that all ledgers in the nodes of a blockchain network are persistently consistent [98]. This survey reviews the following consensus algorithms used in blockchain e-voting systems: Proof of Work, Proof of Stake, Delegated Proof of Stake, Proof of Activity, Proof of Burn, Practical Byzantine Fault Tolerance, Proof of Vote, and Parallel Proof of Vote.

Proof of Work (PoW) is the most popular consensus algorithm deployed by Bitcoin and Ethereum [106]. Nodes in the P2P network, called miners or validators, compete to solve a computationally challenging puzzle also known as a 'hard mathematical problem' to link the new block to the last block in the valid blockchain. The winner is the miner who finds the right solution. They get the right to create a new block in the blockchain. The process is called 'mining' [6].

Proof of Stake (PoS) is a consensus algorithm that makes blockchain networks more efficient by eliminating the computational-intensive mining process used in PoW [107]. In PoS, the miners are called forgers and the mining process is known as forging. Forgers deposit a certain number of coins that they own as stakes. This stake is used by the protocol to select the next forger in the network. PoS has two forger selection methods, namely, the coin-age selection and the randomized block selection [108]. The coin-age selection method is based on the number of days the coins are held at stake. A forger with the maximum value of coin age is selected to forge the next block [107]. The coin age is calculated by multiplying the number of days the coins have been staked by the number of coins staked. The randomized block selection method is based on calculating a hit value, a unique number, using the forger's private key. Each forger encrypts the previous block's hash using its private key to calculate the hit value. A forger with a specific hit value is selected for forging the next block [97]. This is applicable in the consortium or private blockchain where the holding companies need administrative access to the blockchain [106].

Delegated Proof of Stake (DPoS) is a consensus algorithm proposed similar to PoS. In DPoS the nodes in the network select delegates through voting and these delegates validate the blocks [63]. DPoS is divided into two stages: witnesses election and block generation. Witnesses also known as forgers are responsible for witnessing the transaction, verifying the signature, and timestamping the transaction. The forgers generate one block every 3 s, but they do not participate in transactions. If a forger fails to complete their task at a specified time, they are replaced by the next forger. The forgers are elected by the existing members/nodes rather than based on their stake [106], [109]. The more blockchain stakes they have, the higher possibility of them being a forger. This approach aims to prevent double voting by implementing extra scrutiny in the system and solves the issue of ''the rich getting richer'' in PoS [108]. However, the known identity of the forgers makes the blockchain system vulnerable to collusion attacks [110].

Proof of Activity (PoA) is a consensus algorithm that combines PoW and PoS. First, all the miners compete to propose an empty block using PoW to prove its participation in the network and then the consensus process randomly selects N validators based on their stakes as in PoS [63], [111]. The selected validators verify the header of the block and sign the block. Once an empty block receives N signatures, the block is committed to the blockchain. Transactions are added after that [108].

Proof of Burn (PoB) is a consensus algorithm proposed similar to PoW but with a lower rate of energy consumption [112]. PoB is similar to PoW as the miners invest in mining computing resources to increase the probability of mining the next block [108]. The miners send their coins to an irretrievable blockchain address to ''burn'' them [113]. The miner who burns the largest amount of coins during a duration demonstrates their commitment to the network and gains the right to mine and validate transactions [112]. It ensures that the users do not gain dominant power by increasing their stakes in the network [61].

Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm that has a primary node and secondary nodes. The nodes establish a consensus algorithm to solve the Byzantine Generals Problem. The Byzantine Generals Problem is a game theory problem, which describes the difficulty decentralized parties have in reaching a consensus without depending on any trusted central authority. It was designed to work efficiently in asynchronous systems and optimized for low overhead time to solve problems associated with already available Byzantine Fault Tolerance solutions [63]. The consensus process is divided into five phases: request, pre-prepare, prepare, commit, and reply. The request phase is where the client sends a request to the primary node, the leader. In the pre-prepare phase, the primary node communicates the request to the system's other nodes (the secondary nodes). In the prepare and commit phases both the primary and secondary nodes perform the service requested. In the reply phase, all the nodes send back a reply to the client. A faulty node is represented by malicious nodes. The protocol is complete when the client receives $n = 3f + 1$ replies with the same result from different nodes in the network. Here, n is the total number of nodes and f is the number of faulty ones [106].

Proof of Vote (PoV) is a consensus protocol based on a voting mechanism and consortium blockchain. PoV separates voting rights and executive rights. It mimics the voting campaign by designing four types of network participants, namely commissioner, butler, butler candidates, and ordinary participants. Commissioner is the highest member of this hierarchy and is in charge of the consortium. Butler is responsible for creating blocks in the network. Butler candidates are the entities from which butlers are elected. These three types of participants are involved in the administrative activities of the network and ordinary participants can join and exit the network to vote without administrative rights [114].

Parallel Proof of Vote (PPoV) is an efficient permissioned PBFT consensus, which allows multiple bookkeepers to generate blocks in a consensus cycle, thereby improving the system throughput. PPoV has three roles: **bookkeeper**, which can generate records and is responsible for packaging the clients' transactions into blocks; **voter** receives a block from the bookkeeper and votes on the legality of the block; and the **leader** who is in charge of collecting votes from voters and generating a complete block. Every consensus cycle has a unique leader selected from the bookkeepers [115].

C. FRAMEWORKS

This section overviews the existing blockchain e-voting frameworks. Table 4 categorizes the frameworks adopted by blockchain e-voting systems based on the consensus algorithm used, whether they are fully or partially decentralized, the throughput in terms of the number of transactions per second (tps), and scalability in terms of the number of votes the system can handle at a specific time or throughout the duration of the election.

Bitcoin was released by Satoshi Nakamoto in 2009 as an open-source software [116]. It is a peer-to-peer payment network that uses PoW. It is a public blockchain and is able to handle between 4.6 and 7 tps. Bitcoin is difficult to scale and less programmable. The network requires an ad hoc decentralized network of volunteers where messages are broadcast on a best-effort basis [3].

Ethereum is a P2P network that uses PoW that can handle up to 15 tps, thus having low scalability. The main difference between Bitcoin and Ethereum is that Ethereum is programmable so users can build and deploy decentralized applications on its P2P network [117].

Exonum is a decentralized public blockchain that uses a custom-built Byzantine consensus algorithm. It is reported that it can handle up to 5,000 tps [118].

Hyperledger Fabric is a popular consortium blockchain platform hosted by the Linux Foundation's Hyperledger project. It is designed to meet the confidentiality, privacy, and scalability requirements of applications [119]. The supported consensus algorithms are PBFT, Raft, and Kafka. It uses a modular architecture where only designated users can access the data. This blockchain can achieve approximately 3,500 tps [120].

Quorum is a private blockchain used to provide an implementation of a permissioned blockchain on Ethereum [3]. Quorum uses a Constellation P2P network that encrypts specific messages in an enclave and stores information about previous transactions. Quorum is reported to handle more than 100 tps [121].

ZCash is a decentralized blockchain payment system that aims to provide anonymity and privacy. The main difference between ZCash and Bitcoin is that ZCash enables private transactions by using zero-knowledge proof [122]. It supports anonymous and transparent transactions with two types of addresses, while Bitcoins have a single address. These addresses are z-address that preserves anonymity in transactions and t-address that resembles the Bitcoin addresses in structure and allows for transparent transactions [122].

D. CRYPTOGRAPHY

In this section, we present the cryptographic algorithms used in blockchain e-voting systems.

TABLE 4. Comparison of blockchain frameworks.

Name	Consensus	Generation Time	Access	Transaction rate (tps)	Scalability
Bitcoin	PoW	9.7 min	public	≤ 7	very low
Ethereum	PoW	≤ 19 s	public	15	low
Exorum	Custom-built Byzantine algorithm	not mentioned	private	5000	N/A
Hyperledger-Fabric	PBFT, Raft or Kafka	10 ms	private	3500	good
Quorum	QuorumChain	not mentioned	private	$\leq$1200	good
ZCash	PoW	75 s	private	$\leq$25	N/A

Hashing is the process of mapping an arbitrary and variable-sized input into a fixed-sized output. It uses mathematical functions that take data as input and output a string that is illegible to the non-intended receivers [24].

Blind Signature is a mathematical scheme used to verify the authenticity of digital messages or documents where the message is disguised before it is signed. It is used for signing encrypted messages with no need for decryption. The sender's message is blinded prior to the recipient signing it [59].

Merkle Tree is a cryptographic tree in which nodes also called leaf nodes are assigned individually with the cryptographic hash of a data block [50]. Every other node that is not a leaf node is called a branch, inner node, or inode. An inode is tagged with the cryptographic hash of the labels of their child nodes [35].

Secure Hashing Algorithms (SHA) are a group of cryptographic hash functions published by the United States National Security Agency. There are multiple versions of SHA. SHA-256 takes an input of any length and uses it to create a 256-bit fixed-length hash value. A collision attack is a cryptography attack that tries to find two inputs producing the same hash value. SHA-256 and SHA-512 are hash functions that are collision attack-resistant and are deemed secure [61].

Zero-knowledge proof (ZKP) is a cryptographic mechanism where one party, called the prover can prove to another party, called the validator that a given message is true without revealing the content of the message [123]. This scheme requires a prover and a validator. The prover avoids communicating additional information except for the fact that the message is true [96]. ZKP increases the transparency level of a system. It can be used for any sensitive information. ZKP adds a layer of security to the blockchain ledger and can be integrated with other blockchain systems [105], [124].

E. CHARACTERISTICS OF A SUCCESSFUL SYSTEM

Several works report different features that blockchain-based e-voting systems need to satisfy for an unbiased and accurate election, easy deployment, and transparency with the ability of voting and process scrutiny [4], [14], [30], [59], [63], [98], [125], [126], [127]. Here, we define these features.

Accuracy is the characteristic of an e-voting system to ensure that all cast votes are counted correctly and that the declared results correspond precisely to the election results. This feature guarantees that nobody can change the voting of others and that the final result includes all legitimate votes [125].

Anonymity is the attribute of a system where the information of the voters including their personal data and the candidate they voted for are protected. Voters use generated addresses in conducting transactions and other interactions in a blockchain network, as opposed to personal details [126].

Auditability is a property used to record and validate transactions, making the data in the blockchain transparent and accessible for examination. All recorded transactions can be traced by conducting an iterative search across the blockchain ledgers [63].

Eligibility is the attribute of a blockchain e-voting system where only eligible voters can participate in the election. The system checks the requirements of a specific election to verify if the voter is eligible to vote [14].

Integrity is a property that guarantees that votes cannot be tampered with in any manner once recorded [4].

Privacy is an attribute of the system that ensures there is no link between a voter and their vote. The identity of voters and whom they vote for should not be public [30].

Reliability is an attribute of the system where all active nodes keep full copies of the blockchain ledger. A blockchain e-voting system is reliable when there is a copy of the voting procedures available for everyone to check [58].

Security is the property of an e-voting system that is immune to hacks and attacks against the voter identification and voting process. A system is secure when the necessary measures were considered so voting is not vulnerable to manipulations [126].

Transparency is the property of the system where the blockchain maintains a complete history of past transactions within the network, where users can track the full history of data in the system [127].

Verifiability is the characteristic where voters should be able to confirm that their ballots are counted correctly [30].

F. TOOLS

The tools that can be used to implement a blockchain e-voting system include the following:

Ganache is a local blockchain for testing and developing distributed applications in Ethereum [37], [39], [52].

Go-Ethereum/Geth is an implementation Ethereum blockchain that runs smart contracts and applications using the Go programming language. It has an optional decentralized mechanism based on either PoW, PoS, or PoA [128].

Metamask is a browser-based wallet application that manages keys, transactions, and user accounts in blockchain networks. It connects a web client to the Ethereum network [129].

Truffle is a development framework comprising a collection of tools for creating and developing blockchain applications in the Ethereum network [18], [39].

III. ACADEMIC PROPOSALS

This section summarizes and categorizes the current proposals for e-voting systems using blockchain technology based on the concerns they attempt to address. The registration method, the type of implemented framework, and whether it is a conceptual or implemented framework are outlined in Table 5. The registration method is organized as internal if the registration process is part of the proposed blockchain system and external if the registration is done by a trusted third party or through verifiable databases provided by government or authoritative entities, or in some cases the registration process is not mentioned in the literature.

Awalu et al. [63] addressed the system **accuracy** issue by proposing a theoretical model based on a permissioned blockchain to ensure all votes are counted. The system's registration is done internally. The system uses a unique ID for registration, vote casting, and vote calculation to deliver the election results. The system ensures the confidentiality of the pattern of votes during the tallying phase in the voting process to avoid biasing the result and only generate a report of casted votes after the election is over.

Most of the proposed systems that address the **anonymity** concern follow either a theoretical approach [50], [66], [55], [58], or with an implemented system [33]. Tarasov and Tewari [66] and Patidar and Jain [33] present an Ethereum model while Sun et al. [55] use Quantum Blockchain. A unique genesis block that represents a candidate serves as a foundation block, also known as the genesis block. All the votes for that particular candidate are linked to the genesis block [58]. No links between the voters' identities and the ballots are created. Quantum secure communication prevents voters from accessing other voters' ballots other than their own [55]. Biohash, where users' biometric information is hashed, was implemented to protect the voter's identity [50]. Here, voters are given a public key to access the system and together with their fingerprint and voter ID authenticate themselves to cast their vote.

Auditability was addressed by Awalu et al. [63] who proposed a theoretical model based on permissioned blockchain, while Fusco et al. [49] proposed a blockchain cryptographic model using ZCash. The registration for both systems is done internally. To preserve the auditability of the voting results, an automatically generated vote count is proposed using blockchain's system architecture [63]. Fusco et al. [49] propose the use of crypto-voting and two linked blockchains as a one-way pegged sidechain where the first chain records the voters and their voting operations and the second sidechain is assigned to count the votes corresponding to each candidate [49].

Integrity was addressed by various proposed systems. The majority of these proposed systems follow a theoretical approach, while Khoury et al. [36], and Khan et al. [37] implemented the system using Ethereum. Only trusted miners can participate in the consensus process to avoid biasing the result [63]. The blind signature used by Liu and Wang [59] protects voters' identity and guarantees that there is no link between a person and their candidate of choice. Their approach together with the introduction of inspectors, entities that limit the organizer's power, ensure a fair election [59]. Khoury et al. [36] proposed a combination of two different smart contracts, namely the registration contract and the voting contract. The registration contract is deployed once for all voters and takes care of registration and authentication. The voting contract is written once at the development stage and deployed several times depending on the election. Simple random sampling was used to determine the survey implementation of research trust in blockchain utilization on e-voting [62].

Privacy was addressed in both theoretical and implemented approaches. Ethereum remains the most considered framework. However, Bitcoin [47], Quantum Blockchain [56], and Blockchain Biometrics using Internet of Things (IoT) devices [45] are also considered. Wang et al. [53] propose an un-linkable signature model where the voter's privacy is preserved during and after the voting process, while Liu and Wang [59] introduce a blind signature approach that encrypted the voters' information to maintain their privacy for their vote. Two-phase verification for voters before casting their vote was also adopted [51]. Biometrics are also adopted to maintain voter privacy [45]. Some proposals handle the privacy of the whole system [38], [47], [50], while the others focus only on the voter privacy [13], [33], [37], [45], [53].

Reliability was addressed by Gonzalez et al. [54] who proposed a theoretical system based on Hyperledger Fabric, while Yavuz et al. [34] proposed an implementation model using Ethereum. The reliability property is achieved based on the reliability of the Ethereum framework [34]. The voting system was divided into three main phases: pre-voting, voting, and post-voting to ensure the system is reliable [54].

The majority of the systems that focus on **scalability** use Ethereum. These systems are either proposed as a theoretical concept or have been implemented. Some of the scalability was achieved based on the consensus algorithms they adopted in the Ethereum framework [33], [36], while others tackle it by breaking down the election system into different stages and sub-stages making the system easier to scale [34].

TABLE 5. Improvement objective classification.

Target Feature	Registration Method	Framework	Implemented?	Proposed Strategy
Accuracy	Internal	Permissioned blockchain [63]		Unique ID & vote calculation [63]
Anonymity	Internal	Ethereum [50] ZCash [66]		Biohash (fingerprint) [50] Cryptography [66]
	External	Not mentioned [58]		A unique genesis block [58]
		Ethereum [33]	✓	Design considerations (Ethereum) [33]
	Not mentioned	Quantum blockchain [55]		Quantum computation [55]
Auditablity	Internal	Permissioned blockchain [63] Crypto [49]		Vote calculation algorithm [63] Cryptography [49]
Integrity	Internal	Ethereum [36]	✓	Three-phase system [36]
		Not mentioned [59] Permissioned blockchain [63]		Blind signature [59]
	External	Bitcoin [48] Not mentioned [60]		Bitcoin [48] Smart contracts & ATAM [60]
	Not Mentioned	Ethereum [37]	✓	
		Not mentioned [62]		Simple random sample [62]
Privacy	Internal	Blockchain biometrics [45] Ethereum [13], [40], [50], [51], [53] Not mentioned [59] Quantum blockchain [56]		IoT-based system [45] Un-linkable signatures (Ring Signature) [53] Blind signature [59] Quantum-assisted blockchain [56]
	External	Bitcoin [47]		Private blockchain [47]
		Ethereum [33], [38]	✓	Two-phase verification [51]
	Not mentioned	Ethereum [37]	✓	Design considerations [33]
Reliability	Internal	Hyperledger fabric [54]		Hyperledger fabric [54]
	External	Not mentioned [58]		
	Not mentioned	Ethereum [34]	✓	
Scalability	Internal	Ethereum [36]	✓	System components [36]
		Ethereum [53]		DPoS [53]
	External	Ethereum [33]	✓	Design considerations [33]
	Not mentioned	Ethereum [34]		Different election stages [34]
Security	Internal	Not mentioned [59], [62]		Simple random sample [62]
		Blockchain biometrics (fingerprint) [46]		Biometrics (fingerprint) [46]
		Ethereum [13], [50], [52], [53]		Biometrics [13], [50]
		Quantum blockchain [56]		Quantum-assisted blockchain [56]
		ZCash [66]		Cryptography [66]
	External	Not mentioned [47], [57], [58], [60], [61]		Improved JP Cruz & Y Kaji algorithm [47]
		Ethereum [33], [38]–[40]	✓	Encrypted voter ID & name & vote count [39]
	Not mentioned	Bitcoin [48]		Bitcoin [48]
		Ethereum [37]	✓	
		Permission-free blockchain [64]		Secure IoT devices at polling stations [64]
		Not mentioned [42]	✓	Biometrics (fingerprint) [42]
Transparency	Internal	Ethereum [13]		Biometrics (fingerprint, face-recognition) [13]
		Cryptography [49]		Cryptography [49]
		Permissioned blockchain [63]		Permissioned blockchain [63]

Security was addressed in both the theoretical approach and implemented systems. Ethereum remains the mostly considered framework. However, Bitcoin [47], biometrics [13], [42], [46], [50], Quantum Blockchain [56], Cryptography [66], and public blockchain [64] are also considered. To preserve the security of the elections the following methods were proposed: fingerprint authentication [13], [42], [46], [50], simple random algorithm [62], cryptography and

TABLE 5. *(Continued.)* **Improvement objective classification.**

		Ethereum [35], [41]	✓	Smart contracts [41]
		Blockchain Waves [65]		RIDE Language [65]
	External	Ethereum [33], [38], [40]	✓	Design considerations [33]
	Not mentioned	Bitcoin [48]		Bitcoin [48]
		Ethereum [34], [37]		
		Permission-free blockchain [64]		IoT devices at polling stations [64]
Verifiability	Internal	Ethereum [35]	✓	System architecture [35]
		Cryptography [49]		Cryptography [49]
		Not mentioned [43]	✓	Double envelope encryption [43]
	External	Not mentioned [58]		System components [58]
	Not mentioned	ABVS [44]		Intelligent agents [44]
		Ethereum [37]	✓	
		Quantum blockchain [55]		Quantum computing [55]

encryption algorithms [39], [48], [66] and secure IoT devices at polling stations [64].

Some of the proposed systems that address **transparency** are theoretical models, while the rest are implemented. Ethereum remains the mostly considered framework, however, Bitcoin [48], Multichannel Hybrid Blockchain [49] and public blockchain [64] are also considered. These systems adopt the transparency feature of a public and hybrid blockchain to ensure information is accessible by authorized users. For this, biometric authentication using fingerprint or face recognition was used to guarantee the authenticity of the voters while allowing the system to keep the vote count transparent [13]. Cryptography concepts such as encryption of personal data and vote details were also adopted [48], [49]. Smart IoT devices were installed at the polling stations [64], or different smart contracts were implemented to ensure that the election was transparent [41].

Verifiability was addressed in both implementation models and theoretical systems. Among them, Ethereum is still the most used framework, in addition, Auditable Blockchain Voting System (ABVS) [44], Multichannel Hybrid Blockchain [49], and Quantum Blockchain [55] are also used. The unique system architecture [35], quantum computing principles [55], double envelope encryption technique [43], cryptography concepts [49], or a combination between intelligent agents and multi-agent systems [44] were taken into consideration to guarantee the verifiability of the system.

IV. SYSTEMS USED BY GOVERNMENT INSTITUTIONS AND COMPANIES

There are numerous commercial blockchain e-voting systems that have been adopted by governments and institutions as well as those developed by companies. We review some of the popular ones in this section.

A. SYSTEMS USED BY GOVERNMENT INSTITUTIONS

This section presents the blockchain-based e-voting systems adopted by various countries and governments, a description of these systems, and the evolution of their system. Table 6 summarizes the countries and regions that implemented blockchain in their voting processes. Estonia, Australia, Norway, and Switzerland have implemented e-voting pilots for binding elections. Estonia has provided e-voting options for every election and census since 2013, while other countries such as India and Japan are in the process of developing e-voting systems for future elections [67]. Australia, Germany, Norway, Sierra Leone, and Switzerland use commercial systems to conduct blockchain-based e-voting [13], [31], [57], [72], [74], [75]. Estonia, Russia, South Korea, and the United States (Washington D.C.) have their proprietary systems [58], [67], [69], [70].

Australia piloted blockchain e-voting in 2015 for the State General Election of New South Wales where about 280,000 citizens exercised e-voting through an application called Scytl [31]. The voter registers with authorities and receives their voter ID and chooses a 6-digit pin after the registration process is done. They log into the system using their ID and PIN and get a 12-digit receipt number after casting their vote. In order for the voter to verify their vote, they use the ID, PIN, and receipt number to retrieve the information [72].

Estonia is the first country to use electronic e-voting for elections. It started the e-voting implementation in 2005 [67], [68], [130], [131], [132], [133]. In 2013 Estonia gave the population a choice to use either e-voting or in-person elections that lasted for 7 days, about 21.2% of the population voted using e-voting. The system has partially decentralized software, that provides anonymity and voter verification [134]. It needs the Internet and an Electronic National Identification Card that is used for authentication, encryption, and signature [67]. Voters need to download the voting application, authenticate using the electronic ID, and if eligible, a list of candidates will be displayed for them to cast their vote [68], [135].

Germany uses Polyas for parliamentary elections [136]. Polyas is the only e-voting software company certified by the German Federal Office for Information Security, for its e-voting system [16], [73].

Norway used e-voting in 2011 for council elections [58]. The software is anonymous and partially decentralized. The

TABLE 6. Governments that use blockchain in their voting process.

Country	System Adopted
Australia	iVote by Scytl [71], [72]
Estonia	Proprietary Blockchain [67], [68]
Germany	Polyas [16], [73]
Norway	Scytl [58]
Russia	Proprietary Blockchain [69]
Sierra Leone	Agora [31]
South Korea	Proprietary Blockchain [31], [70]
Switzerland	Luxoft, Scytl, and Ethereum [74], [75]
United States of America	Voatez [85] & proprietary implementation [58]

country stopped using e-voting platforms due to cyberattack concerns [137].

Russia implemented e-voting in 2014 for more than two million users [31]. In 2017 Moscow residents used blockchain to vote for council members [138], [139]. Russia also used Waves's blockchain e-voting system [140]. The system uses a crash fault tolerance consensus algorithm based on Proof of Authority. Smart contracts are used to store the rules of the voting process, registration information, and vote verification [69].

Sierra Leone used Agora as their e-voting system for the presidential election in 2018 representing the first time in history that blockchain technology was used in a presidential election [31], [76].

In **South Korea**, approximately 9,000 residents voted for a project using Blockchain in 2017 using a smart contract based on blockchain systems [31], [70].

Switzerland conducted municipal elections using e-voting systems created by Luxoft [83]. The **Swiss** e-voting system is used for the majority of their national voting protocols from state-wide elections and referendums [75]. The proposed system is a mobile phone application that uses a Short Message Service (SMS) confirmation. Voters log onto the e-voting website using their ID and follow the site's instructions to cast their vote; they enter a PIN and compare a security symbol with the one they received in the mail. If the two matches, the system accepts the vote. After that, citizens enter codes for their PIN, the name of the referendum, and the answer (yes/no) [74].

Some states in **the United States** have implemented e-voting using blockchain for different elections. **Massachusetts** used Votez for student government elections, church-group, NGO, union voting, subnational political-party events, and even town-hall meetings [31]. **Washington D.C.** piloted a blockchain-based digital vote-by-mail system that was canceled because of the received public critisism [58].

B. COMMERCIAL BLOCKCHAIN-BASED E-VOTING SYSTEMS

This section presents some popular commercial blockchain e-voting systems developed by companies and how they are used. Table 7 summarizes these commercial blockchain e-voting systems and their important features. Agora, Netvote, OV-net, Polyas, Polys, PublicVotes, and Scytl propose systems that use Ethereum, while Follow My Vote proposes Bitcoin-based systems, Luxoft, and Voatz propose hyperledger fabric systems and Votebook proposes permissioned blockchain systems.

Agora is a blockchain voting system developed as part of a project funded by the European Commission [140]. The Spanish political party Podemos used Agora for an election within the party where 155,000 members participated in 2017. It was also used in wevotem **Sierra Leone** [16], [31]. The citizens' identity was verified by ID card and their ballot was later manually entered into a private blockchain Bulletin Board [141]. Voters got recorded in various layers guaranteeing the results are not tampered with [14]. The data was available to any third party including voters themselves while keeping user privacy [83].

Follow My Vote is a secure web-based, decentralized voting platform that audits the ballot box and allows users to see progress in real-time [78]. The process includes the authentication phase that ensures voter eligibility by allowing them to locate their unique voter ID. It uses a webcam and user ID to check that their identity matches the identification documents in the database [16]. The process allows the user to open the ballot box, locate their vote and check if both are existing and accurate. Follow My Vote was created in 2015. All voters had to install the ''voting booth'' on their device (computer, phone, tablet) and then they need to verify their identity by submitting legal documents (passport, etc) to an Identity Identifier that would be already approved by the organization holding the election. After their identity is verified, the voter requests an online ballot and submits their vote to the blockchain allowing them to vote early or even have the ability to change their mind and vote for another candidate [77].

Luxoft is a global IT service provider that together with the Lucerne University of Applied Sciences of Switzerland and the City of Zug created the first customized blockchain e-voting system [16], [84]. The system is deployed in three different data centers, two in Switzerland and one in Ireland, to increase security and reduce data loss risks [83].

TABLE 7. Commercial blockchains e-voting systems.

Commercial e-voting systems	Blockchain Frameworks
Agora	Bitcoin [76]
Follow my vote	Bitcoin [77], [78]
Luxoft	Hyperledger Fabric [84]
Netvote	Ethereum [79]
OV-net	Ethereum [80]
Polys	Ethereum [81]
Polyas	Ethereum [73], [82]
PublicVotes	Ethereum [83]
Scytl	Proprietary Blockchain [71]
Voatz	Hyperledger Fabric [85]
Votebook	Proprietary Blockchain [88]
Votem	Proprietary Blockchain [86]
VoteWatcher	Proprietary Blockchain [87]

NetVote is a decentralized application based on blockchain technology using Ethereum [121]. The administrator chooses one of two types of voting: open elections, or private elections, which allows voters to have the required amount of tokens issued specially for the elections [40], [79].

OV-net is a two-round decentralized protocol implemented on Ethereum that has four voting phases. Setup is the phase where a valid list of voters is uploaded to a smart contract [40]. Signing Up is the phase where voters send their electoral key, and uses ZKP to confirm the electoral key. Voting is the phase where voters send an encrypted vote either 1 (yes) or 0 (no), miners verify it, and then store it. Votes are counted in the voting count phase [80], [142].

Polyas was declared secure enough for electronic voting applications by the German Federal Office for Information Security in 2016 being a blockchain technology that provides a secure and auditable e-voting system [16]. Major companies in Germany together with companies around the United States and Europe use Polyas for their elections [136].

Polys is blockchain-based voting system created by Kaspersky Lab [81]. It has three main components: the organizer panel, the voter application, and the observer application. The *organizer panel* is the application used for creating a vote where voting parameters such as title, ballot options or candidate names, number of voters, and how they will be authorized are created. The panel enables the organizer of the elections to start and stop voting. The *voter app* uses three types of voter authorization email, PIN, and open voting. Voters receive a link from the organizer, where they can cast their vote. Polys ensures that voter IDs are verified, votes are encrypted and added to the blockchain, and the results are counted correctly. The *observer application* allows all participants and third parties to monitor the voting process in real-time without compromising anonymity. Voters can verify that their votes have been recorded on the blockchain and counted correctly [143]. They state that the systems are secure, transparent, and auditable, but they still have many challenges such as scalability, immaturity, acceptability, and coercion [81].

PublicVotes is a voting application built using Ethereum to provide fairness and transparency. All voters are recorded in the blockchain ledger. The description is a comprehensive explanation of what users vote exactly about. The election has three main components: publicPoll, vote limit, and timeLimit. PublicPoll is where it is decided if a poll should be private or public. The vote Limit is the limit of the number of voters. TimeLimit is the time requirement as the account will eventually run out of Ether [83].

Scytl was founded in 2001 and owns more than 40 international patents in the area of security applied to election processes [144]. Depending on the applicable jurisdiction and election topology of each country their iVote tool adapts from a design and cryptographic standpoint to the specific requirements and manages over 100,000 electoral events across more than 20 countries. In 2019, Swiss intended to use Scytl for 100 percent of the cantons that chose to use it [137], [145].

Voatz is a smartphone-based voting system based on blockchain that enables voters to vote remotely and anonymously, and verify that their vote was accurately counted [85]. The system has been reportedly used by various governments and political parties in elections around the U.S. [31].

Votebook was created in 2016 with voting machines that resemble traditional voting machines as the nodes in the blockchain [57]. After the polls are open the voting machines collect the votes and organize them into a block that would be broadcasted on the network. If all the conditions are met, receiving nodes will append the existing database with a new node, and a second node will keep track of all the votes [88].

Votem is a blockchain-based mobile application that uses a Proof of Vote protocol and an end-to-end digital system to ensure verifiability, security, and transparency [83]. The protocol uses ElGamal encryption for anonymity, a multi-signature scheme for authentication, and verifiable decryption for encrypted votes [86].

VoteWatcher is a voting method that combines both traditional voting and e-voting based on blockchain. The voters register using traditional methods and are given a paper ballot at the voting station, that contains three QR codes — one for the blockchain address, one for the ballot ID, and one for the election ID. After the ballot is scanned, the appropriate vote is sent to the proper candidate's unique address on a local blockchain. Images of every paper ballot will be kept and all data from the current machine will be compressed and stored on a DVD [87].

Votez is a blockchain-based voting system that uses a live photo of the voter and their ID and also asks for biometric proof (retina scan, fingerprint) [16]. The system allocates each voter a wallet which contains the user's credentials in the form of encrypted keys and a tamper-proof personal ID. Votez is a mobile-phone-based system that is used for student government elections, church-group, NGO, union voting, sub-national political-party events, and town-hall meetings [85].

The systems presented in this section can be used as examples that countries and other organizations can consider using blockchain-based e-voting systems in their elections. The systems might be implemented and customized according to the needs of the voting processes.

V. FUTURE WORK

As future work, a blockchain e-voting system implementation that is inclusive and accessible to all eligible voters is of interest to create. User authentication and registration are two major issues discussed in various blockchain e-voting implementations. It would be of interest to explore IoT, biometrics, and other convenient and secure ways for user authentication and verification in blockchain e-voting systems.

A blockchain e-voting system should be interoperable with other legacy systems. The scalability of the system is also an important factor to consider in the cost-effectiveness analysis. For a small number of users, the system is less expensive than a system with a large number of voters which results in higher costs and longer transaction confirmation time. Sharding would potentially solve the scalability issue of blockchain e-voting. Sharding implies dividing the whole network of a blockchain into several smaller networks.

In terms of design challenges, security, adaptability, and trustworthiness should be explored more in a combination of identification management, and authority management to ensure equal access to the voting systems. It would also be of interest to examine the trust in the blockchain e-voting system compared to the traditional voting system by voters. This knowledge can further guide the outreach methods for acceptance by the general public for such systems. A blockchain e-voting system should be more inclusive taking into consideration those who are not familiar with accessing the Internet, people with disabilities, people with limited access to technology, or simply technology novices. The system should be designed to be more friendly and accessible.

VI. CONCLUSION

With the rapid development and acceptance of blockchain technologies, there is an increasing interest in creating e-voting systems using blockchain technologies. This survey gives a review of traditional, electronic, and blockchain electronic voting systems. It categorizes terminologies used in the introduction and implementation of blockchain e-voting systems including consensus algorithms, frameworks, performance evaluation, characteristics for a successful system, cryptography, and tools to implement such systems. We provide an updated overview of the current blockchain e-voting systems adopted by governmental institutions, companies, and those proposed by academics and classify them based on the type of concerns the systems address, the required registration process, the adopted blockchain framework, and implementation status. We analyze the challenges blockchain e-voting systems face and how the reviewed systems address them, discuss security and privacy considerations, and suggest a few research directions to consider for trustworthy and more acceptable e-voting systems.

REFERENCES

[1] U. Can Cabuk, E. Adiguzel, and E. Karaarslan, "A survey on feasibility and suitability of blockchain techniques for the E-voting systems," 2020, *arXiv:2002.07175*.

[2] J. Ben-Nun, N. Fahri, M. Llewellyn, B. Riva, A. Rosen, A. Ta-Shma, and D. Wikström, "A new implementation of a dual (paper and cryptographic) voting system," in *Proc. 5th Int. Conf. Electron. Voting (EVOTE)*, 2012, pp. 315–329.

[3] S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas, and M. Namratha, "E-voting systems using blockchain: An exploratory literature survey," in *Proc. 2nd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Jul. 2020, pp. 890–895.

[4] S. A. Adeshina and A. Ojo, "Maintaining voting integrity using blockchain," in *Proc. 15th Int. Conf. Electron., Comput. Comput. (ICECCO)*, Dec. 2019, pp. 1–5.

[5] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A review of E-voting: The past, present and future," *Ann. Telecommun.*, vol. 71, nos. 7–8, pp. 279–286, Aug. 2016.

[6] R. Taş and Ö. Ö. Tanriöver, "A systematic review of challenges and opportunities of blockchain for E-voting," *Symmetry*, vol. 12, no. 8, p. 1328, Aug. 2020.

[7] P. Y. Ryan, D. Bismark, J. Heather, S. Schneider, and Z. Xia, "Prêt à Voter: A voter-verifiable voting system," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 662–673, Dec. 2009.

[8] S. Bell, J. Benaloh, M. D. Byrne, and D. DeBeauvoir, "STAR-Vote: A secure, transparent, auditable, and reliable voting system," in *Proc. Electron. Voting Technol. Workshop/Workshop Trustworthy Elections (EVT/WOTE)*, 2013, pp. 1–20.

[9] D. Lundin and P. Y. Ryan, "Human readable paper verification of Prêt à Voter," in *Proc. Eur. Symp. Res. Comput. Secur.* Berlin, Germany: Springer, 2008, pp. 379–395.

[10] S. M. T. Toapanta, G. A. C. Pacheco, D. W. B. Valencia, and L. E. M. Gallegos, "Optimization of an electronic signature scheme in a voting system in a distributed architecture," in *Proc. 2nd Int. Conf. Saf. Produce Informatization (IICSPI)*, Nov. 2019, pp. 593–596.

[11] S. Heiberg, K. Krips, J. Willemson, and P. Vinkel, "Facial recognition for remote electronic voting–missing piece of the puzzle or yet another liability?" in *Proc. Int. Workshop Emerg. Technol. Authorization Authentication*. Switzerland: Springer, 2021, pp. 77–93.

[12] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[13] V. Vijayalakshmi and S. Vimal, "A novel P2P based system with blockchain for secured voting scheme," in *Proc. 5th Int. Conf. Sci. Technol. Eng. Math. (ICONSTEM)*, Mar. 2019, pp. 153–156.

[14] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—Review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, 2021.

[15] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, "E-voting system based on blockchain technology: A survey," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Jul. 2021, pp. 200–205.

[16] Y. Abuidris, R. Kumar, and W. Wenyong, "A survey of blockchain based on E-voting systems," in *Proc. 2nd Int. Conf. Blockchain Technol. Appl.*, Dec. 2019, pp. 99–104.

[17] K. T. Sri, K. R. Sri, and N. Pedamallu, "E-voting system using blockchain," *J. Xi'an Univ. Archit. Technol.*, vol. 13, no. 5, pp. 527–533, 2021.

[18] V. Anilkumar, J. A. Joji, A. Afzal, and R. Sheik, "Blockchain simulation and development platforms: Survey, issues and challenges," in *Proc. Int. Conf. Intell. Comput. Control Syst. (ICCS)*, May 2019, pp. 935–939.

[19] T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in *Proc. 18th Annu. Int. Conf. Digit. Government Res.*, Jun. 2017, pp. 574–575.

[20] S. Salam and K. P. Kumar, "Survey on applications of blockchain in E-governance," *Revista Gestão Inovação e Tecnologias*, vol. 11, no. 4, pp. 3807–3822, Jul. 2021.

[21] I. Kubjas, "Using blockchain for enabling internet voting," Inst. Comput. Sci., Univ. Tartu, Tartu, Estonia, Tech. Rep. MTAT.03.323 Fall 2016, 2017. [Online]. Available: https://courses.cs.ut.ee/MTAT.03.323/2016_fall/uploads/Main/004.pdf

[22] Y. Abuidris, A. Hassan, A. Hadabi, and I. Elfadul, "Risks and opportunities of blockchain based on E-voting systems," in *Proc. 16th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process.*, Dec. 2019, pp. 365–368.

[23] V. Neziri, R. Dervishi, and B. Rexha, "Survey on using blockchain technologies in electronic voting systems," in *Proc. 25th Int. Conf. Circuits, Syst., Commun. Comput. (CSCC)*, Jul. 2021, pp. 61–65.

[24] F. Rabia, A. Sara, and T. Gadi, "A survey on e-voting based on blockchain," in *Proc. 4th Int. Conf. Netw., Inf. Syst. Acad. Manage. Perspect. Security.*, Apr. 2021, pp. 1–8.

[25] S. Kadam, K. Chavan, I. Kulkarni, and A. Patil, "Survey on digital E-voting system by using blockchain technology," *Int. J. Advance Sci. Res. Eng. Trends*, vol. 4, no. 2, pp. 5–8, Feb. 2019.

[26] S. Sayyad, M. Pawar, A. Patil, V. Pathare, P. Poduval, S. Sayyad, M. Pawar, A. Patil, V. Pathare, and P. Poduval, "Features of blockchain voting: A survey," *Int. J.*, vol. 5, pp. 12–14, Feb. 2019.

[27] A. Khandelwal, "Blockchain implimentation on E-voting system," in *Proc. Int. Conf. Intell. Sustain. Syst. (ICISS)*, Feb. 2019, pp. 385–388.

[28] M. Rezvani and H. Khani, "E-voting over blockchain platforms: A survey," *J. Netw. Secur. Data Mining*, vol. 2, no. 3, pp. 1–14, 2019.

[29] Y. Rosasooria, A. K. Mahamad, S. Saon, M. A. M. Isa, S. Yamaguchi, and M. A. Ahmadon, "E-voting on blockchain using solidity language," in *Proc. 3rd Int. Conf. Vocational Educ. Electr. Eng. (ICVEE)*, Oct. 2020, pp. 1–6.

[30] O. Cetinkaya and D. Cetinkaya, "Verification and validation issues in electronic voting," *Electron. journal E-Government*, vol. 5, no. 2, pp. 117–126, 2007.

[31] N. Kshetri and J. Voas, "Blockchain-enabled E-voting," *IEEE Softw.*, vol. 35, no. 4, pp. 95–99, Jul./Aug. 2018.

[32] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of blockchain solutions for E-voting: A systematic literature review," *IEEE Access*, vol. 10, pp. 70746–70759, 2022.

[33] K. Patidar and S. Jain, "Decentralized E-voting portal using blockchain," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–4.

[34] E. Yavuz, A. K. Koc, U. C. Cabuk, and G. Dalkilic, "Towards secure E-voting using ethereum blockchain," in *Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS)*, Mar. 2018, pp. 1–7.

[35] M. A. Cheema, N. Ashraf, A. Aftab, H. K. Qureshi, M. Kazim, and A. T. Azar, "Machine learning with blockchain for secure E-voting system," in *Proc. 1st Int. Conf. Smart Syst. Emerg. Technol. (SMARTTECH)*, Nov. 2020, pp. 177–182.

[36] D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb, "Decentralized voting platform based on ethereum blockchain," in *Proc. IEEE Int. Multidisciplinary Conf. Eng. Technol. (IMCET)*, Nov. 2018, pp. 1–6.

[37] S. Khan, A. Arshad, G. Mushtaq, A. Khalique, and T. Husein, "Implementation of decentralized blockchain E-voting," *EAI Endorsed Trans. Smart Cities*, vol. 4, no. 10, Jun. 2020, Art. no. 164859.

[38] F. Sheer Hardwick, A. Gioulis, R. Naeem Akram, and K. Markantonakis, "E-voting with blockchain: An E-voting protocol with decentralisation and voter privacy," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1561–1567.

[39] 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 *Proc. Int. Conf. Smart Innov. Design, Environ., Manage., Planning Comput. (ICSIDEMPC)*, Oct. 2020, pp. 176–180.

[40] K. Kost'al, R. Bencel, M. Ries, and I. Kotuliak, "Blockchain E-voting done right: Privacy and transparency with public blockchain," in *Proc. IEEE 10th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Oct. 2019, pp. 592–595.

[41] B. Ahn, "Implementation and early adoption of an ethereum-based electronic voting system for the prevention of fraudulent voting," *Sustainability*, vol. 14, no. 5, p. 2917, Mar. 2022.

[42] H. Yi, "Securing E-voting based on blockchain in P2P network," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–9, Dec. 2019.

[43] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in *Proc. 2nd World Conf. Smart Trends Syst., Secur. Sustainability (WorldS4)*, Oct. 2018, pp. 22–27.

[44] M. Pawlak, A. Poniszewska-Marańda, and N. Kryvinska, "Towards the intelligent agents for blockchain E-voting system," *Proc. Comput. Sci.*, vol. 141, pp. 239–246, Jan. 2018.

[45] A. Alam, S. M. Zia Ur Rashid, M. Abdus Salam, and A. Islam, "Towards blockchain-based E-voting system," in *Proc. Int. Conf. Innov. Sci., Eng. Technol. (ICISET)*, Oct. 2018, pp. 351–354.

[46] T. M. Roopak and R. Sumathi, "Electronic voting based on virtual ID of aadhar using blockchain technology," in *Proc. 2nd Int. Conf. Innov. Mech. for Ind. Appl. (ICIMIA)*, Mar. 2020, pp. 71–75.

[47] M. Doost, A. Kavousi, J. Mohajeri, and M. Salmasizadeh, "Analysis and improvement of an E-voting system based on blockchain," in *Proc. 28th Iranian Conf. Electr. Eng. (ICEE)*, Aug. 2020, pp. 1–4.

[48] R. Hanifatunnisa and B. Rahardjo, "Blockchain based E-voting recording system design," in *Proc. 11th Int. Conf. Telecommun. Syst. Services Appl. (TSSA)*, Oct. 2017, pp. 1–6.

[49] F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, "Crypto-voting, a blockchain based E-voting system," in *Proc. 10th Int. Joint Conf. Knowl. Discovery, Knowl. Eng. Knowl. Manage.*, 2018, pp. 221–225.

[50] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital voting: A blockchain-based E-voting system using biohash and smart contract," in *Proc. 3rd Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Aug. 2020, pp. 228–233.

[51] J. Goyal, M. Ahmed, and D. Gopalani, "A privacy preserving E-voting system with two-phase verification based on ethereum blockchain," *Preprint Res. Square*, pp. 1–33, Jun. 2022.

[52] K. Teja, M. Shravani, C. Y. Simha, and M. R. Kounte, "Secured voting through blockchain technology," in *Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI)*, Apr. 2019, pp. 1416–1419.

[53] B. Wang, J. Sun, Y. He, D. Pang, and N. Lu, "Large-scale election based on blockchain," *Proc. Comput. Sci.*, vol. 129, pp. 234–237, Jan. 2018.
[54] C. Denis González, D. Frias Mena, A. Massó Muñoz, O. Rojas, and G. Sosa-Gómez, "Electronic voting system using an enterprise blockchain," *Appl. Sci.*, vol. 12, no. 2, p. 531, Jan. 2022.
[55] X. Sun, Q. Wang, P. Kulicki, and M. Sopek, "A simple voting protocol on quantum blockchain," *Int. J. Theor. Phys.*, vol. 58, no. 1, pp. 275–281, Jan. 2019.
[56] S. Mishra, K. Thapliyal, S. Krish Rewanth, A. Parakh, and A. Pathak, "Anonymous voting scheme using quantum assisted blockchain," 2022, *arXiv:2206.03182*.
[57] R. Osgood, "The future of democracy: Blockchain voting," *COMP116: Inf. Secur.*, pp. 1–21, Dec. 2016.
[58] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," *Int. J. Netw. Secur. Appl.*, vol. 9, no. 3, pp. 1–9, 2017.
[59] Y. Liu and Q. Wang, "An E-voting protocol based on blockchain," Cryptol. ePrint Arch., 2017.
[60] O. Daramola and D. Thebus, "Architecture-centric evaluation of blockchain-based smart contract E-voting for national elections," *Informatics*, vol. 7, no. 2, p. 16, May 2020.
[61] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019.
[62] E. Febriyanto, N. Rahayu, K. Pangaribuan, and P. A. Sunarya, "Using blockchain data security management for E-voting systems," in *Proc. 8th Int. Conf. Cyber IT Service Manage. (CITSM)*, Oct. 2020, pp. 1–4.
[63] I. L. Awalu, P. H. Kook, and J. S. Lim, "Development of a distributed blockchain eVoting system," in *Proc. 10th Int. Conf. E-Business, Manage. Econ.*, Jul. 2019, pp. 207–216.
[64] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the design and implementation of a blockchain enabled E-voting application within IoT-oriented smart cities," *IEEE Access*, vol. 9, pp. 34165–34176, 2021.
[65] N. Faour, "Transparent E-Voting dApp based on waves blockchain and RIDE language," in *Proc. XVI Int. Symp. 'Problems Redundancy Inf. Control Syst.' (REDUNDANCY)*, Oct. 2019, pp. 219–223.
[66] P. Tarasov and H. Tewari, "The future of E-voting," *IADIS Int. J. Comput. Sci. Inf. Syst.*, vol. 12, no. 2, pp. 148–165, 2017.
[67] P. Martinson. *Estonia—The Digital Republic Secured by Blockchain—PWC*. [Online]. Available: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf
[68] *Estonia Blockchain Technology*. Accessed: Jan. 18, 2023. [Online]. Available: https://e-estonia.com/wp-content/uploads/2020mar-nochanges-faq-a4-v03-blockchain-1-1.pdf
[69] J. Vakarjuk, N. Snetkov, and J. Willemson, "Russian federal remote E-voting scheme of 2021–protocol description and analysis," in *Proc. Eur. Interdiscipl. Cybersecur. Conf. (EICC)*, 2022, pp. 29–35.
[70] (Apr. 2020). *South Korea Uses Blockchain Technology for Elections*. [Online]. Available: https://kryptomoney.com/south-korea-uses-blockchain-technology-for-elections/
[71] (2022). *Invote, an Online Voting Tool Developed by Scytl*. [Online]. Available: https://www.scytl.com/online-voting/invote/
[72] (2022). *Australia E-Voting—Blockchain Voting*. [Online]. Available: https://www.voteaustralia.org.au/blockchainvoting
[73] (2022). *Online Elections, Nominations & Voting With Polyas*. [Online]. Available: https://www.polyas.com
[74] G. E. G. Beroggi, "Secure and easy internet voting," *Computer*, vol. 41, no. 2, pp. 52–56, Feb. 2008.
[75] J. Gerlach and U. Gasser. *Three Case Studies From Switzerland: E-Voting—Berkman Klein Center*. [Online]. Available: https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-GasserSwissCasesEvoting.pdf
[76] *What is Agora Page*. Accessed: Jan. 18, 2023. [Online]. Available: https://www.agora.vote/about
[77] W. Long and A. Ernest. (May 2021). *Secure Decentralized Application Development*. [Online]. Available: https://followmyvote.com/
[78] (Mar. 2021). *Blockchain Technology in Online Voting*. [Online]. Available: https://followmyvote.com/blockchain-technology/
[79] *Netvote*. Accessed: Jan. 18, 2023. [Online]. Available: https://netvote.ch/
[80] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Sliema, Malta: Springer, 2017, pp. 357–375.
[81] A. Korunov, A. Sazonov, and P. Murzin, "Polys online voting system: Lessons learned from utilizing blockchain technology," in *Proc. E-Vote-ID*, 2021, p. 393.
[82] C. Harding. (Nov. 2019). *Online Voting and Blockchain: 'We've Been Using Blockchain for a While'*. [Online]. Available: https://www.polyas.de/blog/en/electoral-research/blockchain-online-voting
[83] K. Curran, "E-voting on the blockchain," *J. Brit. Blockchain Assoc.*, vol. 1, no. 2, p. 4451, 2018.
[84] K. L. Ohammah, S. Thomas, A. Obadiah, S. Mohammed, and Y. S. Lolo, "A survey on electronic voting on blockchain," in *Proc. IEEE Nigeria 4th Int. Conf. Disruptive Technol. Sustain. Develop. (NIGERCON)*, Apr. 2022, pp. 1–4.
[85] (Sep. 2020). *Home—Voatz Secure and Convenient Voting Anywhere*. [Online]. Available: https://voatz.com/
[86] J. Stern. (2021). *Votem Launches Proof of Vote—A Blockchain End-to-End Voter Verified Digital Voting System Protocol*. [Online]. Available: https://votem.com/
[87] *Votewatcher—The World's Most Transparent Voting Machine*. Accessed: Jan. 18, 2023. [Online]. Available: https://votewatcher.com/
[88] K. Kirby, A. Masi, and F. Maymi. *Votebook—Economist.Com*. Accessed: Jan. 18, 2023. [Online]. Available: https://www.economist.com/sites/default/files/nyu.pdf
[89] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: Problems and recommendations," *IEEE Access*, vol. 7, pp. 176838–176869, 2019.
[90] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–11.
[91] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.
[92] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
[93] K. Wüst and A. Gervais, "Do you need a blockchain?" *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 45–54.
[94] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab, "Blockchain for industry 4.0: A comprehensive review," *IEEE Access*, vol. 8, pp. 79764–79800, 2020.
[95] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," *IEEE Access*, vol. 7, pp. 77894–77904, 2019.
[96] A. Fatrah, S. El Kafhali, A. Haqiq, and K. Salah, "Proof of concept blockchain-based voting system," in *Proc. 4th Int. Conf. Big Data Internet Things*, Oct. 2019, pp. 1–5.
[97] (2016). *Nxt Whitepaper—Introduction: Nxt Whitepaper*. [Online]. Available: https://nxtdocs.jelurida.com/NxtWhitepaper
[98] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.
[99] M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," 2017, *arXiv:1710.06372*.
[100] M. H. Nasir, M. Imran, and J. S. Yang, "Study on E-voting systems: A blockchain based approach," in *Proc. IEEE Int. Conf. Consum. Electron.-Asia (ICCE-Asia)*, Nov. 2021, pp. 1–4.
[101] G. D. Arroyo, V. J. Díaz, and E. L. Hernández. (2019). *Blockchain*. [Online]. Available: https://aws.amazon.com/blockchain/decentralization-in-blockchain/#:~:text=In%20a%20decentralized%20blockchain%20network,the%20members%20in%20the%20network
[102] (Aug. 2022). *Decentralized vs. Centralized: A Detailed Comparison*. [Online]. Available: https://101blockchains.com/decentralized-vs-centralized/
[103] A. Abrol. (Nov. 2022). *Decentralized vs. Centralized: A Detailed Comparison*. [Online]. Available: https://www.blockchain-council.org/blockchain/decentralized-vs-centralized/
[104] I. Butun and P. Osterberg, "A review of distributed access control for blockchain systems towards securing the Internet of Things," *IEEE Access*, vol. 9, pp. 5428–5441, 2021.
[105] H. Hellani, L. Sliman, A. E. Samhat, and E. Exposito, "On blockchain integration with supply chain: Overview on data transparency," *Logistics*, vol. 5, no. 3, p. 46, Jul. 2021.

[106] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Exp.*, vol. 6, no. 2, pp. 93–97, Jun. 2020.

[107] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *Self-Published Paper*, vol. 19, no. 1, pp. 1–6, Aug. 2012.

[108] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, p. 1198, Sep. 2019.

[109] Y. Liu and G. Xu, "Fixed degree of decentralization DPoS consensus mechanism in blockchain based on adjacency vote and the average fuzziness of vague value," *Comput. Netw.*, vol. 199, Nov. 2021, Art. no. 108432.

[110] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019.

[111] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] Y," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014.

[112] A. Andrey and C. Petr, "Review of existing consensus algorithms blockchain," in *Proc. Int. Conf. 'Quality Manage., Transp. Inf. Secur., Inf. Technol.' (IT&QM&IS)*, Sep. 2019, pp. 124–127.

[113] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018.

[114] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in *Proc. IEEE 19th Int. Conf. High Perform. Comput. Commun.; IEEE 15th Int. Conf. Smart City; IEEE 3rd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, 2017, pp. 466–473.

[115] Z. Wang, H. Li, H. Wang, Z. Xiao, P. Lu, Z. Yang, M. Zhang, and P. H. J. Chong, "A data lightweight scheme for parallel proof of vote consensus," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2021, pp. 3656–3662.

[116] *Open Source P2P Money*. Accessed: Jan. 18, 2023. [Online]. Available: https://bitcoin.org/en/

[117] *What is Ethereum?* Accessed: Jan. 18, 2023. [Online]. Available: https://ethereum.org/en/what-is-ethereum/

[118] *Build Trust Into Business With Blockchain Technology*. Accessed: Jan. 18, 2023. [Online]. Available: https://exonum.com/index

[119] A. Baliga, N. Solanki, S. Verekar, A. Pednekar, P. Kamat, and S. Chatterjee, "Performance characterization of hyperledger fabric," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 65–74.

[120] *Hyperledger Foundatio—Hyperledger Fabric*. Accessed: Jan. 18, 2023. [Online]. Available: https://www.hyperledger.org/use/fabric

[121] F. T. H. Hjálmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjálmtỳsson, "Blockchain-based E-voting system," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 983–986.

[122] (Jun. 2021). *ZCash: How it Works*. [Online]. Available: https://z.cash/technology/

[123] O. Goldreich and Y. Oren, "Definitions and properties of zero-knowledge proof systems," *J. Cryptol.*, vol. 7, no. 1, pp. 1–32, Dec. 1994.

[124] F. Fatz, P. Hake, and P. Fettke, "Confidentiality-preserving validation of tax documents on the blockchain," in *Proc. Wirtschaftsinformatik (Zentrale Tracks)*, 2020, pp. 1262–1277.

[125] K. Sadia, M. Masuduzzaman, R. K. Paul, and A. Islam, "Blockchain-based secure E-voting with the assistance of smart contract," in *Proc. IC-BCT*. Singapore: Springer, 2020, pp. 161–176.

[126] M. R. Rahman, A. M. Tripathi, and G. Noida, "E-voting with blockchain technology," *YMER*, vol. 21, no. 5, pp. 641–644, May 2022.

[127] A. Poniszewska-Marańda, M. Pawlak, and J. Guziur, "Auditable blockchain voting system-the blockchain technology toward the electronic voting process," *Int. J. Web Grid Services*, vol. 16, no. 1, pp. 1–21, 2020.

[128] *Go Ethereum*. Accessed: Jan. 18, 2023. [Online]. Available: https://geth.ethereum.org/

[129] *The Crypto Wallet for Defi, Web3 Dapps and NFTs*. Accessed: Jan. 18, 2023. [Online]. Available: https://metamask.io/

[130] S. Semenzin, D. Rozas, and S. Hassan, "Blockchain-based application at a governmental level: Disruption or illusion? The case of Estonia," *Policy Soc.*, vol. 41, no. 3, pp. 386–401, 2022.

[131] A. Ojo and S. Adebayo, "Blockchain as a next generation government information infrastructure: A review of initiatives in D5 countries," in *Government 3.0—Next Generation Government Technology Infrastructure and Services*. 2017, pp. 283–298.

[132] N. Heller, "Estonia, the digital republic," The New Yorker, vol. 18, 2017.

[133] M. Goede, "E-Estonia: The E-government cases of Estonia, Singapore, and Curaçao," *Arch. Bus. Res.*, vol. 7, no. 2, pp. 1–13, 2019.

[134] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security analysis of the Estonian internet voting system," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 703–715.

[135] M. Jun, "Blockchain government—A next form of infrastructure for the twenty-first century," *J. Open Innov., Technol., Market, Complex.*, vol. 4, no. 1, p. 7, 2018.

[136] M. M. Olembo, P. Schmidt, and M. Volkamer, "Introducing verifiability in the POLYAS remote electronic voting system," in *Proc. 6th Int. Conf. Availability, Rel. Secur.*, Aug. 2011, pp. 127–134.

[137] D. Y. Marcos del Blanco and M. Gasco, "A protocolized, comparative study of helios voting and Scytl/iVote," in *Proc. 6th Int. Conf. eDemocracy eGovernment (ICEDEG)*, Apr. 2019, pp. 31–38.

[138] M. Hochstein. (Mar. 2018). *Moscow's Blockchain Voting Platform Adds Service for High-Rise Neighbors*. [Online]. Available: https://www.coindesk.com/markets/2018/03/15/moscows-blockchain-voting-platform-adds-service-for-high-rise-neighbors/

[139] M. D. Castillo. (Feb. 2018). *Russia is Leading the Push for Blockchain Democracy*. [Online]. Available: https://www.coindesk.com/markets/2018/02/21/russia-is-leading-the-push-for-blockchain-democracy/

[140] E. Akcagündüz, "Can blockchain technology increase participation in local governments? A review on blockchain-based voting systems in local governments," *R&S-Res. Stud. Anatolia J.*, vol. 5, no. 1, pp. 121–147, Jan. 2022.

[141] D. Di Francesco Maesa and P. Mori, "Blockchain 3.0 applications survey," *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, Apr. 2020.

[142] S. Panja, S. Bag, F. Hao, and B. Roy, "A smart contract system for decentralized Borda count voting," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1323–1339, Nov. 2020.

[143] (2022). *Polys Blockchain-the Technology for 21st Century Elections*. [Online]. Available: https://polys.vote/blockchain

[144] C. Culnane, A. Essex, S. J. Lewis, O. Pereira, and V. Teague, "Knights and knaves run elections: Internet voting and undetectable electoral fraud," *IEEE Secur. Privacy*, vol. 17, no. 4, pp. 62–70, Jul. 2019.

[145] L. Panizo Alonso, M. Gasco, D. Y. Marcos del Blanco, J. A. Hermida Alonso, J. Barrat, and H. Alaiz Moreton, "E-voting system evaluation based on the council of Europe recommendations: Helios voting," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 1, pp. 161–173, Jan. 2021.

MARIA-VICTORIA VLADUCU (Student Member, IEEE) received the B.S. degree (magna cum laude) in computer science and the M.S. degree (Hons.) in data science from the New York Institute of Technology, in 2021 and 2022, respectively. She has been a Research Assistant with the Network and Innovation Laboratory, New York Tech, since 2020. Her research interests include blockchain technologies, supply chain data analytics, and machine learning. She was a recipient of the Data Science Graduate Achievement Award, in 2022.

ZIQIAN DONG (Senior Member, IEEE) received the M.S. and Ph.D. degrees in electrical engineering from the New Jersey Institute of Technology (NJIT). She is currently a Professor with the Department of Electrical and Computer Engineering, New York Institute of Technology (NYIT). Her research interests include the architecture design and analysis of high-performance packet switches, data center networks, network security and forensics, wireless sensor networks, assistive medical devices, and data analytics and innovative sensing technology to improve the sustainability and resilience of both natural and built environments. She is a Senior Member of the IEEE Communications Society and IEEE Women in Engineering and a member of the American Society for Engineering Education (ASEE), ACM, and the Environmental Sensing, Networking and Decision-Making (ESND) Technical Committee. She was served on the Technical Program Committee for IEEE GLOBECOM, ICC, HPSR, Sarnoff, and GREENCOM, and a reviewer for IEEE journals, conferences, and the U.S. National Science Foundation panels. She was a recipient of the 2006 and 2007 Hashimoto Fellowship for Outstanding Scholarship, the 2008 Hashimoto Prize for the Best Ph.D. Dissertation in electrical engineering from NJIT, the New Jersey Inventors Hall of Fame Graduate Student Award for her inventions in network switches, the NYIT Presidential Engagement Award in Student Engagement in Research and Scholarship, and the 2020 ASEE Curtis W. McGraw Research Award.

JORGE MEDINA (Student Member, IEEE) received the B.Sc. degree in electrical and industrial engineering from La Universidad Nacional Autonóma de Honduras and the M.Sc. degree in telecommunication systems from The Blekinge Institute of Technology, Karlskrona, Sweden. He is currently pursuing the Ph.D. degree with the Networking Research Laboratory, Helen and John C. Hartmann Department of Electrical and Computer Engineering, New Jersey Institute of Technology (NJIT), Newark, NJ, USA. His research interests include computer networking, optimization, blockchain, e-health, and machine learning.

ROBERTO ROJAS-CESSA (Senior Member, IEEE) received the B.S. degree from Universidad Veracruzana, Mexico, the M.S. degree from the Research and Advanced Studies Center, Mexico, and the M.S. and Ph.D. degrees in computer and electrical engineering from Polytechnic University (currently, the New York University Tandon School of Engineering, Polytechnic Institute), Brooklyn, NY, USA. He is currently a Professor with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology (NJIT). He has authored the books *Advanced Internet Protocols, Services, and Applications* (Wiley, 2012) and *Interconnections for Computer Communications and Packet Networks* (CRC Press, 2017). His research interests include the wide area of networking, cyber-physical systems, energy, intelligent systems and learning, and emergency communications and systems. He was an Invited Fellow of the Japanese Society for the Advancement of Science, in 2009. He was a recipient of the Excellence Progress in Research by the Department of Electrical and Computer Engineering, in 2005. He was a recipient of the Excellence in Teaching Award from the Newark College of Engineering, NJIT, and the New Jersey Inventors Hall of Fame—Innovators Award, in 2013. He serves in different capacities for IEEE conferences and specialized journals as a reviewer and an editor, and as a Panelist for U.S. National Science Foundation and U.S. Department of Energy. He was the General Chair of IEEE Sarnoff Symposium 2011 and IEEE International Conference on High Performance Switching and Routing 2020. In addition, he has been the Technical Program Committee Chair of the two flagship conferences of the Communications Society: International Conference on Communications (ICC) and Global Communications (GLOBECOM).