IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Decentralized Voting Systems Using Blockchain: A Comprehensive Survey

Janardhan Singh, Anuj Kumar Yadav, Asim Alam, Ayush Raj, Deepak Gupta

Department of Information Science and Engineering

R.N.S Institute of Technology,Bangalore,India

Abstract

The use of electronic voting in elections for pub- lic office is becoming more common around the world. This trend can be attributed to the ad- vantages of these systems, such as remote voting capabilities and rapid vote counting. Addition- ally, electronic voting machines provide greater privacy and increase protection against fraudu- lent voting. Blockchain technology increases the power of the voting process through immutable voting process, thus reducing the threat of vote manipulation and maintaining the legitimacy of the election surge. The technology has been adopted by countries such as Germany, Russia, Estonia and Switzerland for use in electronic vot- ing systems. This study provides an overview of blockchain-based electronic voting systems cur- rently used by countries and companies and sug- gests academic research. Additionally, this study analyzes the challenges faced by blockchain elec- tronic voting systems and identifies areas for fu- ture research to improve the reliability of these systems.

1 Introduction

The implementation of electronic voting (e- voting) has the potential to transform the tra- ditional paper-based voting process into a more inclusive and accessible platform. This change will allow a large part of the population to partic- ipate in exercising their civil rights during elec- tions. Although electronic voting has been im- plemented in various elections as a supplement or alternative to personal voting, the issue of le- gality and authenticity remains an obstacle to wider adoption.

In the traditional ballot-based voting system, eligible voters must be registered at the TPS be- fore they can vote, as shown in Figure 1. Vot- ing can be done in person or by mail on Elec- tion Day. the second requires submission be- fore the deadline for vote counting. Introducing in-person voting makes it more widely accepted than electronic voting. However, this approach is criticized on several grounds.

Efforts to address concerns about electronic voting include implementing strong cyber secu- rity measures, ensuring voter privacy, and pro- viding a transparent and monitoring system. Additionally, educating the public about the se- curity features of electronic voting systems and conducting rigorous testing and auditing is animportant step in building trust in electronic vot-ing.

Despite these challenges, the potential bene- fits of electronic voting, such as increased ac- cess, faster results, and reduced environmental impact, make it an area of interest and growth. As technology and security measures improve, electronic voting may become more accepted and future-proof.

The implementation of electronic voting (e- voting) has the potential to transform the tra- ditional paper-based voting process into a more inclusive and accessible platform. This change will allow a large part of the population to par- ticipate in the exercise of civil rights during elec- tions [1], [2], [3], [4]. Although electronic voting has been implemented in various elections as a supplement or alternative to personal voting, the issue of legality and authenticity remains an ob- stacle to wider adoption.

In the traditional ballot-based voting system, eligible voters must be registered at the TPS be- fore they can vote, as shown in Figure 1. Vot- ing can be done in person or by mail on Elec- tion Day. the second requires submission be- fore the deadline for vote counting. Introducing in-person voting makes it more widely accepted than electronic voting. However, this approach has been criticized for being prone to disruptions such as severe weather conditions, natural disas- ters, lockdowns or long lines at polling stations [5]. In addition, the logistics of an in-person vot- ing system can be costly, requiring measures to verify voter identity, staff polling stations and ensure the integrity of marked ballots, and safe management and storage of paper counts. In some cases, the security of the population gath- ered at the TPS on election day can cause anxi- ety and increase the threat of terrorism [1].

Citizens are concerned about security, privacy, vote authenticity and voter identity in the con- text of electronic voting. For example, voter database storage may be vulnerable to hacking attacks and manipulation by unauthorized par- ties [6]. The lack of transparency in the elec- tronic voting system, the privacy measures im- plemented, and the less visible process for vote processing compared to ballots also cause prob- lems [1].

To solve these security and transparency is- sues, cryptographic and biometric authentica- tion have been proposed [2], [7], [8], [9], [10], [11]. However, a more comprehensive approach is needed to ensure the protection of the voter registration and voting process while protecting voter privacy and maintaining transparency inthe voting process.

Blockchain is a peer-to-peer (P2P) distributed ledger [12]. Its decentralized structure, com- bined with the use of consensus algorithms for blockchain and encrypted records, is a poten- tial solution to improve the security and trans- parency of the electronic voting system. This technology holds great promise for solving many of the security and transparency issues that elec- tronic voting systems face.

Therefore, it is not surprising that various countries are showing increasing interest in im- plementing blockchain-based electronic voting systems to improve their election process. This demand has also led many companies to develop products and academics to develop algorithms that make electronic voting systems fairer and more resistant to various electoral threats. Much of the literature focuses on blockchain-based de- velopment

The rest of this study is organized as follows: Part II defines the terminology including consen- sus algorithm, cryptography, and the properties of secure systems in electronic voting systems. Part III presents the e-voting system proposed by academics. Chapter IV outlines cellular elec- tronic voting systems already in use by govern- ments and companies. Part V discusses chal- lenges and future work. Section VI concludes this survey.

2 Terminology

Terminology related to blockchain e-voting sys- tems includes consensus algorithms, blockchain framework, cryptography, characteristics of a successful system, and development tools. These terms are outlined in Table 3.

2.1 Blockchain

Blockchain is a record of transactions distributed in a peer-to-peer (P2P) network [12]. It contains a series of blocks, each of which contains a set of records of checked operations. This block is implemented in the form of blocking [89], [90]. Each participating peer-to-peer or P2P network node verifies the block it receives, and when the majority of nodes reach consensus, adds the ver- ified block to the chain [91]. No entity can add or change blocks to the ledger without public consent [92]. In addition, the entries in the note- book are irreversible and cannot be altered or destroyed by any node in the network [12], [93], [94].

Blockchain combines the advantages of a consensus algorithm and a permissionless blockchain, and is scalable due to the lim- ited amount in the network. A permissioned blockchain is partially decentralized because different members can have different levels of control [105].

Cryptographic algorithms are used to ensure system integrity [95]. Blockchain's immutability feature.

2.2 Consensus Algorithms

Consensus Algorithms are protocols employed by blockchain to ensure that all ledgers in the nodes of a blockchain network are persistently consis- tent [98]. This survey reviews the following con- sensus algorithms used in blockchain e-voting systems: Proof of Work, Proof of Stake, Dele- gated 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 computation- ally 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 solu- tion. 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 algo- rithm that makes blockchain networks more effi- cient 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 se- lection methods, namely, the coin-age selection and the randomized block selection [108]. The coin-age selection method is based on the num- ber 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 simi- lar to PoS. In DPoS the nodes in the network se- lect 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 sig- nature, 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 possibil- ity of them being a forger. This approach aims to prevent double voting by implementing ex- tra scrutiny in the system and solves the issue of "the rich getting richer" in PoS [108]. How- ever, the known identity of the forgers makes the blockchain system vulnerable to collusion attacks [110]. Proof of Activity (PoA) is a consensus al- gorithm that combines PoW and PoS. First, all the miners compete to propose an empty block using PoW to prove its participation in the net- work 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 in- vest 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 dur- ing 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 increas- ing their stakes in the network [61]. Practical Byzantine Fault Tolerance (PBFT) is a consen- sus algorithm that has a primary node and sec- ondary nodes. The nodes establish a consen- sus algorithm to solve the Byzantine Generals Problem. The Byzantine Generals Problem is a game theory problem, which describes the dif- ficulty decentralized parties have in reaching a consensus without depending on any trusted cen- tral 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 so- lutions [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 pre- pare and commit phases both the primary and secondary nodes perform the service requested. In the reply phase, all the nodes send back a re-ply 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 ex- ecutive 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 chargeof the consortium.

2.3 Frameworks

Proof of Vote (PoV) is a consensus protocol based on a voting mechanism and a consortium blockchain. The PoV separates voting rights and executive rights. It mimics an election cam- paign by proposing four types of network par- ticipants, namely commissioners, butlers, butler candidates, and regular participants. The com- missioner is the highest member of this hierar- chy and is in charge of the consortium. But- ler is responsible for creating blocks in the net- work. Candidates for butler are entities from which butlers are elected. These three types of participants are involved in the administra- tive activities of the network, and ordinary par- ticipants can join and leave the network and vote without administrative rights [114]. Parallel Proof of Vote (PPoV) is an efficient permissioned PBFT consensus that allows multiple accoun- tants to generate blocks in a consensus cycle, im- proving system throughput. A PPoV has three roles: a bookkeeper, who can generate records and is responsible for packing client transactions into blocks; the voter receives the block from the accountant and votes on the legality of the block; and a leader who is in charge of collect- ing votes from voters and generating a complete bloc. Each consensus cycle has a unique leader selected from the accountants [115].

2.4 Cryptography

In this section, we present the cryptographic al- gorithms used in the blockchain electronic voting system. Hashing is the process of mapping ar- bitrary and variable-sized inputs to a fixed size. It uses a mathematical function that takes data as input and outputs a suitable string for an un- intended recipient [24]. A blind signature is a mathematical scheme used to verify the authen- ticity of an encrypted digital message or docu- ment before the message is signed. Used to en- ter encrypted messages. The sender's message is blinded before the receiver is signed [59]. A Merkle tree is a cryptographic tree where the nodes, called leaf nodes, are uniquely identified by the cryptographic hash of the data block [50]. Other nodes that are not leaf nodes are called branches, internal nodes, or inodes. The inode is marked with a cryptographic hash of the child node record [35]. The trusted hashing algorithm (SHA) is a set of cryptographic hash functions published by the United States National Secu- rity Agency. There are several versions of SHA. SHA-256 takes an input of any length and uses it to produce a 256-bitfixed-length value that tries to find two inputs that produce the same Hash value. Acollisionattack is a cryptographic attack. SHA-256 and SHA-512 are hash func- tions that are considered collision resistant and secure [61]. Zero-Knowledge Proof (ZKP) is a cryptographic mechanism by which one party, called the sender, can prove to another party, called the verifier, a message without revealing its content [123]. This scheme requires transfer and validator. The report does not provide ad- ditional information regardless of the accuracy of the report [96]. ZKP increases the level of system transparency. This can be used for any sensitive information. ZKP adds a layer of secu- rity to the blockchain and can be integrated with other blockchain

systems [105], [124].

2.5 Characteristics of a successfull system

In some works, voting and control studies [4], [14], [30], [59], [63], [98], [125], [126], [127]. We define this feature here. Accuracy is the hall- mark of electronic voting systems to ensure that all votes cast are correctly counted and that the declared results are accurate with the results of the election. This feature ensures that no one can change someone else's vote and that the final result includes all valid votes [125]. Anonymity is a feature of the system that protects the personal information of voters and the candidates they vote for. Unlike personal information, voters use their created addresses to conduct transactions and other interactions on the blockchain [126]. Auditing is a property used to record and verify transactions so that the data in the notebook is transparent and reviewable. All recorded trans- actions can be traced by sequentially searching the log block [63]. Voting is a feature of the electronic voting system where only eligible vot- ers can participate in the election. If the voter has the right to vote, the system check will de- termine the requirements [14]. Integrity is the property that guarantees that the sound cannot be overwritten in any way [4]. Privacy is a fea- ture of the system that ensures that there is no connection between voters and their votes. Vot- ers and who they vote for should not be iden- tified [30]. Reliability is a property of a system where all active nodes maintain a complete copy of the block record. A closed electronic voting system is secure if everyone has a copy of the voting procedure for inspection [58]. Security is the ownership of an electronic voting system that is immune from attacks and attacks against voter identification and the voting process. The system is robust when appropriate measures are taken so that voting is not subject to manipula- tion [126]. Transparency is the property of the system that maintains the complete history of past transactions in the network, so users can track the complete history of information in the system [127]. Verification is where voters must confirm that their ballots have been counted cor-rectly [30].

3 Tools

Tools that can be used to implement a blockchain e-voting system include:

Considered for testing and developing dis- tributed applications in Ethereum [37], [39], [52] is a local blockchain. Go-Ethereum/Geth is an implementation Ethereum blockchain that runs smart contracts and applications using the Go programming language. It has an alternative de- centralized mechanism based on PoW, PoS or PoA [128]. MetaMask is a browser-based wal- let application that manages keys, transactions and user accounts in blockchain networks. It connects the web client to the Ethereum net- work [129]. Truffle is a development framework that includes a collection of tools for building and developing blockchain applications in the Ethereum network [18], [39].

4 Academic Proposals

This section summarizes and categorizes current proposals for electronic voting systems based on the problems they aim to address. The account- ing method, the type of framework implemented, and whether it is a conceptual or implemented framework are shown in Table 5. If the registra- tion method is part of the proposed blockchain and the registration is completed, it is registered externally. by a trusted third party or through a verified database provided by the government or a reputable organization, or in some cases the registration process is not mentioned in the literature. Awalu et al. [63] solved the prob- lem of system accuracy by proposing a theoreti- cal model based on permuted blocking to ensure that all votes are counted. System registration is done internally. The system uses a unique iden- tity to register, vote and count votes to deliver election results. The system ensures the confi- dentiality of the type of vote so that the results are not biased in the final stage of voting and the generated vote report is cast only after the election is over. Most of the proposed systems that solve the anonymity problem follow theo- retical approaches [50], [66], [55], [58] or embed- ded systems [33]. Tarasov and Tewari [66] and Patidar and Jain [33] presented the Ethereum model, while Gun et al. [55] Use Quantum Blockchain. A unique genesis block representing a candidate serves as a foundation, also known as a genesis block. All candidate votes were as- sociated with the genesis block [58]. There is no connection between the voter's identity and the ballot. Quantum secure communication pre- vents voters from accessing ballots that are not theirs [55]. Biohash, which washes users' bio- metric data, has been implemented to protect the identity of voters [50]. Here, voters are given a public key to access the system and authen- ticate themselves to vote with their fingerprints and voter ID. Audition Avalu et al. [63] pro- posed a theoretical model based on permissive blocking, Fusco et al. [49] proposed a blockchain cryptographic model using ZCash. Registration for both systems is done internally. To ensure the verifiability of voting results, automatically generated vote numbers are proposed using the blockchain network architecture [63]. Fusco et al.] Integrity has been addressed by various proposed systems. Most of these proposed sys- tems follow a theoretical approach, Khoury et al. [36] and Khan et al. [37] implemented a system using Ethereum. To avoid fraud, only trusted miners can participate in the consensus process [63]. The blind signature used by Liu and Wang [59] protects the voter's identity and guarantees that there is no connection between the person and the candidate they vote for. The observer approach, together with the introduc- tion of institutions that limit the power of the organizer, ensures a fair choice [59]. Khoury et al. [36] proposed to combine two different smart contracts, namely the registration contract and the voting contract. The registration agreement is installed once for all voters and deals with reg- istration and verification. Voting contracts are written once in the development phase and dis- tributed multiple times depending on the elec- tion. Simple random sampling was used to de- termine the reliability of the survey on the use of blocking in electronic voting [62].

Privacy has been addressed in theoretical and practical approaches. Ethereum is the most considered framework. However, Blockchain Biometrics us- ing Bitcoin [47], Quantum Blockchain [56] and Internet of Things (IoT) devices are also consid- ered. Wang et al.] A two-phase screening was also adopted for voters before voting [51]. Bio- metrics are also adopted to protect voter privacy [45]. Some proposals provide privacy for the en- tire system [38], [47], [50], while others focus only
on voter privacy [13], [33], [37], [45], [53]. The reliability of Gonzalez et al. [54] proposed a the- oretical framework based on Hyperledger Fabric, while Awuz et al. [34] proposed an implementa- tion model using Ethereum. The reliability fea- ture is based on the robustness of the Ethereum framework [34]. The voting system is divided into three main phases: the first

5 . Systems used by gover- ment instuitions and com-panies

There are numerous commercial blockchain e- voting systems developed by governments and organizations as well as companies. We review some popular ones in this section.

5.1 Systems used by Goverment Institutions and Companies

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 sum- marizes the countries and regions that imple- mented blockchain in their voting processes. Es- tonia, Australia, Norway, and Switzerland have implemented evoting pilots for binding elections. Estonia has provided e-voting options for every election and census since 2013, while other coun- tries such as India and Japan are in the process of developing e-voting systems for future elec- tions [67]. Australia, Germany, Norway, Sierra Leone, and Switzerland use commercial systems to conduct blockchain-based evoting [13], [31],
[57], [72], [74], [75]. Estonia, Russia, South Ko- rea, 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 popula- tion a choice to use either e-voting or inperson elections that lasted for 7 days, about 21.2% of the population voted using e-voting. The system has partially decentralized software, that pro- vides anonymity and voter verification [134]. It needs the Internet and an Electronic National Identification Card that is used for authenti- cation, encryption, and signature [67]. Voters need to download the voting application, au- thenticate using the electronic ID, and if eligi- ble, 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]. Nor- way used e-voting in 2011 for council elections [58]. The software is anonymous and partially decentralized. The Sierra Leone used Agora as their e-voting system for the presidential elec- tion in 2018 representing the first time in his-tory that blockchain technology was used in a presidential election [31], [76]. In South Ko- rea, 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. Vot- ers 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 im- plemented e-voting using blockchain for differ- ent elections. Massachusetts used Votez for stu- dent government elections, church-group, NGO, union voting, subnational politicalparty 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].

5.2 Commercial Blockchain BasedE-voting System

This section presents some popular commercial blockchain e-voting systems developed by com- panies and how they are used. Table 7 sum- marizes 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 permis- sioned 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 mem- bers participated in 2017. It was also used in wevotem Sierra Leone [16], [31]. The citi- zens' identity was verified by ID card and their ballot was later manually entered into a pri- vate 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 vot- ers themselves while keeping

user privacy [83]. Follow My Vote is a secure web-based, decen- tralized 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 iden- tity 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 (pass- port, etc) to an Identity Identifier that would be already approved by the organization hold- ing 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]. Lux- oft 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 Ire- land, to increase security and reduce data loss risks [83].

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-netisatwo-rounddecentralizedprotocolimplemented 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 votingprocessinreal-timewithoutcompromisinganonymity. Voters can verify that their votes have been recorded on the blockchain and counted correctly [143]. They state that the systems are se- cure, transparent, and auditable, but they still have many challenges such as scalabil- ity, 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 com-prehensive explanation of what users vote exactly about. The election has threemain-components:publicPoll,votelimit,andtimeLimit.
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.

6 Conclusion

With the rapid development and adoption of blockchain technology, interest in creating a mi- gration system using blockchain technology is in- creasing. The survey examines traditional, elec- tronic and block voting systems. Categorizes terminology used in implementing and deploy- ing blockchain-based systems, including consen- sus algorithms, frameworks, performance evalu- ation, characteristics of successful systems, cryp- tography, and tools to implement such sys- tems. We provide an updated review of current blockchain electronic election systems proposed by government agencies, companies, and aca- demics, and categorize the systems in terms of address, required registration process, adopted blockchain framework, and implementation. sit- uation We discuss the challenges faced by e- voting systems and how the reviewed systems overcome them, security and privacy issues, and suggest some research directions to consider for a safer and more secure e-voting system.

7 References

1 U. Can Cabuk, E. Adiguzel, and E. Karaarslan, "Study on Feasibility and Suit- ability of Blocking Techniques for Electronic Voting Systems," 2020, arXiv: 2002.07175.

2 J. Ben-Nun, N. Fahri, M. Llewellin, B. Riva, A. Rosen, A. Ta-Shma, and D. Wik- ström, "A two-way voting (paper and cryp- tographic) system , "Pros. 5 Int. Conf. Electronics. EVOTE, 2012, pages 315–329.

3 S. K. Vivek, R. S. Ashashank, Y. Prashanth, N. Ashhashas and M. Namratha, "Elec- tronic Voting Systems Using Blocks: An Ex- ploratory Survey of the Literature". 2nd Int. Conf. Inventor Res. Account. Pro- gram. (ICIRCA), July 2020, pages 890–895.

4 S. A. Adeshina and A. Ojo, "Maintaining the integrity of voting through blocking". 15 Int. Conf. Electronics, Accounting. Ac- count. (ICECCO), December 2019, pages 1-5.

5 J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A Review of Electronic Vot- ing: Past, Present, and Future," Ann. Telecommunications, volume 71, pages 7–8, 279–286, August 2016. elements [6] R. Tash and O. O. Tanriver, "A systematic review of the challenges and opportunities for bar- riers to electronic voting," Symmetry, vol. 12, no. 8, p. August 1328.

7 P. Y. Ryan, D. Bismarck, J. Heather, S. Schneider, and Z. Xia, "PrêtàVoter: A Voter-Verifiable Voting System," IEEE Trans. Inf. Forensic Security, Volume 4, No. 4, pp. 662–673, December 2009. item [8] S. Bell, J. Benaloh, M. D. Byrne, and D. DeBeauvoir, "Star-Sora: A Safe, Transparent, Audible, and Trusted Vot- ing System". Electronics. Sound technol- ogy. Bengkel/Workshop on Safe Elections(EVT/WOTE), 2013, page 1-20.

9 D. Lundin and P. Y. Ryan, "Human read- able paper test of Prêt à Voter". house Symp. Res. Account. Safe. Berlin, Ger- many: Springer, 2008, pp. 379-395.

10 S. M. T. Toapanta, G. A. C. Pacheco, D. W. B. Valencia and L. E. M. Gallegos, "Opti- mizing electronic signature schemes in voice networks in a distributed architecture". 2nd Int. Conf. Can be relied upon. Manufac- turing Informatization (IICSPI), November 2019, 593–596.

11 S. Heiberg, K. Krips, J. Willemson and P. Winkel, " Remote electronic voting applica- tions, missing pieces of the puzzle or other liabilities? " Int. Workshop Technol. Con- firm authorization. Switzerland: Springer, 2021, pp. 77–93.

12 A. A. Monrath, O. Schelen, and K. Anders- son, "Construction research in terms of ap- plications, challenges, and opportunities," IEEE Access, vol. 7, 117134–117151, 2019.

13 V. Vijayalakshmi and S. Vimal, "A New P2P-Based Network for Block Voting Scheme". 5. Int. Conf. Science. Tech- nology. Eng. Mathematics. (ICONSTEM), March 2019, page 153-156.U. Jafar, M. J. A. Aziz, and Z. Shukur, "Bags for Electronic Voting System - Re- view and Open Research Challenges," Sen- sor, vol. 21, no. 17, p. 5874, 2021.

14 S. Al-Maitah, M. Katawneh and A. Kuz- mar, "Electronic Voting System Based on Blockchain Technology: A Survey". Int. Conf. Inf. Technology. (ICIT), July 2021,pages 200–205.

15 Y. Abuidris, R. Kumar, and W. Wenyong, "Looking for blocking based on electronic voting system". 2nd Int. Conf. Blockchain technology. Proceedings, December 2019, p.99-104.

16 K. T. Sri, K. R. Sri and N. Pedamallu, "Electronic Voting System by Block," J.Sian Univ. Architecture. Technology. 13, no. 5, pages 527-533, 2021.

17 V. Anilkumar, J. A. Joji, A. Afzal, and R. Shaikh, "Blockchain Simulation and De- velopment Platforms: Research, Issues and Challenges". Int. Conf. Intel. Account. Control system. (ICCS), May 2019, pages 935-939.

18 T. Moura and A. Gomes, "Blockchain Vot- ing and its Impact on Election Transparency and Voter Confidence". 18 Annu. Int. Conf. No. Government Res., June, 2017, 574-575.

19 S. Salam and K. P. Kumar, "A study of the application of algorithms in e-governance," Revista Gestão Inovação e Tecnologias, vol. 11, no. 4, 3807–3822, July 2021.

20 I. Kubjas, "Using blockchain to enable on- line voting," Inst. Account. Science. Tartu, Tartu, Estonia, Tech. Deputy MTAT.03.323Fall

21 Y. Abuidris, A. Hassan, A. Hadabi and I. Elfadul, "Risks and Opportunities of Block- ing Based on Electronic Voting System".
16. Int. Account. Conf. Law of waves. Media Technol. Inf. Proceedings, Decem- ber 2019, pages 365–368.

22 V. Neziri, R. Dervishi, and B. Reksha, "A Study on Application of Blocking Technolo- gies in Electronic Voting Systems". 25. Int. Conf. Chain, System, Communication Cal. (CSCC), July 2021, pages 61–65.

23 F. Rabia, A. Sara and T. Gadi, "Elec- tronic Voting Based S. Kadam, K. Chavan,

26 Kulkarni, and A. Patil, "Survey on digital Evoting system by using blockchain technol- ogy," Int. J. Advance Sci. Res.

27 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.

28 A. Khandelwal, "Blockchain implimenta- tion on E-voting system," in Proc. Int. Conf. Intell. Sustain. Syst. (ICISS), Feb.2019, pp. 385–388.

29 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.

30 Y. Rosasooria, A. K. Mahamad, S. Saon, M. A. M. Isa, S. Yamaguchi, and M. A. Ah- madon, "E-voting on blockchain using so- lidity language,"

in Proc. 3rd Int. Conf. Vocational Educ. Electr. Eng. (ICVEE), Oct. 2020, pp. 1–6.

31 O. Cetinkaya and D. Cetinkaya, "Verifica- tion and validation issues in electronic vot- ing," Electron. journal E-Government, vol. 5, no. 2, pp. 117–126, 2007.

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

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

34 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.

35 E. Yavuz, A. K. Koc, U. C. Cabuk, and G. Dalkilic, "Towards secure Evoting us- ing ethereum blockchain," in Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS), Mar. 2018, pp. 1–7.

36 M. A. Cheema, N. Ashraf, A. Aftab, H. K. Qureshi, M. Kazim, and A. T. Azar, "Ma- chine learning with blockchain for secure E- voting system," in Proc. 1st Int. Conf. Smart Syst. Emerg. Technol. (SMART- TECH), Nov. 2020, pp. 177–182.

37 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. (Green- Com) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData),Jul. 2018, pp. 1561–1567.

39 A. M. Al-madani, A. T. Gaikwad, V. Ma- hale, 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., Man- age., 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 adop- tion of an ethereum-based electronic vot- ing system for the prevention of fraudu- lent voting," Sustainability, vol. 14, no. 5, p. 2917, Mar. 2022. [42] H. Yi, "Secur-

50 Manage., 2018, pp. 221–225.

ing 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 blockchainbased electronic vot- ing 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 us- ing 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, "Cryptovoting, a blockchain based E-voting system," in Proc. 10th Int. Joint Conf. Knowl. Discovery, Knowl. Eng. Knowl.