The Application of the Blockchain Technology in Voting Systems: A Review

JUN HUANG and DEBIAO HE, School of Cyber Science and Engineering, Wuhan University, China and Cyberspace Security Research Center, Peng Cheng Laboratory, China
MOHAMMAD S. OBAIDAT, Fellow of IEEE and Fellow of SCS, Founding Dean and Professor, College of Computing and Informatics, University of Sharjah, UAE, King Abdullah II School of Information Technology, University of Jordan, Jordan, and University of Science and Technology Beijing, China
PANDI VIJAYAKUMAR, Department of Computer Science and Engineering, University College of Engineering Tindivanam, India
MIN LUO, School of Cyber Science and Engineering, Wuhan University, China and Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), China
KIM-KWANG RAYMOND CHOO, Department of Information Systems and Cyber Security, University of Texas at San Antonio, USA

Voting is a formal expression of opinion or choice, either positive or negative, made by an individual or a group of individuals. However, conventional voting systems tend to be centralized, which are known to suffer from security and efficiency limitations. Hence, there has been a trend of moving to decentralized voting systems, such as those based on blockchain. The latter is a decentralized digital ledger in a peer-to-peer network, where a copy of the append-only ledger of digitally signed and encrypted transactions is maintained by each participant. Therefore, in this article, we perform a comprehensive review of blockchain-based voting systems and classify them based on a number of features (e.g., the types of blockchain used, the consensus approaches used, and the scale of participants). By systematically analyzing and comparing the different blockchain-based voting systems, we also identify a number of limitations and research opportunities. Hopefully, this survey

The work was supported by the National Natural Science Foundation of China (Nos. 61972294 and 61932016), the Special Project on Science and Technology Program of Hubei Provience (No. 2020AEA013), the Natural Science Foundation of Hubei Province (No. 2020CFA052) and the Wuhan Municipal Science and Technology Project (No. 2020010601012187). The work of K.-K. R. Choo was supported only by the Cloud Technology Endowed Professorship.
Authors' addresses: J. Huang and D. He, School of Cyber Science and Engineering, Wuhan University, Wuhan, China, 430072, Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen, China, 518000; emails: hj10007@whu.edu.cn, hedebiao@163.com; M. S. Obaidat, Fellow of IEEE and Fellow of SCS, College of Computing and Informatics, University of Sharjah, Sharjah, UAE, 27272, King Abdullah II School of Information Technology, University of Jordan, Amman, Jordan, 11942, University of Science and Technology Beijing, Beijing, China, 100083; email: msobaidat@gmail.com; P. Vijayakumar, Department of Computer Science and Engineering, University College of Engineering Tindivanam, Viluppuram, India, 604001; email: vijibond2000@gmail.com; M. Luo, School of Cyber Science and Engineering, Wuhan University, Wuhan, China, 430072 and Shandong Provincial Key Laboratory of Computer Networks, Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan, China, 250014; email: mluo@whu.edu.cn; K.-K. R. Choo, Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, USA, TX 78249; email: raymond.choo@fulbrightmail.org.

0360-0300/2021/04-ART60 $15.00
https://doi.org/10.1145/3439725

will provide an in-depth insight into the potential utility of blockchain in voting systems and device future research agenda.

CCS Concepts: • **Security and privacy → Cryptography**; **Domain-specific security and privacy architectures**; **Privacy-preserving protocols**;

Additional Key Words and Phrases: Blockchain, blockchain-based voting systems, E-voting, privacy protection

ACM Reference format:
Jun Huang, Debiao He, Mohammad S. Obaidat, Pandi Vijayakumar, Min Luo, and Kim-Kwang Raymond Choo. 2021. The Application of the Blockchain Technology in Voting Systems: A Review. *ACM Comput. Surv.* 54, 3, Article 60 (April 2021), 28 pages.
https://doi.org/10.1145/3439725

1 INTRODUCTION

Voting systems have gradually moved away from paper ballots and voting stations.[1] In recent times, there has been a gradual shift to using electronic voting systems. In such a system, voters (including overseas voters) can vote online, and the votes can be processed in real time. Finally, the voting records and the results will be stored and managed in some database, which is generally centralized (e.g., held by the nation's electoral commission). Conventional paper-based voting systems are still used in many scenarios. They are known to have a number of shortcomings. First, the paper ballots are processed by the staf,f and hence there is the possibility of accidental or intentional modification of ballot content. In addition, depending on the actual setup (e.g., in authoritarian nations), voters may be subject to physical coercion. Since the voting records and results are stored and managed centrally, it can be challenging for voters to verify that their votes were counted correctly. There is always the risk that voting records and results of being destroyed due to some natural or human factors (e.g., natural disasters such as floodings, earthquakes or arson).

While electronic voting systems can potentially improve security and efficiency of the voting processes in theory, the benefits have not truly been translated to practice. In addition to the existing concerns about the use of electronic voting systems in U.S. elections, there are limitations associated with the centralized storing and managing of voting records and results [18, 20]. Hence, there have been recent efforts to design decentralized electronic voting systems, such as those based on blockchain. Blockchain is a decentralized digital ledger in a peer-to-peer (P2P) network, where a copy of the append-only ledger of digitally signed and encrypted transactions is maintained by each participant. Blockchain underpins cryptocurrencies such as Bitcoin and also smart contracts such as Ethereum.

Blockchain has a number of characteristics (e.g., decentralization, transparency, and immutability) that make it attractive for designing decentralized electronic voting systems. For example, participants can use blockchain address to represent their identities; hence, achieving pseudo-anonymity. All operations in conventional voting systems can be defined as transactions or transfer of virtual assets between voters and candidates. Moreover, the contents of transactions can be encrypted to protect participants' privacy. The number of votes that a candidate gets are the amount of transactions or virtual assets that the candidate's address receives. After the voting process concludes, all transactions related to the voting event will be stored in a distributed blockchain permanently and irreversibly; hence, ensuring the integrity of the voting process. Stakeholders

[1]In a conventional paper voting system, voters visit the nearest polling station to cast their ballots. After the polling deadline, all ballots will be counted manually by some trusted entity, such as the nation's electoral commission. Eventually, the casted ballots and voting results will be securely stored and managed in some archival venue for a predetermined period of time.

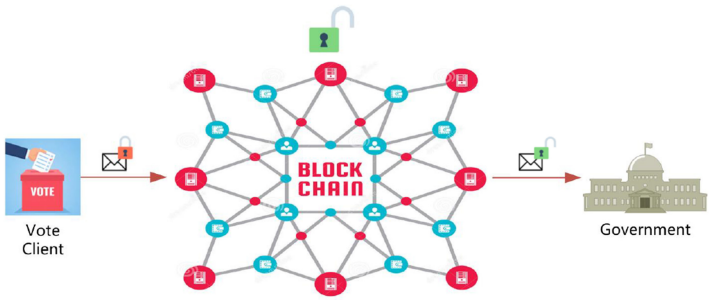

Fig. 1. The logic of blockchain-based e-voting.

and participants can review and verify the voting records anytime and anywhere. The logic of blockchain-based e-voting [34] is shown in Figure 1.

In theory, blockchain-based voting systems have a number of advantages over conventional ones such as decentralization, transparency, and immutability.

(1) *Decentralization.* Every node in the blockchain network has a full backup of all transactions. Hence, the failure or unavailability of a single node will not impact on the entire blockchain network. This makes blockchain-based voting systems more robust.
(2) *Transparency.* Once the voting records are stored in blockchain as transactions, they can be reviewed and verified with minimal risk of modification. Thus, blockchain-based voting systems are more credible.
(3) *Immutability.* Once the transactions are validated and appended to blockchain, the results cannot be modified anymore, which is guaranteed by the use of secure hash functions. The modification of the blockchain in a single node will not impact the consistency of entire blockchain network.

Despite its promises, existing blockchain platforms still have a number of challenges such as those associated with throughput, privacy, and authentication.

(1) *Throughput.* Throughput is measured as the number of successful transactions per second. In a national election event, a large number of voting transactions will be generated within a short period of time, which require high throughput in the blockchain network. However, existing blockchain platforms, especially public blockchain platforms, usually do not have a high throughput. For example, Bitcoin network has a Transaction Per Second (TPS) of about 7 [16], Ethereum platform has a TPS of about 8 [15], and Hyperledger Fabric platform has a TPS between 40 and 500 [44].
(2) *Privacy.* Blockchain addresses are generated at random, it is partially helpful for voters to cast their votes anonymously. However, the study of References [4, 22] has shown that a user's Bitcoin transactions can be linked to reveal user's information. Biryukov et al. [5] also presented a method to link user pseudonyms to IP addresses, even when users are behind network address translation or firewalls. This posed personal safety risks to the voters, particularly in authoritarian nations.
(3) *Authentication.* The current authentication schemes in computing systems require human cognitive ability to remember numerous complex ID and password or rely on a trusted third-party (TTP) and consequently have an additional attack vector [55]. In a distributed blockchain environment, especially those that do not rely on a TTP, it can be challenging to implement a secure method of authentication.

The interest in blockchain-based electronic voting systems is partly evidenced by the small number of literature review and survey articles on the topic. For example, in Reference [50] the authors surveyed the features of blockchain-based voting systems. However, there is insufficient use cases and depth of technical analysis. The authors of Reference [32] analyzed both institutional and technical problems that may occur when applying blockchain to online voting systems. However, the use cases are analyzed independently, and there is no comparison between these use cases. In Reference [31], a literature review of several existing proposals were presented, as well as their proposed methods and limitations. However, the review lacks technical analysis. In Reference [1], a systematic survey of different blockchain-based voting systems focusing on the feasibility and suitability of blockchain was presented. However, no use cases are discussed.

Seeking to contribute to the literature gap, in this article, we first revisit blockchain, prior to presenting a systematic analysis and comparison of different blockchain-based voting systems. Based on the review, we then identify a number of future directions.

The rest of the article is organized as follows. The next section presents the conventional voting systems and their shortcomings. The next two sections present an overview of blockchain technologies and the challenges in blockchain-based voting systems. In the Section 5 and Section 6, we will review some blockchain-based voting systems that are used as voting systems. In Section 7, we present the comparison and analysis for the reviewed voting systems. In the Section 8, we provide some broader perspectives for blockchain-based voting systems. Finally, we conclude this article in the last section.

2 CONVENTIONAL VOTING SYSTEMS

In this article, we broadly define manual (or paper-based) voting systems and the now electronic voting systems to be conventional voting systems, since they have the same design principles and security level. Next, we are going to introduce such a general conventional voting model and the associated challenges.

2.1 Conventional Voting Model

Voting systems are very common in our daily life, as they are used to help express our opinions collectively. In a nation, state, province, or county, citizens can vote to decide whether a proposal can be passed or not. In a company, board members vote on important decisions. In a school, students and teachers vote on who will hold a position.

Voting systems are organized differently and target different groups. However, they generally follow the same voting principles and have the same goal of reflecting the will of the voters as much as possible. The followings are common principles for a voting system [25].

(1) *Secret ballot principle.* The real identity of the voter should not be recorded in the ballot.
(2) *Equal voting rights.* Every voter has the same right to vote, except in some cases where the weight of vote is considered.
(3) *Freedom of ballot filling.* Voters must not be coerced or enticed for any reason.
(4) *Candidate does not need to be present.* Candidates may not be present at the voting.
(5) *Voting results are final.* After the polls close, the election results must agree to the voting results.
(6) *Voting results cannot be modified.* After the result of the vote is determined, no changes can be made.

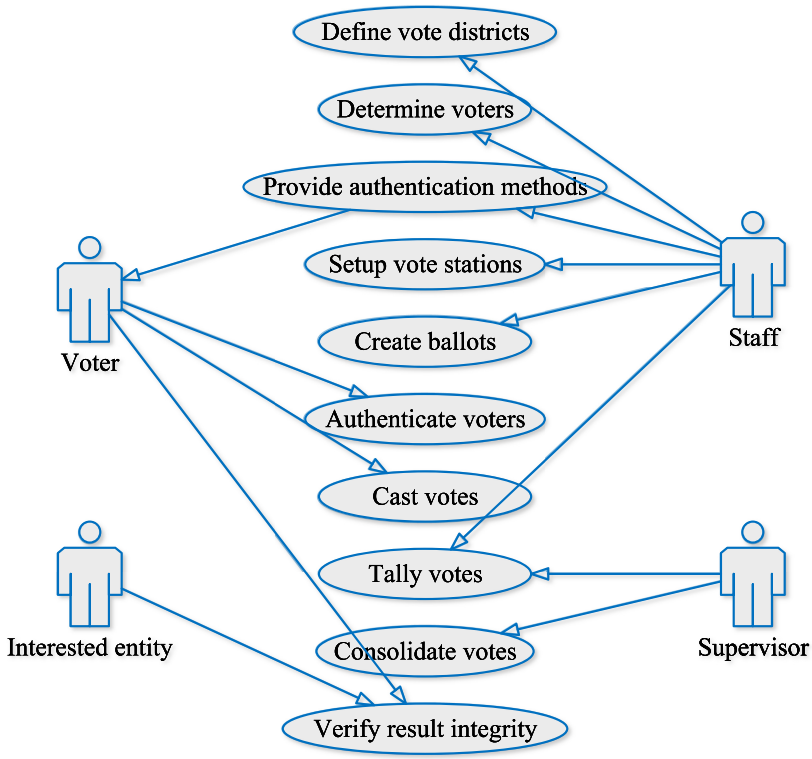

Fig. 2. Use cases for a general elections voting model.

Gritzalis [25] provided a general model for conventional voting systems, and the use cases for a general elections voting model are shown in Figure 2. There are 10 general steps in such a model, as described below:

(1) *Define vote districts.* Before the voting process, all participants may be divided into several parts according to their physical location, so they can go to the corresponding districts to cast their votes. Moreover, candidates will be determined in this period.
(2) *Determine voters.* This stage determines who can or cannot vote. In general, all adults have the right to vote in a national election.
(3) *Provide authentication methods.* Perform to authenticate the voters. The authentication methods should be adequate, so voters can choose an appropriate method to verify their identity.
(4) *Setup vote stations.* After the vote districts have been defined, at least one vote station, as infrastructure, should be setup in a district.
(5) *Create ballots.* The ballots are created in this period. The contents of the ballot should include the information of all candidates, so that voters can choose corresponding candidates when voting process begin.
(6) *Authenticate voters.* Before voters casting their votes, the identity of the voters must be verified.
(7) *Cast votes.* Voters go to corresponding vote station to cast their votes. This process should be performed secretly.

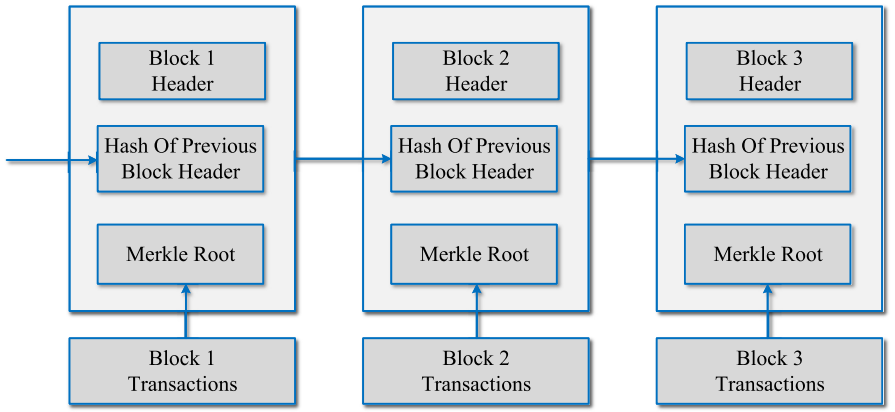

Fig. 3. Blockchain illustration.

(8) *Tally votes.* Perform to validate the cast votes and count the number of votes each candidates got. This process will be done in every district. After all voters finish casting their votes, the vote results in all districts will be summarized.
(9) *Consolidate votes.* After the voting closed, the results of the voting should be stored and managed appropriately. No one can modify the voting results with any reason.
(10) *Verify result integrity.* If any interested entity wants to verity the voting procedure have been conducted properly, then the organization can show the evidence.

2.2 Challenges of Conventional Voting Systems

Conventional voting systems are mostly based on paper ballots and manual operation, or centralized database from electronic voting systems. It is hard to guarantee the security of the whole voting procedure. Conventional voting has disadvantages in many aspects. First, it is hard to guarantee the voters' anonymity. In conventional voting systems, voters get their ballots by using their real identities such as id card. On certain occasions, voters even be asked to fill in personal information in paper ballots, this will lead to the disclosure of voters' privacy. Then, at the end of the voting process, paper-based voting systems count the votes manually. On the one hand, man-made error is hard to avoid, which makes it difficult for the voting result to reflect the will of the voters. Finally, most conventional voting systems save the voting results on a centralized database or paper archive. Centralized database or paper archive once suffered natural disasters, it will lead to irreparable loss of the voting records. This approach also makes it hard for voters to verify whether their votes are correctly counted or not.

3 BLOCKCHAIN TECHNOLOGIES

Blockchain is a decentralized digital ledger in a P2P network, where a copy of the append-only ledger of digitally signed and encrypted transactions is maintained by each participant (show Figure 3). It is the core technology for cryptocurrencies like Bitcoin. Nakamoto first proposed the concept of blockchain in the Bitcoin White Paper [43] in October 2008. In the following years, Bitcoin became a core component of cryptocurrency. Blockchain technology is considered to be the next generation of subversive core technologies after steam engines, electricity, and the Internet [13]. If the steam engine releases people's productivity, then electricity solves people's basic needs of life, and the Internet completely changes the way information is transmitted, then Blockchain, as a machine for constructing trust, will completely change the way human values are transmitted.

Blockchain mainly solves the trust and security problems of transactions. For these two problems, the following technical innovations are proposed.

(1) *Distributed ledger.* The entire blockchain network consists of multiple nodes in peer-to-peer network [51] to maintain the distributed ledger. Each node has a complete backup of the distributed ledger, maintaining consistency of all backups through a peer-to-peer network and consensus mechanism. Different nodes supervise each other to validate the transactions, and they testify each other at the same time. These nodes maintain the order of entire blockchain network.
(2) *Asymmetric encryption and authorization.* The data stored in the blockchain are public, but the data associated with the account, such as the address, public key, private key, and so on, are encrypted using asymmetric encryption technology. Data access can be performed only after the authorization by the data owner, which can separate the public data and the private data, facilitate management, and protect the privacy of users.
(3) *Consensus mechanism.* How the nodes in the entire blockchain network can achieve a consensus to determine the validity of a transaction, which is both a means of determining the validity of the transaction and a means of preventing data tampering. There are many consensus mechanisms for blockchains. They are suitable for different application scenarios and strike a balance between efficiency and security. Bitcoin uses the proof of work (PoW), it is only possible to forge a non-existent transaction if someone controls more than 51% [37] of the nodes in the network. This basically will not happen if there are enough nodes in the entire blockchain network, thus eliminating the possibility of fraud.

To summarize, blockchain technologies have the following important features.

(1) *Decentralization.* The whole network has no central ruler. The system relies on the equitable constraints of multiple players on the network, so each node has equal rights and obligations, and each node stores all the data on the block chain. Even if the node is damaged or attacked, there is no threat to the ledger. The data generated on the blockchain is built on trust through cryptography and mathematical algorithms, rather than by centralized institutions. A distributed point-to-point trading system in which both parties can directly trade without the need for a trusted endorsement by a third party.
(2) *Immutability.* If the ledger is controlled by one or several people, then the likelihood of fraud is very high, but if everyone has a copy of the ledger, then no tampering is effective unless more than 51% of the participants want to change a particular record. This is the advantage of collective maintenance and oversight. When a set of data is generated from the node and recognized by most of the nodes, then the data are written to the blockchain, and each node will copy the data and save it. Therefore, the blockchain data are difficult to change. The conditions are very strict, and it is almost impossible to tampered with, thus ensuring the authenticity of the data.
(3) *Non-repudiation.* When sending a transaction, the sender needs to sign the transaction data using his private key. This signature can always be verified using the signer's public key. According to the characteristics of signature, the transaction sender cannot deny that he/she sent a certain transaction, thus achieving non-repudiation
(4) *Transparency.* In the public blockchain, with the exception of the identity information of the transaction subject that is encrypted, other information is open, and any participant can query relevant records through the public port. Any participant in the blockchain network is equal and can interact with anyone. Any transaction sent by a participant has the same probability of being processed and validated by other nodes in the network.

(5) *Pseudonymity.* Although the data on the blockchain are all public, the blockchain can preserve the privacy of users to a certain extent by randomizing the blockchain addresses. For example, in Reference [56], an application is designed to preserve users' private data by making use of the pseudo-anonymity of blockchain addresses. However, the pseudo-anonymity of blockchain addresses cannot fully preserve the privacy of users, and the real identity of users may be inferred after multiple transactions [2].
(6) *Traceability.* In a nutshell, blockchain is a decentralized database, and the data are stored by nodes, which scatter the data on each computer connected to the network and are not controlled by the centralized server. Because there are a large number of nodes, the blockchain's data storage is tamper-proof. We can track the data in the blockchain. Any data generated in our daily life can be recorded by the block chain, and the transaction id and timestamps are unique, so our transactions can also be traced, and it is convenient for some institutions and departments to manage.

3.1 Smart Contract

Smart contracts are not entirely "new." Nick Szabo, a computer scientist and cryptographer, first proposed the concept of "smart contracts" in 1994. The so-called smart contract is an automatic program contract, which can be triggered automatically once the pre-set conditions are satisfied. For example, the insurance company will automatically reimburse the client when the conditions for the payment are satisfied.

Blockchain makes smart contract possible, because blockchain provides a reliable code execution environment. The smart contract is written into blockchain in a digital form, and the features of blockchain technology ensure that the whole process of storage, reading, and execution is transparent, traceable, and not tampered with. At the same time, a set of state machine systems are built from the consensus algorithm of blockchain, so that the smart contract can execute efficiently. Smart contracts allow trusted transactions to be made without third parties, which are traceable and irreversible. The emergence of smart contract could be a major disruption to business collaboration. For example, the previous business cooperation requires the participation of the third-party public trust agencies or the guarantee of the third party. The emergence of smart contracts based on blockchain has greatly reduced human involvement. Smart contracts are applicable to all situations. They could be financial services, crowdfunding agreements, insurance premiums, defaulted contracts, credit enforcement, and more.

3.2 Taxonomy of Blockchain Systems

Blockchain technologies can be divided into three categories: public blockchain, private blockchain, and consortium blockchain. They all have their own characteristics and different applications, which can be shown in Table 1.

Public Blockchain. Public blockchain is the earliest and most widely used blockchain. It refers to a completely decentralized blockchain like the Bitcoin blockchain that is not controlled by any institution. Any individual or group in the world can send transactions, and the transactions can obtain the effective confirmation of the blockchain, and anyone can participate in its consensus process. Participants in the consensus process maintain database security through cryptography techniques and built-in economic incentives. The most common consensus mechanisms include PoW, Proof of Stack (PoS), and Delegate Proof of Stack (DPoS). Everyone in the world participate in the consensus process through a P2P network.

So how to make people actively participate and maintain the stability of the public blockchain? The coin as a incentive mechanism was introduced, which means that the public blockchain must

Table 1. Taxonomy of Blockchain

	Public Blockchain	Private Blockchain	Consortium Blockchain
Participants	Anyone	Individuals/companies	Consortium members
Consensus Mechanism	PoW/PoS/DPoS	Distributed consistent alg.	Distributed consistent alg.
Bookkeeper	Anyone	Custom	Consortium negotiation
Incentive Mechanism	Need	No need	Optional
Decentralization	Decentralized	Centralized	Polycentric
Validation Speed	Slow	Fast	Medium
Transaction Data	Public	Semi-public	Private
Network	P2P network	Fast network	Fast network
Typical Applications	Cryptocurrency	Audit	Payment/settlement

issue coins like Bitcoin. Once the public blockchain fail to maintain its stability, the coin will be worthless.

Private Blockchain. Private blockchain refers to the blockchain with certain centralized control. Just using the blockchain ledger technology for bookkeeping, the bookkeeper can be a company or an individual, and the privatechain is not much different from other distributed storage schemes. The only participating nodes are the users themselves, and the access and use of data have strict permission management.

Private blockchain is not open to the public, only authorized nodes can participate in and view the blockchain data. The main groups that adopt private blockchain are financial institutions, large enterprises, and government departments. The typical application of the private blockchain is the blockchain developed by the central bank to issue the digital currency. This private blockchain can only be kept by the central bank and is impossible for individuals to participate in. There are also some large companies developing private blockchain, such as alibaba, baidu, and jd.com, which mainly focus on the role of blockchain in data security, supply chain, and other industry pain points.

Consortium Blockchain. Consortium blockchain is generally limited to members of a specific group and a limited number of third parties. Internally, multiple preselected nodes are designated as bookkeepers, and the generation of new block is determined by all preselected nodes. Other later-join nodes can participate in transactions but do not bother with the bookkeeping.

Consortium blockchain is the model of consortium between companies and organizations. The nodes that maintain the data on the blockchain are all from the companies or organizations of the consortium, and the right to record and maintain the data is in the hands of member of the consortium. The main groups that adopt consortium blockchain are banks, securities, insurance, group enterprises and so on. The consortium blockchain is not as open as the public blockchain, that weakens the decentralization, which is a disadvantage of it. At present, the typical project of the consortium blockchain is the hyperledger project. At present, there are more than a dozen different stakeholders such as ABN AMRO, Accenture, and so on, which can meet the needs of their respective industries and simplify the business process [9, 26, 52].

4 CHALLENGES IN BLOCKCHAIN-BASED VOTING SYSTEMS

Applying blockchain technology to voting systems still has a long way to go. Comparing to conventional voting systems, blockchain voting systems are stricter in authentication, anonymity, coercion freeness, and auditability. These requirements should be fulfilled in a voting system for practical production. A proposal for blockchain-based voting systems needs some effort to solve these problems.

Table 2. Proposals' Coverage

	Authentication	Anonymity	Coercion freeness	Auditability
[40]	yes	yes	no	no
[36]	yes	yes	no	yes
[3]	yes	partial	no	no
[6]	no	yes	no	yes
[41]	yes	yes	yes	yes
[53]	not mentioned	yes	no	no
[29]	yes	yes	partial	not mentioned

As mentioned, a good blockchain-based voting system should cover all aspects including, but not limited to, authentication, anonymity, coercion freeness, and auditability. We studied several schemes proposed in recent years and listed their coverage; the results are summarized in Table 2.

4.1 Authentication

In a blockchain-based voting system, participants cast their ballots using virtual identity such as blockchain address. Nevertheless, only individuals in real life have the right to vote. Therefore, virtual identity must be bound to a real-life identity such as Social Security Number (SSN) to make sure every participant is legal.

Authentication is not a difficulty, and there are many mature solutions. However, it is complicated to authenticate without revealing the real-life identity especially in an environment without a TTP. In the scenario of online voting, security and convenience should be both taken into consideration. Remote authentication is used in most of the proposals [45]. However, personal computer and open Internet are not completely safe. There are always some vulnerabilities in online systems. In the scenario of national election, security should be put in the first place; polling stations, which are some terminals specially for voters to cast their ballots, are utilized in most of the proposals for national election. Remote authentication can be utilized in this scenario unless there is a secure authentication scheme for remote environment.

4.2 Anonymity

To avoid the interference of outer environment, all participants should keep anonymous from the voting start to finish. Anonymity is an important aspect for any voting system. Voters' opinions can be expressed freely in an anonymous environment. Therefore, keeping anonymous is the most basic principle to protect voters' privacy.

There are already some methods to achieve anonymity, such as the ring signature invented by Rivest, Shamir, and Tauman in 2001 [49], the group signature introduced by Chaum and Heyst in 1991 [12], and the mix network concept described by Chaum in 1981 [11]. Some of the existing proposals use one or more techniques above to achieve anonymity. Furthermore, there are also some other schemes achieving anonymity by designing a special blockchain or transaction structure. For instance, Hjalmarsson [29] designed a special structure in his proposal that the transaction does not record the sender.

4.3 Coercion Freeness

The coercion in a voting system means that someone is forced to vote for a candidate. A blockchain-based voting system must be coercion-free, which is not an easy problem to solve. Because it is hard for a voting system based on virtual Internet to distinguish if a real-life voter is threatened or not. There are many proposals that have addressed coercion problem. We believe that a good

scheme for blockchain-based voting systems should cover all aspects from voting start to finish. Although coercion problem cannot be completely solved, we should come up with some methods to reduce it at least.

Some modern electronic voting systems allow multiple votes in their policies to reduce coercion. This way, the voter is able a place a new ballot that revokes the old one. Such systems should easy to use and understand against coercion.

Civitas [14] is an open source solution for electronic voting system. It is designed to be completely distributed and one of the few systems, which attest themselves to be coercion-freeness. The Civitas avoids coercion by using fake credentials. To create fake credentials, the voter needs his or her private designation key and then runs a local algorithm. These fake private credentials are indistinguishable from the official credentials provided by Civitas, but the ballots encrypted with them will not be tallied in the last stage of the election. Coercion attacks are not possible with this mechanism, because the coercer can never be sure if the real or the fake credentials were used.

4.4 Auditability

Auditability is critical to the security of voting system. To audit the data generated by the entire voting process, from voting start to finish, all data related to voting should be detailed record. It is very helpful in checking the security status of the blockchain-based voting systems.

Blockchain is auditable, because the all data included in the transaction are stored in blockchain permanently and irreversibly. We can check the validity of a transaction by verifying the signature signed by the transaction sender and the ledger committer. Similarly, in a blockchain-based voting system, the data generated by the entire voting process can be included in a corresponding transaction. However, one thing should be kept in our mind, the privacy of participants cannot be ignored. Voters should keep anonymous throughout the process. No one, even the auditor, can get the information related to voters. Furthermore, the audit authority cannot be controlled by one entity, it can be authorized by a multi-party protocol like the one reported in Reference [21] to scatter authority.

5 REVIEW OF BLOCKCHAIN-BASED VOTING SYSTEMS

We investigated a number of recent papers related to blockchain-based voting system. Here we briefly describe some of the typical cases.

5.1 A Smart Contract for Boardroom Voting with Maximum Voter Privacy

Patric et al. [40] present the first implementation of decentralized and self-tallying voting protocol using blockchain technology. It is a small-scale protocol for boardroom voting with maximum voter privacy.

In the scenario mentioned above, voters only have two choices: binary 1 for yes and binary 0 for no. If there are more than two choices in a vote, then the protocol can be extended to three or more choices, but only the simplest scenario is described in the proposal.

Before the protocol is run, field parameters such as group G and the generator of the group g should be chosen. Moreover, the set $\{P_1, P_2, \ldots, P_n\}$ represents all voters; each voter secretly chooses a voting key x_i. The left part of the protocol can be divided into two steps.

Step 1. P_i broadcasts g^{x_i} and the zero-knowledge proof of x_i (Fiat–Shamir heuristic [23]). Then all voters can calculate $Y_i = \Pi_{j=1}^{i-1} g^{x_j} / \Pi_{j=i+1}^{n} g^{x_j}$, let $Y_i = g^{y_j}$. The calculation above can meet $\sum_i x_i y_i = 0$.

Step 2. Each voter P_i broadcasts $g^{x_i y_i} g^{v_i}$, where v_i is the voter's choice (0 or 1) and the one-out-of-two zero-knowledge proof (CDS-technique) of v_i to proof that v_i is either 0 or 1. Then anyone

(including non-voters) can calculate $\Pi_i g^{x_i y_i} g^{v_i}$ and $y = g^{\sum_i v_i}$. After knowing the value of y, we can get the value of $v = \sum_i v_i$ by traversing all possible exponent from zero (This is one of the reason why the protocol is for small-scale boardroom voting). The value of v is the number of voters who vote yes, and we can get the number of voters who vote "no" by subtracting v from the total number of voters.

The two steps above are based on Open Vote Network protocol [17]. In the original protocol, the last voter could calculate the result before broadcasting his or her vote, and based on the result, the last voter can change the vote. To address to problem, the implementation in Ethereum makes the smart contract to collect all votes first, then the administrator calculates the result and publishes it to all voters.

5.2 Electronic Voting Service Using Block-Chain

Lee et al. [36] proposed a scheme for national level selection using blockchain technology. Three entities are involved in the scheme: the organization (denote as Org) that holds the voting event, which has all voters' true identity (ID), the TTP (who does not know the information about ID), and voters. The voting event is divided into four steps.

Step 1. Preparation. Before voting start, each voter and candidate should have a pair of public key and private key and the corresponding blockchain address. The key pair is used to sign a transaction and verify the validity of a signature. The blockchain address is used to send transactions.

Step 2. Registration. Each voter secretly chooses a message m and then calculates the hash value $H(m)$ of the message and sends it to Org to register the voters (assume every voter has an account linked to his ID to login the registration system).

Step 3. Get Right to Vote. Voters send their hash value $H(m)$ of secretly chosen message to the TTP, and then TTP send the received $H(m)$ to Org to ask whether the $H(m)$ is registered in Org by the corresponding voter. Org answer yes indicates that the voter already registered in the Org; otherwise, abort the received $H(m)$. If the answer is yes, then TTP records the $H(m)$ and $H(pubKey)$ in a table.

Step 4. Casting a Vote. During the vote, anyone (including voters who have no right to vote) can send transactions to corresponding candidate's blockchain address. After the voting closed, only the registered voter's transactions will count, and the newer transaction will cover the older transaction.

The proposed scheme is platform independent. Self-built blockchain network can be used, but the computing power should evenly distributed; otherwise, one node will have the ability to cheat. Current Bitcoin blockchain network can also be used. The advantage is that we do not have to worry about the uneven distribution of computing power, but the disadvantage is that sending transactions costs Bitcoin.

The scheme is secure, because both Org and TTP have only partial information about the vote. Voter chooses a secret message m as his temporary identity. Org have all voters' real ID and $H(m)$ but public key and corresponding blockchain address, so Org cannot know who voted for whom. The TTP knows $H(m)$ and public key, but real ID, so TTP also cannot know who voted for whom.

5.3 An End-to-end Voting-system Based on Bitcoin

Bistarelli [6] proposed an end-to-end voting system based on Bitcoin. The main idea of the paper is that using blockchain to store the vote and associating the vote to a Bitcoin token.

The voting process is roughly divided into three phases: pre-voting phase, voting phase, and post-voting phase.

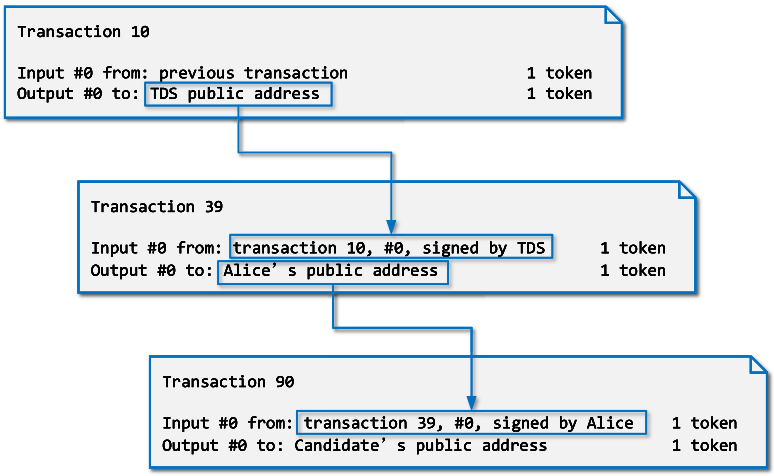

Fig. 4. The audit path of a vote.

Pre-voting Phase. Candidates use their Bitcoin addresses to do candidates nomination. The nominated candidates addresses will be published to all voters. Before the voting starts, all voters need to be registered. Voters generate a pair of public and private key for registration. The successfully registered voters will receive a certain number of Bitcoin as a token for the subsequent voting. It should be noted that the token issuing is an anonymous process. The real identity of voter cannot be linked with his public Bitcoin address. To achieve this, anonymous kerberos (RFC8062 [42]) and blind signature [10] are introduced by the author. Only the voters who are authenticated by the anonymous kerberos will receive the token from Token Distribution Server (TDS).

Voting Phase. Voters who have the right to vote are those who have a token. Legal voters can be easily identified by the token. The vote casting is done simply by sending the token to the corresponding candidate Bitcoin address. The transfer and validation of the vote correspond to the transaction sending and block mining in Bitcoin network.

Post-voting Phase. After the voting is closed, the counting of the votes needs to be done. The number of votes the candidate gets is the number of tokens the corresponding Bitcoin address has received. The auditing of the votes is also important for voters. Unspent Transaction Output model that Bitcoin used makes it easy for all participants to audit the whole procedure of the voting event. For example, the transaction that Alice send for vote must including an input from TDS's transaction, which is signed by TDS and an output to the corresponding candidate's public address. The audit path can be shown as in Figure 4.

5.4 Design of Distributed Voting System

Christian [41] proposed a scheme for distributed voting system using blockchain technology. The scheme assumes that everyone has an electronic ID (eID), and a pair of public and private key generated by the government. The author defined a protocol for voting. The protocol has its own cryptocurrency called BallotCoin. During the voting, voters register themselves with their eID. Voters who are authorized by the system will receive a BallotCoin. When casting the vote, voters simply transfer their BallotCoin to the candidate's address. The vote counting is to count the number of BallotCoin of the candidate's address.

Just like the previous scheme proposed by Bistarelli, the vote casting and vote counting are the same operations. Nevertheless, the method to achieve security and protocol details are different.

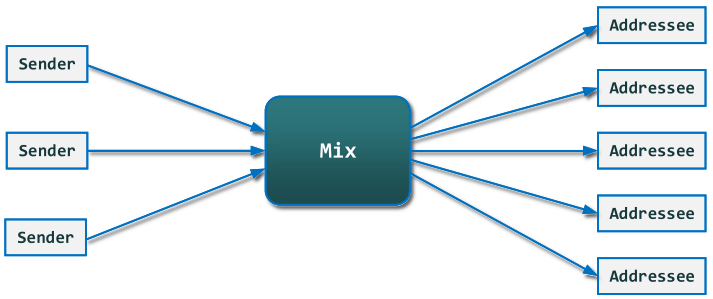

Fig. 5. Illustration on how mix network works.

Christian's scheme used the modified Proof of Stake to reach a consensus. This consensus algorithm will choose commit node from all full nodes, which makes it possible for mobile phones and tablets to become nodes. As long as there are enough nodes running during the voting, the computing power will be evenly distributed. Thus, the security will be guaranteed.

To record the data of voters and voting server, a log server is introduced to the system. It is helpful for the auditing activities. However, the log server is not public to all participants. The interactions between voters and voting server through a dedicated channel, is not distinguishable from a normal channel, otherwise it will get the attacker's attention.

The contents of vote is encrypted with asymmetric encryption algorithm, and the private key is separated with threshold encryption. Multiple authorities must be involved to get the contents of a vote. This is an effective method to prevent corruption and attacks.

Voters could vote more than once, the newer vote will cover the older one. The latest vote is the final vote, the previous votes will be abandoned. It is helpful to prevent voting coercion.

To enhance the anonymity of the voting system, the mix network is introduced into the system. When voters cast their vote, mix network makes the communication between voters and voting server hard to trace. The mix network shuffles the senders' addresses and sends them out in random order, Figure 5 shows how mix network works.

5.5 An E-voting Protocol Based on Blockchain

Liu and Wang [38] proposed an e-voting protocol based on blockchain technology. This is a universal voting protocol; it does not depend on any blockchain platform and does not need a trusted third party. This protocol requires each voter owns two pairs of public and private key one is for signing, its public key can be known to others. Another is for casting vote through blockchain; its public key should keep secret to keep voters anonymous.

Three roles are involved in this protocol: voter, organizer, and inspector. Organizer is the entity who holds the voting event. Organizer needs to verify the eligible voters, record the vote information, and interact with the eligible voters during the voting procedure. The existence of inspectors is to limit the power of organizer and supervise the organizer's behaviors. The protocol is roughly divided into four steps.

Registration Phase. All potential voters need to be registered with their personal information and their signing public keys. The organizer will record the eligible voters based on their personal information.

Pre-voting Phase. Voters need to prepare their ballot by generating a voting string (denote as V), three parts are included in a voting string: x-bit choice code, which represents the voter's choice; y-bit zeros, which is an indication of a well-formed vote; and z-bit random string, which differs the different votes that containing the same choice code; see Figure 6. After the voting string

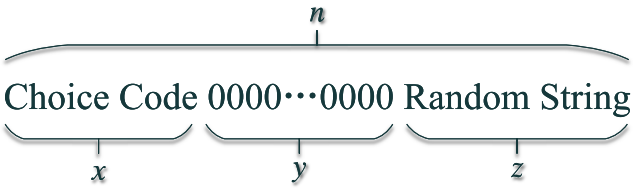

Fig. 6. Voting string formulation.

is prepared, voters interact with organizers and inspectors to make them do a blind signature on the hash of V. Finally, the voting string V and the collected signature of V form a complete ballot.

Voting Phase. Voters construct a transaction, which contains the complete ballot in it. Then they send the transaction to the blockchain network using their secret public key.

Post-voting Phase. The counting of the votes is simply collecting the voting string contained by all transactions.

It should be noted that the information about IP when sending a transaction cannot be traced. Thus, voters are recommended to send their transactions through proxy or TOR network. Another problem is that the intermediate results of voting are public to all participants, which may have an impact on the final results, so the permissioned blockchain is recommended. As an alternative we can make the ballots encrypted by the organizer's key; only the organizer can decrypt the result when voting process is closed.

6 BEING-USED VOTING SYSTEMS

With the development of blockchain technologies, some places of the world has already used blockchain for voting. Next, we will introduce some of the voting systems in use.

6.1 Tsukuba First in Japan to Deploy Online Voting System

In August 2018, Japan used blockchain and My Number cards for the first online voting validation test [30]. The test was conducted in Tsukuba City in Ibaraki Prefecture. The government encourages its citizens to make full use of their intelligence and innovative technologies to come up with new ideas to serve society. These new technologies include the Internet of Things, Artificial Intelligence, and big data analysis. The government supports outstanding works through a review phase. In the final voting phase, they used a blockchain-based voting system to select the final supported works from the candidates. My Number card was used to identify the valid voters.

A fair voting system generally needs to meet the following four basic conditions: (a) distinguish between legitimate and illegal voters, (b) the voting process should be confidential, (c) voters should be prevented from voting multiple times, and (d) the results of voting cannot be tampered with.

The basic idea of this voting is to record voters' votes securely using the characteristics of blockchain, which ensures that voting records are not tampered with. Combining blockchain with voting, and using the existing My Number cards authentication mechanism, an online voting system based on blockchain and meets these four conditions can be implemented.

Although this voting requires Internet Users to vote using terminals at polling stations, the ultimate goal is to enable people to vote using mobile phones or personal computers at home or elsewhere. As technology matures, we can vote from home or anywhere; else through the Internet.

6.2 The Encryption Town of Zug Runs Switzerland's First Municipal Poll Based on Blockchain

According to the swissinfo.ch web site, on June 8, 2018, the small town of Zug in Switzerland held a municipal vote based on blockchain in summer [7]. The event was the first municipal vote in Switzerland using blockchain.

According to the report, the test vote tested the city's digital id card (eID) system, which was launched in November 2017. The system allows citizens to vote on their mobile devices.

In addition to voting on small municipal issues, citizens were asked whether they should vote using the blockchain-based eID system. Since the upcoming vote was an experiment, the results were not binding on municipalities.

After setting up the global cryptocurrency and blockchain development center "Crypto Valley," Zug has become one of the world's leading ecosystems integrating cryptocurrency, blockchain, and distributed ledger technologies. In 2016, Zug launched a program to accept Bitcoin (Blockchain Technologies Corporation (BTC)) as payment for certain municipal services.

Thanks to the existence of "Crypto Valley" and the country's tax-free policy for cryptocurrency investors, Switzerland has become the largest blockchain-friendly country in Europe.

On June 6, 2018, the private bank Hypothekarbank Lenzburg became the first Swiss bank to offer commercial accounts to blockchain and cryptocurrency companies.

6.3 Moscow's Active Citizen Project Introduces Blockchain Technology to Boost Voting Credibility

In 2014, Moscow launched the "active citizen" project, which allows citizens to vote on the color of public lighting, the naming of subway trains, and the color of stadium seats. Now, Moscow has applied blockchain technology to a vote of Active Citizens to make the project more credible [27].

Moscow residents hold 5,000 to 7,000 Active Citizens face-to-face meetings each year on these issues, according to a news release issued in March 2018, but such meetings are increasingly difficult to arrange in busy urban settings. Moreover, residents sometimes question the results of the vote.

Andrey Bezerov, a consultant to the chief information officer in Moscow, said, "sometimes we hear that not all votes are credible, so we decided to use blockchain technology in the Active Citizen project as a platform for building electronic trust."

In December 2017, the Active Citizen project began using blockchain technology to vote. Once the vote is approved, it will is listed in a ledger containing all the votes. This ensures that after the vote, the data will not be lost or changed by one person, so there will be no fraud or third-party interference.

7 COMPARISON AND ANALYSIS

From the beginning of Bitcoin, blockchain has been developed into a variety of types such as public blockchains, private blockchains, and hybrid blockchains. In general, they can be divided into permissioned blockchain and permissionless blockchain according to their permission management. Different blockchains also adopt different approaches to consensus including but not limited to PoW, and PoS [33]. These consensus mechanisms above all have their own characteristics, and they can be used for different voting scenarios, respectively.

We classified these blockchain-based voting systems according to different principles such as the taxonomy of blockchain, approaches to consensus, and approaches to anonymity. Then we analysed these schemes and compared them with each other. The classification of these schemes is shown in Table 3.

Table 3. The Classification of Blockchain-based Voting Systems

Subsections	Classification principles	Classification items	Existing proposals
7.1	Taxonomy of blockchain	Permissioned blockchain	[29][38]
		Permissionless blockchain	[6]
7.2	Approaches to consensus	PoW	[6]
		PoS	[41][53]
7.3	Approaches to anonymity	Ring signature	[53][39]
		Mix network	[41]
7.4	Approaches to hide information	Zero knowledge proof	[29][40][53][46]
		Blind signature	[6][38]
		Homomorphic encryption	[41]
7.5	Platform dependency	Platform independent	[40][38]
		Platform dependent	[29][3]
7.6	TTP dependency	TTP independent	[40][38]
		TTP dependent	[36]
7.7	Scale of participants	Large-scale	[36][53]
		Small-scale	[40]
7.8	Security level	National election level	[36]
		Online voting level	[48]

7.1 Taxonomy of Blockchain

Permissioned blockchain. Private blockchains and hybrid blockchains are all permissioned blockchain. Because their read permission or write permission are restricted more or less. In some blockchain-based voting systems, especially those with TTP involved, permissioned blockchain is used for avoiding unnecessary information leakage. Only specific entities such as TTP or voting organizer have the read and write permissions and voters can read the blockchain by providing their credentials, for example.

Permissioned blockchain has been used in Hjalmarsson's proposal [29] to enable liquid democracy, which is a new form for collective decision making that gives voters full decisional control. In this system, district nodes are given the permission to interact with corresponding smart contracts. When an individual voter cast his vote, the vote data are verified by all of the corresponding district nodes and every vote they agree on are appended onto the blockchain when block time has been reached and voter will receive a transaction ID as feedback. After the voting ends, voters can verify if their ballots have been correctly counted in by providing their transaction IDs to the authorized nodes.

Permissionless blockchain. Permissionless blockchains are known as public blockchains, since they are for all of the Internet users. Anyone can have the read and write permission to the blockchain, and anyone is possible to be the ledger committer. The most famous public blockchains are Bitcoin blockchain and Ethereum blockchain [54]. Most of the proposals that used permissionless blockchain are based on Bitcoin network or Ethereum platform.

Bistarelli's proposal [6] is based on Bitcoin. In pre-voting phase, all legal voters will be sent a token as the right to vote. Furthermore, in voting phase, all they need to do is sending the token to corresponding candidate's blockchain address directly. There is no middleman between voters and candidates, and TTP is not required after registration.

One of the advantages is that the voting systems based on permissionless blockchain are platform independent. The voting process is considered as the transformation of virtual assets such as tokens, Bitcoin, or Ethereum, which is easy to implement.

Table 4. Comparison between Permissioned and Permissionless Blockchain

	Permissioned	Permissionless
Decentralization	no/partial	yes
TPS	high	low
Privacy protection	good	lacking
Nodes Security	high	low

Comparisons. Permissioned blockchain and permissionless blockchain are different in many aspects including, but not limit to decentralization, TPS, Privacy protection, and Nodes security. Table 4 shows the qualitative comparison.

(1) *Decentralization.* Permissioned blockchains are controlled under one organization or a consortium that including several organizations, which compromise the decentralization of blockchain, whereas permissionless blockchains are for all users, which enable full decentralization.
(2) *TPS.* Generally, a small quantity of nodes are included in a permissioned blockchain network, and they are all trusted after participation authorization. There is no need for transactions to be validated by all nodes, which is of crucial importance for increasing the transaction speed, whereas the untrusted network environment of permissionless blockchain makes the transactions have to be validated by all nodes among the network, which is a very slow process.
(3) *Privacy protection.* Data stored in permissioned blockchain is protected by access control regulations. Only authorized entities have the permissions to access the data, which makes it harder to leak the information related to participants' privacy. In contrast, data stored in permissionless blockchain are open to all Internet users. It is highly recommended not to store anything sensitive in a permissionless blockchain.
(4) *Nodes' Security.* As mentioned, permissioned blockchain in an organization or a consortium is well controlled. Strict authorized certification is needed before a node is accepted as a part of permissioned blockchain. Whereas the nodes in a permissionless blockchain are free to participate, there may be some evil nodes among them. Thus, nodes are more secure and trusted in a permissioned blockchain than a permissionless one.

7.2 Approaches to Consensus

PoW. PoW is the abbreviation of Proof of Work. It is the first generation of consensus mechanism, and it is the foundation of Bitcoin system. All nodes in the network compete with each other to be the ledger committer by solving some computationally intensive puzzles, which is known as mining. Furthermore, the difficulty of mining can be adjusted dynamically. To solve the puzzles, a lot of computing power needs to be available. This is both an advantage and a disadvantage. On one hand, it is impossible for someone to control more than 51% of computing power if there are enough participants in this network, thereby eliminating the possibility of fraud; on the other hand, computation needs a lot of time, which cuts down the transaction throughput of the network.

Most blockchain-based voting systems that used PoW is based on Bitcoin, or Ethereum platform, or other permissionless blockchain. Bistarelli's proposal [6] is an example. This scheme is based on Bitcoin system and uses PoW consensus mechanism. One of the advantages of PoW is that more participants will be attracted to mining, which strengthen the security of blockchain-based voting

Table 5. Comparisons between PoW and PoS

	Proof of Work	Proof of Stake
Nodes anonymity	strong	weak
Mining cost	high	low
Transaction delay	high	low

system. However, systems that used PoW usually cannot achieve a high transaction throughput, which limits its application scenarios.

PoS. The mechanism of PoS to create a new block is totally different from PoW. The interest each community member receives is determined by the stake of each community member hold. In Peercoin's proof-of-stake system [33], the stake here is the product of the number coins and the coin holding days. The longer you hold the coin and the more coins you hold, the more likely you can get the bookkeeping right. After the time of holding coin is more than 30 days, the node can participate in the competition of bookkeepers. Once the bookkeeping right is obtained, the number of holding days will return to zero, and the next competition needs to wait at least 30 days. The number of holding days will not continuously increase; its maximum is 90 days, which can prevent the node holding a large number of coins from controlling the bookkeeping right. This consensus mechanism can generate coins continuously without consuming a lot of computational power.

There is another consensus mechanism called DPoS [35]. Community members in DPoS systems do not commit the ledger themselves, instead they just delegate a super representative they chose to validate the transactions for the next block. The main difference between DPoS and PoS is in DPoS consensus system; community members have more governance rights in the network.

Wang et al. proposed a blockchain-based voting solution for large-scale election [53]; DPoS is utilized in this proposal. The voting system can get a high transaction throughput because of DPoS; this is very important for a large-scale voting system. In addition, DPoS makes it become a more decentralized system with a democratic, self-governing voting procedure.

Comparisons. There are a lot of differences between PoW and PoS, and blockchain networks based on them are different to each other. We analyzed the aspects of nodes' anonymity, mining cost, and transaction delay, and compared with each other. The result is shown below, Table 5.

(1) *Nodes anonymity.* In Proof-of-Work blockchain system, all nodes join the blockchain network freely, no need for authorization. This makes all nodes keep anonymous in the network, which protects the privacy of all users. On the contrary, nodes in Proof-of-Stake blockchain network cannot join freely. They need coin balance in the account first. To get balance, they have to transact with others. This raised the threshold of participation, and weakened anonymity.
(2) *Mining cost.* As mentioned, miners participate in bookkeeping by solving some computationally intensive puzzles. It is time consuming and power consuming. However, in PoS-based network, there is no puzzle to solve. The ledger committer is determined by coin age, and then the ledger committer just signs a signature to create a new block. It is computation-friendly.
(3) *Transaction delay.* In PoW-based blockchain network such as Bitcoin, about every 10 minutes, a new block is created. Moreover, a transaction needs to wait until six blocks is created to get its confirmation. Therefore, the average delay of a transaction is 1 hour. In PoS-based blockchain network, transactions can be packed immediately after receiving them and then can be broadcast. There is no waiting time. Thus, the delay can keep at a very low level. Almost negligible compared to PoW.

7.3 Approaches to Anonymity

Ring signature. In 2001, Rivest, Shamir, and Tauman described ring signature at asiacrypt [49]. Ring signature is a special kind of signature. After a message is signed by ring signature, we can only know that the signer is from a group, not who exactly signed it. It is computationally impossible to know which key was used for the ring signature. There are some differences between ring signatures and group signatures: (a) there is no administrator and the anonymity of a member cannot be disclosed and (b) any specified member can form a group.

Ring signature provides unconditional anonymity. That is, even if the attackers illegally obtained the private keys of all possible signers, the probability that the attackers can find out the true signer is no more than $1/n$, where n is the number of all possible signers. The unconditional anonymity that ring signature provide is consistent with the requirement of voters in a blockchain-based voting system.

Wang et al. proposed a scheme for large-scale election based on blockchain [53], in which the election organizer acts as a trusted third party. During the ballot preparation phase, voters encrypt their ballot content with a system public key. Then, voters sign the encrypted ballot with a ring signature. Next, the encrypted ballot and ring signature will be sent to election organizer. The organizer verifies the validity of the ballot by checking the ring signature, but without revealing the true signer, and then decrypts the ballot with system private key to tally the vote.

Mix network. In 1981, Chaum first introduced the concept of mix network [11]. Since then, many mix-network-based applications have been developed, such as anonymous remailers and onion routing. Mix networks are routing protocols that use proxy servers to mediate user traffic, making it difficult to track traffic between users. The proxy server confuses the incoming messages and sends them randomly to the next proxy server. This process of obfuscation makes the source address of the message and the target address no longer match, which makes it difficult for the attacker to trace the source address of the message.

Hanifatunnisa proposed a scheme for blockchain based e-voting system [28], which suggests to use a mix-network and homomorphic encryption as they provide a reliable mechanism to anonymize the ballot. It is very easy to understand and all steps can be published for universal verifiability. To fulfill all cryptographic requirements for a mix-network, the homomorphic encryption scheme must support re-encryption. After the mix-network, all ballots are anonymized and still encrypted. Therefore, the stored ballots have no connection to the voters.

7.4 Approaches to Hide Information

Zero knowledge proof. In the 1980s, Goldwasser put forward the concept of zero-knowledge proof [24]. Zero knowledge proof is a protocol involving three objects: Prover, Verifier, and Secret. In the zero-knowledge proof protocol, the Prover tries to prove that it knows a Secret but cannot reveal any information of the Secret in the proof process. Zero-knowledge proof protocol satisfies three properties below.

(1) **Feasibility.** If the Prover provides a true Secret, then the Verifier will accept Prover's assertion with a high probability;
(2) **Reliability.** If the Prover provides a false Secret, then the Verifier will reject Prover's assertion with a high probability;
(3) **Zero knowledge.** If the Prover provides a Secret that is true, and the Verifier dose not violate the protocol rules, then no matter how Verifier verifies, the Verifier cannot obtain any information related to the Secret except accepting the assertion.

One the one hand, a blockchain-based voting system needs to verify the legitimacy of certain information, such as whether participants have the right to vote; on the other hand, the system needs to prevent the disclosure of sensitive information, such as the true identity of voters, the content of ballots, and the key related to voting. These requirements of the voting system are exactly met by zero-knowledge proof.

Zero-knowledge proof is used several times in Patrick et al.'s proposal [40]. In the registration phase, participant P_i will choose an x_i as its private voting key. Before casting the ballot, every P_i will broadcast its public voting key g^{x_i} and the zero-knowledge proof (Fiat–Shamir heuristic [23]) of x_i. Not only does this verify that P_i is a legitimate participant, but also it prevents the disclosure of its private voting key. In voting phase, a one-out-of-two zero-knowledge proof [17] will be contained in the ballot in order for the one who counts votes to verify the validity of the ballot.

Blind signature. Blind signature was first proposed by Chaum in 1983 [10]. Blind signature is a special digital signature that signer signs the signature without obtaining the details of the signed message. In addition to satisfying general digital signature's condition, it must also satisfy the following two properties.

(1) **Blindness.** Although the signer signs a message, he cannot get the specific content of the message;
(2) **Unlinkability.** Once the signature of the message is made public, the signer cannot be sure when he signed the message.

Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes. Blind signature not only support blindness, but also can be used to provide unlinkability, which prevents the signer from linking the blinded message it signs to a later un-blinded version that it may be called upon to verify. In this case, the signer's response is first "un-blinded" prior to verification in such a way that the signature remains valid for the un-blinded message. This can be useful in schemes where anonymity is required.

Liu et al. proposed an e-voting protocol based on blockchain [38], in which blind signature was used to keep ballot contents from voting organizer and inspectors. During the ballot preparation phase, voters generate a vote string according to their choices. The vote string is subsequently encrypted and sent to the organizer and inspectors to check the validity of ballot format, and then sign a signature. After blind signature, voters decrypt the blind signature and get the signature of organizer and inspectors. The organizer and inspectors cannot get any information about voters' choices during the process above.

Homomorphic encryption. Homomorphic encryption is a kind of encryption method that has some special nature attributes, this concept is Rivest et al., first put forward in the 1970's, compared with the general encryption algorithm, homomorphic encryption not only can realize the basic cryptographic operations, but also can achieve a variety of computing functions between the ciphertext. That is, computation after decryption is equivalent to encryption after calculation. This feature is of great significance for protecting the security of information. The homomorphic encryption technology can be used to calculate multiple ciphertexts and then decrypt them, rather than to decrypt each ciphertext at a high computational cost. Homomorphic encryption can be used to calculate ciphertext without decryption, can not only reduce the communication cost, but also transfer the computing task, so as to balance the computing cost of each party. Homomorphic encryption can be used so that the decryption party only knows the final result, but not every message of the ciphertext, which can improve the security of information. Because of the advantages of homomorphic encryption in computing complexity, communication complexity and security, more and more research attentions are put into the exploration of its theory and application.

In a blockchain-based voting system, there is usually some sensitive data such as the true identity of voters, ballot contents, and keys related to voting. Moreover, these sensitive data often perform some essential computation, which cannot be performed under plaintext because of the security sake. In Christian's proposal [41], homomorphic encryption was used to protect the ballot contents. The validity of the ballot can be verified by organizer when tallying under ciphertext, but the organizer cannot obtain the details of the ballot contents.

7.5 Platform Dependency

Platform independent. A platform independent protocol for blockchain-based voting can be adopted to different platforms without huge modification, which is good for the promotion and implementation of the protocol. Generally, the data of voting protocol will be contained in a transaction as the data section. These data have their own data structures, and they contain the all ballot contents. They are independent of the other data in the transaction. Furthermore, the blockchain system does not care about the data section. Therefore, the voting protocol should handle all possible problems that may occur during the voting process.

Liu et al. proposed an e-voting protocol based on blockchain [38]. It is a platform-independent protocol. In ballot preparation phase, voter will generate a voting string according to its choice. Then the voter will encrypt the voting string and send the encrypted result to voting organizer and inspectors to sign with blind signature. Voter decrypts the blind signature and gets the signed voting string. The signed voting string will be included in a transaction as the data section and will be stored in blockchain. After the voting is closed, the organizer collects all transactions that include signed voting string to verify the signature and count the ballot.

Platform dependent. A platform-dependent protocol for blockchain-based voting is designed for a special platform such as Bitcoin system or Ethereum platform. The design of platform-dependent protocols should give fully consideration to the features of the platform and make full use of the advantages of the platform. For example, Bitcoin is a universal payment system, and the security of Proof of Work consensus mechanism that Bitcoin system used can be proved mathematically. To make use of the specialty of Bitcoin, some blockchain-based voting proposals convert the voting operations to the transfer of virtual assets such as Bitcoin or token. It simplifies the protocol.

Bistarelli et al. proposed an end-to-end voting system based on Bitcoin [6]. The voting operation is defined as the transfer of virtual assets. During pre-voting phase, participants who have finished registration will be charge a certain amount of Bitcoin as the sign of completion of registration. Then, participants need to authenticate by Anonymous Kerberos Authentication Protocol [42] with blind signature. Participants who finished the authentication are valid voters and they will receive a token for voting. In voting phase, voters transfer the token to corresponding candidate's account according to their choices. After the voting is closed, the amount of the tokens in a candidate's account is the total votes that this candidate got.

7.6 TTP Dependency

TTP independent. A trusted third party is an entity, which facilitates interactions between two parties who both trust the third party. Blockchain-based voting systems without TTP are more decentralized and independent.

Liu et al. proposed a protocol [38] for blockchain-based voting system in which only organizers and inspectors are involved besides voters and candidates. The organizers' duties are to hold the election, verify and record eligible voters' information, and interact with voters during the election. The inspectors are introduced to limit the power of the organizers and inspect the behaviors of the organizers. Inspectors also interact with voters during the election. During the ballot preparation

phase, voters generate a vote string according to their choices. The vote string is subsequently encrypted and sent to the organizer and inspectors to check the validity of ballot format, and next sign a signature. After blind signature, voters decrypt the blind signature and get the signature of organizer and inspectors. The organizer and inspectors cannot get any information about voters' choices during the process above.

TTP dependent. A trusted third party in blockchain-based voting system can facilitate the interactions between two entities such as voters and organizer, and the power of organizer can be limited. Some sensitive data can be processed by trusted third party rather than organizers in some blockchain-based voting systems without trusted third party.

Lee et al. proposed an electronic voting system [36] as an application of blockchain, in which a trusted third party is involved. If there is not a trusted third party, then the voting organizer should authenticate the voters, count the vote, and potentially provide the majority of nonce mining. The organizer is able to find out who the voters voted for and it can potentially forge the blockchain ledger in the way that it wants. This is why the proposal needs a trusted third party. Trusted third party checks if the voter is authenticated by the voting organizer according to their identification information such as SSN. Moreover, the trusted third party counts the vote during the voting process. The trusted third party only knows whether a virtual identity has right to vote or not, but it cannot find out the SSN behind a virtual identity. Therefore, the organizer and the trusted third party cannot know both the real identity and ballot content.

7.7 Scale of Participants

Large-scale. Large-scale voting events such as national election or online voting usually involve a large group of people, which raises the requirements for blockchain-based voting system. With the increase in number of participants, a higher transaction throughput is needed to handle a large influx of votes in a short period of time. A large-scale blockchain-based voting system should process data efficiently each stage and the storage capacity should also increase accordingly. Another problem is that transaction fee should keep at a very low level, or it will be a large amount of monetary cost.

Wang et al. proposed a scheme of large-scale election based on blockchain [53]. This proposal is based on the Ethereum platform, but the consensus algorithm is not Proof of Work anymore. The original consensus mechanism was not suitable for large-scale online voting, because the PoW consensus mechanism would consume a lot of computational power, which would lead to a lot of energy waste. It can also lead to mining centerized and slow down transaction confirmation. DPoS can greatly reduce the frequency of transaction validation and the number of nodes participating in the consensus, thus increasing the transaction throughput of the network. DPoS is typically used in high-throughput blockchain networks such as elections, where transaction confirmations are very fast.

Small-scale. Small-scale voting events such as boardroom voting usually involve a small group of people in a limited space. So, the design of small-scale voting systems is totally different from the large-scale one. The aspects that small-scale blockchain-based voting systems need to consider are different, too. In a large-scale voting system, the efficiency and the cost might be the primary consideration. Whereas in a small-scale voting system, the privacy and security might be the primary consideration, because participants of a small-scale voting event in a limited space, they might be familiar to each other in real life. Any information related to the contents of a ballot is sensitive.

McCorry et al. designed and implemented a boardroom voting system with maximum voter privacy based on Ethereum smart contract [40]. It is a binary-choice boardroom voting system, participants can only choose either yes (recorded as binary 1) or no (recorded as binary 0). Voters

Table 6. Comparisons between Large-scale and Small-scale Voting Systems

	Large-scale	Small-scale
Transaction throughput	high	low
Voting cost	high	low
Participants distribution	unlimited space	limited space

cast their ballot by broadcasting $g^{x_i y_i} g^{v_i}$, where x_i is a secret voting key, y_i is a public median, and v_i is voter's choice. Moreover, $\prod g^{x_i y_i} g^{v_i}$ can be calculated after the voting ends. As we have $\sum_i x_i y_i = 0$, we can get $g^{\sum v_i}$. As mentioned, it is a small-scale voting system, and $\sum v_i$ can be guessed out by trying constantly from zero. So, we get the value of $\sum v_i$, which is the number of voters whose choice is yes. Furthermore, we can get the number of voters whose choice is no by subtracting $\sum v_i$ from total number of participants.

Comparisons. The design of large-scale and small-scale blockchain-based voting systems are different in many aspects such as transaction throughput, voting cost, and participants distribution. We did a qualitative comparison, and the results are shown in Table 6.

7.8 Security Level

National election level. The security of national election should reach the highest level because of the great influence on the country. The design of national election voting systems is very strict. Any vulnerability in the system cannot be ignored. For example, real-name authentication is an indispensable step in pre-voting phase. However, online real-name authentication is vulnerable because of the insecure personal computers and untrusted network environment. Therefore, to achieve a higher level of security, so many proposals for national election compromised the convenience of online authentication and replaced it with on-site authentication.

VoteWatcher [8] is a blockchain-based voting system for governments, proposed by BTC. For safety's sake, participants in VoteWatcher system cannot cast their ballot remotely. Instead, they need to come to a vote station to get a paper ballot, in which three QR codes are included and they represent the blockchain address, ballot ID, and vote ID, respectively. Voters cast their ballots by scanning these three QR code. After scanning the ballot, the ballot is then cast for the corresponding candidate. Before the voting ends, all voting records are stored in an offline blockchain. After polls close, data in an offline vote station will be uploaded to an online blockchain. The advantage of doing this is that the remote attack from network during voting process can be prevented.

Online voting level. Online voting systems are generally systems for daily use, an important feature is that online voting is significantly more frequently used than national election, and hackers are not as interested in the results of online voting as they are in national elections. Therefore, in an online voting system, convenience and security are of equal importance. In some cases, we have to compromise the security of the system to get a friendly operation experience. For example, users must be able to participate the voting events using their smart phones or personal computers through the open internet, although there are some risks.

8 BROADER PERSPECTIVES

8.1 Efficiency and Security Coexistence

In a large voting system, efficiency and security are what we are looking for. However, at the moment it is hard to achieve both. As we all know, among the many blockchain consensus algorithms, the security of PoW should be second to none. Its security can be proved mathematically, so it is

used in many blockchain platforms. However, the drawback of requiring heavy computational power to get blockchain networks to reach consensus. If we reduce the difficulty of the PoW, then the speed of consensus will be much faster but with a decrease in security. There are many similar situations in the blockchain, for example, encryption and signature algorithm to be more secure; this will inevitably lead to an increase in operation time. At this stage, some possible solutions have emerged, such as replacing PoW with consensus algorithms such as PoS, but their security has not been proven. For encryption and signature algorithms, we try to reduce the length of the key to improve efficiency under the condition of ensuring security. To further improve efficiency, we can only expect more lightweight cryptographic signature algorithms to be designed. There seems to be a contradiction between efficiency and security. How to make efficiency and security coexist will be the future focus of research.

8.2 Transparency and Privacy Coexistence

In the public blockchain, data transparency has been maximized, but privacy is lacking. In contrast, in a private blockchain, permissions are tightly controlled at the expense of data transparency. In the blockchain voting system, the data transparency of blockchain is applied in the system as an important feature. Voters want as much data as possible to be transparent, so they know that the voting system presents the wishes of all voters fairly and fairly. However, in a blockchain system, more transparent data means less privacy for users. Privacy in blockchain has always been a hot topic in research, and privacy protection that takes into account data transparency will make the issue more challenging. The current solution is to use consortium blockchains. Consortium blockchain combines the advantages of public blockchain and private blockchain, with the advantages of transparency and privacy, which makes consortium blockchain applied in many scenarios. However, in many scenarios that require the use of public blockchains, transparency, and privacy are still hard to balance.

8.3 High Concurrency and High Throughput Coexistence

In a large voting system, there is usually a large number of users participating in the voting at the same time, and the system needs to process many voting requests at the same time, which requires the voting system to have high concurrency capability. However, existing blockchain solutions are generally unable to achieve high transaction throughput, especially on some public blockchain platforms. For example, the Bitcoin system has a throughput of 7 TPS, and Ethereum has a throughput of 8 TPS, which is far from meeting the requirements of large voting systems. Low throughput can be said to be a common problem of chain-structured blockchain. This is because the chain-structured blockchain adopts synchronous consensus, and transactions need to be verified before they can be appended to blockchain, so that the state of all nodes in the network can be synchronized. To achieve high concurrency and high throughput coexistence, there are some asynchronous consensus solutions such as Tangle, IOTA, and XDAG with Directed Acyclic Graph– (DAG) structured blockchain [19, 47], on which transactions are appended to blockchain first and then validate them. In theory, the higher the concurrency of a DAG-structured blockchain, the higher its throughput.

9 CONCLUSION

In recent years, there have been interest in designing blockchain-based voting systems to circumvent limitations in existing paper-based and electronic voting systems. Hence, we investigated these schemes and classified them according to their characteristics such as the type of blockchain used, the consensus approach used, and the scale of participants. We also presented a systematic,

in-depth analysis of the different blockchain-based voting systems and identified a number of potential research opportunities.

REFERENCES

[1] Umut Çabuk, Eylul Adiguzel, and Enis Karaarslan. 2018. A survey on feasibility and suitability of blockchain techniques for the E-voting systems. *Int. J. Adv. Res. Comput. Commun. Eng.* 7, 03 (2018), 124–134. DOI: https://doi.org/10.17148/IJARCCE.2018.7324

[2] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. 2018. Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* 21, 2 (2018), 1676–1717.

[3] A. B. Ayed. 2017. A conceptual secure blockchain-based electronic voting system. *Int. J. Netw. Secur. Appl.* 9, 3 (2017).

[4] Jaume Barcelo. 2014. User Privacy in the Public Bitcoin Blockchain. Retrieved August 2, 2019 from https://pdfs.semanticscholar.org/549e/7f042fe0aa979d95348f0e04939b2b451f18.pdf.

[5] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. 2014. Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 15–29.

[6] Stefano Bistarelli, Marco Mantilacci, Paolo Santancini, and Francesco Santini. 2017. An end-to-end voting-system based on bitcoin. In *Proceedings of the Symposium on Applied Computing (SAC'17)*. ACM, New York, NY, 1836–1841. DOI: https://doi.org/10.1145/3019612.3019841

[7] Blockchain Pencil. 2018. The Encryption Town of Zug Runs Switzerland's First Municipal Poll Based on Blockchain. Retrieved March 6, 2020 from http://www.bite5.com/index.php/article-872.

[8] Blockchain Technologies Corp. 2016. VoteWatcher—The World's Most Transparent Voting Machine. Retrieved July 28, 2019 from https://pdfs.semanticscholar.org/5b6a/0b0ff2c574d9bb8bad9e191b22f44c92add7.pdf.

[9] Umesh Bodkhe, Pronaya Bhattacharya, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, and M. S. Obaidat. 2019. Blohost: Blockchain enabled smart tourism and hospitality management. In *Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS'19)*. IEEE, 1–5.

[10] David Chaum. 1983. Blind signatures for untraceable payments. In *Advances in Cryptology*, David Chaum, Ronald L. Rivest, and Alan T. Sherman (Eds.). Springer US, Boston, MA, 199–203.

[11] David Chaum. 2003. *Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms*. Springer US, Boston, MA, 211–219. DOI: https://doi.org/10.1007/978-1-4615-0239-5_14

[12] David Chaum and Eugene Van Heyst. 1991. Group signatures. In *Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'91)*. Springer-Verlag, Berlin, 257–265. http://dl.acm.org/citation.cfm?id=1754868.1754897

[13] Kim-Kwang Raymond Choo, A. Miglani, Neeraj Kumar, M. S. Obaidat, and Debiao He. 2020. Machine learning-based blockchain management in IoT environment: Trends, challenges, and opportunities. (unpublished).

[14] M. R. Clarkson, S. Chong, and A. C. Myers. 2008. Civitas: Toward a secure voting system. In *Proceedings of the IEEE Symposium on Security and Privacy (SP'08)*. 354–368. DOI: https://doi.org/10.1109/SP.2008.32

[15] Ethereum contributors. 2019. Ethereum Blockchain Explorer. Retrieved August 2, 2019 from https://etherscan.io/.

[16] Wikipedia contributors. 2019. Bitcoin scalability problem. Retrieved August 2, 2019 from https://en.wikipedia.org/w/index.php?title=Bitcoin_scalability_problem&oldid=908933182.

[17] Ronald Cramer, Ivan Damgard, and Berry Schoenmakers. 1994. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Proceedings of the Conference on Advances in Cryptology (CRYPTO'94)*, Yvo G. Desmedt (Ed.). Springer, Berlin, 174–187.

[18] Chris Culnane, Aleksander Essex, Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. 2019. Knights and knaves run elections: Internet voting and undetectable electoral fraud. *IEEE Secur. Priv.* 17, 4 (2019), 62–70.

[19] M. Divya and Nagaveni B. Biradar. 2018. IOTA-next generation block chain. *Int. J. Eng. Comput. Sci.* 7, 04 (2018), 23823–23826.

[20] Philip Ewing. 2019. What You Need to Know about U.S. Election Security and Voting Machines. Retrieved from https://www.npr.org/2019/08/31/754412132/what-you-need-to-know-about-u-s-election-security-and-voting-machines.

[21] Qi Feng, Debiao He, Zhe Liu, Ding Wang, and Kim-Kwang Raymond Choo. 2020. Multi-party signing protocol for the identity-based signature scheme in IEEE P1363 standard. *IET Inf. Secur.* 1, 99 (2020), 1–10. DOI: 10.1049/iet-ifs.2019.0559

[22] Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. 2019. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* 126 (2019), 45–58. DOI: https://doi.org/10.1016/j.jnca.2018.10.020

[23] Amos Fiat and Adi Shamir. 1987. How to prove yourself: Practical solutions to identification and signature problems. In *Proceedings of the Conference on Advances in Cryptology (CRYPTO'86)*, Andrew M. Odlyzko (Ed.). Springer, Berlin, 186–194.

[24] S. Goldwasser, S. Micali, and C. Rackoff. 1989. The knowledge complexity of interactive proof systems. *SIAM J. Comput.* 18, 1 (1989), 186–208. DOI: https://doi.org/10.1137/0218012 arXiv:https://doi.org/10.1137/0218012

[25] Dimitris A. Gritzalis. 2002. Principles and requirements for a secure e-voting system. *Comput. Secur.* 21, 6 (2002), 539–556.

[26] Rajesh Gupta, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, Mohammad S. Obaidat, and Balqies Sadoun. 2019. Habits: Blockchain-based telesurgery framework for healthcare 4.0. In *Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS'19)*. IEEE, 1–5.

[27] Guru Network. 2018. Moscow's Active Citizen Project Introduces Blockchain Technology to Boost Voting Credibility. Retrieved March 6, 2020 from http://mini.eastday.com/mobile/180315175458878.html.

[28] R. Hanifatunnisa and B. Rahardjo. 2017. Blockchain based e-voting recording system design. In *Proceedings of the 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA'17)*. 1–6. DOI: https://doi.org/10.1109/TSSA.2017.8272896

[29] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjálmtýsson. 2018. Blockchain-based E-voting system. In *Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD'18)*. 983–986. DOI: https://doi.org/10.1109/CLOUD.2018.00151

[30] Japan Times. 2018. Tsukuba First in Japan to Deploy Online Voting System. Retrieved March 5, 2020 from https://www.japantimes.co.jp/news/2018/09/02/national/politics-diplomacy/new-online-voting-system-introduced-city-tsukuba.

[31] Snehal Kadam, Khushaboo Chavan, Ishita Kulkarni, and Amrut Patil. 2019. Survey on digital E-voting system by using blockchain technology. *Int. J. Adv. Sci. Res. Eng. Trends* 4, 2 (2019).

[32] Hye Ri Kim, Kyoungsik Min, and Seng-phil Hong. 2017. A study on ways to apply the blockchain-based online voting system. *Int. J. Contr. Autom.* 10, 12 (2017), 121–130.

[33] Sunny King and Scott Nadal. 2012. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Retrieved from https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf.

[34] Marko Kovic. 2017. Blockchain for the people: Blockchain technology as the basis for a secure and reliable e-voting system. DOI: https://doi.org/10.31235/osf.io/9qdz3

[35] Daniel Larimer. 2014. Delegated Proof of Stake (DPoS). Retrieved from https://en.bitcoinwiki.org/wiki/DPoS.

[36] K. Lee, J. James, T. Ejeta, and H. Kim. 2016. Electronic voting service using block-chain. *J. Dig. Forens. Secur. Law* 11 (2016). DOI: https://doi.org/10.15394/jdfsl.2016.1383

[37] Iuon Chang Lin and Tzu Chun Liao. 2017. A Survey of Blockchain Security Issues and Challenges. Retrieved from https://pdfs.semanticscholar.org/f61e/db500c023c4c4ef665bd7ed2423170773340.pdf.

[38] Y. Liu and Q. Wang. 2017. An E-voting Protocol Based on Blockchain. Retrieved July 28, 2019 from http://votewatcher.com/.

[39] Jiazhuo Lyu, Zoe L. Jiang, Xuan Wang, Zhenhao Nong, Man Ho Au, and Junbin Fang. 2019. A secure decentralized trustless E-voting system based on smart contract. In *Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE'19)*. IEEE, 570–577.

[40] Patrick McCorry, Siamak F. Shahandashti, and Feng Hao. 2017. A smart contract for boardroom voting with maximum voter privacy. In *Financial Cryptography and Data Security*, Aggelos Kiayias (Ed.). Springer International Publishing, Cham, 357–375.

[41] Christian Meter. 2017. Design of Distributed Voting Systems. arxiv:1702.02566. Retrieved from http://arxiv.org/abs/1702.02566.

[42] Microsoft CZcash: Privacy-protectingorporation. 2017. Anonymity Support for Kerberos. Retrieved July 28, 2019 from https://tools.ietf.org/html/rfc8062.

[43] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-peer Electronic Cash System. Retrieved from http://www.academia.edu/download/54517945/Bitcoin_paper_Original_2.pdf.

[44] Qassim Nasir, Ilham A. Qasse, Manar Abu Talib, and Ali Bou Nassif. 2018. Performance analysis of hyperledger fabric platforms. *Secur. Commun. Netw.* 2018 (2018). DOI: https://doi.org/10.1155/2018/3976093

[45] Mohammad Obaidat and Noureddine Boudriga. 2007. *Security of E-systems and Computer Networks*. Cambridge University Press.

[46] Somnath Panja, Samiran Bag, Feng Hao, and Bimal Roy. 2020. A smart contract system for decentralized borda count voting. *IEEE Trans. Eng. Manage.* 67, 4 (2020), 1323–1339. DOI: https://doi.org/10.1109/TEM.2020.2986371

[47] Serguei Popov. 2016. The tangle. 1 (2016), 3. Retrieved March 2019 from http://arxiv.org/abs/1705.04480.

[48] Robert Riemann and Stéphane Grumbach. 2017. Distributed Protocols at the Rescue for Trustworthy Online Voting. arxiv:1705.04480. Retrieved from http://arxiv.org/abs/1705.04480.

[49] Ronald L. Rivest, Adi Shamir, and Yael Tauman. 2001. How to leak a secret. In *Proceedings of the Confernece on Advances in Cryptology (ASIACRYPT'01)*, Colin Boyd (Ed.). Springer, Berlin, 552–565.

[50] S. F. Sayyad, Mangesh Pawar, Ashutosh Patil, Vandana Pathare, Prayag Poduval, S. F. Sayyad, Mangesh Pawar, Ashutosh Patil, Vandana Pathare, and Prayag Poduval. 2019. Features of blockchain voting: A survey. *Int. J. Innov. Res. Sci. Technol.* 5 (2019), 12–14. Retrieved from https://www.academia.edu/download/58599085/IJIRSTV5I9012.pdf.

[51] R. Schollmeier. 2001. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In *Proceedings of the 1st International Conference on Peer-to-Peer Computing*. 101–102. DOI: https://doi.org/10.1109/P2P.2001.990434

[52] Jayneel Vora, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, Mohammad S. Obaidat, and Joel J. P. C. Rodrigues. 2018. Bheem: A blockchain-based framework for securing electronic health records. In *Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps'18)*. IEEE, 1–6.

[53] Baocheng Wang, Jiawei Sun, Yunhua He, Dandan Pang, and Ningxiao Lu. 2018. Large-scale election based on blockchain. *Proc. Comput. Sci.* 129 (2018), 234–237. DOI: https://doi.org/10.1016/j.procs.2018.03.063

[54] Dr. Gavin Wood. 2014. Ethereum: A Secure Decentralised Generalized Transaction Ledger. Retrieved from https://ljk.imag.fr/membres/Jean-Guillaume.Dumas/Enseignements/ProjetsCrypto/Ethereum/ethereum-yellowpaper.pdf.

[55] Lin Zhang, Hong Li, Limin Sun, Zhiqiang Shi, and Yunhua He. 2017. Poster: Towards fully distributed user authentication with blockchain. In *Proceedings of the 2017 IEEE Symposium on Privacy-Aware Computing (PAC'17)*. IEEE, 202–203.

[56] Guy Zyskind, Oz Nathan, et al. 2015. Decentralizing privacy: Using blockchain to protect personal data. In *Proceedings of the 2015 IEEE Security and Privacy Workshops*. IEEE, 180–184.

Received March 2020; revised August 2020; accepted November 2020