A Blockchain-Based Voting System for E-Elections in Totalitarian States

Mohammad Reza Esfandyari [1], Mohammad Hossin shafiabadi [2]*

[1] Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
Email: 777.re28@gmail.com

[2] Department of Computer Engineering, IslamShahhr Branch, Islamic Azad University, IslamShahr, Iran
*Corresponding author's Email: shafiabadi@iiau.ac.ir

Abstract
The purpose of the present research was to introduce a blockchain-based voting system so that any state, including totalitarian states, can show interest in using it. In this method, a hybrid voting system with two centralized and distributed systems was used. Its centralized system is one of the most common voter identification and polling models, and its distributed system, which is designed with Ethereum public blockchain, is voting for voters. Totalitarian states are not interested in announcing the results online. Also, the lack of trust in E-voting systems by both states and voters has led to E-voting in important political elections in most states as support for manual or paper voting. Based on the results of field research with this voting system, it was possible to create a 7 min break between the end of the voting process and the announcement of the results for political considerations. This break can be increased by agreement. The results of the votes cannot be manipulated in any way. Survey results should also be communicated to voters before the voting process. This voting system can improve the level of democracy and maximum participation. It is hoped that the spread of distributed technologies, especially the blockchain, will pave the way for the spread of justice and democracy around the world.

Keywords: E-Voting, Blockchain, Ethereum, Distributed Systems, Electronic Democracy, Electronic elections

1. Introduction

Democracy means not distinguishing between members of society and when political parties see their interests at stake. It loses its meaning. New governance patterns in countries have led to some major challenges, such as poverty, gender inequality, religious strife, and many other problems. [1]. Today, there are three main threats to existing voting systems.

- Economic barriers to voting
- Confusion about votes through mail-in ballots
- An unsafe way to count votes

These barriers certainly reduce participation [2]. voting and even the concept of the Chinese blockchain have been used publicly and Electronic commercially before academic studies [3].

E-elections and blockchain technology can be a tool for expanding justice and democracy. There are different voting methods, each with different advantages and disadvantages. Despite many efforts in this area, a comprehensive

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

solution is not yet available. Paper or manual voting, in addition to wasting human time and energy, has always led to many mistakes and mistrust. It also costs a lot of money. E-voting has always been a nightmare for the organizers of such voting, with problems such as denial of mistrust systems. The study seeks to provide a way for totalitarian states to go to the voting with distributed systems. Voting is the basis of democracy, and despite complex security measures, it is not free of fraud. The introduction of an E-voting system is inherently associated with many challenges. Legal and technical procedures are among the most important of these challenges. The study aims to assess the feasibility and appropriateness of using blockchain technology in electronic voting systems in terms of technical and non-technical aspects, as well as a strategy for e-elections in totalitarian governments.

This paper introduces a two-part voting system called Hybrid Voting, in which the voting platform is designed from two separate parts. The platform's centralized system, which is in the hands of centralized institutions or the state, identifies voters and monitors public opinion. A centralized state with having this system can avoid facing the results it does not expect. The distributed system of hybrid voting is at the hands of a popular representative and will receive a vote from voters who have been identified by the state and a permission has been issued for them. Hybrid voting seeks different goals. The most important of these goals are to persuade totalitarian states to use distributed voting systems, to create public trust between voters and organizers to protect the votes received, maximum participation, raising the level of democracy and social justice in totalitarian states. The rest of the paper is organized as follows: In Section 2, the background will be introduced. In Section 3, we will introduce the presented method. Also, in Section 4, we will describe the user interface, In Section 5, we introduce the benefits of the method and in Section 6, we examine the experimental results obtained from field research, and we also compare this research with the research of others. Finally, in Section 7, we will draw conclusions.

2. Research Background and related work

GEETANJALI RATHEE and et al. [4] purposed the Smart City is an environment that interacts with smart sensors, the Internet of Things, and 5G technology. One of the demands of the users of these cities is electronic voting, which leads to problems such as privacy and security violations. In order to create a legal communication environment and prevent data changes and other security issues, we can use the Blockchain platform. Manish Verma. [5] provided Voting is one of the most important processes in democracy. In an mature democracy, people vote for their representatives. The main concern in a voting system is voter privacy. One of the most agile forms of electronic voting is the blockchain platform. The platform uses a distributed ledger with a consensus algorithm. V N Killer et al. [6] stated One of the consensus protocols for a blockchain voting platform is the Knowledge Proof Protocol, which is based on asymmetric and zero encryption and digital signatures. This protocol is implemented using AVISPA software. Zuo Et al. [7] believed the security is one of the main concerns of voting systems. Hackers can forge the legal signature of any message. The provided executive plan is able to detect an invalid signature by analyzing the actual package. The plan warns at regular intervals that the system administrator will take steps to reduce intrusion into the system. Hjálmarsson et al [8] said the implementing a voting system that leads to public satisfaction is a difficult task. Legal requirements and limitations are another challenge. As a service for conducting E-elections, the blockchain can meet some of these challenges. It can also reduce costs Wei et al. [9] expressed data security and integrity is another major challenge in cloud computing, with solutions offering overly computational complexity or non-scalability. By creating a blockchain-based cloud and "block and response" mode, as well as hash blocks, data integrity can be ensured. Noizat [10] stated the most existing E-voting systems rely on a centralized and specialized system that simultaneously controls the system's database and output. As a database, Blockchain generates secure transactions and can also provide transparency and trust between voter and organizer. Zhu et al. [11] expressed blockchain distributed system is used in a wide range of applications and various financial and infrastructure areas. Blockchain is a fair and transparent data-sharing environment in which unauthorized data manipulation can be tracked and monitored. It also has limitations, including 51% attacks. Lee and lee [12] mentioned blockchain was first introduced by Satoshi Nakamoto in 2009. It was first used to verify financial transactions without third-party for Bitcoin, which is a digital currency. In the blockchain, blocks are used to store transactions. Each block is linked to the previous block by hash. Each header consists of a block and a block body. In Bitcoin, a transaction is played across the network. Ho Huh and Seo [13]believed identification and security issues are one of the challenges of identity verification. The problem of opening with a stolen pin or such issues can be problematic. Blockchain can be used to design an integrated login platform to automatic system based on fingerprint recognition which have enough security

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

against manipulation, forgery and hacking by hackers. Gohar et al. [14] stated one of the best modes for voting services is that voters cannot coordinate their actions, but they are allowed to change their votes after seeing the current results. Thus, changing the votes by the voter can be good results for a comprehensive social choice. Jr Lai et al. [15] provided transparency with privacy is one of the hallmarks of reliable voting systems. Every vote must be anonymous and be counted correctly. At the same time, it must have the least dependence on the state. Ethereum blockchain can meet these expectations, and anyone can access the network, meaning that third-party interference after voting is almost impossible. Khoury et al. [16]proposed given that most voting systems are centralized and in the hands of the state bodies. Ethereum blockchain can solve the problem of centralization in addition to maintaining privacy, integrity and transparency. Ethereum blockchain is a good choice for a distributed voting system as it can support smart contracts with a distributed user interface. Fan et al. [17]believed online voting plan use a digital signature algorithm to verify the identity of the voter so that the voter's identity is undeniable. This imposes a heavy workload on the network. Using Homomorphic Encryption (HSE) can enhance the privacy, security, and validity of votes while simultaneously creating encryption and signing of paper and adjusting the workload. Mehboob Khan et al. [18] suggested voting is the base of democracy, and blockchain technology can serve that purpose However, its use requires a wide range of factors, such as blockchain generartion, transaction speed, and block size which plays a decisive role in its performance. Scalability and efficiency are among the determinant factors of a distributed system. Hardwick et al. [19] expressed blockchain can be used as a transparent voting box and can also be designed so that voters can change their vote during the authorized voting period. This view can have both social positive and negative aspects. Voas and Kshetri [20] mentioned e-voting with the blockchaink can greatly reduce fraud, and voters can vote using a computer or mobile. One of the main challenges of voting with the blockchain is the public's trust in distributed systems. ZHU et al. [21] proposed with the blockchain, a different voting protocol can be created. It is also possible to introduce a new consensus mechanism that does not involve lateral costs and unnecessary blocks, and it is also possible to provide new signature schemes to ensure immediate approval and avoid the problem of re-spending. Malomo et al. [22] suggested with blockchain technology, the BDG gap for cyberattacks can be reduced. Given that minimizing BDG is a major concern for organizations and states, blockchain could be a solution. Jiang et al. [23] believed blockchain-based distributed storage allows users to share their data without the help of a centralized service provider. Therefore, server failure cannot cause data loss, but it is facing with the problem of privacy. Serchain recovers and maintains reasonable costs without disappearing privacy. Osgood and Chow [24] stated the current voting system is fraught with problems. Blockchain gives us a lot of potential and can be one of the most lucrative technologies in recent years. Although voting with blockchain is not perfect, it can make a big difference. Danish et al. [25]believed one of the security issues is the replay attacks that occur when connecting to the LoRaWAN network. Blockchain can provide a way to join LoRaWAN networks to develop a reliable and trustworthy authentication system for LoRaWAN networks. Yu et al. [26] expressed encryption techniques are used to ensure voting systems. Third parties in these systems must be trusted by the public. Blockchain-based solutions can solve this problem. Homomorphic encryption and signature with PoKs between voters and blockchain can ensure the accuracy and security of the voting system. Pavithran et al. [27] mentioned blockchain can also run IoT-based networks and solve many of the current problems in IoT. Of course, efficient architecture is not yet available for the blockchain IoT. Blockchain can provide a wide range of benefits for IoT. Feng et al. [28] said consensus is one of the key features of Blockchain networks. Also, the mechanism of traditional consensus algorithms mechanisms is such that it may provide opportunities for attackers to attack system denials to miners. Proof-of-negotiation (PON) is a new consensus algorithm that can replace traditional consensus algorithms and solve the problem of system denial attacks. FENG et al. [29] provided blockchain has a low speed as a distributed database technology in transaction transmission. To solve this problem, we can use a new architecture called Double-Channel Parallel model (DCPB). SHAHZAD and CROWCROFT [30]suggested the failure of E-voting systems is a security and privacy flaw, and it makes the E-voting has not had a bright past. Effective techniques of hashing blockchain settings and the concept of blocking can solve the problems in the voting process. Ayed [31] stated blockchain can be used in local or national elections. Blockchain-based system is secure and reliable and anonymous, and will help increase voter turnout as well as people's trust in states. Liu and Wang [32] saiad by using the blind signature model in permitted blockchain, a new protocol can be suggested which allowing some access for individuals. Kubjas et al. [33] declared although the Internet and the blockchain are tools of democracy, by examining some of the protocols and solutions presented, it can be seen that the solutions presented are without considering some basic issues and still have to wait for further progress in this area. Lu et al. [34] provided as a service (BaaS), blockchain is a solution for improving and developing services. However, designing blockchain-based programs can be used to track

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

quality in the real world in terms of feasibility and scalability. Hanifatunnisa and Rahardjo [35] said for preventing fraud in the blockchain voting system, it is recommended that instead of a POW consensus algorithm, a one-time predetermined system-based approach for each blockchain node can be used for each blockchain node. In this way, the collision of packages during transfer is also prevented. Pawlak et al. [36] proposed the combination of smart factors and the concept of a multifunctional system that integrates the E-voting process with Blockchain technology (ABVS) can provide an end-to-end voting system. One of the advantages of such a system is security, as well as the lack of congestion in voting stations. Wang et al. [37] mentioned one of E-voting methods is non-interactive and non-receivable method with a smart contract and one-time ring signature and homomorphic encryption. This signature model is used to keep the voter anonymous. Smart contract seeks for all operations of recording, management and computing during the voting process. Saqib et al. [38] expressed numerous E-voting methods have been proposed so far, none of which are complete. One of these methods is the E-voting protocol based on double signatures, which guarantees the viewing of voting information only for the intended parties. The double-signature E-voting protocol can be used for large-scale elections because it is a cost-effective solution for the voting process. The only limitation of the proposed protocol is that voting information with the voter's identity can only be identified if both the authentication server and the voting server want to know it. CasaDo-VaRa and CoRCHaDo [39] stated during the political election campaign, citizens receive information about the candidates and decide who to support. After the end of this period, they go to vote for their trusted candidate. However, we need to question the validity of our voting methods and see how this technology can be used to make these methods safer. The use of blockchain technology can prevent election fraud.

Although there are several different technologies used to solve the problem of e-elections, each of which has its advantages and disadvantages, but almost none of them are comprehensive, and cannot meet all the needs of a comprehensive E-voting system. In most elections of high political importance, the state turns to the voting paper system, and e-elections are backing up. Totalitarian states are not interested in using distributed voting systems. This paper presents a blockchain-based voting system that uses a centralized, state- authentication system and can be of interest to organizers with different tastes. The organs involved in this system, the voting steps, monitoring and security are the main topics of this voting method. The main goals of this paper include:

- Provide a blockchain-based voting system for states, especially totalitarian states
- Monitor public opinion before the election and using collective wisdom
- Create public trust between states and nations and maximize participation in elections
- Delay between the end of voting and the announcement of the results, in order to apply political consideration
- Consensus on a fully E-voting system
- Control of the voting process by the people and the state

3. Proposed Method

By presenting a two-part platform consisting of two centralized and distributed parts, hybrid voting tries to minimize the problems of E-voting and to get an acceptable result from an e-voting system that is approved by states and the nations. It is tried that centralized system to act as a flexible regulator, and if the organizer doesn't need it, it can be deleted

3.1 Centralized System

In this system, hybrid voting has used a common authentication model in voting systems and uses this model to authenticate voters and issue permissions. This system is entirely in the hands of states, and authentication of the voter is done by it, who finally sends an identification number or pin to the voter after verification, which the voter uses to log in to the user interface. He will be sent to Blockchain to get a vote. In fact, this system creates a regulatory role for the entire voting system, and it allows centralized states to control the voting system. In this system, it is possible that states, in addition to identifying and issuing the necessary permissions to participate in the voting process, monitor the opinions of voters and have a clearer view of the results of the voting process by reviewing and analyzing public opinion. In the survey form, each organizer can ask questions to the voter according to their social, cultural and spatial

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

consideration. Voters were asked to predict the election results and were informed of the survey results to the participants from the collective wisdom before the election.

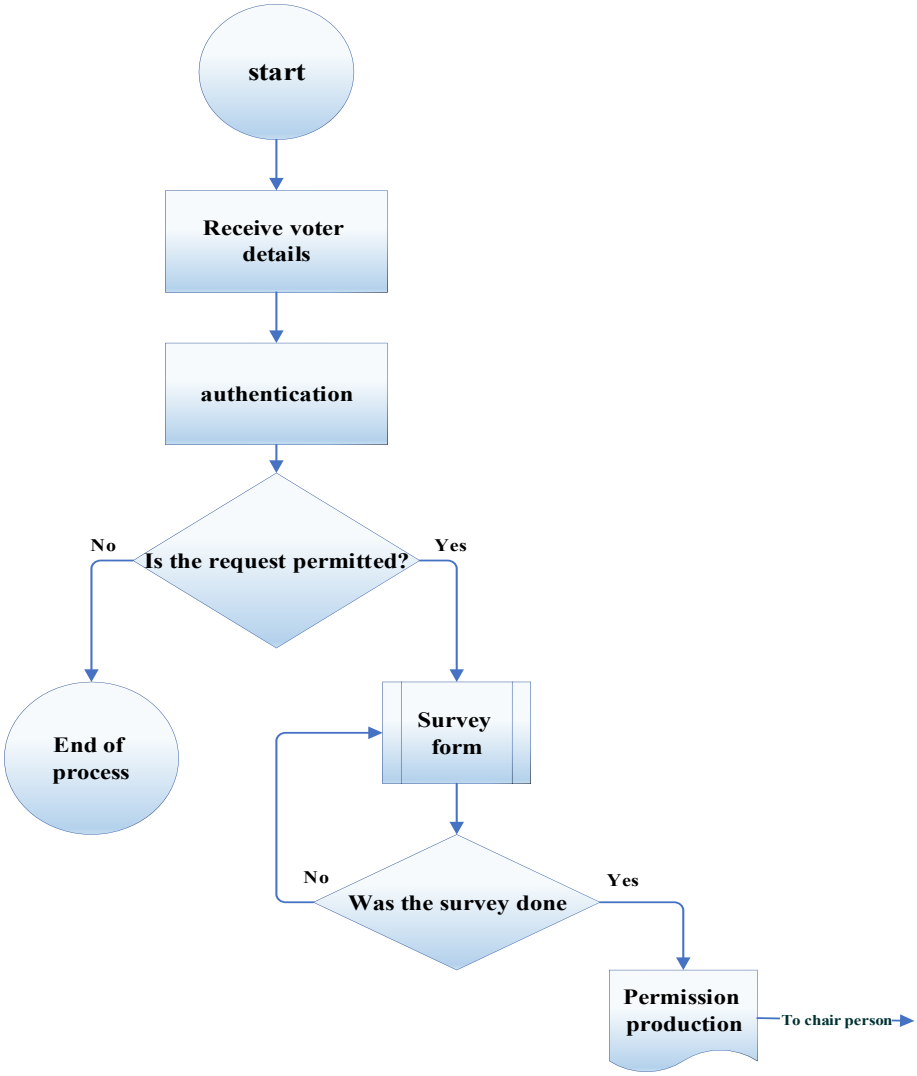


Fig. 1: Flowchart of centralized system

Figure 1 shows the voter identification process in the form of a flowchart. The authentication body can provide a questionnaire to monitor the voter's thoughts after authentication. This plan is such that the voter can act voluntarily to answer the questionnaire questions and not answer the questions.

3.2 Distributed System

In this system, hybrid voting uses Rinkeby test network server, the codes is executed on the Remix platform and has been implemented to test and get the network report on the Rinkeby platform. These are the most fundamental changes to the distributed system of hybrid voting. Definition is a function that performed the return of results with a delay that had already been agreed between the organizing agents, the representative of the centralized system and the representative of the distributed system.

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

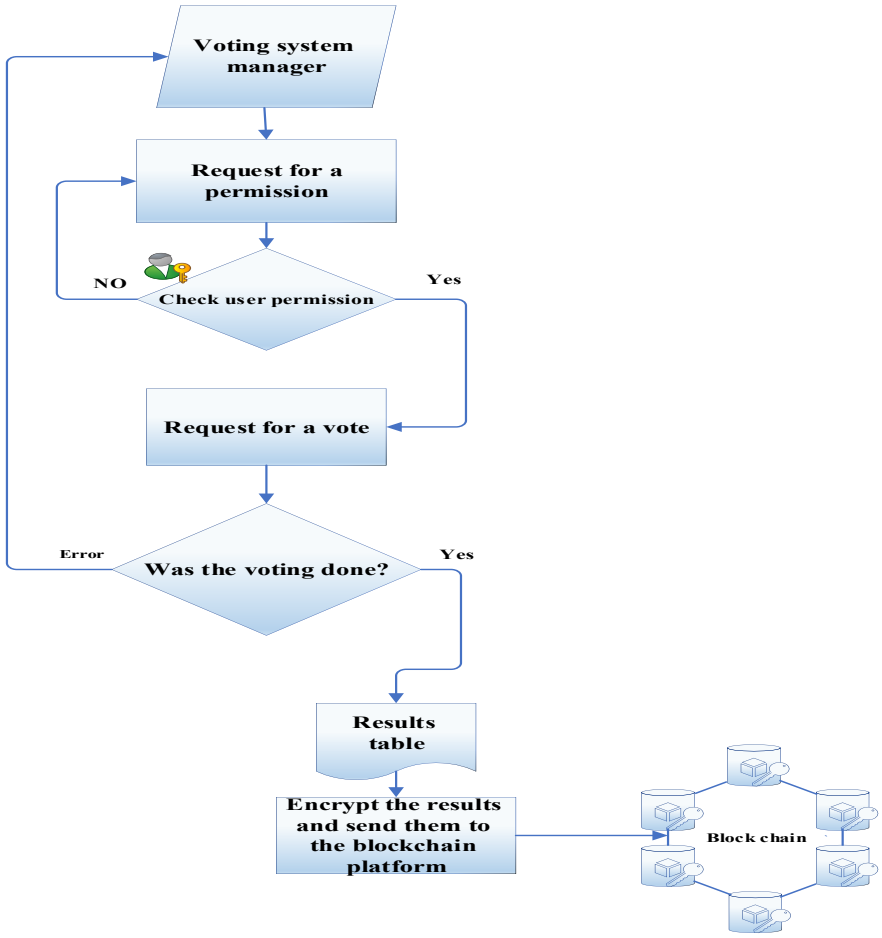


Fig. 2: Flowchart of distributed system

Figure 2 summarizes the login steps for permitted voters to the Blockchain platform and the voting process.

4. Blockchain-Based User Interface

This architecture is suitable for all types of mobile devices or personal computers and any other computing device. It is also one of the easiest ways to run, which includes the three steps of registration, electronic meeting and ending the voting process, which are described below.

4.1 Registration Process

a- Download and install the software, b- Production of a pair of public and private keys through the user interface, c- Provide voter details, d- Confirmation of documents by the server and provide ID to the voter.

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

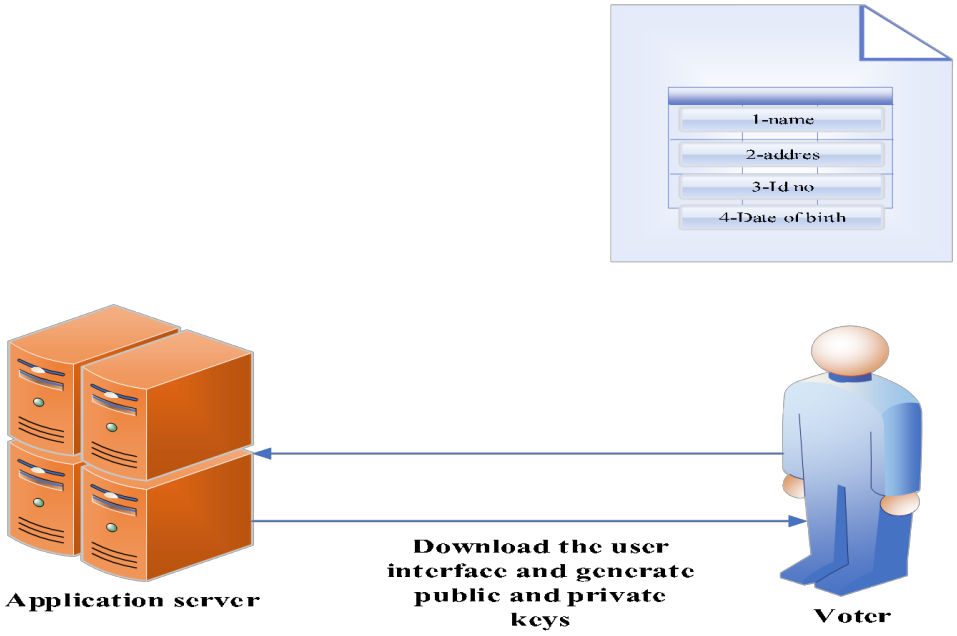
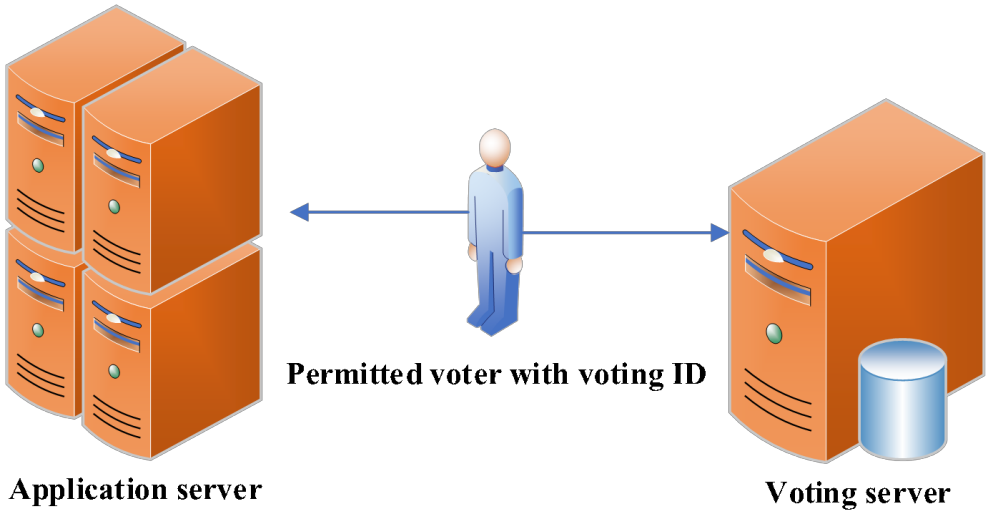


Fig. 3: Registration process

4.2 Connect to the Voting Server

a-Voter documents and voting ID will be sent to the application server. b- The server processes the files. c- A unique ID is created in the relevant paper. d- This voting ID can only be used once. e- The relevant owner encrypts the application server. f- ID shall be sent to the relevant owner with the general voter key. g- Private key will prevent identity fraud because attackers cannot access votes without it. h- The E-voting system will never accept inappropriate voting



DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

Fig. 4: The connection of permitted voter to the voting server

The application server and the E-voting server are separate, and there is only one network node between the application server and the E-voting server to communicate and exchange voter information and ID. This application server stores all the relevant information of the voters and the voting information is counted at the same time as it is stored on the voting server. However, the results of the counted votes cannot be seen until they have been identified between the organizing body and the authentication body.

4.3 Voting Electronic Meeting

At the voting meeting, voters can apply their votes by an E-voting server. The voting page includes the voter and the voter's public address and digital signature. Digital signatures are just a pseudonym. Voters can only see their vote. Verification is done through the voting server. All provided and encrypted votes of voting results will not be visible before the end of the voting period. At the end of the meeting, it is not possible to change the votes and connect to the blockchain network.

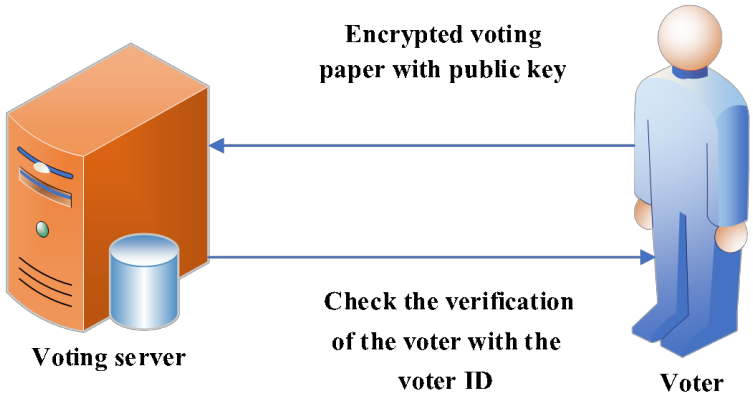


Fig. 5: Voting Electronic meeting

4.4 After Voting

After the end of the voting meeting, the operation begins after the voting. Figure 6 shows the private key of the application server, and it decrypts encrypted votes, and the results can be counted. The system uses blockchain technology and a hidden key to maintain the integrity and confidentiality of the results.

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

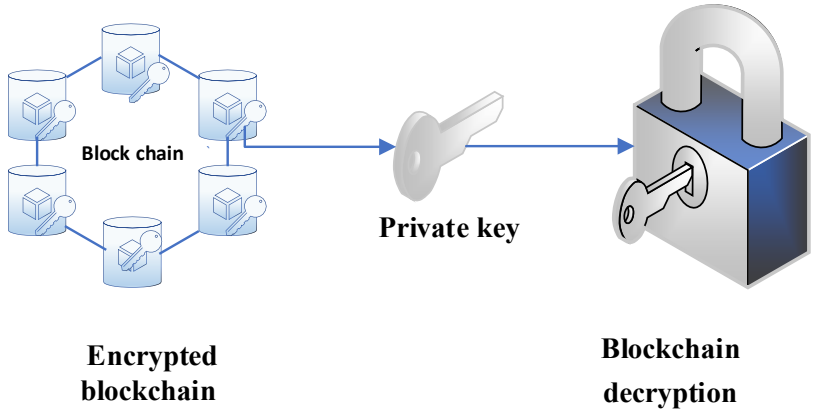


Fig. 6: End of voting procedure

The blockchain of the voting result consists the following elements:

1- Previous block value, 2- Voting excel information and a random number, 3- Candidate information, 4- Information of the first voting block, 5- Last voting block, 6- Block, after the end of voting, containing a special ID indicates the end of the voting steps.

5. Advantages of Hybrid Voting System

This system only records the votes of the voters who have already registered. This system is able to verify the identities of the voters and fraud does not occur in the identity. Documents are with digital signatures and asymmetrical encryption. Since all blocks are connected, whenever the existence of a block is compromised, anyone can easily recover it. Also, given the above and the properties of blockchain technology, anyone can prove that he/she is the sender of the desired vote. All votes received by the system must be accurate and any open vote must be counted and cannot be repeated. Voting integrity is supported by hashing technology. The sequence is the previous hash block and the current voting information of this cycle forms a continuous chain related to the hash block. Votes will be decrypted after the end of the voting process, and the election results will be made available to the public. Everyone is watching the non-participation in the elections. The results of the voting will be shared publicly. Any voter can see both the result and the vote alone. The final result of the election will be visible without dependence on the central authorities.

5.1 Performing field voting operations manually and online and comparing it with hybrid voting

To test hybrid voting system, three methods of manual or paper voting and online voting, as well as voting using the method provided by hybrid voting in a 50-member statistical population were first tested. The tools required in this application are two parts hybrid voting application and a common and online voting software, as well as a human group that performed manual or paper voting operations. The statistical population was the same in terms of number in the above three methods.

In the traditional voting method, it was tried to act exactly like the traditional voting stations. A statistical population of fifty people was selected in which all steps of voting, from authentication to voting, were performed in a manner similar to actual voting by paper and manual. The online voting method used an online voting robot as well as a statistical population of fifty people, and the identification process was performed by the admin. In the voting method, hybrid voting method used a statistical population of fifty people, whose authentication was performed by a centralized system, and each permitted voter was directed to the blockchain platform to obtain a vote.

6. Experimental results

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

In each of voting methods, the voting process was repeated to ensure that the result was repeated in five steps, in order to achieve more accurate results. Figure 7 shows the average identification time, the voting time and the counting time, as well as the total time of the voting process on average in five steps of manual or paper voting as bar charts. Figure 8 shows the above values in online voting as bar charts, and Figure 9 shows the same values in the voting using the proposed hybrid voting method. Comparing the above times, it can be seen that the proposed method of hybrid vetting has been able to create a seven-minute delay between the end of voting and the announcement of results, in addition to taking advantage of E-voting.

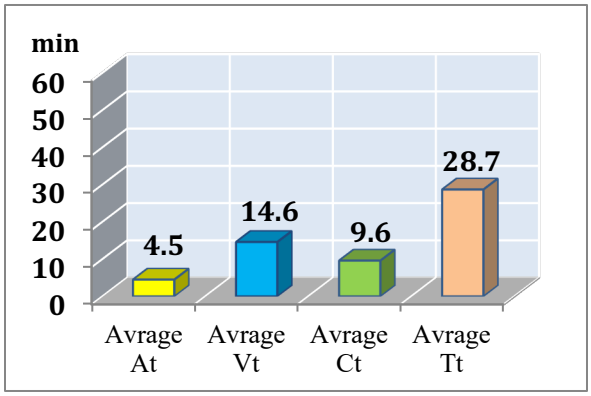


Fig. 7: Average manual voting times

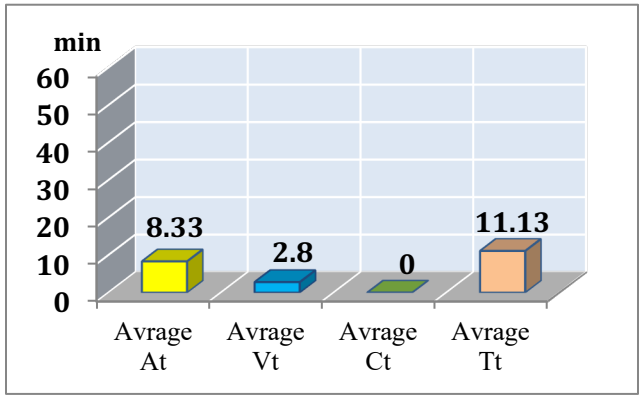
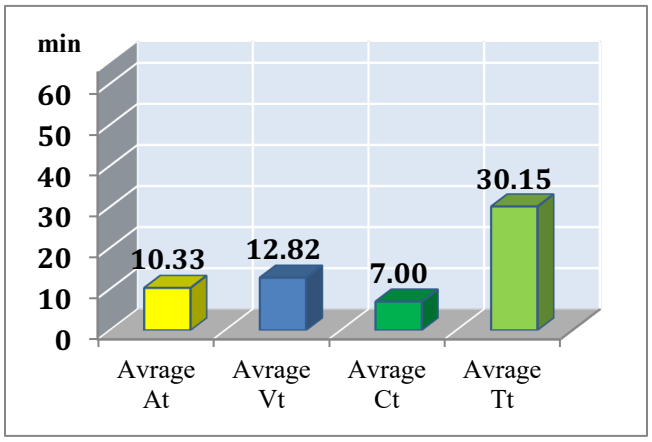


Fig. 8: Average online voting times



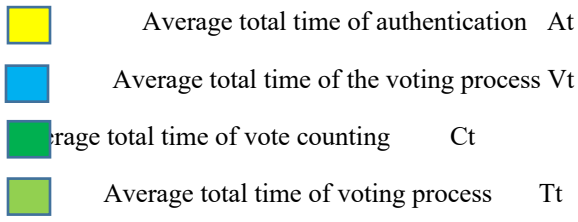


Fig. 9: Average hybrid voting time

In the traditional voting method, the following findings were obtained

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

1- Act time refers to all the time wasted by the organizing human factors.

2- React time is all the time wasted by the voter and depends on human factors. In traditional voting, these two factors are inseparable, and in all voting operations where these two factors are separable, they are not separated. Due to the correct comparison in voting in the traditional way, a lot of human time and money is wasted, while the cost of materials (paper) is high. In addition, the possibility of fraud and error in it is very high. The times are round.

In the online voting method, spending time and money is not in the traditional way. Execution time and human error have been significantly reduced. While the security of this method is extremely risky, this method is usually used for low-value surveys or as support is used in voting operations. The counting time of the votes and announcement of the results in different software and hardware depend on the source of the software and the hardware clock for each vote can be a fraction of a second. In this method, the voting process was completed before the expiration of the legal time.

In this method, in addition to minimizing the problems of the traditional voting method, the time of the voting process has increased due to the increase in the authentication process, which is related to the two-part authentication process. Meanwhile, the problem of 51% attacks remains if the system is implemented on Ethereum. In this method, the voting process is completed before the legal time. In this method, the advantage of distribution is used, which ensures the preservation of the integrity of the votes. The data obtained from the voting is rounded up in the above three methods.

6.1 Verification

Table 1 deals with the time of the transaction verification on the Rinkeby network. As can be seen, the transaction verification is increasing from the first voter to the third voter, respectively, except for the creator of the smart contract, which takes more time. Table 2 shows the numerical values for reference 5 for comparison. The above times are usually no more than one minute due to the limited size of a block. The time difference is due to network occupancy. Definitely in a wide and real voting on the Ethereum platform, it faces problems such as high number of addressability and scalability, as well as the speed of transaction verification, and another solution must be found to solve these problems. We suggest using faster algorithms with better performance.

Table 1: Reports of the verification times of the first three transactions of the Rinkeby network

	Contract Creation	**Voter-1 Transaction**	**Voter-2 Transaction**	**Voter-3 Transaction**
Voting-1	42s	30s	35s	40s
Voting-2	37s	20s	27s	32s
Voting-3	45s	25s	31s	35s
Voting-4	48s	32s	35s	60s
Voting-5	57s	35s	40s	57s

Table 2: Report of the verification times of the first three transactions related to reference 5

	Contract Creation	**Voter-1 Transaction**	**Voter-2 Transaction**	**Voter-3 Transaction**
Voting-1	38s	33s	47s	49s
Voting-2	32s	32s	45s	45s
Voting-3	42s	39s	56s	56s

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

Voting-4	47s	36s	54s	54s
Voting-5	1m 1s	32s	28s	28s

6.2 Validation

- **Comparison of three parameters of speed, accuracy, security and democracy in voting systems**

As can be seen in Table 3, in the manual voting system, the parameters of security, speed, accuracy and democracy are also completely dependent on the organizer, and the possibility of any forgery and misuse in it is not far from expectation. Also, in the types of online voting systems, it can be seen that the voting process, while having a very high speed and accuracy, has a very low level of security and democracy in terms of centralized database. In the proposed hybrid voting system, while taking advantage of E-voting systems, given that the blockchain is a distributed system and has a very high level of security and transparency, we can expect that our proposed system will be safe and democratic, which is the need for voting system. We compared our experimental observations recorded in Table 3 with the reference results [1] listed in Table 4.

Table 3: Comparison of four parameters of security, accuracy, speed and democracy in voting systems

Voting systems	Security	Accuracy	Speed	Democracy
Manual	Completely depending on the organizer	Depending on the organizer	Depending on the organizer	Depending on the organizer
Online	Unsecured DDOS denial attacks	Relatively good	High	Low
Hybrid voting	Secured	Excellent with authentication	High	High

Table 4: Comparison of the security services of different solutions Reference Number [1]

	Blockchain	***Database***	***Distributed data base***
Integrity of the Records	High	Moderate	Moderate
Availlitabiy	High	Low	Moderate
Fault Tolerance	High	Low	Low

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

Privacy	Low	High	Moderate

Table 5 is for reference [1], which includes four voting projects in terms of the type of Ledger programming language and token, as well as their consensus algorithm. In Table 6, we compared the same specifications of Hybrid voting with the above four projects. In addition, our suggestion for consensus algorithms for a scalable voting system is to use faster consensus algorithms with better performance.

Table 5: Classification of Selected Voting Projects Based on Blockchain Reference Number [1]

	Ledger	***Language***	***Token***	***Consensus Protocol***
StakeWeighted Voting	BitShares Blockchain	C++	Bitshares BTS	Delegated PoS (DPoS)
Polys.me	Ethereum	Solidity	Unspecified	PoW
Boulé	Ethereum	Solidity	Boulé BOU Token	PoS
Sovereign	Bitcoin	Python	Bitcoin BTC	PoW

Table 6: Hybrid Voting Project

	Ledger	***Language***	***Token***	***Consensus Protocol***
Hybrid voting	Ethereum	Solidity	No token	PoA

6.3 Disccussion

Hybrid voting has proposed a voting system that is agreed upon by the organizer and the voter, as well as an election for totalitarian states in the hope that it will increase democracy. Online voting is usually a nightmare for organizers. Voting in the traditional way leads to many problems, such as fraud, mistrust, fraud and organizing cost. One of the problems with the proposed system is its widespread addressability and scalability, and its most fundamental problem is proof-of-work algorithm of Ethereum. Gaps are one of the weaknesses for 51% attacks, and it is recommended that other algorithms be used for voting systems. Given that the field of consensus algorithms is a very complex and extensive field for research, e-voting systems do not yet have a coherent consensus algorithm. This field is recommended for further research. With the design of hybrid voting, it is concluded that it is better to consider the following points in the design of future voting systems for designers and developers. 1- The production of a permitted private blockchain should be considered. 2- In the field of consensus algorithms, serious research has been done to finally reach an acceptable consensus for the production of an algorithm that meets the expectations of a coherent voting system. It is recommended that the algorithm be designed to monitor candidates' votes at alternate times and replace the transaction verifier according to the maximum number of votes. In this way, the transactions verifier is in fact the same as the majority of the participants in the elections. One of the discussed issues was in the survey form

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

and the announcement of the results before the voting. Our goal in proposing this form was to raise awareness of collective wisdom for participants, which was accompanied by discussions, including the effect on participants' votes, which seems to need to be examined by experts in the field of social cognitive sciences. For the centralized system, in addition to the form of monitoring the votes, it is suggested that the election results be contested as a token. This plan can lead to maximum participation. This plan can lead to maximum participation. Due to the fact that the research method is field operations and the limitation of the research until the above reforms are done, the research cannot be generalized more than what has been studied.

7. Conclusion

Hybrid voting was designed on a two-part platform with the goal of being used by centralized states. It seems that totalitarian states are not interested in announcing the results at the moment of end of the voting process. One of the main goals is the delay between the end of the voting process and the announcement of the results in a mechanized manner and free from factional and human decisions. Considering this break is for political reasons. We think that this voting system, in addition to improving the level of democracy, can provide the opinion of these states.

This system takes advantage of a centralized mode in which the authentication and issuance of a permission is done by the government or a state agency. The second part, which is distributed, uses a public blockchain managed by a public body. The effort is to create an election without manipulation of votes and with a mechanized delay in announcing the results, which is of interest to totalitarian states. Hybrid voting was tested in two common paper or manual and online voting methods in a field research. Hybrid voting presented a method in which, in addition to solving the problems of traditional voting, it also did not have the problems of online voting and enjoyed relatively good security and transparency. Overall, China's blockchain technology is still immature for use in a comprehensive and complete voting system, but it has great potential for implementing a comprehensive voting system.

- Encourage totalitarian states to use distributed systems in E-elections
- Create a break in agreement between the organizer and the voter representative for political considerations
- Encourage as many participants as possible to participate in the election process to the maximum
- Create a survey form and monitor public opinion and share it before the election process
- No manipulate votes after voting
- Observe the voting process by the state and voters

References

[1] A. Behera, “Shivarthu : A new blockchain based , decentralized fair democracy inspired by,” 2020.

[2] J. Susskind, “Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System,” *San Diego Law Rev.*, vol. 54, no. 4, p. 785, 2017.

[3] U. C. Çabuk, E. Adıgüzel, and E. Karaarslan, “A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems,” *Ijarcce*, vol. 7, no. 3, pp. 124–134, 2018, doi: 10.17148/ijarcce.2018.7324.

[4] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, “A review of E-voting: the past, present and future,” *Ann. des Telecommun. Telecommun.*, vol. 71, no. 7–8, pp. 279–286, 2016, doi: 10.1007/s12243-016-0525-8.

[5] A. K. Koç, E. Yavuz, U. C. Çabuk, and G. Dalkiliç, “Towards secure e-voting using ethereum blockchain,” *6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding*, vol. 2018-Janua, no. February, pp. 1–6, 2018, doi: 10.1109/ISDFS.2018.8355340.

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

[6] G. Dini, "A secure and available electronic voting service for a large-scale distributed system," *Futur. Gener. Comput. Syst.*, vol. 19, no. 1, pp. 69–85, 2003, doi: 10.1016/S0167-739X(02)00109-7.

[7] L. Zuo, N. Kumar, H. Tu, A. Singh, N. Chilamkurti, and S. Rho, "Detection and analysis of secure intelligent universal designated verifier signature scheme for electronic voting system," *J. Supercomput.*, vol. 70, no. 1, pp. 177–199, 2014, doi: 10.1007/s11227-014-1149-2.

[8] A. Alam, S. M. Zia Ur Rashid, M. Abdus Salam, and A. Islam, "Towards Blockchain-Based E-voting System," *2018 Int. Conf. Innov. Sci. Eng. Technol. ICISET 2018*, pp. 351–354, 2018, doi: 10.1109/ICISET.2018.8745613.

[9] P. C. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Futur. Gener. Comput. Syst.*, vol. 102, pp. 902–911, 2020, doi: 10.1016/j.future.2019.09.028.

[10] P. Noizat, *Blockchain Electronic Vote*. Elsevier Inc., 2015.

[11] L. Zhu, Y. Wu, K. Gai, and K. K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Futur. Gener. Comput. Syst.*, vol. 91, pp. 527–535, 2019, doi: 10.1016/j.future.2018.09.019.

[12] B. Lee and J. H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, 2017, doi: 10.1007/s11227-016-1870-0.

[13] J. H. Huh and K. Seo, "Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing," *J. Supercomput.*, vol. 75, no. 6, pp. 3123–3139, 2019, doi: 10.1007/s11227-018-2496-1.

[14] N. Gohar, S. Noor, F. F. Babar, A. Malik, and S. Shaheen, "Dynamics of manipulation in voting, veto and plurality," *Cluster Comput.*, vol. 22, pp. 7333–7345, 2019, doi: 10.1007/s10586-018-1921-9.

[15] W. J. Lai, Y. C. Hsieh, C. W. Hsueh, and J. L. Wu, "DATE: A Decentralized, Anonymous, and Transparent E-voting System," *Proc. 2018 1st IEEE Int. Conf. Hot Information-Centric Networking, HotICN 2018*, no. HotICN, pp. 24–29, 2019, doi: 10.1109/HOTICN.2018.8605994.

[16] D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain," *2018 IEEE Int. Multidiscip. Conf. Eng. Technol. IMCET 2018*, pp. 224–229, 2019, doi: 10.1109/IMCET.2018.8603050.

[17] X. Fan, T. Wu, Q. Zheng, Y. Chen, M. Alam, and X. Xiao, "HSE-Voting: A secure high-efficiency electronic voting scheme based on homomorphic signcryption," *Futur. Gener. Comput. Syst.*, 2019, doi: 10.1016/j.future.2019.10.016.

[18] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Futur. Gener. Comput. Syst.*, vol. 105, pp. 13–26, 2020, doi: 10.1016/j.future.2019.11.005.

[19] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," *Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree*, pp. 1561–1567, 2018, doi: 10.1109/Cybermatics_2018.2018.00262.

[20] "Blockchain-Enabled E-voting By: Nir Kshetri and Jeffrey Voas Kshetri, Nir and Voas, J. (2018)." Blockchain-Enabled E-voting ", IEEE," vol. 35, pp. 95–99, 2018.

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

[21] Y. Zhu, K. Riad, R. Guo, G. Gan, and R. Feng, "New instant confirmation mechanism based on interactive incontestable signature in consortium blockchain," *Front. Comput. Sci.*, vol. 13, no. 6, pp. 1182–1197, 2019, doi: 10.1007/s11704-017-6338-8.

[22] O. O. Malomo, D. B. Rawat, and M. Garuba, "Next-generation cybersecurity through a blockchain-enabled federated cloud framework," *J. Supercomput.*, vol. 74, no. 10, pp. 5099–5126, 2018, doi: 10.1007/s11227-018-2385-7.

[23] P. Jiang, F. Guo, K. Liang, J. Lai, and Q. Wen, "Searchain: Blockchain-based private keyword search in decentralized storage," *Futur. Gener. Comput. Syst.*, 2017, doi: 10.1016/j.future.2017.08.036.

[24] R. Sakwa, "The Future of Russian Democracy," *Gov. Oppos.*, vol. 46, no. 4, pp. 517–537, 2011, doi: 10.1111/j.1477-7053.2011.01348.x.

[25] S. M. Danish, M. Lestas, H. K. Qureshi, K. Zhang, W. Asif, and M. Rajarajan, "Securing the LoRaWAN join procedure using blockchains," *Cluster Comput.*, vol. 8, 2020, doi: 10.1007/s10586-020-03064-8.

[26] B. Yu *et al.*, "Platform-Independent Secure Blockchain-Based Voting System," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11060 LNCS, pp. 369–386, 2018, doi: 10.1007/978-3-319-99136-8_20.

[27] D. Pavithran, K. Shaalan, J. N. Al-Karaki, and A. Gawanmeh, "Towards building a blockchain framework for IoT," *Cluster Comput.*, 2020, doi: 10.1007/s10586-020-03059-5.

[28] J. Feng, X. Zhao, K. Chen, F. Zhao, and G. Zhang, "Towards random-honest miners selection and multi-blocks creation: Proof-of-negotiation consensus mechanism in blockchain networks," *Futur. Gener. Comput. Syst.*, vol. 105, pp. 248–258, 2020, doi: 10.1016/j.future.2019.11.026.

[29] L. Feng, H. Zhang, W. T. Tsai, and S. Sun, "System architecture for high-performance permissioned blockchains," *Front. Comput. Sci.*, vol. 13, no. 6, pp. 1151–1165, 2019, doi: 10.1007/s11704-018-6345-4.

[30] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.

[31] A. Ben Ayed, "A Conceptual Secure Blockchain Based Electronic Voting System," *Int. J. Netw. Secur. Its Appl.*, vol. 9, no. 3, pp. 01–09, 2017, doi: 10.5121/ijnsa.2017.9301.

[32] Y. Liu and Q. Wang, "An E-voting Protocol Based on Blockchain," *IACR Cryptol. ePrint Arch.*, p. 1043, 2017.

[33] I. Kubjas, "Using blockchain for enabling internet voting," pp. 1–6, 2017, doi: 10.1007/s00216-001-1099-4.

[34] Q. Lu, X. Xu, Y. Liu, I. Weber, L. Zhu, and W. Zhang, "uBaaS: A unified blockchain as a service platform," *Futur. Gener. Comput. Syst.*, vol. 101, pp. 564–575, 2019, doi: 10.1016/j.future.2019.05.051.

[35] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," *Proceeding 2017 11th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/TSSA.2017.8272896.

[36] M. Pawlak, A. Poniszewska-Maránda, and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," *Procedia Comput. Sci.*, vol. 141, pp. 239–246, 2018, doi: 10.1016/j.procs.2018.10.177.

[37] B. Wang, J. Sun, Y. He, D. Pang, and N. Lu, "Large-scale Election Based on Blockchain," *Procedia Comput. Sci.*, vol. 129, pp. 234–237, 2018, doi: 10.1016/j.procs.2018.03.063.

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021

[38] M. N. Saqib *et al.*, "Anonymous and formally verified dual signature based online e-voting protocol," *Cluster Comput.*, vol. 22, pp. 1703–1716, 2019, doi: 10.1007/s10586-018-2162-7.

[39] R. Casado-Vara and J. M. Corch ado, "Blockchain for Democratic Voting: How Blockchain Could Cast off Voter Fraud," *Orient. J. Comput. Sci. Technol.*, vol. 11, no. 1, pp. 01–03, 2018, doi: 10.13005/ojcst11.01.01.

DOI: 10.5281/zenodo.5197845
Received: December 26, 2020 Accepted: May 19, 2021