Online Voting System Based on IoT and Ethereum Blockchain

5 authors, including:

Awsan Othman
Taiz University
1 PUBLICATION   **15** CITATIONS

SEE PROFILE

Mogeeb Mosleh
Taiz University
55 PUBLICATIONS   **444** CITATIONS

SEE PROFILE

Online Voting System Based on IoT and Ethereum Blockchain

Awsan A. H. Othman
Dept. of Software Engineering
Taiz University
Taiz, Yemen
AwsanOthman@gmail.com

Emarn A. A. Muhammed
Dept. of Software Engineering
Taiz University
Taiz, Yemen
AlhaddadEmran@gmail.com

Haneen K. M. Mujahid
Dept. of Software Engineering
Taiz University
Taiz, Yemen
Han988KM@gmail.com

Hamzah A. A. Muhammed
Dept. of Software Engineering
Taiz University
Taiz, Yemen
Alhamza2012@gmail.com

Prof. Mogeeb A. A. Mosleh
Dept. of Software Engineering
Taiz University
Taiz, Yemen
MogeebMosleh@gmail.com

Abstract— **voting process is a democratic practice that has been used over the years as a primary method used by people in democratic countries to express their opinions on issues and discussions that concern them. This paper seeks to facilitate and protect the voting process by making an online voting system for elections and referendums connected with voting devices. The IoT and Blockchain have been used with this system to ensure that users' data are protected from theft and prevent eavesdropping or vote tampering to guarantee the integrity of the voting. The blockchain encrypts votes in order to protect every vote from forgery. This system is not directed to governments only, but to all governmental and private agencies. For example, governments can establish referendums or elections, and anyone who has reached the legal age and has a voting card issued by the government will be able to vote, thus we get rid of the traditional methods and dispense with ballot boxes, standing in long queues and delay counting the votes that cost governments a lot of time, effort and money. Also, any institution or private corporation that wishes to conduct polls and questionnaires or to conduct a specific study in order to collect opinions from people of society can simply use this system to reach them. The system assists the concerned authorities in obtaining results quickly without delay, taking into account the differences in voting process between government and private organizations.**

Keywords—**Voting, Internet of Things (IoT), Blockchain, Ethereum, smart contract, One Day Password (ODP).**

I. INTRODUCTION

The rapid development and astonishing spread of technology in various areas of life has a great role in facilitating life matters for all humanity[1]. The voting process is a democratic practice that has been used over the years as the primary method for individuals to express their opinions on issues and discussions that concern them[2]. In democratic countries, the election process is very important because it happens periodically with the participation of citizens who have reached the legal age and are allowed to vote. That is why there is an urgent need to ensure the integrity of the elections by offering safety and security for citizens so that they can cast their votes comfortably[3]. Many countries have faced authoritarian administrations that are not characterized by integrity and transparency in the electoral process. Therefore, having an electoral system based on integrity, safety, preserving votes from tampering, manipulation, and repetition in addition to obtaining results faster is a solution for many governments wishing to improve and prove their credibility and transparency in front of their citizens[4]. Voting is a process that is used in democratic governments in order to enable the people to choose their representatives in government. Since the IoT and its applications has become the future of countries seeking to develop their fields[5], our proposed system relies on the technology of the IoT and the blockchain to ensure high performance and security. The IoT is understood as a combination of a large number of devices connected with each other in a network to share data between them which can be used after processing to make appropriate decisions at the right time. In general, the IoT term refers to a network of interconnected things. It consists of billions of "things" or devices that are connected and can sense, communicate, calculate, and potentially stimulate[6]. Blockchain technology has appeared since the eighties of the last century, and the reason for the increasing interest in this technology today is due to the electronic currency called Bitcoin, which was developed in 2009[7], and was considered as a digital currency used in conducting financial transactions, the technology used in the development of Bitcoin is Blockchain equations[4]. Citizens in the election process suffer from credibility and security terms when it comes to their votes. While some of them avoid going to vote in order to avoid chaos and standing in long queues[3]. There are many problems associated with using the traditional voting methods in elections, such as fraud involved in voting, stuffing additional ballot papers, falsifying some papers, in addition to problems related to counting and delay in announcing the results. All these difficulties make the voting process difficult for governments. It is a good idea to have a safe, reliable and fast system to solve these problems[4]. There is a problem in voting centers (kiosks) in some countries, such as India for example, centers are not widespread, they need staff to manage them, because of these centers are in separate places far from some areas, voters must travel long distances to cast their vote, therefore, the number of citizens that should participate in voting will be

reduced[4], so our system is considered a solution to this problem because the voting machines do not need people present next to them to manage and thus the government will be able to deploy these devices in many places to be close to all populated areas, and can put more than one device in the same area. Some examples of technologies that were used in electronic voting are optical scan voting, punch-cards voting, and voting centers (kiosks). It also includes different types of networks such as the mobile network, the private use of a computer network and the use of social media on the Internet. However, after the technological development, these old methods of electronic voting have changed, and there has been an increased interest by research community on voting technology using IoT[8]. This system will not only be limited to government elections, but will also be used in referendums and questionnaires, in governmental and private organizations in order to know the opinions of people about a specific topic or service, or for institutions or community organizations that want to know the views of society about a certain matter. The system relies on combining the IoT with the blockchain to achieve speed, efficiency and security. This paper is divided as follows: in section II the related works were mentioned, after that section III describes the proposed methodology of the system, in section V we talked about the desired results of this system, finally, the section VI gives the conclusion of the work that was mentioned.

II. Related works

To enable decentralization for electronic voting process and its services, we will present in this section many solutions that were mentioned in works of previous researchers, in which they merged electronic voting and blockchain, in addition to the proposed works in this paper to improve the electronic voting process and increase its efficiency and reliability. South Korea conducted its part of experiments related to Blockchain electronic voting. It was first implemented in March 2018 by Gyeonggi-do Province. Although this was tested in a small scale with the number of participants around 9,000 only, but officials believe this shows the potential of using Blockchain technology in online voting[3]. researchers[4] have proposed a specific mechanism that aims to solve the problems occurring in the central electronic voting process by using Ethereum blockchain technology based on a decentralized network that ensures a secure vote by encrypting and fragmenting the data and creating a peer-to-peer network linked to a distributed ledger that concealed the internal complications from the user, which is the process of identifying the vote uniquely by Aadhar number given by the government in order to ensure the verification of the voter and not repeat the voter's vote more than once by linking each voter with a public key and a private key. The mechanism for verifying the voter by the Aadhar number is not completely safe, and other factors must be added such as verification by methods of biometric authentication and a verification code One Time Password (OTP). In another work[2] they improve and develop electronic voting and increase its efficiency in Ethereum Blockchain. A decentralized and reliable method has been proposed to ensure integrity and transparency of data through the voter's mobile phone number using the OTP verification mechanism that sends a code to the voter's phone number, after that voter can cast his vote so that every single vote is

linked to only one phone number, which increases efficiency to verify the vote as they claim, but the need to verification through biometric properties is necessary and required to remove all doubts about verifying to make sure that the person did the voting process by himself not someone else, also the lack of verification by a voting card number issued by government is considered as a security weakness. In paper [9], a proposal was presented to build an electronic voting system based on blockchain and smart contracts in which it guarantees security and privacy for voters. The two mechanisms were also linked to verify the vote before casting by linking both the Aadhar card and a phone number, OTP is sent to voter's phone in order to be able to cast his vote only once, but the main drawback is the possibility of falsifying the vote of the voter and there is no way to guarantee that the one who casts the vote is the voter himself. In our paper, we have proposed a mechanism that helped solve some of the problems and defects that were mentioned previously, as well as additional improvements that make our proposed system more reliable.

III. PROPOSED SYSTEM

In this section, we presented the proposed voting system based on IoT and blockchain that aims to solve the obstacles of traditional voting methods and improve electronic voting process by facilitating the process of accessing the system, adding protective methods that enable the voter to vote comfortably and ensure that the voting data are correct and there is no tampering or fraud in votes. Our proposed system contains a website connected with the governmental database of citizens records in order to verify citizens' data. The structure of our proposed system is based on two situations, the first if a citizen votes for governmental elections and the second if casts his vote in a referendum or questionnaire. Both the questionnaire and the referendum are for government institutions or private corporations. The system employs blockchain technology that protects and saves the voting process and the data it contains. Blockchain is a database and a network at the same time[10], it consists of a group of nodes that are linked to each other in a peer-to-peer network. This network consists of computers which considers the link within the entire network so that it shares data or digital events within that network. When a new computer connects inside a blockchain network, it becomes a node within that network that can communicate and share data with other nodes on the same network. When a node sends new data in the blockchain network, the data will be verified and approved by the majority of other nodes connected to this network, so that it is very difficult for a deceptive node to publish or repost data due to the blockchain infrastructure[11].

Any block in the blockchain contains (data, hash of the determinant, hash of the previous block) the first block in blockchain called the configuration block, it doesn't have the hash field of the previous block[4].

A. Ethereum

It is a public, decentralized blockchain network without permissions, programmers use it as a platform for developing and writing decentralized applications using the blockchain[12]. Ethereum consists of two types of accounts:

- Wallet accounts: owned and used by network users, as a way to interact with the Ethereum blockchain,

public and private key cryptography is used as a way to organize these accounts.

- Contract accounts: smart contracts written in high-level programming languages such as solidity language that we used in this project.

  These contracts are characterized by performing tasks according to the required conditions[13], they are executed automatically when these conditions are met, and these accounts are used and stored in Ether. As a cryptocurrency, it is denoted by "ETH", to pay for services and transactions within the blockchain.

B. Smart contract

It is a coded digital agreement used to conclude an agreement between two parties, like manual contracts. We have used the smart contract in our system as a formal agreement for voting so that this contract is only executed after the conditions are met (Not to vote more than once by the same person).

C. Tools and techniques used in building this system

Block diagram of the system shown in Fig. 1, this system consists of two parts:

- *Hardware*

  The hardware of this system means voting machines which contain:

  - Arduino device which is an open platform device.
  - esp8266 microcontroller device used to keep the Arduino board connected to the Internet periodically in order to synchronize the voting process.
  - Keypad board to get inputs from a voter.
  - Finger print sensor connected to the Arduino to verify the fingerprint of a voter in the election process.
  - LCD display.

- *Software*

  Front end: It is the front end of the system built with HTML5, CSS3, JavaScript and Bootstrap.

  Back end: It's the hidden part of the system, and it's the work the system does behind the scenes, including PHP to deal with database, NodeJS and Web3. To perform the blockchain we used decentralized Ethereum blockchain with smart contract wrote in solidity language programming[14].

As for the tools to be installed, they are:

- *Node Package Manager (NPM)*

  It is a required bundle that comes with Node.js .

- *Truffle Framework*

  It is a framework used to build decentralized Ethereum blockchain applications, it gives us a set of tools used in writing smart contracts and examining them using the Solidity programming language as well as publishing them on the blockchain network.

- *Ganache*

  Used to create blockchain accounts with Ether locally inside the computer, it gives 10 accounts used within the local Ethereum blockchain network (to simulate the work of the project before its launch). Each account contains 100 ether units.

- *MetaMask*

  It is a tool installed on the Google Chrome browser to make a link between the browser and the blockchain so that we can connect to the Ethereum blockchain and control smart contracts.

D. Voting Strategy

The voting process was divided into two sections:

- Voting for governments activities.
- Voting for private corporations.

In the first section, it is classified into two types:

- Governmental elections.
- Governmental questionnaires or referendum.

In the second section -private corporations- there is voting for questionnaires only.

We will mention the mechanism for casting a vote in each of these types based on what was suggested in this paper as follows.

Governmental elections: (see Fig. 2)

i- voter displays the voting page on his/her internet browser.

ii- The voter enters his/her data (voting card number, personal information, phone number)

iii- The site verifies this data based on the citizens database records and matches it with the voter's data.

iv- If the voter's data are incorrect, a message is displayed explaining to the voter that there is a mistake in his/her data and asking him to enter the correct data.

v- If the voter's data are correct, the status of the voter is verified (cast his/her vote or not).

vi- If the voter had previously cast his/her vote, the ability to vote will be suspended and a message is displayed to explain the reason and moved the voter to a page that displays the percentage of votes obtained by the candidates to follow the number of votes.

vii- If the voter did not cast his/her vote in advance, a verification code called One Time Password (OTP) is generated and sent to the voter's phone number as a kind of increased security, and at the same time the code is saved in the database.

viii- The voter enters the OTP code -connecting to his phone- on the voting page and it is verified by the site.

ix- The voter cast his/her vote by clicking on one of the buttons in front of each candidate's picture.

x- Another verification code called One Day Password (ODP) is generated, this password is valid for 24 hours. The voter enters it into one of the voting

machines that are deployed in streets in order to be able to give his/her fingerprint to confirm and count his vote, this step called (vote confirmation).

xi- If the time available for vote confirmation (24 hours maximum) expired, the vote cast by this voter will be ignored, and he/she must vote again from the website.

xii- Before the time allowed for vote confirmation elapses, the voter can go to one of the voting machines and enters the ODP code in it.

xiii- This code is verified by the voting machine, if the code is incorrect, a warning sound will be issued and a message clarifying this warning will be displayed.

xiv- After entering the ODP code and verifying its authenticity, the voter data that was previously entered is fetched from webserver to the Arduino through the Esp8266, then he is asked to enter his fingerprint to confirm the vote.

xv- The voting machine checks fingerprint's voter and compares it based on the governmental database of citizens records.

xvi- If the fingerprint is verified, the vote of the voter is committed and calculated.

xvii- If the fingerprint does not match, a warning sound will be issued and a message clarifying this matter to the voter will be displayed.

Governmental questionnaires or referendums: (see Fig. 3)

i- The voter displays the voting page on his/her internet browser.

ii- The voter selects a questionnaire from the voting page.

i- The voter enters his/her data (voting card number, personal information, phone number)

ii- The site verifies this data based on the citizen's database records and matches it with the voter's data.

iii- If the voter's data are incorrect, a message is displayed explaining to the voter that there is a mistake in his/her data and asking him/her to enter the correct data.

iv- If the voter's data are correct, the status of the voter is verified (cast his/her vote or not).

v- If the voter had previously cast his/her vote, the ability to vote will be suspended and a message is displayed explaining the reason and moved to questionnaires states page.

vi- If the voter did not cast his/her vote in advance, a verification code called (OTP) is generated and sent to the voter's phone number as a kind of increased security, and at the same time the code is saved in the database.

vii- The voter enters the OTP code -connecting to his phone- on the voting page and it is verified by the site.

viii- The voter cast his/her vote and write his/her opinion.

ix- The vote of the voter is committed and calculated.

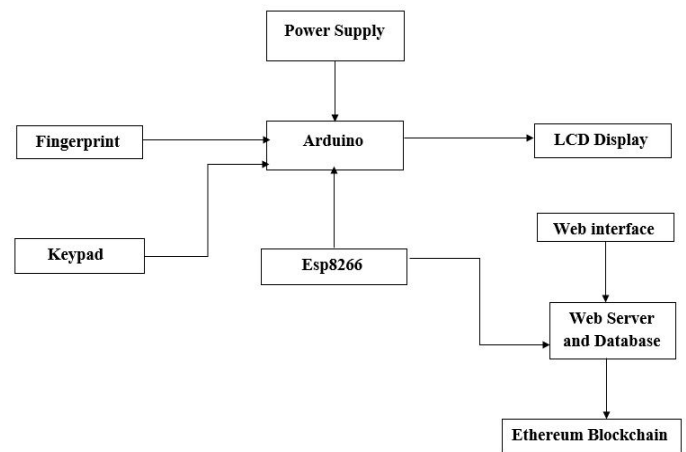x- There is no need for confirmation by fingerprint in questionnaires or referendums.
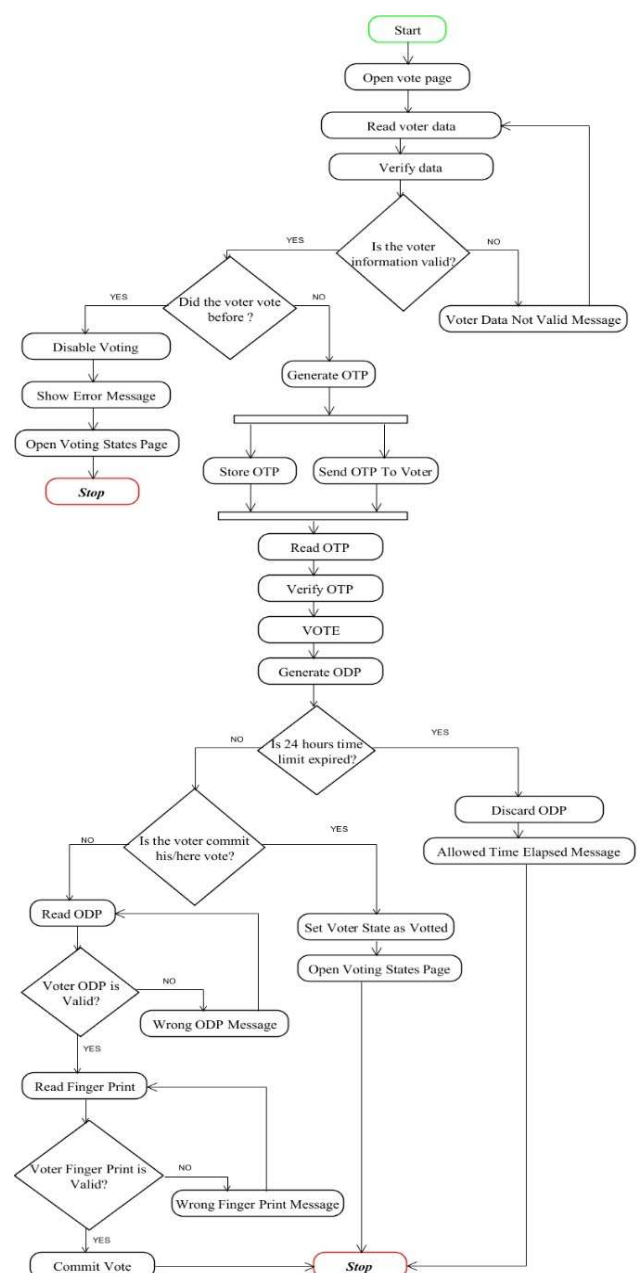

Fig. 1. Block Diagram of the system

Fig. 2. Governmental elections process

Private corporations questionnaires: (see Fig. 4)

i- The voter displays the voting page on his/her internet browser.

ii- The voter selects a questionnaire from the voting page.

iii- The site gets the stored data of the voter including (username - email)

iv- After getting voter information, the status of the voter is verified (cast his/her vote or not).

v- If the voter had previously cast his/her vote, the ability to vote will be suspended and a message is displayed explaining the reason and moved to questionnaires states page.

vi- If the voter did not cast his/her vote in advance, the site allows the voter to cast his/her vote once.

vii- The voter cast his/her vote and write his/her opinion.
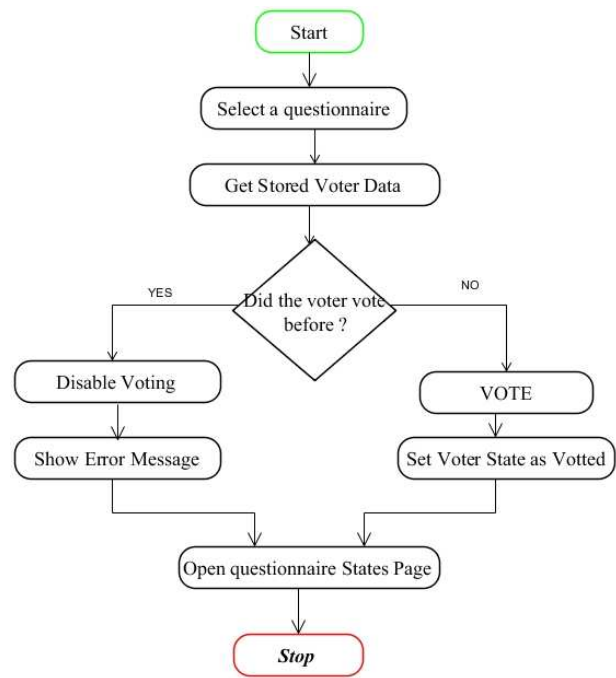
viii- The vote of the voter is committed and calculated.
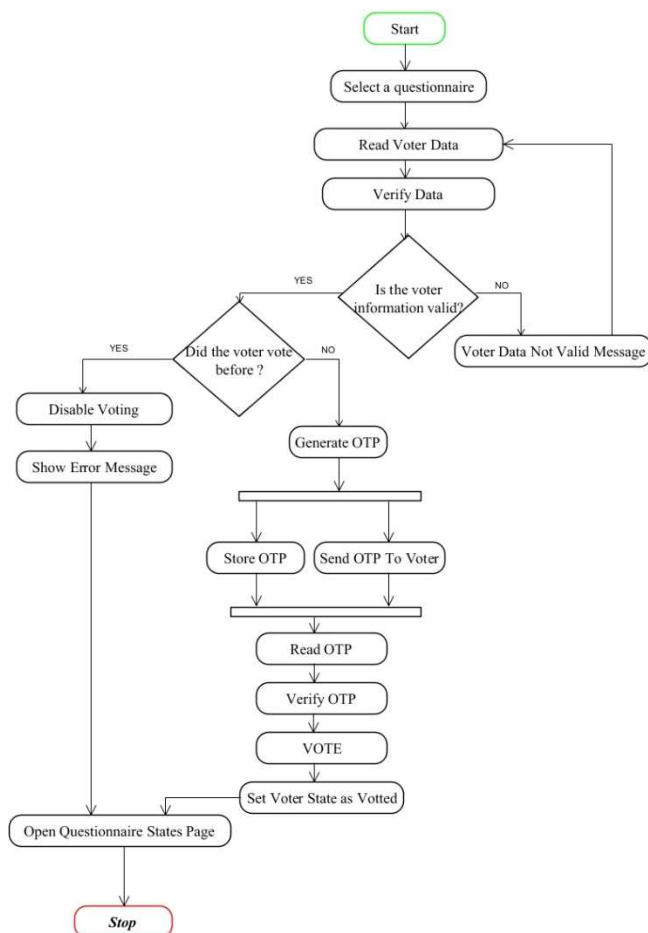

Fig. 4. Private corporations questionnaires process

Fig. 3. Governmental questionnaires process

IV. RESULTS

In this section, we explain the results of the tasks that the system performs, and the possibility of voting in governmental elections or questionnaires and polls for government and private corporations. The government sector includes its public and service institutions, citizens can involve in elections or referendums easily through the web system linked to the IoT devices, and access to all people with ease to take their opinions and obtain the results of elections or referendums quickly, accurately and prevent the repetition of votes. Citizens' data are dealt with, so the system provides protection and privacy for it through the blockchain. When log in to vote, after a citizen enters his personal required data and his electoral card number, the entered data are verified and compared with the governmental database of citizens records, only adults or any person who is eligible to vote can vote. In voting of governmental elections, after the voting process is completed on the website, the voter must go to one of the voting machines that are widespread in several places to confirm the vote through his fingerprint and be matched with his previously recorded data based on the governmental database of citizens records, this confirmation process by finger print is required for governmental elections only. In governmental questionnaires or referendums, it is the same process of voting in governmental elections with the exception of verification by fingerprint to facilitate the voting process, because it is not as important as elections. The verification of the voter's data is done by comparing the entered data with the governmental database of citizens records. On the other hand, the private sector which includes institutions or corporations that work in society field and wish to conduct a referendum or make questionnaires in order to obtain the opinions of citizens, they can set up referendums, and the system helps in taking citizens' opinions quickly and accurately. Citizens can enter directly to the website to fill out

the questionnaire and vote on it without the need for the verification and confirmation process as in voting of government sector, because it is a normal process and does not need to verify and confirm the identity of the person. The organization or institution that conducted the referendum or questionnaire can get the results of voting easily. Every vote whether in government or private sector voting, a new node is created for it in the blockchain by the smart contract, thus ensuring that the vote is protected from tampering or fraud, after that the vote is stored in the database.

V. CONCLUSION

This paper proposed a decentralized electronic voting system to develop and facilitate the online voting process for elections and referendums based on the IoT with Ethereum blockchain technology, which in turn works to ensure that users' data are protected from tampering and guarantee integrity of voting process. The system works on both governmental and private institutions, and aimed to get rid of traditional methods and improve the electronic voting process, in order to reduce costs, save money, time and effort. System makes sure that the one who cast the vote is the same voter and no one else, through the electoral card number and the one-time password verification (OTP), as well as the one-day password verification (ODP) and also the biometric verification which is a fingerprint of a voter compared with his/her data in the government. Verification by fingerprint, (OTP) and (ODP) is required only when voting on governmental elections, while in referendums or questionnaires, whether in governmental or private corporations, the fingerprint verification process is not required. We seek to develop this system by adding other tools for verification, such as the fingerprint sensors that exists in phones, to make the voting process much easier.

REFERENCES

[1]   S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," *J. Clean. Prod.*, vol. 274, 2020, doi: 10.1016/j.jclepro.2020.122877.

[2]   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. 1–6, 2019, doi: 10.1109/IMCET.2018.8603050.

[3]   R. K. Geetanjali and R. Naveen, "An enhanced security mechanism through blockchain for E-polling / counting process using IoT devices," *Wirel. Networks*, vol. 5, 2019, doi: 10.1007/s11276-019-02112-5.

[4]   S. Shukla, A. N. Thasmiya, D. O. Shashank, and H. R. Mamatha, "Online Voting Application Using," *2018 Int. Conf. Adv. Comput. Commun. Informatics*, pp. 873–880, 2018.

[5]   BusinessInsider Intelligence, "The Internet of Things Report," 2020. https://www.businessinsider.com/internet-of-things-report.

[6]   J. R. Gil-Garcia, T. A. Pardo, and M. Gasco-Hernandez, "Internet of Things and the Public Sector," in *Beyond Smart and Connected Governments*, Springer, 2020, pp. 3–24.

[7]   A. Berentsen, "Aleksander Berentsen Recommends 'Bitcoin: A Peer-to-Peer Electronic Cash System' by Satoshi Nakamoto," in *21st Century Economics*, Springer, 2019, pp. 7–8.

[8]   K. Srikrishnaswetha, S. Kumar, and R. Mahmood, *A Study on Smart Electronics Voting Machine Using Face Recognition and Aadhar Verification with IOT*. Springer Singapore.

[9]   M. V Varalakshmi, S. Malarvizhi, A. Shamitha, S. Srimathi, and V. Vinisha, "Blockvote : Aadhar Based Electronic Voting System Using Blockchain," *Int. J. Sci. Res. Eng. Dev.*, vol. 3, no. 3, pp. 421–427, 2020.

[10]   G. Han, Y. Li, Y. Yu, K. K. R. Choo, and N. Guizani, "Blockchain-based self-tallying voting system with software updates in decentralized IoT," *IEEE Netw.*, vol. 34, no. 4, pp. 166–172, 2020, doi: 10.1109/MNET.001.1900439.

[11]   S. Ølnes and A. Jansen, "Blockchain Technology as s Support Infrastructure in e-Government," vol. 2, pp. 215–227, 2017, doi: 10.1007/978-3-319-64677-0.

[12]   K. Teja, M. B. Shravani, C. Y. Simha, and M. R. Kounte, "Secured voting through Blockchain technology," *Proc. Int. Conf. Trends Electron. Informatics, ICOEI 2019*, no. Icoei, pp. 1416–1419, 2019, doi: 10.1109/ICOEI.2019.8862743.

[13]   E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 2018, pp. 1–7.

[14]   K. L. S. Priya and C. Rupa, "Block Chain Technology based Electoral Franchise," *2nd Int. Conf. Innov. Mech. Ind. Appl. ICIMIA 2020 - Conf. Proc.*, no. Icimia, pp. 1–5, 2020, doi: 10.1109/ICIMIA48430.2020.9074931.