

Blockchain Technology – A New Technology to Store Your Data and Implement Voting

Omkar Jadhav, Gunja Gupta, Siddhesh Wankhede

Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India

ABSTRACT

Article Info

Volume 9, Issue 2

Page Number : 427-431

Publication Issue :

March-April-2022

Article History

Accepted : 15 March 2022

Published: 30 March 2022

The current situation of the Covid-19 pandemic is currently increasing public concern about the community. The government has especially recommended Stay at Home and the implementation of PSBB in various regions. One of the concerns is when the election of regional leaders to the general chairman. Even though there is already a safeguard regulation, this is not considered safe in the current Covid19 pandemic. The solution in this research is the use of a blockchain based E-voting system to help tackle election unrest during Covid-19. Where e-voting with blockchain technology can be carried out anywhere through the device without the need to be present in the voting booth, reducing data fraud, accurate and decentralized voting results that can be accessed by the public in real-time. The use of cryptographic protocols is applied for data transfer between system components as well as valid system security. This research method uses SUS trial analysis in a significant system of the Covid-19 pandemic situation. The implication that the SUS Score analysis shows 90 shows an acceptable E-voting system, meaning that the community can accept it because it brings positive and significant impacts such as effectiveness and efficiency.

Keywords - Blockchain, Covid-19 Pandemic, e-voting, Biomedical imaging, Public, E-Voting

I. INTRODUCTION

to Technology has now entered the 4.0 era; all activities in all fields should be supported by the digitalization of transformation [1], [2]. However, in the case of voting activities in Indonesia that we still feel at this time are still using conventional methods, namely voting on paper. Fraud that often occurs in elections is no longer denied by the manipulation of ballot data sent to the center because it is done directly

at the polling stations (polling stations), where the funding of this election project can add to the burden of the state in 5 years [3][4]. Then the outbreak of Covid-19 is the government's consideration for the election. Covid-19, which has now looted to various worlds, begins with the spread of China [5]. Graphic Fig1 is a case of Covid-19 globally when the beginning of the pandemic continues to increase from China, Europe, and others [6]. Common signs of infection will be Covid-19 infection with an average incubation

period of 5-6 days to 14 days, namely in acute breathing with, for example, shortness of breath, fever, and cough

The biggest impact of Covid-19 influences distance learning in order to maintain social distancing [8]. So, when the general chair (election) or regional elections (pilkada) that occur in Indonesia indeed become a question of how it can go according to the Covid-19 protocol in order to maintain social distancing. As a result of the COVID-19 pandemic, the KPU has issued a KPU decision letter Number: 179 / PL.02-kpt / 01 / KPU / III / 2020 explaining the rules for delaying several stages of the 2020 elections, including the inauguration and the working period of the Voting Committee (PPS), verification of the support requirements of individual candidates, the establishment of the Voter Data Update Officer (PPDP) and the implementation of matching and research (coklit), as well as updating and compiling the voter list [9]. The importance of the government's role in announcing the restriction order during this pandemic is to prevent the spread of the Covid-19 virus [10]. This will be discussed in this study that E-voting with blockchain technology can assist in the electoral process in the situation of the Covid-19 pandemic with the blockchain e-voting framework [11]. This e-voting is a modern voting activity. Therefore, the system and application that will be created will answer some voting needs with the implementation of blockchain technology [12] [13]. The blockchain technology application can answer with the nature of the blockchain, which is transparency, meaning that the data stored is open to the public, thereby increasing fairness and truth. Anonymity, only the voter himself knows information about votes, and all ballots collected have nothing to do with voters. Dependability means that every vote will be counted and cannot be replaced, duplicated or deleted, and produces credible results. Eligibility is only a verified user and has voting rights who can vote and vote. Verifiability is a system that is open to checking the system procedures' truth to the results issued [14]

II. LITERATURE SURVEY

2.1. Blockchain

This research also collected ten literature reviews to strengthen perspective from E-voting and blockchain. Satria Damai Kurnia Hu, et al. conducted this research discussing electronic voting or voting using the media of an application and by using blockchain technology, because conventional voting itself is still hampered by its security aspects, as well as more expensive cost issues, and also the implementation of an E-voting only in terms of security is still in doubt, therefore in this E-voting, blockchain technology is included. Where this blockchain we cannot modify, delete data so, the authenticity of the data is guaranteed [15]. Research on blockchain applied in the education sector has also succeeded in making students more active and motivated in blockchain-based iLearning learning [16]. Research conducted by Sandi Rahmadika et al., who discussed blockchain technology is a technology to maintain data security at a low cost that has been decentralized to maintain data confidentiality without the involvement of third parties [17].

Furthermore, 2017 research that discusses, blockchain technology is an up-and-coming technology behind bitcoin and is very interesting to face a challenge that arises in managing authorization that utilizes the consistency of blockchain technology, to manage access control on behalf of restricted devices [18]. Then research on an election guard application was made to be a real count media by using blockchain technology so that data can be distributed well without worrying about hacking attacks [19]. Another study by Snehal Kadam, Khushaboo Chavan, et al. explained the application of the blockchain as a service to implement a distributed electronic voting system with an E-voting application to increase security and reduce the costs of holding elections [20]. Next research Rasim Alguliyev et al about exploring the E-voting system as one of the main tools of e-democracy and analyzing its strengths and weaknesses for effective decision making [21]. Other blockchain research on the application of

blockchain technology in higher education assessment systems so that the information delivered is transparent and decentralized [22]. Kashif Mehboob Khan conducted the study, Junaid Arshad and Muhammad Mubashir Khan, entitled "Secure Digital Voting System Based on Blockchain Technology." This study discusses the e-voting system using blockchain technology to improve system resilience and utilize the benefits of blockchain to achieve an effective scheme on e-voting systems [23]. The latest research is the application of E-voting with SMS (Short Message Service) technology to get speed, security, and accuracy of data that is designed simply so that the costs incurred are relatively inexpensive [24].

III. MOTIVATION

- Currently, Reverse Transcription-Polymerase Chain Reaction (RT-PCR) test serves as the gold standard of confirming COVID-19 patients.
 - But RT-PCR tends to be inadequate due to insufficient sensitivity mainly due to sample preparation and quality control issues. Moreover, many suspected patients have to be tested multiple times several days apart before reaching a confident diagnosis.
 - Other methods of detection involve taking thoracic CT which is a tedious 3 step process which involves:-
 1. pre-scan preparation
 2. image acquisition
 3. disease diagnosis
 - In the pre-scan preparation stage, each subject is instructed and assisted by a technician to pose on the patient bed according to a given protocol. In the image acquisition stage, CT images are acquired during a single breath-hold. From the acquired raw data, CT images are reconstructed and then transmitted through picture archiving and communication systems (PACS) for subsequent reading and diagnosis by experts.
- **We can see that these current methods are tedious and can be improved using AI by automating error prone and time consuming steps.**

IV. OBJECTIVE

- Artificial intelligence (AI), an emerging technology in the field of medical imaging, has contributed actively to fight COVID-19. Compared to the traditional imaging workflow that heavily relies on human labors, AI enables more safe, accurate and efficient imaging solutions.
- The objective of this review is to extensively discuss the role of medical imaging, especially empowered by AI, in fighting the COVID-19, which will inspire future practical applications and methodological research.
- Objective also involves introduction to intelligent imaging platforms for COVID-19, and then summarize popular machine learning methods in the imaging workflow, including segmentation, diagnosis and prognosis.

V. METHODOLOGY

Figure 1 depicts that the voter needs to enter the Name, Email, Phone, Aadhar card number and voter Id number in order to sign in to vote. All data is then encrypted and stored as a transaction. An OTP is sent to the registered email Id and phone number, all the process needs to have a stable internet connection. When user votes to a candidate, voting information is added with block chain and sent across the network. Blockchain [5] : A blockchain is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. It is resistant to tempering of the data. It is an open and distributed ledger to record transactions between two parties efficiently and in a verifiable and permanent way. It is managed by peer-to-peer network which obeys the protocol for inter-

node communication and validate new blocks. Once the data recorded, it cannot be altered. Blockchain may be considered secure as it has high fault tolerance. Decentralized consensus has therefore been claimed with a Blockchain. OTP [6]: It is one time password which is valid for the given login session only on any digital device. They are random numbers which are used as the traditional password-based authentication. Static passwords are vulnerable to threats while OTP are not. OTP are used only for a certain logged in session and time, hence if an intruder tries to record the OTP that was already used to log in, it will not be possible as it will not be valid to perform any activities related to the OTP. And if any person have same password for almost all the system used by him/her then they are more vulnerable to the attack, while OTP authentication is a very safe method to use. Secure Hash Algorithm 3 (SHA-3) [7]: SHA-3 is recently added to secure hash algorithm standards. It uses mathematical algorithm to map data of any size (message) to a fixed size bit string (hash). It uses Keccak algorithm which is based on un-keyed permutations as opposed to other usual hash functions' constructions. Keccak algorithm [8]: A new approach called sponge and squeeze construction is used in Keccak, which is a random permutation model. The variant used in this project is SHA-3 with 256-bit of output (SHA3256). Universally Unique Identifier (UUID) [9]: It is a 128-bit number used to identify information in computer systems and are unique. The probability of the similarities between two UUID is 0 or $\frac{1}{2^{128}}$ which is negligible. It can be created by anyone of us and use it to identify something. They are later combined into one database and transmitted on the same channel. Elliptic Curve Digital Signature Algorithm (ECDSA) [10]: It is a cryptographic algorithm which is used to ensure that votes are spent by the rightful.

Following are the concepts of ECDSA:

- Private Key: A secretly randomly generated single unsigned (32 bytes) number key by a person.
- Public Key: A 65 byte number which is not secretly generated and calculated by private key. It is

mainly used to check if the digital signature key is legit or not.

- Signature: A mathematically generated hash with 71 – 73 bytes long. It is used along with public key and produced from hash and private key
- Remote Login: A login system will allow a user terminal to connect to a host computer via a network to interact with host.

VI. APPLICATIONS

In Fig3, use case diagram E-voting blockchain flow from each actor. The interface design of the website application is adjusted to the existing access rights, namely the Organizer Admin, Organizer, and Voters. Each application design aimed at each access right has different according to function and needs. The application design for the organizer admin has functions to manage to vote, manage organizer data, and manage data access rights from those who run the voting. The interface design for the organizer admin consists of a change password page, view results, manage elections, manage organizers, and manage access right. The organizer's application design has functions for managing voter data and managing candidate data that follows the voting. The interface design for the organizer consists of a change password page, view results, manage voters, and manage candidates. While the design of applications for voters has the function to vote, see and check the votes that have been done. The voter interface design consists of the change password, view result, vote, and individual ballot verification pages. Besides, some pages can be accessed by all users, including the login page, register, account setup, and universal ballot verification. The login, register, and account setup pages have functions to help users manage their accounts when they first access the application. The universal ballot verification page has a function to check the sound that has entered the system.

Fig4 explains the architecture system design on blockchain-based E-voting. This architecture system

has components in the form of Blockchain Node, Web Server, and Client Computer. The client computer component is a computer that is used at an election place to be used in voting. The client computer accesses web pages on the webserver. All data and web application interactions between client computers and web servers use HTTP or HTTPS methods. The web server component is a web application that provides voters and organizers services in the voting process. Web Server uses a computer (centralized) to manage all activities carried out from the client computer (voter). Web Server is also connected to a local database to store data needed in voting, such as election data, user data (voter, candidate, organizer), and other supporting data. The webserver is also connected to a blockchain node to make API calls. The blockchain component of the node provides an API call with the JSON RPC method. This component is a computer in a peer-to-peer network of blockchain. The JSON RPC API call is used by the webserver to manage the blockchain in meeting voting needs. Ballot generated by the voter (client computer) will be saved to the blockchain on the blockchain node by the webserver. With blockchain technology accompanied by Multi Chain tools can sort out the results of valid and invalid votes. A valid ballot is a ballot that has; 1) Signature (digital, sender's address) of an organizer, voters who vote, and the node where the ballot was sent as proof of the validity of the ballot. 2) The recipient's address as the polling place for the ballot is addressed. 3) An asset as a voting right or means of voters to vote and send ballots. 4) Data in the form of candidates chosen by voters with a particular format signifies a valid election (voting). 5) Valid status (on the blockchain) as a ballot sign is valid and has been accepted in the voting system.

VII. CONCLUSION

The Covid-19 pandemic situation has delayed the holding of elections and the extension of office in the present. Increasingly sophisticated technology must

participate in these problems. So this study discusses the use of blockchain-based E-voting for digitizing voting. The hope with this E-voting system is to reduce the meeting of human physical contact in election activities without having to be present in the voting booth. The use of blockchain technology with a strong cryptographic protocol makes a secure encryption block so that the results of votes made by the public are real, safe, and transparent without being able to be manipulated. Using ballot, which has a function as proof validity of a vote that has been chosen by the voter/community against the candidates. Then the multi-chain function is useful in order to facilitate storing large amounts of E-voting data. New information and previous information are stored to produce new blocks. The system will continue to monitor the incoming blocks and continue to renew the chain when new blocks arrive, so there is no duplication of data or collisions between incoming data.