

Implementation of Smart Contracts Ethereum Blockchain in Web-Based Electronic Voting (e-voting)

Faiq Dzulfikar¹, Ajib Susanto²

¹Universitas Dian Nuswantoro

Jl. Imam Bonjol 207, Semarang 50131, (024) 3517261, e-mail: ¹faiqdzulfikar@gmail.com

¹Universitas Dian Nuswantoro

Jl. Imam Bonjol 207, Semarang 50131, (024) 3517261, e-mail: ²ajib.susanto@dsn.dinus.ac.id

ARTICLE INFO

Article history:

Received 16 December 2019

Received in revised form 15 January 2020

Accepted 16 July 2020

Available online 30 July 2020

ABSTRACT

The increasing of digital technology today has helped many people to fulfill their needs. But the election system, still conventionally using paper in its implementation. Elections in general still use a centralized system, where there is an organization that manages it. Some of the problems that may occur in traditional electoral systems are that there are organizations that have full control over the database and system, so the possibility of hacking the database is quite a big opportunity.

Blockchain innovation is one arrangement that can be utilized in light of the fact that it has a decentralized framework and the whole database is duplicated by all clients. Blockchain itself has been used by Bitcoin and Ethereum cryptocurrency which is known as a decentralized system. By using the blockchain in database recording on an e-voting system can reduce one source of fraud that is database manipulation. This study discusses the recording of voting data using blockchain technology. The implementation of Smart Contracts contained in the Ethereum Blockchain will be implemented to create this voting system.

Keywords: Blockchain, Ethereum, Smart Contracts, Voting, E-voting

1. Introduction

In a large scope like a country, conventional voting systems are still often used. The system is inefficient because it causes various problems such as the length of time required, requires substantial costs, often occurs damaged or invalid ballots, cheating and so on. These problems arise because the voting system is managed centrally. Voting data from voters can easily be manipulated by the manager without anyone knowing. This makes the centralized voting system not safe to do in Indonesia which has a very large population.

Blockchain innovation is one arrangement that can be utilized to lessen issues that happen in democratic by e-casting a ballot. Blockchain itself is known to have been used in the Bitcoin and Ethereum transaction database systems. Blockchain is a technology for recording transactions that are interconnected using unique codes in it that are eternal and cannot be changed [1].

Previously, it was hard to accomplish fair election without gambling extortion and manipulation of results. With the approach of Ethereum, numerous analysts on blockchain innovation and smart contracts have proposed this is a suitable reason for electronic voting. In addition, it can have the possibility of making electronic voting progressively worthy and dependable in the public eye. Smart contracts are computer programs that are run through blockchain transactions that can maintain status, interact with cryptocurrency in a decentralized way, and take user input [2]. Smart contracts are a significant code to be incorporated in the blockchain and executed by timetable at each progression of the blockchain update. Electronic voting, then again, is another theme that is trending, however significant identified with online services. Blockchain with smart contracts, shows up as a decent possibility to be utilized in the improvement of electronic voting that are less expensive, more secure, more transparent, and simpler to utilize [3]. Ethereum and its system is one of the most sensible, because of its consistency, its wide use, and the stock of smart contracts logic.

This e-voting system can overcome problems such as a centralized server that is very likely to be disabled or hacked by hackers, data changes unilaterally, and prevent the possibility of fraud. This e-voting system can also overcome the general problems of efficiency in the form of cost, time and so on. This system can also create transparency in the voting process. In this work, we have implemented and tested e-voting application examples as smart contracts for the Ethereum network using the Ethereum network and the Solidity language. With the blockchain technology, the public can monitor data recording in a database safely without being able to mess up the data. The process of counting of votes which is fairly fast and efficient as well as data from voters that can be easily audited is an added value of this system.

2. Research Method

2.1 Blockchain

Blockchain technology was discovered in 2009 along with the emergence of Bitcoin cryptocurrency, a virtual currency that is becoming a trend now [4]. Blockchain technology was born in response to the concerns of a number of parties about the workings of centralized or centralized software. Centralized software raises concerns because it is basically designed to send data from one party to another, requiring a centralized server as a publisher and data manager. When there is a disruption to the server, the website cannot be accessed and users cannot automatically use the service optimally. Blockchain is a technology for recording transactions that are interconnected using unique codes in it that are eternal and cannot be changed [1]. The way the blockchain works is that when another transaction or alter to a current transaction enters the blockchain, by and large most node in the blockchain execution must run an algorithm to evaluate and check the history of the recently proposed individual blockchain. In the event that most of node reach consensus a legitimate signature, another transaction block is inserted into the database and another block is added to the transaction chain. If the majority does not approve the addition or modification of database entries, it is rejected and not added to the blockchain chain. This distributed model is the thing that permits the blockchain to keep running as a disseminated database without the requirement for various specialists, the binding together focus says which exchanges are substantial and (maybe progressively significant) which ones are most certainly not.

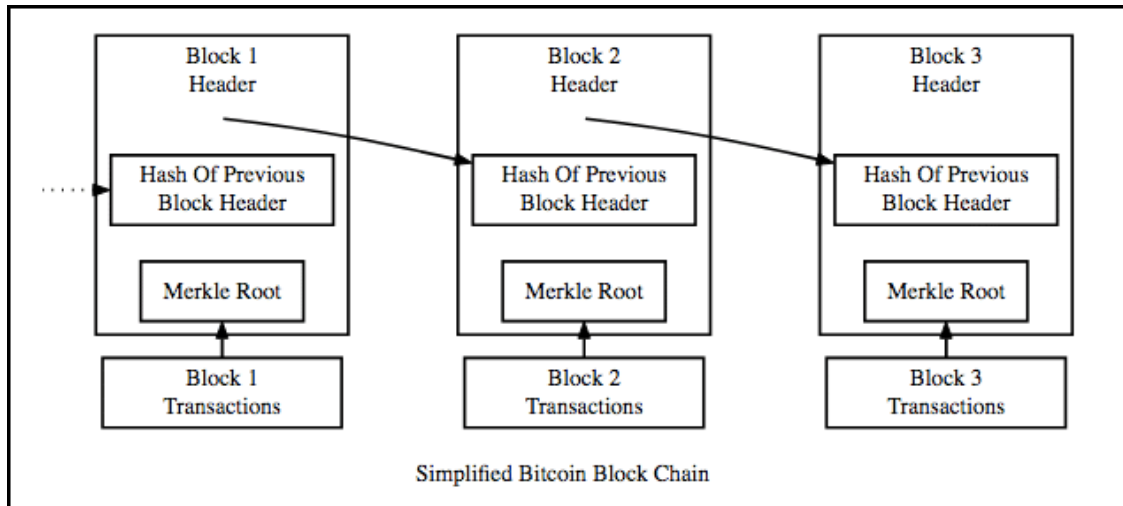


Figure 1. Simplified Bitcoin Block Chain

There are several types of Blockchain [5] namely:

1. Permissionless Blockchain, as Bitcoin or Ethereum, all can be clients or run a node, anybody can "compose", and anybody can partake in consensus in deciding the validity of the state.
2. Permission Blockchain which is conversely corresponding to the past sort, worked by referred to elements, for example, the consortium blockchains, where consortium individuals or partners in certain business settings work the Blockchain authorization arrange. This Blockchain permission system has the way to distinguish node that can control and update shared information, and frequently has an approach to control who can give exchanges.
3. Private blockchain is a special blockchain that is allowed by one entity, where there is just one trust domain.

2.2 Ethereum

Ethereum is the second largest cryptocurrency of all market capitalization which has extensive documentation and an active developer community [6]. Ethereum Blockchain is an open source distributed computing platform that highlights smart contracts (scripting) usefulness. Engineers can without much of a stretch write decentralized applications at a significant level and advantage from distributions acquired from Blockchain technology [7].

Ethereum, as Bitcoin, is a hyper ledger of public blockchain cryptocurrency. The thing that matters is the Bitcoin blockchain just stores transactions that trade Bitcoin between addresses, though Ethereum Blockchain stores addresses with EVM codes. Transactions that are recorded on the blockchain are code calls referenced above, and contain data about the information go to the program as input. These projects are interpreted by a constrained virtual machine called Ethereum Virtual Machine (EVM) and expressed in the fitting language [2].

In this section, some basic ethereum concepts are explained: accounts, transactions, and clients. The basic unit of ethereum is the account. An account is required for everyone who wants to send any transaction to the blockchain. Ethereum itself includes two types of accounts namely: Externally Owned Accounts (EOA), users directly send transactions through them, and Contract Accounts, which are based on the code of the contract if necessary to call another contract then send an internal transaction. Each account in Ethereum is divided by two keys, a private key and a public key. Each account address comes from 20 bytes of a public key which is an important part of every transaction. It is important to understand the difference between a transaction and EOA's private key, the sender of the transaction, and after confirmation of the return of the hash value that we can track all the blockchain transactions. Different sources use call or message conditions for internal transactions [8].

2.3 Smart Contracts

Smart contracts are computer programs that are run through blockchain transactions that can maintain status, interact with cryptocurrency in a decentralized way, and take user input [2]. Smart Contracts are written in the Solidity programming language, which is a mix of C++ and JavaScript. Smart Contract is controlled by peers from the Ethereum organize at regular intervals, and they should be approved by at any rate two different clients to be initiated. From that point forward, contract functions can be executed, and contracts can be imparted to different applicants [9].

To have the option to hold full e-voting, we have to solve the accompanying issues. Straightforwardness, validation and capacity are required in the voting stage. We have to guarantee that everybody who goes to the election is genuine individuals and utilizations the right qualifications that we know in the electronic condition, and we should have the option to prove this whenever, we likewise need our election to be 100% transparent as we wanted. Along these lines, we have to gather and analyze election information that are signed and timestamped. Because nobody should have the option to change the vote after the vote is thrown. Likewise, we need independence in election, with the goal that nobody can pick other candidates. These issues can be overwhelmed by utilizing distributed blockchain technology. We can characterize self-executable smart contracts that are required in the blockchain. Just the same as composing code, we create rules, objects, data models, and in this manner the contracts can start to run. After smart contracts are deployed, they can't be discharged from the blockchain, and individuals can see whether the result of the execution of smart contracts are right or not. In Ethereum network, there is no requirement for focal position to give proof-of-work. All peers can figure contract results without interference. Indeed, even the Ethereum network can likewise give its very own figurings.

The use of the Ethereum network in fact for testing experimental software related to the development of new smart contracts is quite expensive (because it requires the expenditure of several ethereum coins) and does not need to occupy large memory in the system. Therefore, Ethereum's private network was created and made available to developers to enable them to test their software without worrying about actual network congestion [9].

Ethereum enables developers to utilize smart contracts that will be executed when an occasion is activated. In this exploration smart contracts are interpreted by the Ethereum web3.js API and are utilized to control site pages. Clients connect with the Ethereum organize through Metamask, which is a Chrome extention that can interface with the Ethereum wallet. A client with cryptocurrency wallet and Metamask extension in their program can interface with the application and send or get coins. This makes programming on blockchain extremely conceivable.

2.4 E-Voting

E-voting systems have many advantages compared to conventional voting systems. An e-voting system requires less time, energy and costs compared to conventional voting systems. This system eliminates the possibility of invalid or doubtful sounds so the results are far more accurate. This system is also very environmentally friendly because it saves a lot of trees which are supposed to be ballot papers. The e-voting system can also prevent the manipulation or sale and purchase of votes that is common at polling stations. The e-voting system not only modernizes the electoral process but also has the potential to increase interaction between citizens and government, through platforms based on information and communication technology (ICT).

Implementation of Smart Contracts Ethereum Blockchain in Web-Based Electronic Voting (e-voting) (Faiq Dzulfikar)

Sophisticated security measures must be put forward to overcome the lack of e-voting, inherent transparency and to increase confidence in the new system for both voters and electoral authorities [10].

The e-voting system also has some disadvantages compared to conventional voting systems. Not everyone will agree with e-voting. Some people will be too afraid to think ahead using more technologically advanced systems. The community will tend to think superficially so that this system will be difficult to implement even though it has far more benefits than conventional systems. Especially for the elderly will be difficult to understand because their youth occurs when traditional times are not familiar with technology. The security of the e-voting system is also questionable because it is very difficult to make a system that is completely safe from hacker attacks.

3. Results and Analysis

This research requires data of each user who will vote. The data needed is only limited to the private key because the writer focuses only on voting functionality. The private key will later be used as a unique key for each account. Here is the data of each user.

Table 1. User Account

| No | User Account | Private Key |
|----|--------------|--|
| 1 | Account 1 | fbd0da79152ad9a274485edb74387f28d6fc4e3192c45c6b8d6d45e21c8e14f9 |
| 2 | Account 2 | 87c8d0b69944a6d225114581a723e18a84545e14033b5a1c4a3252f42be12fcf |
| 3 | Account 3 | 5db6f783aa0677127895aec30575159d6cbab320675128eda8ee462f556a8128 |
| 4 | Account 4 | 1cfe9bcaa9bfaf441cf2e7f50aedbd2097c5400a471ebff48b50375b5abe31dc |
| 5 | Account 5 | 1f97e938e642dc4c774dc33e0c9539e3e00dc304801fa3df2876c98500f92fe3 |
| 6 | Account 6 | 142a6ce9dc57b672fb32f531c92c768b4dc16bdd5b703139253ca625ae8343ba |
| 7 | Account 7 | 8b65e2a096bf66fc9f8b6868cf6fdcfb45ed77a58d441882009d4649208ac240 |
| 8 | Account 8 | 9959b7941a57df4bd4b98c3b118f9c81244b13a0d37c4b016263d15537b34190 |
| 9 | Account 9 | 6e36a7639b84a01a6e8dcc0a63b3717568e385d6107e288b6e464bd3a20be8b2 |
| 10 | Account 10 | d1cada2966277dfcc64c364df1fc83da16f025d20e63d4346b6e6a9d01163804 |

To vote, there are a number of things that must be prepared before the start of voting.

1. Preparation of an internet connection and running application support programs such as Ganache, Truffle, and Metamask need to be done
2. After that, confirm whether there is already an active account. If not, then creating a new account must be done first
3. Then after the account has been active, voters can start voting by first selecting candidates.

3.1 System Evaluation

To conduct the voting process, voters must go through the following stages:

1. Ensure that the account used is correct by checking in Metamask.

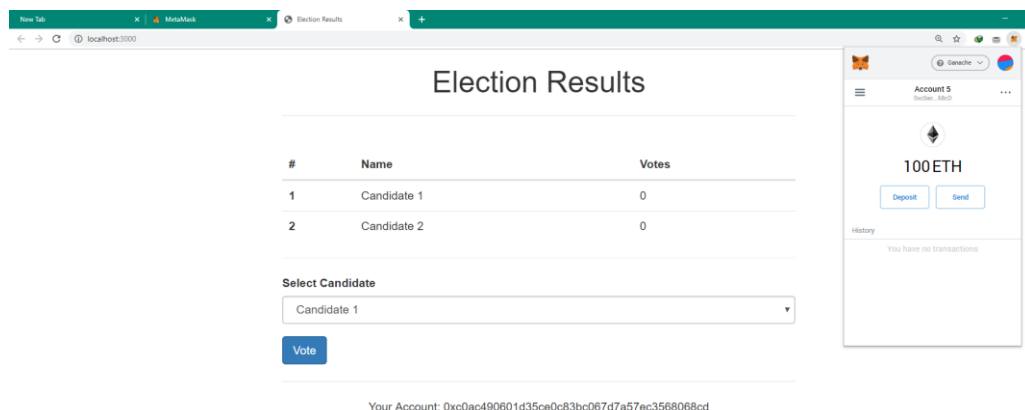


Figure 2.

2. After selecting the correct account, the user can vote directly by selecting the candidate first then pressing the vote button to vote.
3. After pressing the vote button, a new page will appear to confirm that the voter account will send a Gas Fee as a condition for voting. This transaction is a proof that the voting has been done and entered into the blockchain.

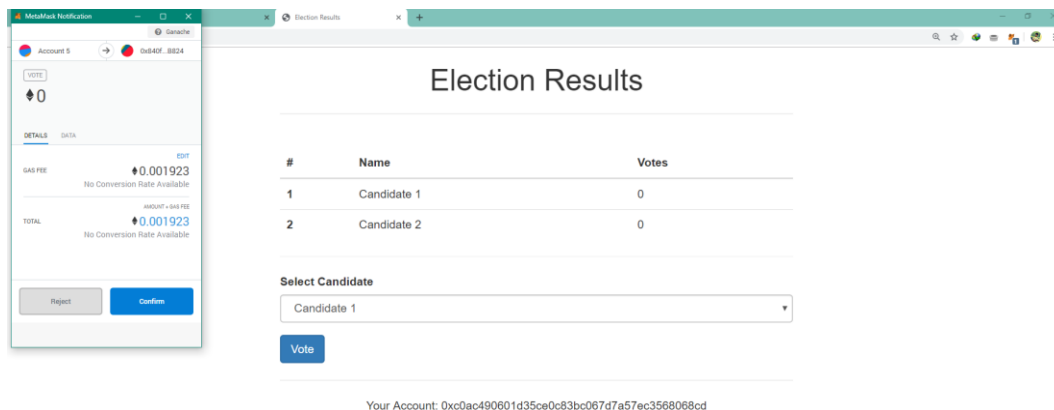


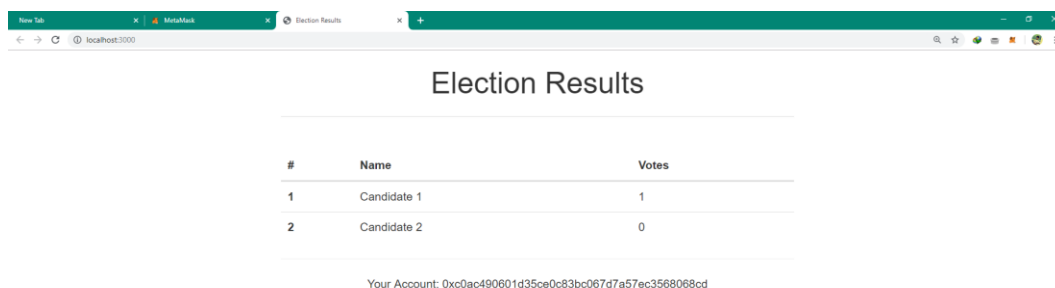
Figure 4.

4. Then after confirming, then the votes are sent and immediately displayed on the start page in real-time.



Figure 5.

5. Users who have voted can no longer vote. After voting, the candidate's choice and vote button are removed from the main page.



The screenshot shows a web browser window with the title 'Election Results'. The browser's address bar shows 'localhost:3000'. The page content includes a table with the following data:

| # | Name | Votes |
|---|-------------|-------|
| 1 | Candidate 1 | 1 |
| 2 | Candidate 2 | 0 |

Below the table, the text 'Your Account: 0xc0ac490601d35ce0c83bc067d7a57ec3568068cd' is displayed.

Figure 6.

4. Conclusion

From the design and implementation of the e-voting system based on the Ethereum Blockchain, conclusions can be drawn including:

1. The e-voting system based on the Ethereum Blockchain can work well.
2. This e-voting system is able to validate the voter's identity well and prevent repeating the election.
3. This e-voting system can store data safely and reliably.
4. By using this electoral system, the voting process will be much faster and safer.
5. The voting process and the calculation of the number of votes will be faster because the voting process is done in real-time.

5. Suggestion

To improve the quality of e-voting in the future, here are some suggestions that might be applied for the next research:

1. Beautify the appearance of the interface so that users are more comfortable in conducting e-voting.
2. Establish an admin dashboard system to be able to manage and audit the system better.
3. Reducing the use of supporting software so that it becomes a better whole system.

References

- [1] I. B. P. Bhiantara, "Teknologi Blockchain Cryptocurrency Di Era Revolusi Digital," *Semin. Nas. Pendidik. Tek. Inform.*, vol. 9, no. September, pp. 173–177, 2018.
- [2] E. Hildenbrandt *et al.*, "KEVM : A Complete Formal Semantics of the Ethereum Virtual Machine," *2018 IEEE 31st Comput. Secur. Found. Symp. KEVM*, pp. 204–217, 2018.
- [3] A. K. Koç, E. Yavuz, G. Dalkılıç, and U. C. Çabuk, "Towards Secure E-Voting Using Ethereum Blockchain," 2018.
- [4] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009.
- [5] C. Cachin and M. Vukolic, "Blockchain Consensus Protocols in the Wild," 2017.
- [6] R. V. Prasad, R. Dantu, A. Paul, and P. Mears, "A Decentralized Marketplace Application on The Ethereum Blockchain," pp. 90–97, 2018.
- [7] E. F. Kfoury and D. J. Khoury, "Secure End-to-End VoLTE based on Ethereum Blockchain," *2018 41st Int. Conf. Telecommun. Signal Process.*, pp. 1–5, 2018.
- [8] S. Rouhani and R. Deters, "Performance Analysis of Ethereum Transaction in Private Blockchain," 2017.
- [9] A. K. Koç, E. Yavuz, U. C. Çabuk, and G. Dalkılıç, "Towards Secure E-Voting Using Ethereum Blockchain," 2018.
- [10] M. Habibi, "Dinamika Impelmentasi E-Voting di Berbagai Negara," pp. 1–23, 2002.