International Journal of Application on Sciences, Technology and Engineering
(IJASTE)
Volume 1, Issue 2,2023.ISSN:2987-2499

Blockchain Technology Implementation on Simple Microcontroller Based Ballots System

Wiryo Tanjung[1 a)], Joni Fat[1 b)] and Hugeng Hugeng[1 c)]

[1] Electrical Engineering Department, Faculty of Engineering, Tarumanagara University

[a)] *wiryo.525190009@stu.untar.ac.id*
[b)] *Corresponding author: jonif@ft.untar.ac.id*
[c)] *hugeng@ft.untar.ac.id*

Submitted: January-February 2023, Revised: March 22 2023, Accepted: May 23, 2023

ABSTRACT

Ballots security and reliability is two of the crucial things that makes digital based ballots system not widely implemented. Paper-based ballots have the downsides of environmental impact on making paper. Blockchain has one of the advantages on the security aspect where the blocks are secured using cryptographic protocol that makes it hard to be hacked. This paper will be examining the possibility of ballots implementation using a microcontroller-based ballots system. The microcontroller is used because it is cheap to implement and it has the capability to sign the blockchain transaction. This paper is a proof of concept for a smaller scale ballots system for a small organization with two candidate option. The blockchain network used in this paper is a Ethereum test network provided by Ropsten. The number of testing done is 60 times total for the two candidate. The smaller scale testing proven to be successful with the transaction confirmed successful in etherscan.io.

INTRODUCTION

Ballots is one of the most important things to keep it's integrity and security, because it can change the course of decision making whether it's in a small organization level or a whole nation [1]. But with every election, paper-based ballots are still used due to it is being less likely to be hacked compared to a digital based ballots [2][3][4]. The downsides of still using paper-based ballots are the environmental impact of producing paper [5]. Digital based ballots need to be more secure and reliable so that the transition into digital based ballots can be used more mainstream. One of the advantages of Blockchain is the security aspect of it [6][7][8]. Compared to a normal cloud-based system, Blockchain uses cryptography and distributed ledger so it is hard for someone with malicious intent to hack it [9]. Using blockchain is also beneficial because it is decentralized so that if there is outage on one station, the other station keeps a copy of the data so that it is safe.

One of the ways to use blockchain is using a microcontroller. A microcontroller is a cheap device that can be the processing module. A microcontroller can be used to sign and send the transaction on the blockchain. This can help with reducing cost of implementation for the transition from paper-based ballots into digital-based ballots. In this proceeding, a simple ballot system will be designed for a proof of concept that utilize a microcontroller with a button system to choose the candidate.

Blockchain

Blockchain is a technology that utilize a distributed database records system for the transaction that happened in a peer-to-peer network [10]. Blockchain uses a cryptographic protocol for the database system so the transactions can be ensured its integrity, and authenticity[6][8]. Blockchain uses different algorithm to ensure the anonymity but still can be trusted, by validating the transaction using different consensus algorithm[6]. Two of the most common blockchain consensus protocol is Proof of Work (PoW) and Proof of Stake (PoS). Proof of Work is a algorithm where to validate a block, it guesses the hash function until it can be linked into the blockchain database [6]. Proof of Stake is an algorithm where it uses a stake system to choose who can create the next block[6].

Blockchain can be beneficial to a ballot system because the integrity and availability of the transaction is better compared to a traditional cloud system. Blockchain also has an advantage for ballots because the data cannot be deleted or modified once the transaction is validated, so there is no manipulation on the data stored in the blockchain[6]. In this design, the nodeRemote Procedure Call (RPC) of the blockchain will be provided by Infura. Infura is a service to help sends the transaction from a microcontroller into the blockchain network. The blockchain network chosen for this design is using the an Ethereum test network provided by Ropsten.

SYSTEM DESIGN

In this system design, there is a hardware design and software design. The hardware used in this design consist of a microcontroller and a button mechanism. The microcontroller is the center of the operation, the purpose of the microcontroller is to process the input from the button mechanism then sends the chosen candidate from the input and sends it into Infura for it to be uploaded into the blockchain. Another purpose of the microcontroller is to sign the transaction using the predetermined private key of the sender, the transaction needs to be signed so that Infura can know who sends the transaction and if the transaction is valid or not. The microcontroller used in this design is the ESP-32. ESP-32 is chosen in this design because it has built-in Wi-Fi for a microcontroller. This gives the capability of the microcontroller to communicate to the internet and upload the transaction into the Blockchain. The button mechanism is used in this design as the input for choosing between the first and second candidate. The button mechanism is connected into the microcontroller digital GPIO pins. The hardware prototype can be seen in Figure 1.

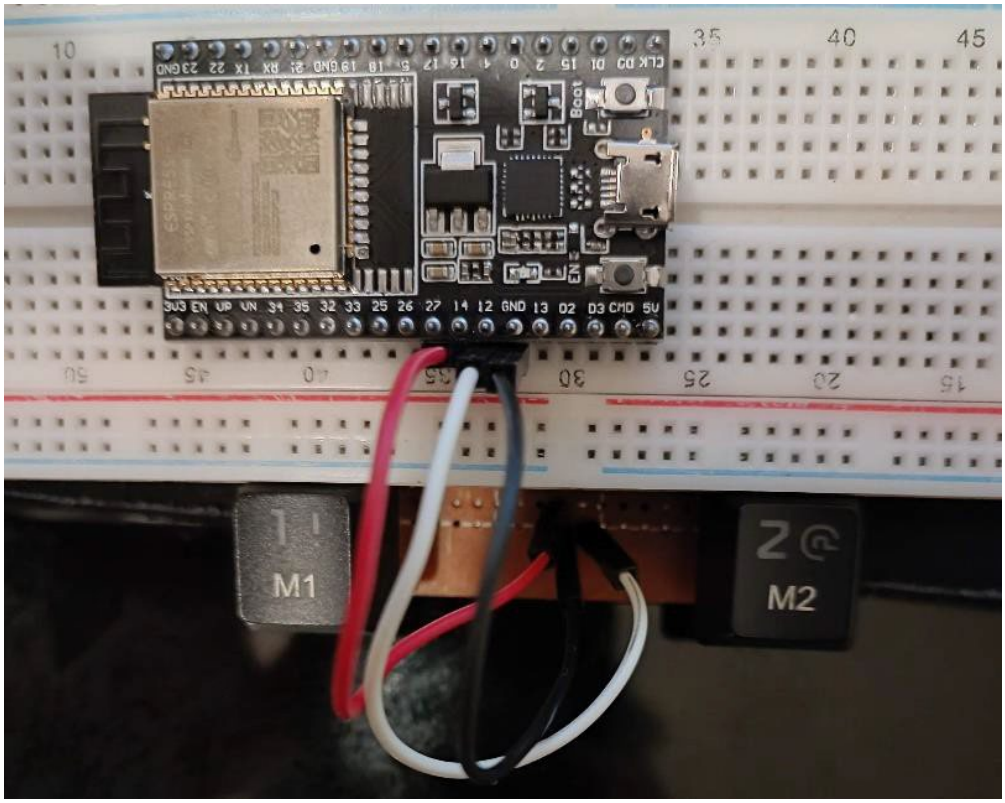

Figure 1. Hardware Prototype used in this Design.

The software in this design is the program used to upload the data for the candidate choice into Infura RPC. This program first connect to Wi-Fi, then check the user's Ethereum balance to see how much balance they have. Then the program prepare for transaction by setting gas price and waits for the button inputs for the candidate choice. Once the candidate has been chosen, the program sends the candidate's name into the blockchain and restart the microcontroller for the next input. The program block diagram is in Figure 2.

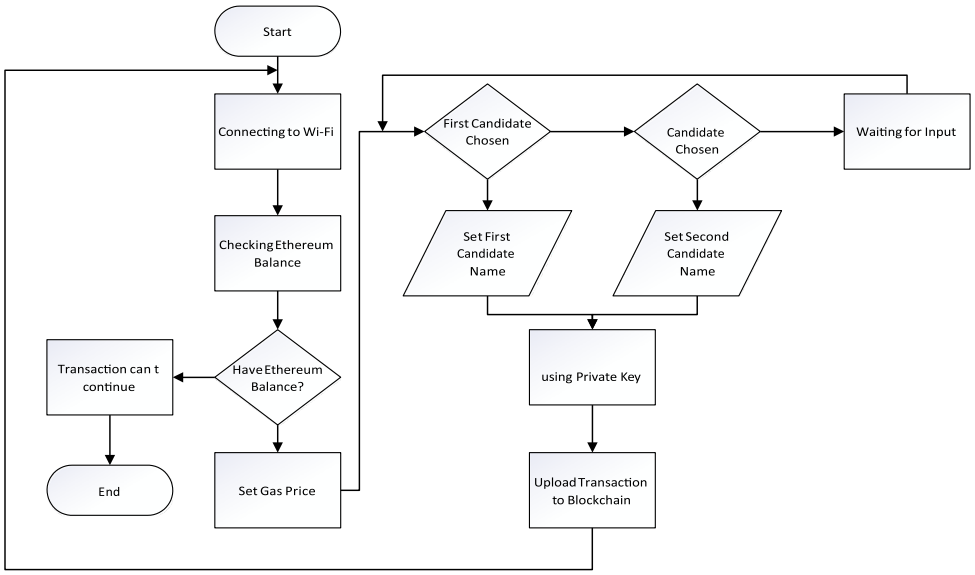

Figure 2. Block Diagram

RESULTS AND DISCUSSION

Testing is done until 60 times with sending both candidate name, “Candidate One” and “Candidate Two” into Ropsten Ethereum test network. The latest results of the transaction can be seen both candidates outputted into the microcontroller console and verified in etherscan.io website. The data sent from the microcontroller is using a hexadecimal format which is a translation from UTF-8 format.

The output of the microcontroller console can be seen in Figure 3 and Figure 4.

Figure 3. First Candidate Sent Transaction.

Figure 4. Second Candidate Sent Transaction.

Confirmation of the transaction success can be seen in Figure 5 and Figure 6, with the "Nonce" number acting as the number of transactions done.

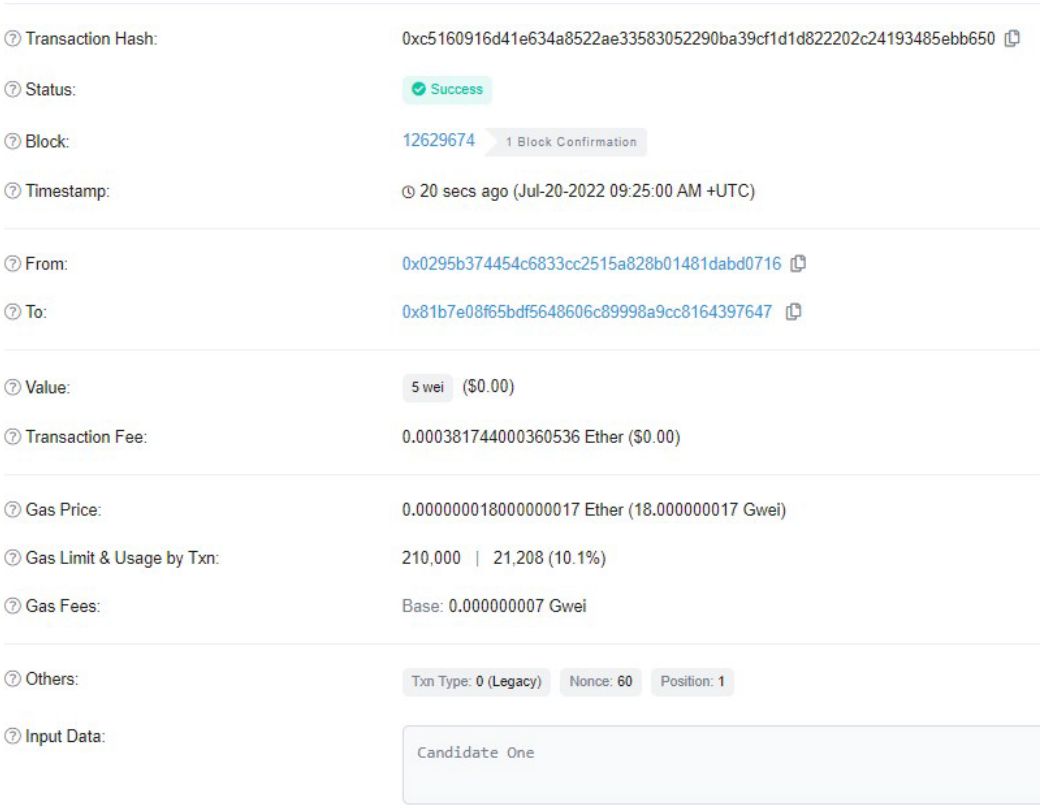

Figure 5. First Candidate as 60th Transaction Done Confirmed in Etherscan.io

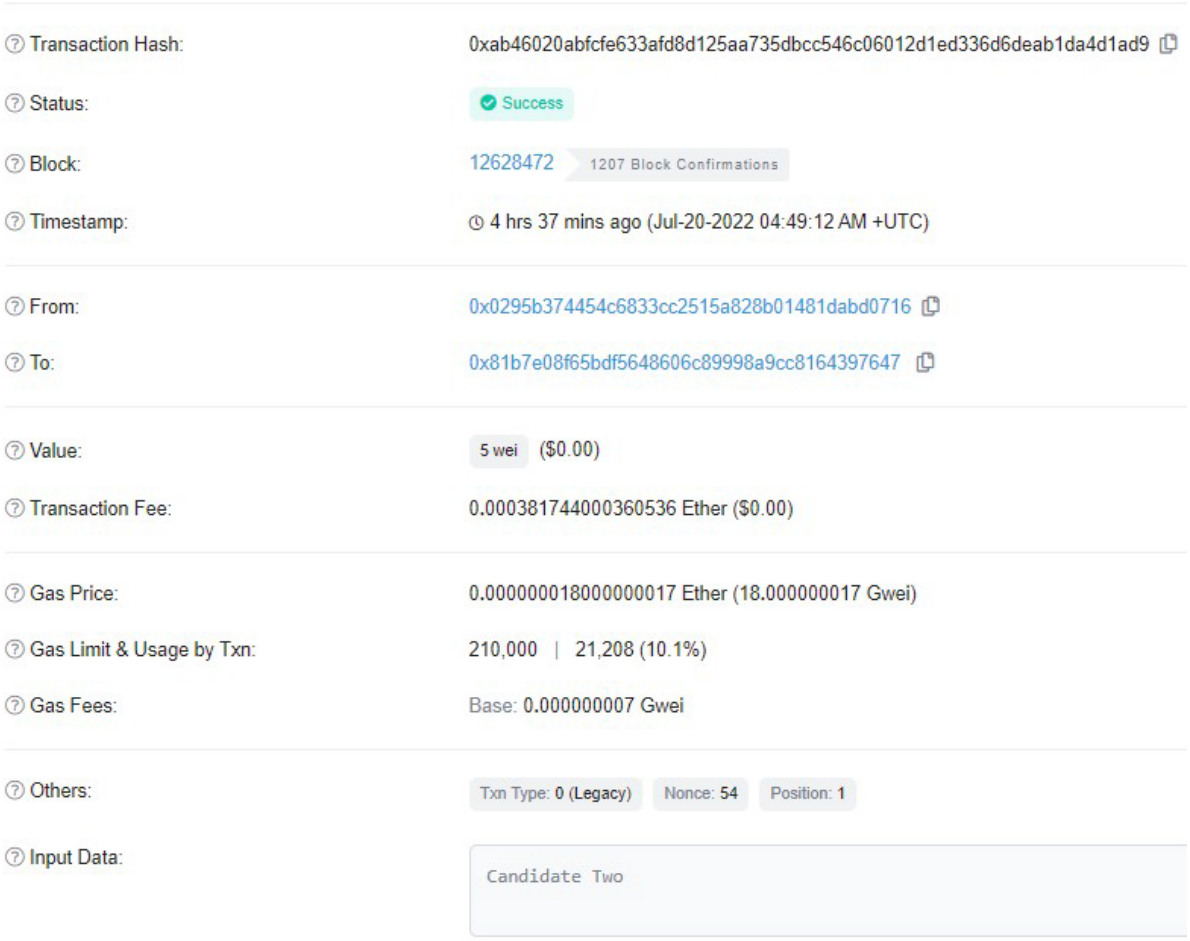

Figure 6. Second Candidate as 54th Transaction Done Confirmed in Etherscan.io

The Transaction both shown success in the transaction and the data being sent is secured on the blockchain network with the Data Input can be shown directly in Etherscan.io using the UTF-8 Format.

Each transaction in this blockchain cost 18 Gwei of Ethereum which if it is in the Main Network of Ethereum would cost $0.0000279 US Dollars or 0.42 Rupiah. 60 Total transactions would cost around $0.001674 US Dollars or 25.2 Rupiah.

CONCLUSION

The system of a blockchain implementation for a microcontroller-based ballot system is proven successful on a smaller scale. This system design is tested 60 times with all of the data sent into the Ethereum test network proven by etherscan.io.

REFERENCES

[1] Key Jr, V. O. (1955). A theory of critical elections. The Journal of Politics, 17(1), 3-18.

[2] Gupta, V., Hypolite, J., Mell, S., & Sanghvi, H. Securing Election Infrastructure with Hand-Marked Paper Ballots.

[3] Alvarez, R. M., Levin, I., & Li, Y. (2018). Fraud, convenience, and e-voting: how voting experience shapes opinions about voting technology. Journal of Information Technology & Politics, 15(2), 94-105.

[4] Alvarez, R. M., Beckett, D., & Stewart III, C. (2013). Voting technology, vote-by-mail, and residual votes in California, 1990–2010. Political Research Quarterly, 66(3), 658-670.

[5] Suraj, M., & Khan, A. (2015). Environmental impact of paper industry. International Journal of Engineering Research & Technology, 3(20), 1-3.

[6] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), 100067.

[7] White, B. S., King, C. G., & Holladay, J. (2020). Blockchain security risk assessment and the auditor. Journal of Corporate Accounting & Finance, 31(2), 47-53.

[8] Picone, M., Cirani, S., & Veltri, L. (2021). Blockchain security and privacy for the Internet of Things. Sensors, 21(3), 892.

[9] Banchhor, P., Sahu, D., Mishra, A., & Ahmed, M. B. (2021). A systematic review on blockchain security attacks, challenges, and issues. International Journal of Engineering Research and Technology (IJERT), 10(04), 386-391.

[10] Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-peer Networking and Applications, 14, 2901-2925.