International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Electronic Voting Machine using Arduino and Blockchain

Pritipriya Singh, Darshan Rajpurohit, Vaishak Vijayan, Saurabh Sahane, Prof. Supriya Vishal Dicholkar

[1,2,3,4] *Department of Electronics and Telecommunication Engineering*
[5]*Professor, Department of Electronics and Telecommunication Engineering*
Atharva College Of Engineering, Malad (West), Mumbai, India

Abstract - It has generally been challenging to develop a secure electronic voting system that provides the transparency and flexibility that electronic systems give while maintaining the integrity and privacy of current voting schemes. In this paper, We investigate a blockchain application for the implementation of distributed electronic voting systems. The research offers a novel blockchain-based electronic voting system that addresses some of the shortcomings of existing systems and evaluates certain well-known blockchain frameworks in order to develop a blockchain-based voting system with IoT. We explicitly analyze the possibilities of distributed ledger technology through the explanation of a case study, namely the election process and the deployment of a blockchain-based application that boosts security and lowers the cost of conducting a national election.

Key Words: blockchain, electronic voting machine, IOT

1.INTRODUCTION *(Size 11, Times New roman)*

Research on electronic voting systems has been ongoing for decades with the aim of reducing
election costs while maintaining election integrity by meeting security, privacy, and compliance criteria.The existing e-voting system consists of EVM and Ballot papers in democratic countries around the world. EVM is an electronic voting machine used by countries like India, Pakistan, etc. Here the machines are used to cast votes. A ballot paper is a slip of paper used to register a vote. Even with advancements in technology, many democratic countries like the
USA continues to use Ballot papers. This depends mostly on the availability, security, and population of the country. It is often seen that densely populated countries gravitate towards
using EVM over Ballot

2. EVM &Shortcoming

There are many underlying problems associated with the existing voting system. To name a
few:
- Ballot papers can tamper.
- EVM machines can be hacked by advanced hackers
- Relying on one centralized authority - Election commission
.[1]. Replacing the traditional pen-and-paper scheme with a new election system has the
potential to limit fraud while making the voting process traceable and verifiable
[2]. Blockchain is a distributed, immutable, incontrovertible, public ledger. This new
technology has three main features:
(i) Immutability: Any proposed "new block" to the ledger must reference the previous version of the ledger. This creates an immutable chain, which is where the
blockchain gets its name from and prevents tampering with the integrity of the
previous entries.
(ii) Verifiability: The ledger is decentralized, replicated, and distributed over multiple
locations. This ensures high availability (by eliminating a single point of failure) and
provides third-party verifiability as all nodes maintain the consensus version of the
ledger.
(iii) Distributed Consensus: A distributed consensus protocol to determine who can
append the next new transaction to the ledger. A majority of the network nodes must
reach a consensus before any new proposed block of entries becomes a permanent
part of the ledger.
After evaluating both existing e-voting systems and the requirements for such systems to be
effectively used in a national election, we constructed the following list of requirements for a
viable e-voting system:
(i) An election system should not enable coerced voting.
(ii) An election system should allow a method of secure authentication via an identity
verification service.
(iii) An election system should not allow traceability from votes to respective voters.
(iv) An election system should provide transparency, in the form of a verifiable assurance to
each voter that their vote was counted, correctly, and without risking the voter's privacy.
(v) An election system should prevent any third party from tampering with any vote. (vi) An
election system should not afford any single entity control over tallying votes and
determining the result of an election.
(vii) An election system should only allow eligible individuals to vote in an election

3. Methodology

After carefully analyzing all the components and needs for the usage, the process of connecting an Arduino with a blockchain using a NodeMCU can be broken down into several steps. Firstly, you need to choose a blockchain platform that best meets your requirements and design a smart contract that will

interact with your Arduino. Secondly, set up the NodeMCU by installing the necessary libraries and drivers. Thirdly, write code for both the Arduino and the NodeMCU that will allow them to communicate with each other and the blockchain network. Fourthly, test the code to ensure that data is correctly transmitted to the blockchain network. Finally, deploy the smart contract to the blockchain network and use the API to interact with it from a web interface. By following this methodology, you can successfully connect your Arduino with a blockchain network and start exploring its capabilities. At the first occurrence of an acronym, spell it out followed by the acronym in parentheses, e.g., charge-coupled diode (CCD).

3. Working

Connecting an Arduino with a blockchain can be accomplished using several methods, but one popular method involves using a NodeMCU to communicate with the blockchain. Here are the basic steps:

Set up your blockchain network: You will need to choose a blockchain platform such as Ethereum, Tron, or Bitcoin. Then, create a smart contract on the blockchain network that will interact with your Arduino.

Connect the NodeMCU to the Arduino: The NodeMCU is a Wi-Fi-enabled microcontroller that can communicate with the blockchain network. You can connect the NodeMCU to the Arduino using serial communication or using the I2C bus.

Install the necessary libraries: To communicate with the blockchain network from the NodeMCU, you will need to install some libraries. For example, if you are using the Ethereum network, you will need to install the web3 library.

Write the code: You will need to write code for both the Arduino and the NodeMCU. The code for the Arduino will read input from the push buttons and send it to the NodeMCU using serial communication or the I2C bus. The code for the NodeMCU will then use the web3 library to interact with the smart contract on the blockchain network.

Test the code: Once the code is written, you can test it by pressing the push buttons and seeing if the data is correctly transmitted to the blockchain network.

Deploy the smart contract: Once the code is working correctly, you can deploy the smart contract to the blockchain network.

Use the API: Finally, you can use the API to interact with the smart contract from a web interface. The API can be used to read data from the smart contract or to send new data to the smart contract.

3.1 Block Diagram

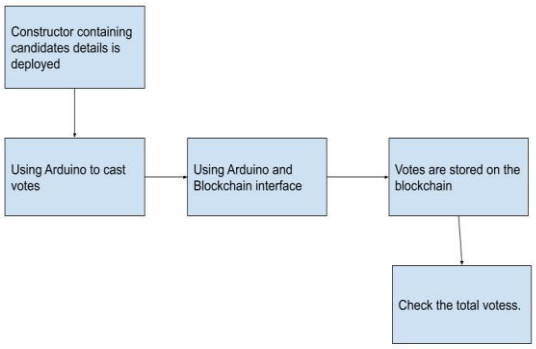

Fig -1: Block Diagram

3.2.Modal Architecture

The modal architecture for an IoT and blockchain-powered electronic voting system is as follows:
User Interface: To make voting on the voting machine simple, it should have an intuitive and user-friendly interface. The user interface needs to be made to function on a variety of gadgets, including laptops, tablets, and smartphones.
Blockchain: To assure the voting data's confidentiality, transparency, and immutability, it can be stored on a blockchain network. Each vote can be recorded on the blockchain as a transaction, which once added to the blockchain cannot be changed or removed. This will stop any voting data manipulation.
Using smart contracts, it is possible to automate the voting process and make sure it is conducted fairly and openly. Voting regulations like guaranteeing that voters are qualified to vote and prohibiting them from voting more than once can be written into smart contracts.
Encryption: The voting machine should employ encryption methods to safeguard the voting data's secrecy both during transmission and storage.

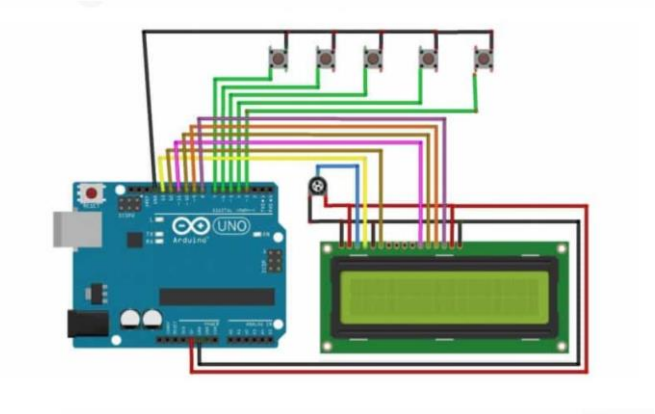

Fig -2: Circuit Diagram

4. CONCLUSIONS

In this paper, we introduced a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient elections while guaranteeing voters' privacy. We have shown that blockchain technology offers a new possibility to overcome the limitations and adoption barriers of electronic voting systems which ensures election security and integrity and lays the ground for transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. For countries of greater size, some additional measures would be needed to support greater throughput of transactions per second.

REFERENCES

1.] K. Ashton, “That ‘Internet of Things’ Thing - RFID Journal,” RFiD J., vol. 22, no. 7, pp. 97–114, 2009.
2. J. Gubbi, R. Buyya, S. Marusic, and M.Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,”Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660,2013.
3. C. Doukas and I. Maglogiannis, “Bringing IoT and cloud computing towards pervasive healthcare,” in Proceedings - 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2012, 2012, pp. 922–926.
4. A. R. Biswas and R. Giaffreda, “IoT and Cloud Convergence: Opportunities and Challenges,” 2014 IEEE World Forum Internet Things, pp. 375–376,
5. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” p. 9, 2008.
6. Blockchain-Based E-Voting System by Friðrik Þ. Hjálmarsson; Gunnlaugur K. Hreiðarsson; Mohammad Hamdaqa; Gísli Hjálmtýsson
7. Using Blockchain and CLIPS to make Things Autonomous by Mayra Samaniego and Ralph Deters
8. BlockChain Based Cloud Computing Model on EVM Transactions for Secure Voting by Sathya V.; Arpan Sarkar; Aritra Paul; Sanchay Mishra
9. Ajit Kulkarni, (2018), "How To Choose Between Public And Permissioned Blockchain For Your Project", Chronicled, 2018.
10. Supriya Vishal Dicholkar, "Review-IoT Security Research Opportunities",2020 IEEE International Conference on convergence to Digital World- Quo Wadis