International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.9756/INTJECSE/V14I5.51 ISSN: 1308-5581 Vol 14, Issue 05 2022

Blockchain Based Voting System

Paramesh A,
mailtoparamesha@gmail.com

Hemrishi Kumar G,
hemrishikumarg@gmail.com

Ebenazer Roselin S,
ebenazerroselin89@gmail.com

Deepa R
r.deepacse@princedrkvasudevan.com
Department of Computer Science and Engineering
Prince Dr K Vasudevan College of Engineering and Technology

***Abstract*— Structuring an electronic voting system which fulfills the legitimate requirements of representatives has been a challenge for a long time. Conducting the free, systematic and impartial election is the vital goal of every democracy nation. Every country follows a different voting system from old paper ballot system to electronic voting system. The main problem is location and accessibility, people are suffering to go to their native place polling booth for casting their vote. This needs to be considered as every people’s vote plays a significant role in deciding the right leaders. Blockchain technology offers the transparency and security requisites for the impartial election. It is a complete decentralized, immutable ledger system. The online voting system allows the voters to cast their vote from any place at any time which leads to increasing the voters participation count. The objective of the project is to create a voting system which provides transparency and security using Blockchain technology, the Python flask tool is used for setting up a local blockchain network over an network.**

***Keywords*— Blockchain, Smart Contract, Voting system, Decentralized application, E-voting.**

I. Introduction

Generally, a single organization maintains the database. This makes the single organization, a central authority with complete control over it. The central authority has the facility to fiddle with the database and influence the data. The organization maintains the database for two purposes one is for storage purpose which is not require any modification of the data. The other one involves the monetary matters or sensitive data such as voting, account transaction details which requires many people to involve in the data entry and modification. Through the organization enable only the authenticated people to access the central database still the hackers will find a way to access database easily. To evade such circumstances blockchain consider the database as public which provide every user to store the data in the database. Nevertheless, the user data must always be updated to keep consistency. The consensus algorithm is being used in blockchain technology in order to maintain a consistent decentralized database. The blockchain is one of the evolving technologies and plays a major role in many fields such as health care, supply chain management, market monitoring, etc.

Different types of voting mechanisms are followed across the world. Voice vote, rising vote show of hands, ballot vote are the traditional voting system. E-voting denotes that an electronic equipment is used to troupe votes in an election. The significance of the e-voting is to proliferate the participation, to reduce the expenses of organizing elections and to improve the accurateness of the results. The security civic observing the Electronic Voting Machines (EVM) as defective because the corporal security is required for such systems. The voting machine may damage due to physical access by a person hence affects the existing vote cast on the machine. In general, the EVM has less security or integrity then online voting system. The online voting system also enables the voters to cast their vote using their personal devices like mobile, laptop, etc. Hence the secrecy is maintained and there increases a number of participants to cast their vote. Blockchain is Distributed Ledger Technology (DLT), which has digital asset unchangeable and translucent through the usage of decentralization and cryptographic hashing. The features of blockchain technology are as follows.

A. Distributed ledger enables no single point of failure.
B. New transaction can be inserted into the ledger by anyone who is having the distributed control.
C. The block is created or inserted based on its previous block details.
D. Consensus algorithm plays a major role in constructing their new block and performs transaction in it.

The objective of this project is to create a voting system which provides transparency on security using blockchain technology. To explore the various available options in the blockchain technology and to choose the right platform to develop the voting system. With blockchain based voting, the voter turn up might also increase as people can cast their vote from any place at any time, making this as a perfect alternate to the current voting system. This project is organized as the literature review is explained in the section 2, the proposed architecture is discussed in Section 3 and the implementation details, and the conclusion is discussed in Section 4 and Section 5 respectively.

II. LITERATURE SURVEY

There are many researchers shown their interest to
implement a novel research work in the area of block chain technology as this becoming the mandatory of many applications.

[1] Adida, B., Helios (2008). “Web-based open-audit voting.”, in Proceedings of the 17th Conference on Security Symposium, ser. SS’08. Berkeley, CA, USA: USENIX Association, 2008. This paper proposes associated justify an adequate security model and criteria to judge comprehensibility. It additionally describes a web ballot theme, pretty graspable Democracy, show that it satisfies the adequate security model which it’s a lot of graspable than Pretty smart Democracy, presently the sole theme that additionally satisfies the planned security model. [2] Chaum D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008).“Scantegrity: End-to-end voter veriable optical- scan voting.", IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.This paper describes Scantegrity that minimally impacts election procedures and is the first independent E2E verification mechanism that preserves optical scan as the underlying voting system and doesn’t interfere with a manual recount. [3] Dalia, K., Ben, R., Peter Y. A, and Feng, H. (2012). “A fair and robust voting system by broadcast.”, 5th International Conference on E-voting, 2012.This paper proposes a recovery round to enable the election result to be announced if voters abort and also added a commitment round to ensure fairness. In addition, it also provided a computational security proof of ballot secrecy. [4] Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). “Star-vote: A secure, transparent, auditable, and reliable voting system.”, in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.This paper describes the STAR-Vote design, that may preferably be the next-generation electoral system for Travis County and maybe elsewhere.

III. PROPOSED SYSTEM

The simple rationalization could be a 'chain' of blocks. A block is associate degree mass set of information. knowledge square measure collected and methodical to suit in an exceedingly block through a process known as mining every block may be known employing a science hash (also referred to as a digital fingerprint). The block shaped can contain a hash of the previous block, so blocks will kind a sequence from the primary block ever (known because the Genesis Block) to the shaped block. during this method, all the information may be connected via a connected list structure. We implement the proposed protocol using smart contract in such a way that the Ethereum bock chain's consensus mechanism enforces the execution of the voting protocol. We propose a smart contract implementation of our protocol on Ethereum in order to enforce the execution of the voting protocol. We are using Ethereum since it can store and execute programs that are written as smart contracts.

A Analysis of Algorithm

WORKING:

SHA-256 Algorithm

1. The SHA-256 algorithm takes an input of any random length and produces an output of a fixed length (256 bits).
2. In the case of SHA-256 algorithm no matter how big or small is the input, the output is of fixed length (256 bits).

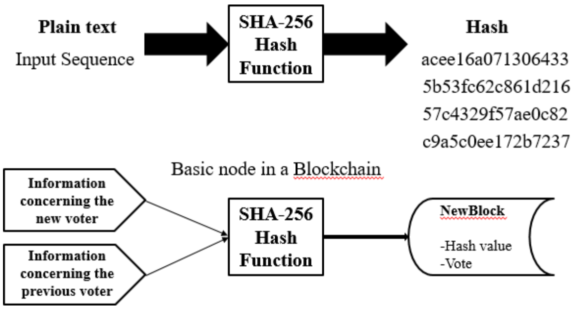
A cryptographic hash function has the following properties:

1. Deterministic: This means that no matter how many times we enter the same input we will get the same result.
2. Quick Computation: This means that the result is generated quickly, and this leads to an increase in the system effiency.
3. Small changes in Input change the whole Output: A minor change in the input significantly changes the whole output.
4. Collision Resistant: Every input will have a unique hash value.
5. Puzzle friendly: The combination of two values gives the hash value of new variable.

The whole system can be divided into four main activities:

1. **Registration -** Before participating in voting, each valid voter is given a public address and a private key, which will be used later for authentication. Each voter account is filled with enough ethers to carry out one single transaction. Both public address and private key should not be revealed to anyone. This helps the voters to cast their votes anonymously.

2. **Authentication** - The voting process starts with Authentication. Each valid voter is given an address and key for verifying their identity. Each voter is asked to enter his public address and private key (authentication credentials). Once the credentials is valid, the voter is allowed to cast their vote.



3. **Voting -** Once authenticated, they can choose a candidate from the list of available candidates by using the Front-end

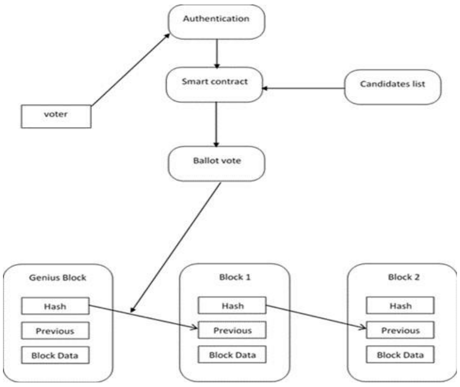
application. Only one chance is being given to every voter. To cast a vote, a function call is made to the deployed smart contract with the candidateid.

4. **Results -** The transaction of the block is successful only when the transaction id conformed by the miner (any one) and acknowledged by all the miners.

IV. Implementation of Blockchain

The system is designed with these following points in consideration: -

1. Only one chance is given to the voter to prevent double voting.
2. Only eligible voters are enabled to cast the vote by checking their identity.
3. While vote counting, the system should not depend on a single authority.
4. The privacy of the voters should be maintained.
5. The stored votes should be verifiable and tamperproof

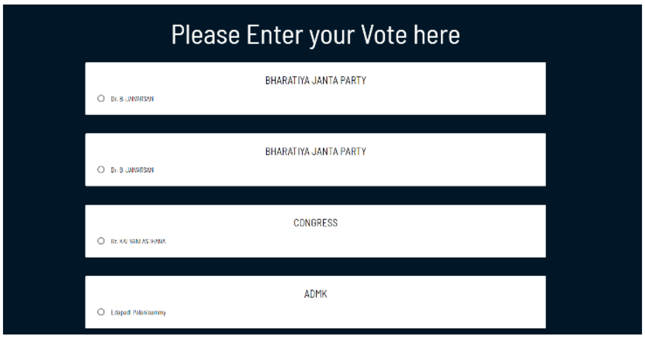


C Implementation of Blockchain Network

For implementing the network, we use Python and one of its frameworks called Flask to run on the machine over the network. Flask is one of the frameworks of python to implement the blockchain over the network and it is one of the alternatives to web development by using the languages like html, css and java script. Here to implement the blockchain we use python to build the block using many native algorithms. In blockchain, each and every block is chained with its next block and its previous block. Hence if the hackers tries to access the Block N then it will be notified to Block N+1, and the changes in Block N+1 also reflects in Block N+2 and so on. The hash value of Block N+1 is computer using the below formula

Hash (block (n+1)) = f (timestamp + hash (block (n)) + payload + (hash (mark root) + target + N once))

First the voter should register their identity by signing up with their profile using a unique identifier like Aadhar card along with his voter-id and he gets a confirmation in his mobile number when he successfully creates his account. After the account is created the voter must login with their credentials and a voter window opens like the below picture



Please Enter your Vote here

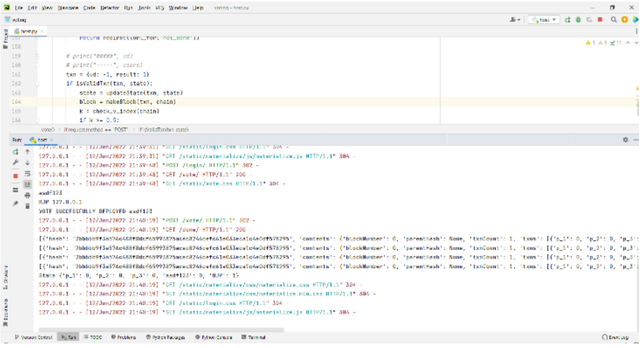
BHARATIYA JANTA PARTY
○ Dr. B. JAWARSAN

BHARATIYA JANTA PARTY
○ Dr. B JAWARSAN

CONGRESS
○ Dr. KAI YANI ASTHANA

ADMK
○ Edapadi Palanisammy

When the account is created the block gets created



```
        return redirect(url_for('not_done'))

    # print("#####", ud)
    # print("-----", users)
    txn = {ud: -1, result: 1}
    if isValidTxn(txn, state):
        state = updateState(txn, state)
        block = makeBlock(txn, chain)
        k = check_v_index(chain)
        if k >= 0.5:
```

```
127.0.0.1 - - [12/Jun/2022 21:39:31] "GET /static/login.css HTTP/1.1" 304 -
127.0.0.1 - - [12/Jun/2022 21:39:31] "GET /static/materialize/js/materialize.js HTTP/1.1" 304 -
127.0.0.1 - - [12/Jun/2022 21:39:48] "POST /login/ HTTP/1.1" 302 -
127.0.0.1 - - [12/Jun/2022 21:39:48] "GET /vote/ HTTP/1.1" 200 -
127.0.0.1 - - [12/Jun/2022 21:39:48] "GET /static/vote.css HTTP/1.1" 304 -
asdf123
BJP 127.0.0.1
VOTE SUCCESSFULLY DEPLOYED asdf123
127.0.0.1 - - [12/Jun/2022 21:40:19] "POST /vote/ HTTP/1.1" 302 -
127.0.0.1 - - [12/Jun/2022 21:40:19] "GET /done/ HTTP/1.1" 200 -
[{'hash': '2bbbbb9f3a576c488f8dcf65993875acec8246cefc61e633eca1c4e0df578295', 'contents': {'blockNumber': 0, 'parentHash': None, 'txnCount': 1, 'txns': [{'p_1': 0, 'p_2': 0, 'p_3':
[{'hash': '2bbbbb9f3a576c488f8dcf65993875acec8246cefc61e633eca1c4e0df578295', 'contents': {'blockNumber': 0, 'parentHash': None, 'txnCount': 1, 'txns': [{'p_1': 0, 'p_2': 0, 'p_3':
[{'hash': '2bbbbb9f3a576c488f8dcf65993875acec8246cefc61e633eca1c4e0df578295', 'contents': {'blockNumber': 0, 'parentHash': None, 'txnCount': 1, 'txns': [{'p_1': 0, 'p_2': 0, 'p_3':
[{'hash': '2bbbbb9f3a576c488f8dcf65993875acec8246cefc61e633eca1c4e0df578295', 'contents': {'blockNumber': 0, 'parentHash': None, 'txnCount': 1, 'txns': [{'p_1': 0, 'p_2': 0, 'p_3':
State {'p_1': 0, 'p_2': 0, 'p_3': 0, 'asdf123': 0, 'BJP': 1}
127.0.0.1 - - [12/Jun/2022 21:40:19] "GET /static/materialize/css/materialize.css HTTP/1.1" 304 -
127.0.0.1 - - [12/Jun/2022 21:40:19] "GET /static/materialize/css/materialize.min.css HTTP/1.1" 304 -
127.0.0.1 - - [12/Jun/2022 21:40:19] "GET /static/login.css HTTP/1.1" 304 -
127.0.0.1 - - [12/Jun/2022 21:40:19] "GET /static/materialize/js/materialize.js HTTP/1.1" 304 -
```

since in blockchain every transaction is considered as a block. So the registration details are considered as a transaction and these transaction are stored as pickle files and they are encrypted using SHA-256 Algorithm. And after these steps a window opens where the user need to click the any of the party whichever they wish to choose. After deciding the checkbox needed to clicked will be highlighted making sure that they click the correct checkbox. When a checkbox is pressed and submitted a window shows that the vote is done successfully and block is created after that which shows the vote is done and the results can be seen there at that instant of time which is shown in the below picture

This is the window from the backend which shows the transaction which has been done by the voter by successfully voting his desired party and it shows the current number of successive votes for all the parties so they can announce the results very fast without missing the voting count.

V. Conclusion And Future Works

This project provides an electronic voting system using a blockchain network without the use of Metamask and Truffle wallets since they can’t be used by elderly people who has less knowledge about the world of WEB 3.0 . Many research works proved that the block chain technology helps in improving the existing system hence it also provide a better way to conduct the Election. It also used to evade the drawbacks of centralized voting systems. This voting system is implemented using Flask framework in python to check the working of the voting system. After the Votes are casted by the voters, it is stowed as immutable and tamper-proof. This addresses the security issues with the current Electronic Voting system. Though it provides transparency, as the transactions are visible to everyone, it conserves voter’s confidentiality and secrecy. It helps in announcing the result fast. It takes more than 2 weeks to announce result in the current system. The voting results are publicly auditable.

The idea of adapting digital selection systems to create the general public electoral method cheaper, quicker and easier, could be a compelling one in trendy society. Creating the electoral method low cost and fast, normalizes it within the eyes of the voters, removes an explicit power barrier between the elector and therefore the functionary and puts an explicit quantity of pressure on the functionary. It additionally opens the door for a additional direct sort of democracy, permitting voters to precise their canon individual bills and propositions.

The Scope of the system and its future works is included in these points

1. Linking application with Government voting system data
2. Enhancing the GUI of the application.
3. Local languages can be included which will play a vital role for people living in rural areas as well as uneducated people
4. Also, adding suggestion system for voters that enables the public to give suggestions to the current winner.
5. A complaint system can be included, that allows the people to file complaint against a candidate.
6. Any other authentication methods can be integrated to further add security and trust to the voting system.

VI. References

1. Adida, B.; 'Helios (2008). "Web-based open-audit voting.", in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335348.
2. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008). "Scantegrity: End-to-end voter-veriable optical scan voting.", IEEE Security Privacy, vol.

6, no. 3, pp. 40-46, May 2008.

3. Dalia, K., Ben, R., Peter Y. A, and Feng, H. (2012). "A fair and robust voting system." by broadcast, 5th International Conference on E-voting, 2012.
4. Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). "Star-vote: A se cure, transparent, auditable, and reliable voting sys tem.", in 2013 Electronic Voting Technology Work shop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.
5. Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). "Bingo voting: Secure and coercion- free voting us ing a trusted random number generator.", in Pro ceedings of the 1st International Conference on E voting and Identity, ser. VOTE-ID'07. Berlin, Heidel berg: Springer-Verlag, 2007, pp. 111-124.
6. Adida B. and Rivest, R. L. (2006). "Scratch and vote: Self-contained paper-based cryptographic voting.", in Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, ser. WPES '06. New York, NY, USA: ACM, 2006, pp. 29-40.
7. Chaum, D., Ryan, P. Y. A. and Schneider, P. Y. A. (2005). "A practical voter-verifiable election scheme.", in Proceedings of the 10th European Conference on Research in Computer Security, ser. ESORICS 05. Berlin, Heidelberg: Springer-Verlag, 2005,pp. 118-139.
8. Chaum, D. (2004). "Secret-ballot receipts: True voter-verifiable elections.", IEEE Security Privacy, vol. 2, no. 1, pp. 38-47, Jan 2004.
9. Chaum, D. (1981)."Untraceable electronic mail, re turn addresses, and digital pseudonym.", Commun. ACM, vol. 24, no. 2, pp. 84-90, Feb.