e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

E-VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY

Vikrant Neve[*1], Ravi Prajapati[*2], Sujit Sharma[*3], Siddhesh Kawatgi[*4], Sheeba P.S[*5]

[*1,2,3,4]Students, Electronics Engineering, Lokmanya Tilak College Of Engineering, Navi Mumbai, Maharashtra, India.

[*5]Associate Professor, Electronics Engineering, Lokmanya Tilak College Of Engineering, Navi Mumbai, Maharashtra, India.

ABSTRACT

Since the 1970s, electronic voting, often known as e-voting, has been utilized in many forms with key advantages over paper-based systems, including enhanced efficiency and reduced errors. However, there are still obstacles to widespread adoption of such systems, particularly in terms of enhancing performance. Their ability to withstand potential flaws Blockchain is a cutting-edge technology that promises to transform the contemporary era. To make e-voting systems more resilient in general This paper outlines a strategy for maximizing the benefits. Blockchain should have cryptographic principles and transparency voting. The proposed scheme complies with the basic standards for Electronic voting systems. End-to-end verifiability is achieved. The proposed e-voting mechanism is described in depth in this document, together with its advantages and disadvantages. In-depth information is presented in this publication.

Keywords: Voting, Analysis, Blockchain Technology, Research.

I. INTRODUCTION

Electoral integrity is critical not only for democratic nations, but also for the transparency and trust of state voters. Political voting methods are crucial in this respect. Electronic voting technology can increase voter participation and confidence, as well as reignite interest in the voting system, from a government perspective. Elections have long been a social concern as a valid method of making democratic decisions. as the number of votes cast in real life increases, citizens are becoming more aware of the significance of the electoral system. The traditional or paper-based polling method increased people's trust in the majority voting selection. It has helped make the democratic process and the electoral system worthwhile for electing constituencies and governments more democratized It is critical to guarantee that voter confidence does not decrease. A recent study revealed that the traditional voting process was not wholly hygienic, posing several questions, including fairness, equality, and people's will, was not adequately quantified and understood in the form of government. A blockchain is must be designed and constructed of blocks that are cryptographically joined simultaneously. A cryptographic hash of the previous blocks, a timestamp, and transaction data were included in each block (generally represented as a Merkle tree). The timestamp verifies that the transaction data was there at the time the block was released, allowing it to be hashed. Each block carries information on the one before it, forming a chain with each new block reinforcing the ones before it. as a result, data manipulation is difficult with blockchains since, once recorded, the data in any one block cannot be updated retrospectively without impacting all subsequent blocks. A peer-to-peer network often manages blockchains for use as a publicly distributed ledger, with nodes adhering to a set of rules. A blockchain is a decentralized, distributed, and frequently public digital ledger made up of documents called blocks that are used to record transactions across many computers in such a way that any one block can't be changed without affecting all subsequent blocks. This allows the participants to independently check and audit transactions at a cheap cost. A blockchain database is run independently using a peer-to-peer network and a distributed timestamping server. Widespread collaboration, which is powered by collective self-interest, validates them. This style of architecture encourages a consistent workflow with minimum data security issues among participants. The implementation of a blockchain removes a digital asset's attribute of limitless reproduction. It verifies that each unit of value was only transmitted once, putting a stop to the long-standing issue of double-spending. The word "blockchain" refers to a value exchange protocol. when correctly set up to explain the trade agreement, a blockchain can safeguard title rights by providing a record that compels offer and acceptance.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

II. REVIEW OF LITERATURE

In 1991, A cryptographically secured chain of blocks was described for the first time by Stuart Haber and W Scott Stornetta. Nick Szabo, a computer scientist, developed 'bit gold,' a decentralised digital money, in 1998. In 2000, Stefan Konst published his theory of cryptographically secured chains, plus ideas for implementation. In 2008, Developers (s) working under the pseudonym Satoshi Nakamoto released a white paper establishing the model for a blockchain. Then in 2009, Nakamoto implemented the first blockchain as the public ledger for transactions made using bitcoin. In 2014, Blockchain technology was separated from the currency and its potential for other financial, inter-organizational transactions were explored. The Ethereum blockchain architecture incorporates software applications that represent financial assets such as bonds into the blocks. These become known as smart contracts. Election processes and methods are also being affected by advances in information technology. Researchers are working to improve the contribution of such systems to voting systems by contributing to existing methods. Electronic voting is compared to traditional voting systems from a variety of perspectives, including simplicity, reduced margins of error, and speedy results.

During the election, election commissions may encounter a variety of issues. The most common problems are improper approval regarding voting, duplication, or illegal voting. To ensuring that the eligible voter casts the ballot, secure authentication is critical. As an example, regarding the vote duplication problem, E-voting refers to the endto end process of registration, voting and counting on a digital election management platform. Electronic voting systems strive to be as simple to use and secure as traditional voting methods while eliminating human error. In general, there are two types of electronic voting systems. Ballots can be used remotely, as well as through closed systems allocated in election offices The voters engage physically in pooling site electronic voting, but the ballots are removed and the votes are recorded electronically. Remote online voting entails casting ballots from a distance, usually via a personal device connected to the Internet. Voting kiosks, laptops, tablet phones, paper-based electronic systems, and even televisions are examples of alternate technologies.

III. PROBLEM DEFINITION

A manual voting system has been deployed for many years in our country. However, many people in our country are unable to vote due to diverse of reasons. To illustrate, sometimes people may not be in their registration region and due to this fact, they cannot fulfil their voting duties. To solve these problems, there is a need for an online election voting system with this keeping in mind that EVM votes tampering issues are also encountered, so this online election system will be integrated with Blockchain Technology to make it tamper-proof. All Data is stored in a centralized way. There is the possibility of data manipulation. Manufacturing and Maintenance cost is very high. The centralized database that stores electoral data is a major vulnerability. This vulnerability could be a single point of failure.

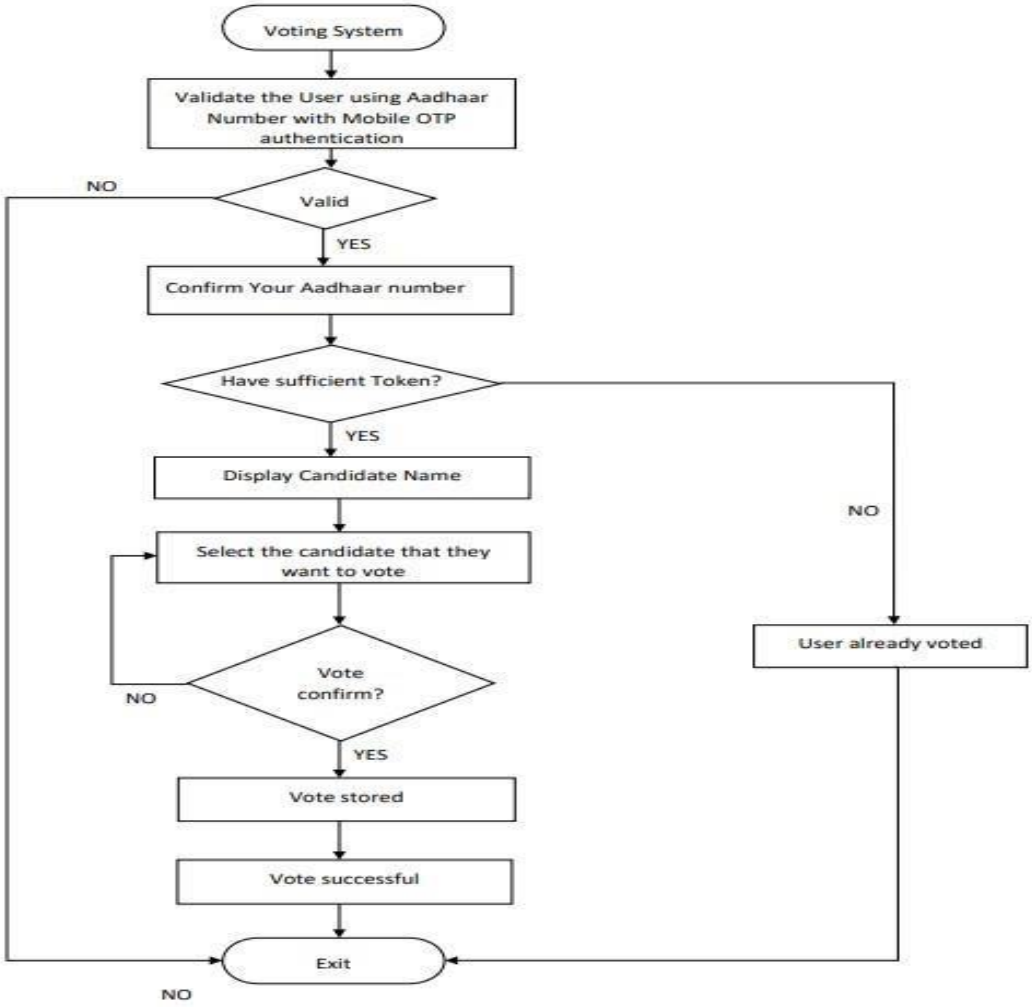
IV. METHODOLOGY

In one survey held at Jaipur Election commission, it was found that there are 1.12 lakhs fake votes. A same person's name appears in two, three, or even six different locations. Thousands of voters in Rajasthan, on the other hand, hold several voter cards. The best way to make each voter unique is to use blockchain technology. Each voter and their vote can be easily identified and validated.

The Proposed Model of Our Project While starting the voting process the first system will validate the user. Users will be validated on Aadhaar OTP verification. A user Aadhaar number and mobile number data are already stored in the database of the system. So, the system will match user data with data in the system. If user data is not matching then the process will end. If user data is matched then the system will generate OTP and send it to user mobile number. If OTP is not valid the process will exit. And if OTP is valid all candidate names will be displayed. The user will select one candidate name which the user wants to vote for. Users have to confirm the vote. One pop up will be displayed to confirm the vote. If the user selects No then the system will display all candidate names again. Once the user clicks on the yes on the popup box it will go to the next decision box. One user can vote only once i.e., each user has one token. After voting, that token will be deducted from the user. So, in this box, system will check if the user has sufficient tokens or not? If the token is not sufficient it will display User is already Voted and the process will end. If the token is sufficient (i.e., the user is

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

eligible to vote) then the user vote will be saved. The system will display votes. After the successful storing of vote, it will show "Vote successful". The user will exit and the program will be stopped.



A. WORKING FLOWCHART

What are the issues with the current voting system?

Voters confront a variety of issues during the voting process, therefore we decided to make a list of all of the issues that would support us in developing our project.

1) During elections, an unknown person casts a bogus vote in both rural and urban areas.

2) Many people will be unable to reach their constituency. the reason for this is that the pooling Centre is located far from home, and many people transfer from one location to another for work.

3) Some individuals believe that on election day, we shall celebrate and entertain. That's because the attitude that "my vote doesn't matter" expands throughout the country, raising the number of non-voters.

Distributed ledger technology is a system of interconnected blocks that stores transaction records and other user information. It operates on the decentralized distributed digital ledger idea. This system allows for cryptographically safe and private financial transactions as among network's user nodes, the with transactions being authenticated and accepted by all users in a visible manner. It is a ground-breaking technology that has grown in popularity as a result of the use of digital currencies.

V. THE BLOCKCHAIN TECHNOLOGY

1. BLOCKCHAIN TECHNOLOGY

There are different types of blockchain technology we can use to make electronic voting. We are using pycryptodome. As we are using python programming language for coding purpose so we have used pycrptodome blockchain technology. PyCryptodome is a Python module that contains low-level cryptographic

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

primitives. Python 2.7 and Python 3.5 are all supported. To utilise them successfully, you must have a thorough understanding of cryptography and security engineering. PyCryptodome exposes nearly the same API as PyCrypto, allowing most programmes to run without modification. However, for those sections of the API that posed a security risk or were too difficult to maintain, a few compatibility breaks had to be made. PyCryptodome's source code is partially in the public domain and partly under the BSD 2-Clause licence. PyCrypto's code is all free and open-source software that has been published into the public domain. This software may be copied, modified, published, used, compiled, sold, or distributed in any form, whether in source code or as a compiled binary, for any commercial or non-commercial purpose, and by any means.

2. TOKEN GENERATION

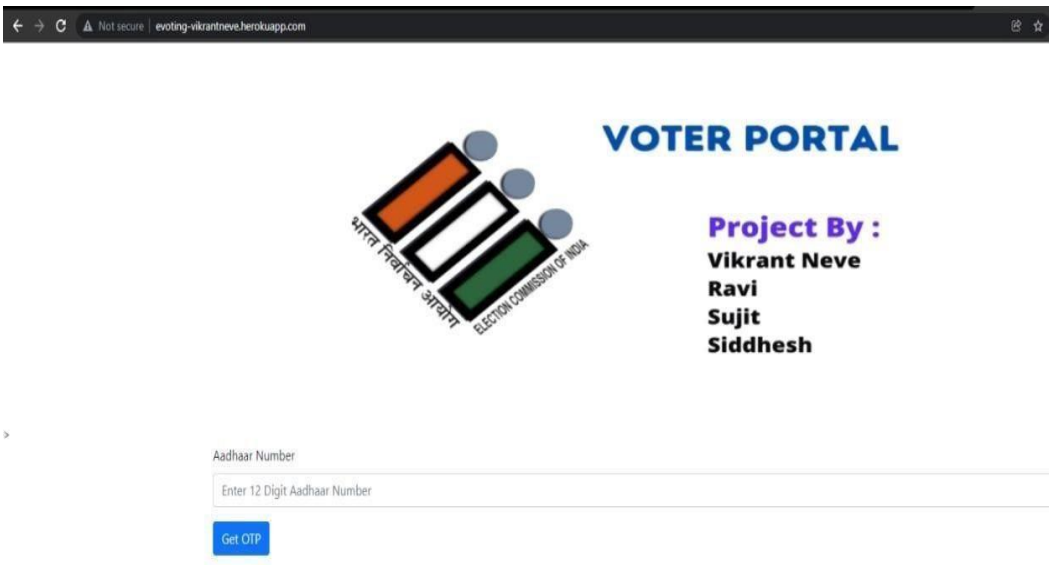
Tokens are fungible, transferable assets or utilities that are stored on own blockchains. Blockchains are based on the idea of smart contracts, or decentralised apps, in which programmable, self-executing code is used to handle and manage the many transactions that take place on the blockchain. Tokens are commonly used to raise funds for crowd sales, but they can also be used to replace other things. The traditional initial coin offering (ICO) process is used to produce, distribute, sell, and circulate these tokens. In our system, By default all users have one token which used to vote. After voting that token will be deducted. Cryptography refers to the many encryption methods and cryptographic approaches used to protect these entries, such as elliptical curve encryption, public-private key pairs, and hashing functions. We have used python module named Pycrypto for handling all Hashing and encryption part.

3. TRANSACTION VERIFICATION

Blockchain does not require any third-party to verify transactions. The system is said to be 'trustless'. Miners verify transactions. Miners are computer machines that validate all transactions and block any malicious actors. The list of transactions and the Block Header are the two most important parts of a block. The current block's hash, the prior block's hash, and the timestamp of when the current block was hashed make up the Block Header. To 'hash' data into a 256-bit number, use the SHA256 algorithm. This means you can feed the algorithm any data and it will return a 256-bit number that uniquely identifies it. Our blockchain uses SHA256 and Virtual nodes are verifying transactions. Every nodes get 10 points as rewards. A blockchain's entire concept is based on this. A and B are two blocks. A is the first person to be joined to the network. Miners aggregate transactions into Block A and hash them all together to generate a 256-bit number that uniquely identifies Block A. It's known as Hash A. The miners then work to build Block B, which will be stacked on top of Block A. Miners add Hash A to Block B after collecting another round of transactions. The new set of transactions is then hashed with Hash A to produce Hash B. Now, if a malicious actor were to go back and change even the smallest detail in Block A's transactions, Hash A would completely change, causing Hash B to change as well.

VI. RESULTS

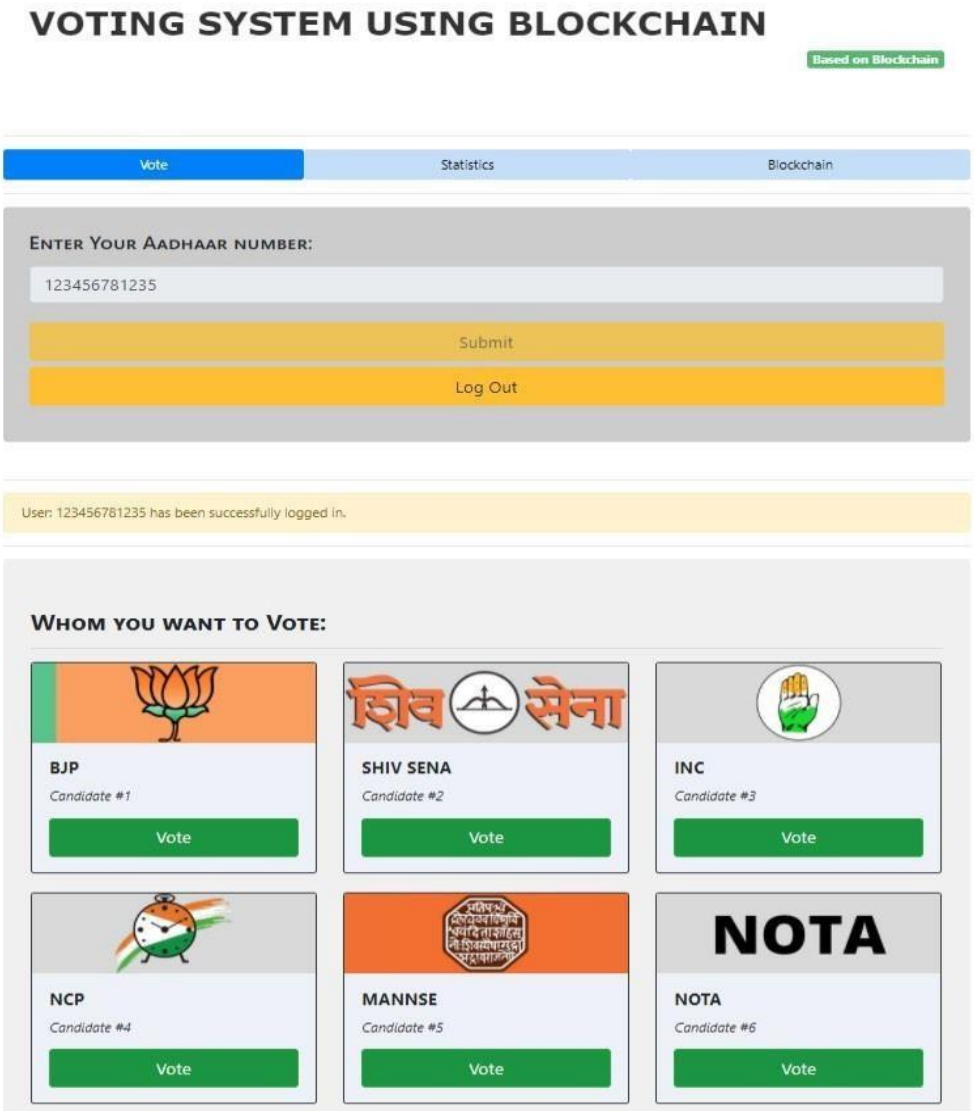
A. LOGIN PANEL



e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

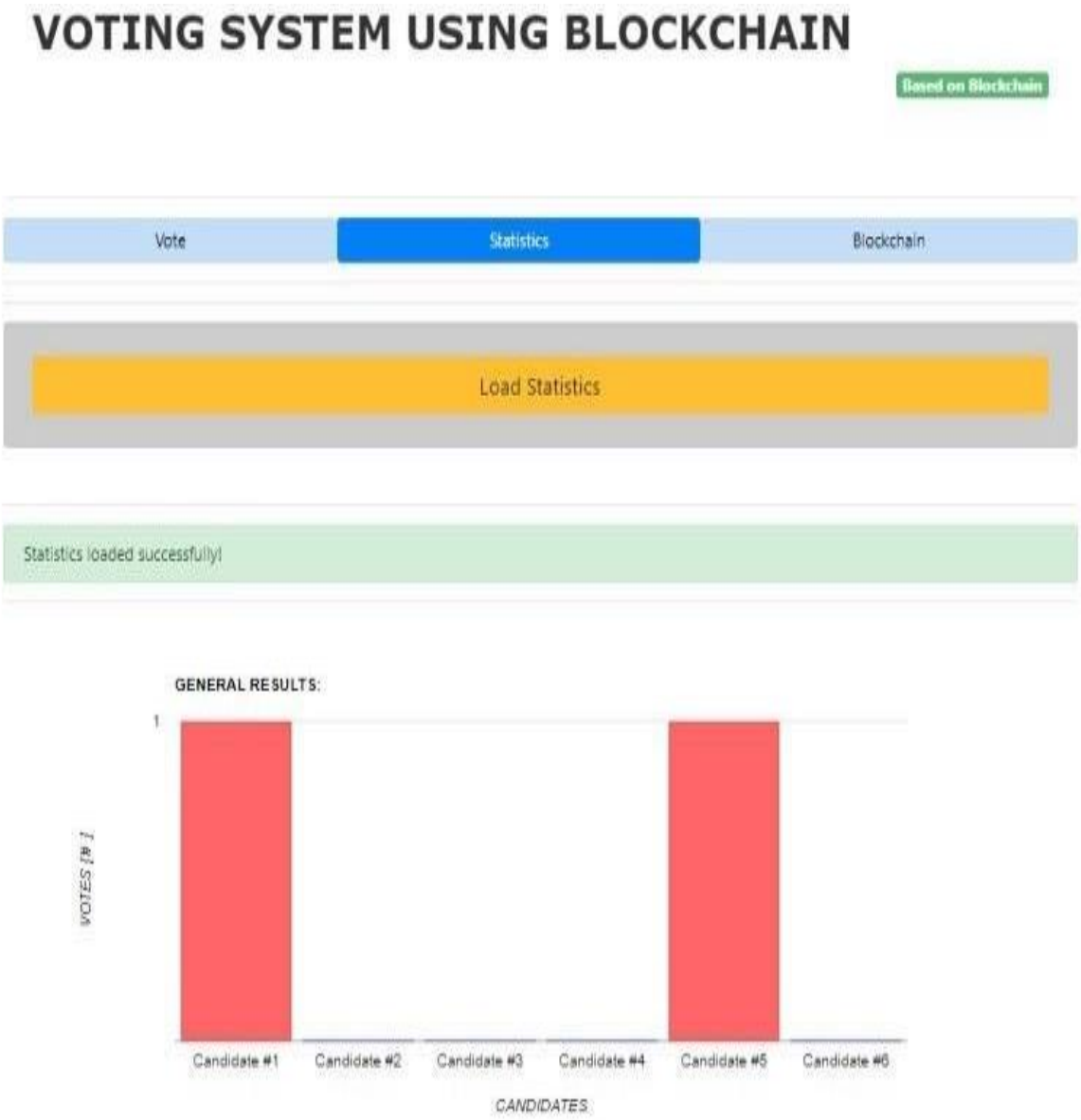
B. FACE CAPTURING

C. VOTER'S DASHBOARD



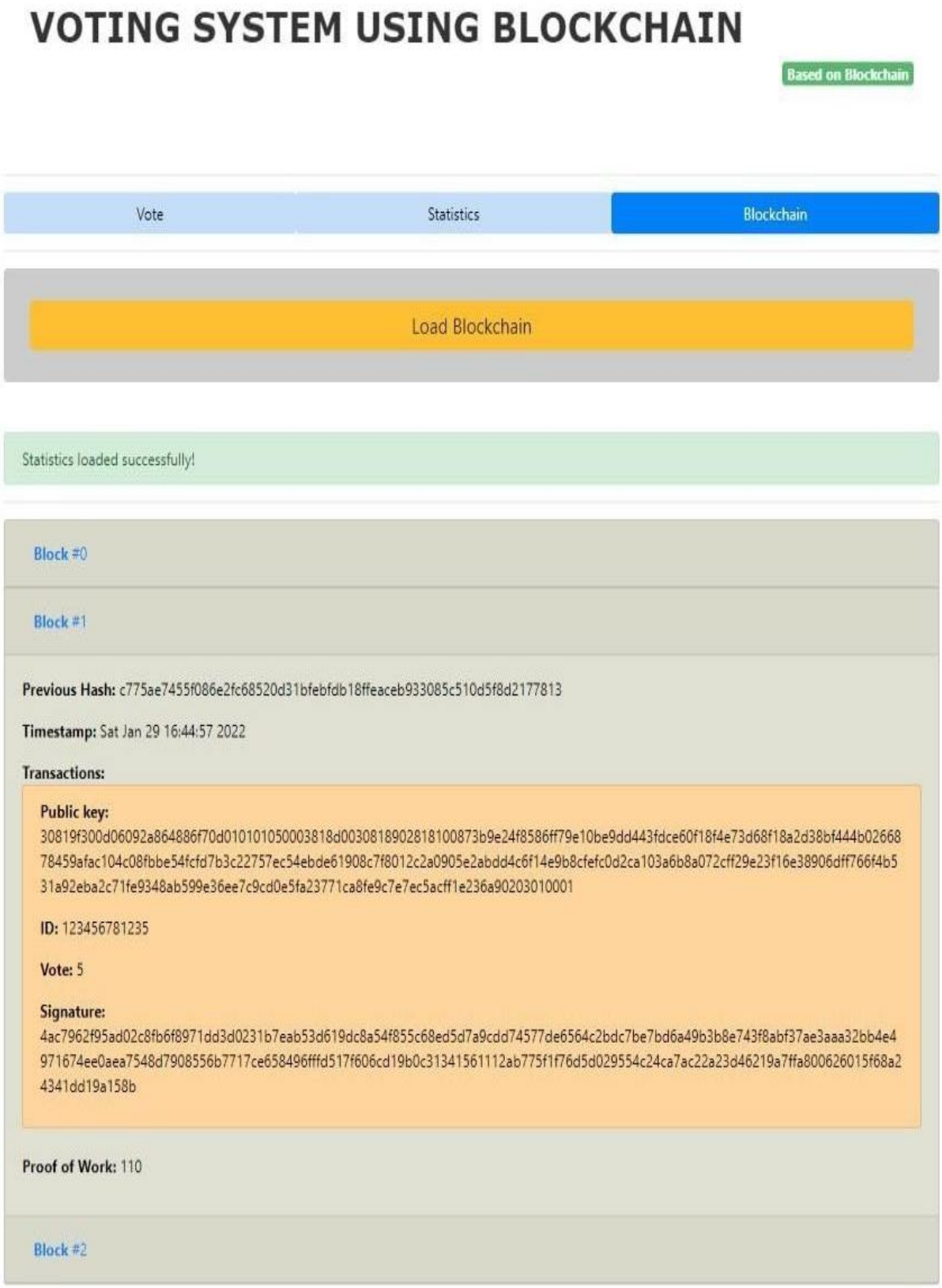
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

D. GRAPHICAL STATISTICS



e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

E. TRANSACTION (VOTE) VERIFICATION



VII. CONCLUSION

Trusted elections are essential for strong democracies, and citizens should have faith in the electoral system. Traditional paper-based elections, on the other hand, are unreliable. The concept of utilizing new voting technology to help to vote to be more accessible to the general public. In society today, the desire to make the

electoral process cheaper, faster and easier is tempting. Despite the fact that electronic voting has been a popular issue for several years, it is still not totally resolved. Authorities may be able to perform fraud or manipulations that are difficult to detect by other users in online voting systems due to a security conflict.

In this paper, a two-layer security model is suggested and validated in order to prevent election-related and vote manipulations. It is ensured that the election results may be counted after all participants have participated. The model ensures voter privacy, eliminates the need for a central authority, and keeps the recorded votes in a distributed database. Potential manipulations can thus be avoided during the process.

VIII. REFERENCES

[1] Ahm ed Ben Ayad, A conceptual Secure Blockchain -Based Electronic Voting System,lnternational Journal Of Network Security and its application(IJNSA) ,Vol.09, issue no .03, May 2017.

[2] https://www.researchgate.net/publication/341498272_A_CONCEPTUAL_SECURE_BLOCKCHAIN-BASED_ELECTRONIC_VOTING_SYSTEM

[3] Ong Kang Yi and Debashish Das , Blockchain Technology For Electronic Voting, Multidisciplinary Review Journal, Vol.07, issues no. 03, March 2020.

[4] https://www.jcreview.com/fulltext/197- 1583404985.pdf

[5] Chang-Hyun Roh and lm -Yeonglee, A Study on Electronic Voting System Using Private Blockchain, JINF Process System, vol.16, Issue no.02, PP.421,

[6] April 2020. http://jips-k.org/digital-library/2020/16/2/421

[7] Mrs. Harsha V. Patil, Mrs. Kanchan G. Rathi and Mrs. Malati V. Tribhuwan, A Study On Decentralized E-Voting System Using Blockchain Technology, International Research Journal Of Engineering And Technology (IRJET), Vol.OS, issue no.11, Nov 2018.

[8] https://www.irjet.net/archives/V5/i11/IRJETV5I1109.pdf

[9] Prof. Anita A. Lahane, Junaid Patel, Talif Pathan, and Prathmesh Potdar, Blockchain technology based evoting system, ITM Web of Conferences 32, ICACC2020.

[10] https://www.itmconferences.org/articles/itmconf/abs/2020/02/itmconf_icacc2020_03001/itmconf_icacc2020_03001.html