Block Chain Based Secure Voting System

1 2
Mrs.A.Nandhni ,Sanjith S

[1]Assistant Professor (SG), Department of Computer Applications, Nehru College of Management, Coimbatore,

Tamil Nadu, India
II MCA, Department of Computer Applications, Nehru College of Management, Coimbatore,
Tamil Nadu, India Sanjithsankar0123@gmail.com

ABSTRACT

Every nation currently uses either paper ballots or electronic voting machines (EVMs) for voting, which makes democratic voting an important and serious event. These procedures have a number of disadvantages, including lack of transparency, low voter turnout, vote tampering, mistrust of the electoral body, forged voter identification cards, delays in results distribution, and—above all—security concerns. The primary consideration when deciding whether to adopt a digital voting system is security. There can be no question regarding the system's capacity to protect against future assaults and secure data, especially with such significant judgments at stake. The usage of blockchain technology is one possible solution to the security problems. Blockchain technology provides limitless

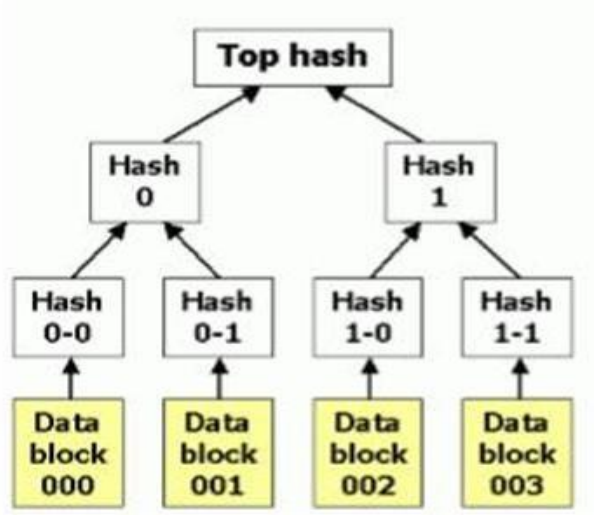
KEYWORDS:

E-voting, Smart-contracts, Blockchain, Ethereum

Introduction:

Blockchain technology that emerges as a bright spot following the
When Bitcoin [1], the first cryptocurrency, entered and became widely accepted in people's daily lives, it became a a hot topic in the field of software today[2]. Blockchain Technology comes from the underlying structural design. the first concept of the cryptocurrency Bitcoin exposed to the world of the internet and soon after became a attractive technology because of its great level of openness in The system has developed into a busy area of investigation and analysis.
for its use in a number of other fields As an illustration, in Because the wallets in Bitcoin are distributed, the total number of coins and volume of transactions in real time in the Blockchain technology that emerges as a bright spot following the When Bitcoin [1], the first cryptocurrency, entered and became widely accepted in people's daily lives, it became a a hot topic in the field of software today[2]. Blockchain Technology comes from the underlying structural designthe first concept of the cryptocurrency Bitcoin exposed to the world of the internet and soon after became a attractive technology because of its great level of openness in The system has developed into a busy area of investigation and analysis. for its use in a number of other fields As an illustration, in Because the wallets in Bitcoin are distributed, the total number of coins and volume of transactions in real time in theA blockchain's first block is referred to as the "Block 0" or "Genesis block" Usually, thegenesis block is hardcoded into the program; however, this one is unique in that it doesn't include a citation to an earlier block. ("Genesis Block") 2015) After "Block 1" has been initialized, the genesis block is produced, and once finished, it is joined to the genesis

block. Every block contains a portion of transaction data, duplicates of each transaction hashes are paired after the hashes are
hashed once more, and so on until only one hash is left; additionally called a merkle root



RELATED WORK:

A blockchain's first block is referred to as the "Block 0" or "Genesis block" Usually, the genesis block is hardcoded into the program; however, this one is unique in that it doesn't include a citation to an earlier block. ("Genesis Block") 2015) After "Block 1" has been initialized, the genesis block is produced, and once finished, it is joined to the genesis
block. Every block contains a portion of transaction data, duplicates of each
transaction hashes are paired after the hashes are hashed once more, and so on until only one hash is left; additionally called a merkle root.

Moreover, people can electronically draft suggestions and petitions. for acts and laws see the http://rahvaalgatus.ee website of the parliament. These requests are available online signed by any person who want to using their smart ID card back the plan. If a specific amount of suggestions are made,
of signatures are debated in the legislature. That is one more excellent illustration of how technology can bolster democratic principlesDespite its notable success—it had a nearly 30% penetration rate during the most recent elections—the Estonian model is not without its problems. By its very nature, the centralized solution introduces a single point of failure and leaves itself vulnerable to hackers and theft attempts.

Attacks known as Distributed Denial of Service (DDoS) have the potential to damage servers, databases, and software. In the event of an election, the administrators of such a system might act maliciously and steal or manipulate some important information. Another question is if this technology can be scaled.

PROPOSED SYSTEM:

In this section we will explain the design and functional phase of our application, The User accesses the web application where the platform is located and register's itself as well as cast its vote in a secured and transparent manner.

1. **Registration Phase**: First, the voter must register using their unique ID and other details like name, roll number, and mobile number. The database has all of this information.

2. Login: Following registration, the voter attempts to log in in order to cast a ballot. Voter first uses their password to log in during this phase. The voter must authenticate themselves in order to cast their ballot following a successful login.

To improve security, OTP verification is utilized for real-time authentication.

3. Technology calledblockchain: This technology is primarily utilized because of its security attributes. Blockchain offers a transparent and safe environment. Blockchain uses to encrypt the voter communication (cast vote)
algorithm for asymmetric encryption. A public key is given by Blockchain, and the private key is attached to host. The public key is utilized by to verify ledger.

4. Database: User database is stored in database. Details like name, gender, Unique Id are stored is database. MySQL is the proposed database to be used

5. Ethereum Network: Ethereum network provides a framework for blockchain creation

and storage. Every block is created and its details are stored in an encrypted ledger. These created blocks are distributed among nodes which provides high fault tolerance to the system.

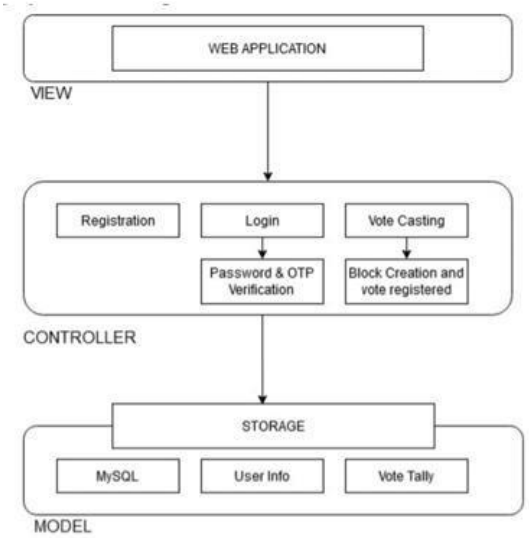
6. Result phase: The processing and tallying of votes is done in results phase. Results are generated and displayed on website. Users can verify their votes using their own public key. This provides transparency to the voting system

View: The top layer is where the user interacts with the application by typing information, pressing buttons, accessing the camera, choosing the radio button, uploading music, and so on. Depending on the needs of the application, this layer is in charge of showing the user all or some of the data. In addition, this layer serves as a conduit between the user and the application.

Controller: The application's primary functionality and business logic are housed in this middle layer. This layer processes the response as soon as the user interacts with the application. This layer includes all background functions, such as vote casting and login. This mostly consists of transmitting output to the display layer and all of the functions.

Model: Data maintenance for users is the responsibility of this layer. User data is kept in the MySQL relational database.

use the Ethereum Virtual Machine (EVM) to run smart contract code on a blockchain. In our application, smart contracts carry out logic and are in charge of reading and writing data to the blockchain. Solidity is a computer language used to write smart contracts. All of the business logic that deals with the data is stored in smart contracts, if the public ledger is the blockchain's database layer. In our application, smart contracts signify a covenant or agreement that states that user votes will be
counted, other votes will only be counted once, and the candidate with the most votes will be proclaimed the winner.



In order to cast a vote on our program, a user must have an Ethereum wallet address and some Ether cryptocurrency. They cast their ballots and pay a tiny transaction fee to get their votes written to the blockchain after logging in to the network. In our application, this transaction charge is referred to as "gas" and is associated with certain coins. The miner-node of the network receives this "gas" transaction fee after he completes the transaction. It's crucial to remember that while voting on the blockchain requires some Ether, viewing the list of candidates is free. This is because reading data from the blockchain is free, but writing to it charges.

CONCLUSION:

In this paper, we introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy By comparison to previous work, we have shown that the blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time efficient election scheme, while increasing the security measures of the todays scheme and offer new possibilities of transparency. E-voting is still a controversial topic within both political and scientific circles. Despite the existence of a few very good examples, most of which are still in use; many more attempts were either failed to provide the security and privacy features of a traditional election or have serious usability and scalability

issuesn. On the contrary, blockchain-based e-voting solutions, including the one we have implemented using the smart contracts and the Ethereum network, address (or may address with relevant modifications) almost all of the security concerns, like privacy of voters, integrity, verification and non-repudiation of votes, and transparency of counting. Yet, there are also some properties that cannot be addressed solely using the blockchain, for example authentication of voters (on the personal level, not on the account level) requires additional mechanisms to be integrated, such as use of biometric factors Blockchain technology has lot of promise, but in its current state its require lot more research and currently might not reach till its full potential. There needs a concerted effort in the core blockchain technology to improve its support for more complex applications.

REFERENCES

[1] "Bitcoin: a peer-to-peer electronic cash system," by S. Nakamoto, [Online]. Bitcoin.org/bitcoin.pdf is accessible.

[2] Gökhan Dalkılıç, Emre Yavuz, Ali Kaan Koç, and Umut Can Çabuk "Towards Secure E-Voting Using Ethereum Blockchain"

[3] Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014; G. Wood, "Ethereum: a secure decentralised generalised transaction ledger,"

[4] “Smart contract templates: foundations, design landscape and research directions”, C.D. Clack, V.A. Bakshi, and L. Braine, arXiv:1608.00771, Mar 2017.

[5] Electronic Voting in Europe-Technology, Law, Politics and Society, vol. 47, pp. 83-100, 2004; E. Maaten, "Towards remote e-voting: Estonian case."

[6] "An anonymous distributed electronic voting system using Zerocoin," Y. Takabatake, D. Kotani, and Y. Okabe, IEICE Technical Report, pp. 127–131, 2016.

[7] A proposal for initial remote user enrollment for IVR-based voice authentication systems was made by U.C. Çabuk, T. \enocak, E. Demir, and A. Çavdar in the July 2017 issue of International Journal of Advanced Research in Computer and Communication Engineering, vol. 6, pp. 118–123.