

elections are 100% transparent as desired. So, we would like to collect and check signed and time stamped knowledge of the elections. Because, no one have to be ready to change the votes once they're casted. Also, we need individuality in elections, so that nobody can vote for someone else. These issues can be solved by using the biometric authentication. In this paper we have used, Ethereum environment for our system it is blockchain platform. That is because, while Bitcoin is only intended to validate coinage transactions, Ethereum network provides comprehensive use cases, with the power of smart contracts. Many applications, that may normally require a web server, can be run through these smart contracts, without using a server. Thus, it's terribly exhausting, if not impossible, to manipulate or harm the source codes of the intended software. In the Ethereum network, all operations are in real time, and all the blocks are written in the ultimate chain in exchange for some Ethers [3].

3. IMPLEMENTATION

Our primary goal is to create functional and working model of proposed system and conduct trail elections in our institutions for various post. We would like to do it in a way that everyone can check and keep track of the election process and election process will be completely online so that everyone may attend voting easily in elections. Our primary contribution to the online elections concept is integrating them with the Ethereum blockchain platform and gives it biometric authentication. We built Ethereum smart contracts that allow checking and counting the votes when the time of the election is over. In our contract we can include any Ethereum account to the elections. By using the accounts' hash values, people's identity cannot be exposed. Biometric Authentication will further provide solution to in person or proxy voting authentication is considered a different problem.

As per Yavuz after sensible contracts are initialized, they cannot be discarded from the blockchain, and people can look back whether results of execution of smart contracts are true or not [1]. In Ethereum network, there is no need for a central authority to provide the proof-of-work. All peers will calculate the results of the contracts with none interference. These are given as prize to the miners, who execute these writing and validation operations, which are costly in terms of computation time and power. We have outlined our sensible contracts as we tend to in brief mentioned on top of. These contracts are written in Solidity artificial language, which is a combination of C++ and JavaScript. Smart contracts are executed by the peers of the Ethereum network in every 15 seconds, and they should be validated at least by 2 other users to be activated. After that, functions of contracts can be executed, and contracts can be shared with other candidates. To be able to hold fully on-line elections, we would like to resolve the subsequent issues. After an election is held, eventually, the Ethereum blockchain will hold the records of ballots and votes. Users can submit their votes via an Android device or directly from their Ethereum wallets, and these transaction requests are handled with the consensus of every single Ethereum node. This consensus creates a transparent environment for e-voting [2].

4. PROPOSED SYSTEMS ARCHITECTURE

In digital voting there are some disadvantages like security of data and potential attacks. One way to resolve these security credentials issues through the blockchain technology. In easy terms, blockchain may be an affiliation between the varied blocks. Now we will further describe below the issues and effectiveness of blockchain technology on digital voting. Our main motivation in this paper is to provide a secure voting environment and show that a reliable e-voting scheme is possible using blockchain and biometric authentication. Because, when e-voting is available for everybody who encompasses a computer, or a mobile phone, each single administrative call can be created by individuals and members; or a minimum of people's opinion will be more public and more accessible by democracy.

5. SYSTEM MODEL

We are creating system which is going to be used by many types of users for example people abroad and people who don't know to operate e-voting. Usually the remote voting operation can be done via mobile devices or personal computers. Thanks to blockchain voting system it will be possible to guarantee the continuity with the old simple voting process where illiterate can also vote. People can vote in a traditional way reaching an e-voting polling station. The voting operation consists in two steps first biometric authentication and marking right candidate or

ballot on display screen. Biometric authentication is useful and which can avoid proxy voting or can authenticate the right voter [4].

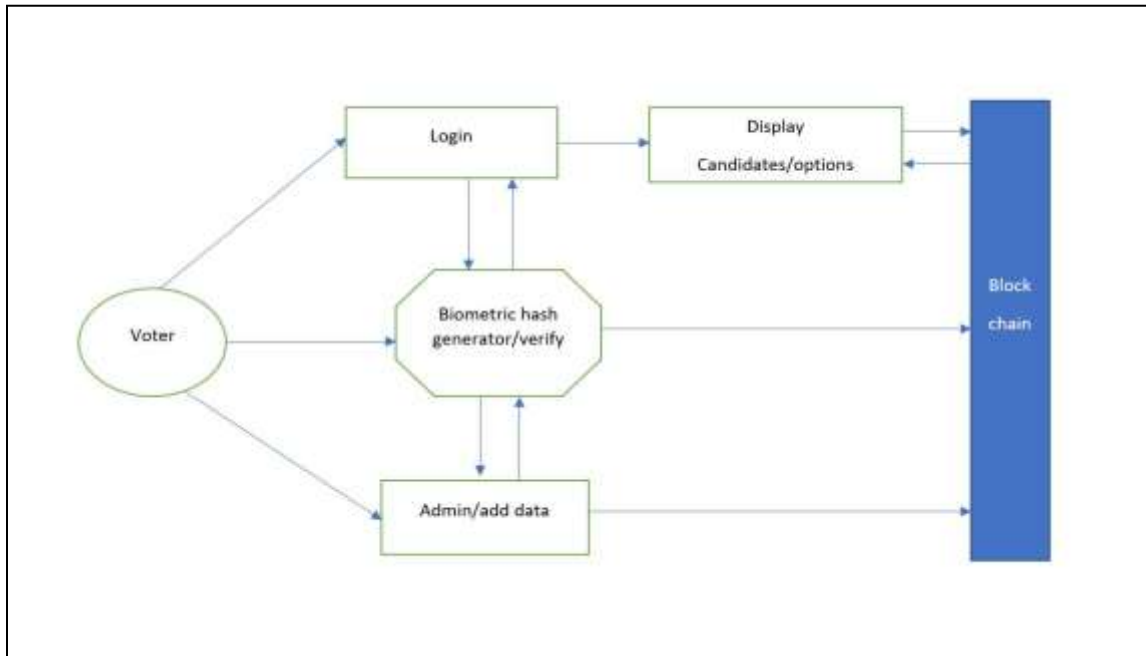


Fig -1 System Architecture

Candidate Registration: -

The candidates or opinions on which we are contesting poll are registered on the blockchain by writing smart contract on a main Blockchain. The candidates and their data should be verified and certified. The administrator can verify and arrange the poll for given data.

Voter Registration: - The Voters are registered before voting basically we are going to provide polling solutions to different organizations. We can add the voter and store there biometric hash on blockchain which will provide robust security to the data. The main goal is to keep data safe from violation as biometric data posse's great risk of data theft.

Administrator: -

The administrator will arrange the election. Administrator will collect and store candidate data on blockchain any one on the application who wish to create poll can become admin and operate the separate process on the system. We can create simultaneously many numbers of polls at same time which increases its efficiency.

Biometric Authentication:-

Authentication and security are the crucial part of the system to solve this problem we are using biometric authentication. Biometric means fingerprint, facial and iris which are unique for everyone and cannot be changed. For authentication we will store the hash of biometrics on blockchain which will add additional layer of security to the data. We are using two way combine authentication one otp and other face or fingerprint biometric [4].

Face biometric authentication: -

Face biometric is very useful in avoiding proxy voting in public voting system if someone tries to give vote on behalf of other it is not possible because of face recognition system. It helps for illiterate and old age people who don't have proper finger biometric and don't know to operate e-system, face id will automatically verify the person presence with camera and with simple button press they can vote. In today's mobile world everyone has mini camera in their pocket known as selfie camera which will help to ensure efficient transparent voting process if carried for larger and corporate and private voting or remote voting elections.

Finger biometric authentication:-

Fingerprint biometric authentication is the most secured authentication system we are using this as second authentication system if first fails or the system requires fingerprint authentication for more security.

Biometric Hash Generation: -

To store the biometric data we need very safe storage and robust structure. To store biometric data we will first generate hash of biometric data and then store it on blockchain for authentication.

Tools:-**Metamask : -**

MetaMask was created to increase the accessibility of the Ethereum blockchain to the average user. A plug-in for chrome, MetaMask acts as an Ethereum browser, allowing users to manage their Ethereum wallet and interact with decentralized applications and smart contracts without running a full node. Through MetaMask, users are able to manage multiple accounts and easily switch between different networks. In order to allow users the flexibility of using the Ethereum blockchain without running a full node, MetaMask relies on trusted nodes to broadcast the transactions of MetaMask users in order to be mined. Since transactions are signed using the sender's private key, which is stored locally on the user's machine, MetaMask cannot impersonate the user and send transactions on the user's behalf. Acting as an intermediary between Chrome and the Ethereum blockchain, MetaMask allows users the convenience and security of the blockchain within a popular browser.

Truffle: - Truffle may be a well-liked testing development framework for Ethereum. It includes a development blockchain, compilation and migration scripts to deploy your contract to the Blockchain, contract testing, and so on. It makes development easier! Truffle Contracts is an abstraction on high of the Web3 Javascript API, permitting you to simply connect and act together with your smart Contract.

6. CONCLUSIONS

For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on blockchain technology. The proposed scheme solves the fairness, eligibility, uniqueness, efficiency security and privacy issues, of the basic voting system and is very suitable for implementation on the internet. E-voting will be more transparent, and autonomously auditable, a good solution based on blockchain technology. This scheme is more suitable for meeting the voting demands in future.

7. REFERENCES

- [1]. E. Yavuz," Towards Secure E-Voting Using Ethereum Blockchain", IEEE paper, 2018
- [2]. S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", [Online]. Available: <https://bitcoin.org/bitcoin.pdf>.
- [3]. G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.
- [4]G. Kaur, Dheerendra Singh, Simran Jeet Kaur, "Electrocardiogram (ECG) as a Biometric Characteristic: A Review", International Journal of Emerging Research in Management &Technology, vol. 4, no. 5, May 2015, ISSN 2278-9359.