Decentralized E-voting system based on Smart Contract by using Blockchain Technology

1st Ali Mansour Al-madani
Ph.D. Research Scholar, Department of Computer Science
Dr. Babasaheb Ambedkar Marathwada University
Aurangabad, India
ali.m.almadani1992@gmail.com

2nd Dr.Ashok T. Gaikwad
Institute of Management Studies and Information Technology
Aurangabad, India
drashokgaikwad@gmail.com

3rd Vivek Mahale
Assistant professor
Institute of Management Studies and Information Technology
Aurangabad, India
mahalevh@gmail.com

4th Zeyad A.T.Ahmed
Ph.D. Research Scholar, Department of Computer Science
Dr. Babasaheb Ambedkar Marathwada University
Aurangabad, India
zeyad.ahmed2019@yahoo.com

***Abstract*— Nowadays the use of the Internet is growing; E-voting system has been used by different countries because it reduces the cost and the time which used to consumed by using traditional voting. When the voter wants to access the E-voting system through the web application, there are requirements such as a web browser and a server. The voter uses the web browser to reach to a centralized database. The use of a centralized database for the voting system has some security issues such as Data modification through the third party in the network due to the use of the central database system as well as the result of the voting is not shown in real-time. However, this paper aims to provide an E-voting system with high security by using blockchain. Blockchain provides a decentralized model that makes the network Reliable, safe, flexible, and able to support real-time services.**

Keywords*— Blockchain, Ethereum, smart contract, E-voting, MetaMask, Ganache, Truffle framework.

I. INTRODUCTION

E-casting a ballot is broadly utilized in the public eye life, yet, it isn't evident how to guarantee the result is regarded when the choice is monetarily or politically related. Secure e-casting a ballot is a sort of secure multi-party calculation. In the voting process, a set of people are free to make their choices. The casting a ballot could be transparently and im-partially and keep secretly. Wherefore, the blockchain solves those problems which the centralized application is facing, that's why blockchain is a better choice for building a voting application. In the blockchain, all the data does not allocate on a central server, but the data allocated via decentralized called a distributed database. The data distributed across each device connected to the blockchain using a peer-to-peer network of nodes which talk to one another. Suppose your device is connected to the blockchain, your device is called a node. This node able to talk to all the other nodes and you will share some of the same responsibilities. In the decentralized database system, every node in the system ought to have a copy of the considerable number of data that is shared over the Blockchain, every one of these data are contained in bundles of records called blocks which are connected together to make the ledger. The ledger used as records of data for sure the data unchanged, this is important for the voting application, which means the voter always knows that his account sent the transaction whenever he votes and that vote goes to the correct candidate, and be recorded forever. All the data is shared across devices on the blockchain. The Blockchain on a very basic level is a database and in light of the fact that the entirety of the nodes connected with each other on the Blockchain it's become a network. So that we used blockchain rather than the conventional web model. In this paper, the researchers applying voting application using a blockchain to ensure election results and away from electronic fraud.

II. RELATED WORKS

This paper presents in this area different arrangements that endeavor to incorporate E-casting a ballot and Blockchain to empower the decentralization of casting a ballot administra- tions. The most significant of them are going to be reported here.Maintaining the Integrity of the Specifications.

All the noteworthy data like results and votes stored on a blockchain. There was no authority access to the data or the information to change it from any node or ledger [1].

Y. Zhang, et al., [2] developed an electronic voting system based on the smart contract, they made blind signature and homomorphic encryption to ensure the privacy of voters.

W. Zhang et al., [3] proposed a receipt-free peer-to-peer voting protocol and privacy preservation that can help facilitate voting for peers on the blockchain network. No reliable third parties are required to identify voters or count the votes.

III. BLOCKCHAIN TECHNOLOGY

The web application architecture is consists of three tires such as browser, server and application. The request sent to the webserver from the user by using a web browser and the central server response by fetching the data from the centralized database to the web Brower. So when the user

needs any data he should request from the centralized databases shown in Fig.1 that the drawback of using a traditional web application and that technique is not suitable for the voting application.

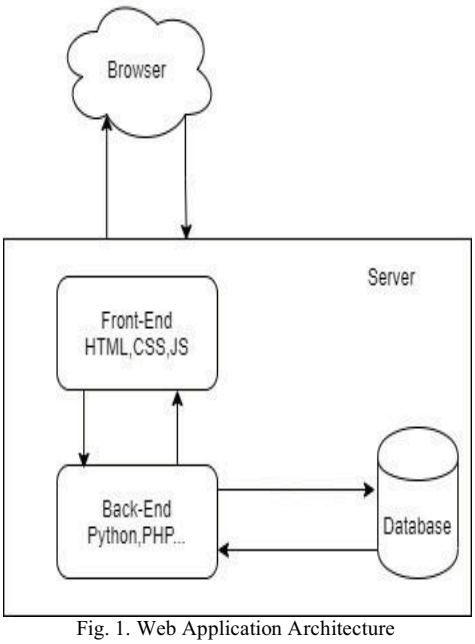

Fig. 1. Web Application Architecture

In the traditional web application one of those cases may be happened in the centralized databases:

A. *Data modification through the third party in the network due to the use of the central database system.*

B. *The rules in the election could change and show fake result.*

In this paper the researcher proposed an E-voting application with a decentralized database using Blockchain to avoid the drawback of the traditional web application. The purpose of developing E-voting application is to ensure that the vote is counted, all the votes are only kind of once, and the correct candidates with most votes are actually going to win the election. To achieve this purpose the application needs blockchain which provides the decentralized voting application.

IV. PROCESS OF E-VOTING

E-voting application based on Blockchain is decentralized, and all data does not allocate on a central server. The voter and candidate registration process must be done in advance. Identity must be verified before creating accounts. After verifying Identity, the authorized person must authenticate eligible users by verifying a coin or token [11]. Blockchain will ensure the verification process will not be allowed double coin or token. The user cannot vote more than one vote.

V. IMPLEMENTATION

The implement of the E-voting application based on the blockchain. The data stored on Ethereum blockchain decentralized and secured, the code on the blockchain is shared and unchangeable. Ethereum Blockchain allows us to write a code that can be deployed to blockchain, and nodes on the network will execute this code. In this application, the

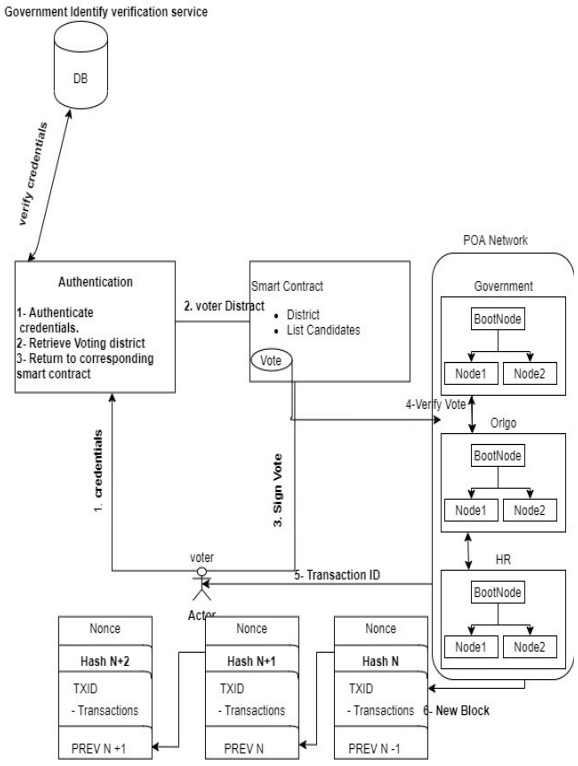

Fig. 2. Process of E-voting

code writes to the decentralized application, by using smart contract protocol in ethereum blockchain. The Ethereum allows to write a code and executes it on Ethereum virtual machine smart contracts as shown in fig.3.

This is where all the business logic, and E-voting application is placed. All the codes also could be written here. Ethereum virtual machine smart contracts provide the writing of code and change of reading and writing. Data is transfer in value and executing any business logic that the program a smart contract is a kind of like a microservice that placed on the web.

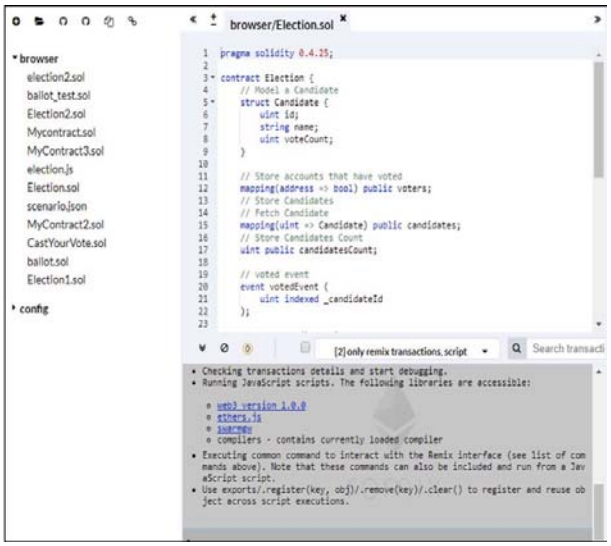

Fig. 3. Ethereum blockchain

In order to build Decentralized application (DAP) there are requirements such as node package manager, truffle frame- work, Ganache and MetaMask , Details of each one are as follows:-

A. node package manager

The node package manager (NPM). All those comes bundled with nodejs Command Prompt.

Fig. 4. Node.js Command Prompt

B. Truffle Framework

Truffle structure (framework), which empowers the making of a decentralized application on the blockchain by using the Ethereum network.

Truffle offers a set-up of instruments, which encourage programming to compose Smart_Contracts with the Solidity programming language. It additionally gives a structure to testing Smart_Contracts and gives the tools required to make transaction (Deploy) Smart_contract in the blockchain network Technology. The install of truffle by typing ”npm install –g truffle” in the terminal.

Fig. 5. Truffle Framework

C. Ganache

Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development [12]. In this application Ganache used as local storage for development e-voting decentralized.

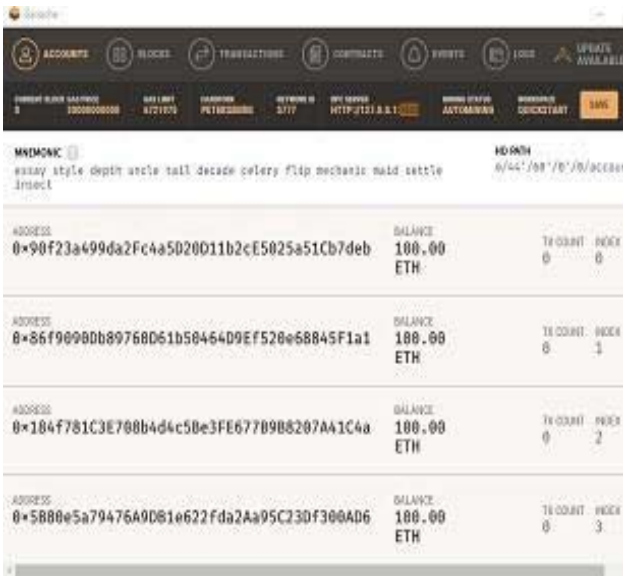

Fig. 6. Ganache

D. MetaMask

MetaMask is a google chrome extension. It is used to connected to Ethereum blockchain. The fig.7 shown MetaMask after the installed.

Now MetaMask connects to the local Ethereum network which is used for this application with the personal account and the ability to interact with smart contract application which has been created before this step.

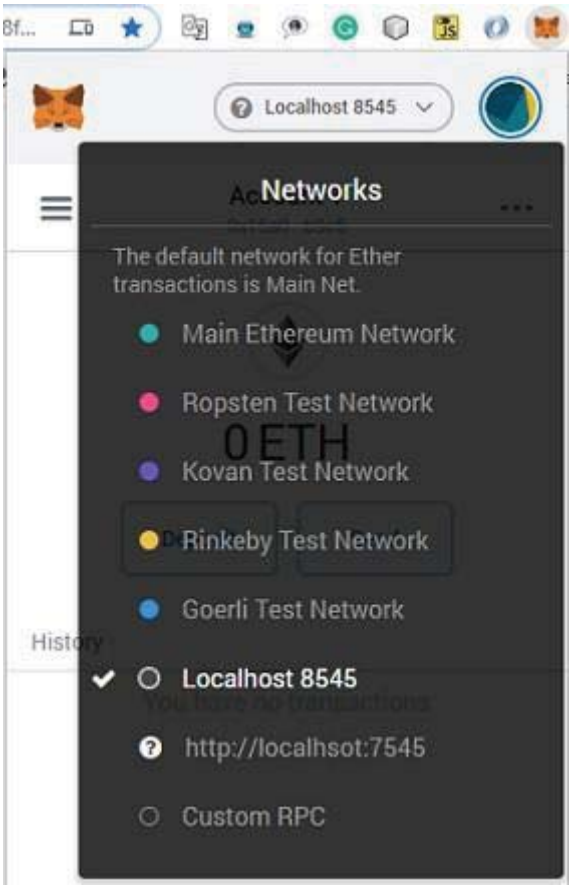

Fig. 7. MetaMask

VI. BUILD INTERACTING WITH SMART CONTRACT

Built interact with a smart contract this is the election result page where in a table of candidates, and each candidate has an ID, and a name. Each candidate will have a vote count. The voter is able to see the account that he logged in such as following_address:

(0x6a12129ebecaaab7650b77cdae2912dc3842c17e) it is an account used to connect to the blockchain. The form supports the dropbox to select which candidate the voter wants to vote for him.

A. Implementation in Ethereum

Fig. 8. Election voting with results

The interaction with the smart contract in this application has been done, and the result page of the election is shown in Fig.8. There is a table of candidates, each candidate has an ID, a name, and each candidate will have a vote count. This is the account that is used to login as a test in this application (0x6a12129ebecaaab7650b77cdae2912dc3842c17e). The user interface of the application supports the Dropbox field to select the candidate whom the voter wants to vote for him.

A smart contacts are written in the language called solidity which looks a lot like JavaScript and we will be using solidity to write smart contracts in this system.

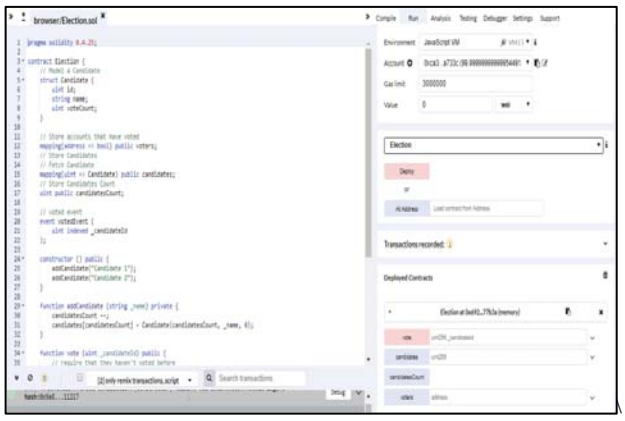

Fig. 9. Remix. Ethereum.

The idea is a clarification of what is adapting well. Adapt is a decentralized application and it's decentralized. In every way the network is decentralized. Because it's a peer to peer the data is decentralized. Because it's shared across devices in the network and the code is decentralized, it's also shared and executed across devices into the network.

B. Implementation in Ethereum by using Front-End in local Network

The application of a client-side is written in JavaScript, HTML, and CSS. Rather than interfacing this to a back-end web server, it connects with a blockchain that installs and composes the entirety of the code to this decentralized application with a Smart_Contract. After the compile of the Smart_Contract make a transaction (deploys) it to Ethereum blockchain of this application, it permits the voters to make accounts in the system to utilize the application and vote in the Election_System.

Now the platform of the voting application is ready for use with the support the feature of showing the result of the election in real-time. The voter realized that his vote goes to his right candidate as well as the application secured based on the blockchain. The voter has only one vote because the application does not allow for the duplicate vote.

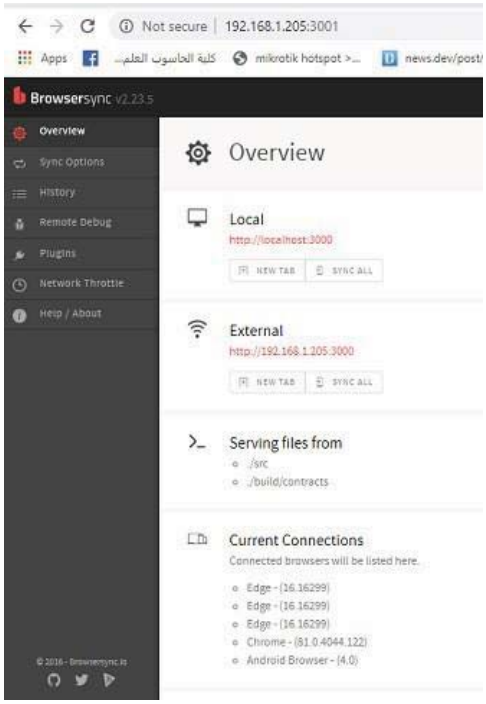

Fig. 10. Current connections.

VII. CONCLUSION

This paper introduces Ethereum's Blockchain based electronic voting system. This paper introduces Ethereum's Blockchain based electronic voting system. This application is able to overcome the limitations and security issues of the centralized voting system by using Blockchain technology. This study proofed how a blockchain works to secure the data.. The researchers developed voting application in a decentralized method with a smart contract. Then deployed a

smart contract to local blockchain for this application. The application based on Ethereum Blockchain technology as a network and a decentralized database all in one for storing voter's accounts, votes, and candidates details. Blockchain provides a decentralized model that makes the network reliable, safe, flexible and able to support real-time services. the voter realizes his vote goes to his right candidate as well as he has only one vote because the application does not allow for the duplicate vote by this method electronic voting could be highly reliable.

Fig. 11. Voting one time.

REFERENCES

[1] "South Korea Uses Blockchain Technology for Elections," KryptoMoney, https://kryptomoney.com/south-korea-usesblockchain-technology-for-elections, 2017.

[2] Y. Zhang, Y. Li, L. Fang, P. Chen, and X. Dong, "Privacy-protected Electronic Voting System Based on Blockchin and Trusted Execution Environment," 2020, doi: 10.1109/iccc47050.2019.9064387.

[3] W. Zhang et al., "A Privacy-Preserving Voting Protocol on Blockchain," in IEEE International Conference on Cloud Computing, CLOUD, 2018, doi: 10.1109/CLOUD.2018.00057.

[4] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson, "Blockchain-Based E-Voting System," IEEE Int. Conf. Cloud Comput. CLOUD, vol. 2018-July, pp. 983–986, 2018, doi: 10.1109/CLOUD.2018.00151.

[5] R. A. Canessane, N. Srinivasan, A. Beuria, A. Singh, and B. M. Kumar, "Decentralised Applications Using Ethereum Blockchain," 5th Int. Conf. Sci. Technol. Eng. Math. ICONSTEM 2019, pp. 75–79, Mar. 2019, doi: 10.1109/ICONSTEM.2019.8918887.

[6] M. Erdenebileg, "e -Voting Anwendung auf Ethereum Plattform als Smart Contract," Fachhochschule Campus Wien, 2019.

[7] M. Tawfik, A. Almadani, and A. A. Alharbi, "A Review: the Risks And weakness Security on the IoT," SSRN Electron. J., 2020, doi: 10.2139/ssrn.3558835.

[8] Truffle : https://truffleframework.com

[9] Ethereum project: https://ethereum.org

[10] Ganache: https://truffleframework.com/ganache

[11] D. Khader, B. Smyth, P. Y. Ryan, and F. Hao, "A fair and robust voting system by broadcast", in 5th International Conference on Electronic Voting, Vol. 205, pp 285-299, 2012.

[12] https://www.trufflesuite.com/docs/ganache/overview

[13] A. M. Al-madani and A. T. Gaikwad, "IoT Data Security Via Blockchain Technology and Service-Centric Networking," 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2020, pp. 17-21, doi: 10.1109/ICICT48043.2020.9112521.