



Block Chain based e-Voting System using Design Thinking Approach

A. Aruna¹, P. Madhan², M. Narendranath³, S. Karthik⁴

Assistant Professor, Department of Information Technology, SNS College of Technology, Coimbatore, TamilNadu¹

UG Scholar, Department of Information Technology, SNS College of Technology, Coimbatore, TamilNadu²

UG scholar, Department of Information Technology, SNS College of Technology, Coimbatore, TamilNadu³

UG Scholar, Department of Information Technology, SNS College of Technology, Coimbatore, TamilNadu⁴

Abstract: Building an online voting system that satisfies the legal requirements of legislators has been a challenging task for a long time. The exciting technology with respect to the same is the Distributed Ledger technologies. Block chain is one such technology that offers an infinite range of applications. In this paper, block chain technology is used as a service to implement distributed online voting system by identifying the legal and technological limitations of using block chain as a service. A novel online voting system has been proposed that addresses all the limitations discovered. The paper evaluates the potential of distributed ledger technologies such as the process of election and implementing a block chain-based application. As a result, the security is improved and the cost of hosting a nation-wide election is drastically reduced.

Keywords: Block chain, Distributed Ledger

I. INTRODUCTION

A block chain-based electoral system through a web site, optimizing for the necessities and concerns known. Every vote is kept as dealing on the block chain whereas every citizen receives the dealings ID for his or her vote for validating functions. By exploitation this technique, one can eliminate the wastage of our time and that we can save time. It can't be manipulated or modification the vote that we tend to solid, it's changeless and it is additionally safer. It eliminates the necessity to print ballot papers or open polling stations wherever voters will vote from where there's an online affiliation.

Despite these advantages, on-line balloting solutions are viewed with an excellent deal of caution as a result of they introduce new threats. The main goal of this analysis was to look at this standing of block chain primarily based balloting analysis and on-line balloting systems and any connected difficulties to predict future development.

II. LITERATURE SURVEY

A lot of practices are made to introduce the variations in electronic and online voting systems where different techniques and methodologies are used. Some of them guarantee the confidentiality and security of the system to some extent, still the voting information and process need to be controlled and managed with advanced systems that will ensure and guarantee the security and privacy of voters and voter's information.

A. Basic E-voting approach/architecture

The systems that are developed to forged the vote by means that of a digital approach victimization on-line portals and electronic devices use numerous encoding and decipherment techniques to ensure the secure information dealing.

B. Homomorphic Encryption Technique

Homomorphic encoding may be a well-known powerful technique with several helpful applications. Recently, it's been applied the look of on-line electoral system. The electoral system supported this encoding uses the exponential ElGamal cryptosystem. Before submission, the contents of every forged ballot are encrypted victimization the exponential ElGamal encoding. The additive homomorphism property of this crypto system makes it doable to tally encrypted ballots directly while not decrypting them.



C. Centralized Architecture:

Various techniques are used to convert the information in coded format to forestall manipulation whereas transferring to the network. One downside is mentioned here that when the right information is hold on within the information trust and security is needed at substantial level. Centralized storage is inconvenient if the information is prestigious as a result of unauthorized access and attack by hackers can challenge the system in terms of responsibility.

Previous models and designs ar used with the assistance of a centralized architecture approach. that will cause moral and security issues. Assembling the information at a centralized location takes the information in danger. It is controlled below the belt. So, a good framework overcomes this drawback of storing info to the distributed format with the assistance of block chain. Block chain may be a distributed ledger that stores all processed transactions in written account order.

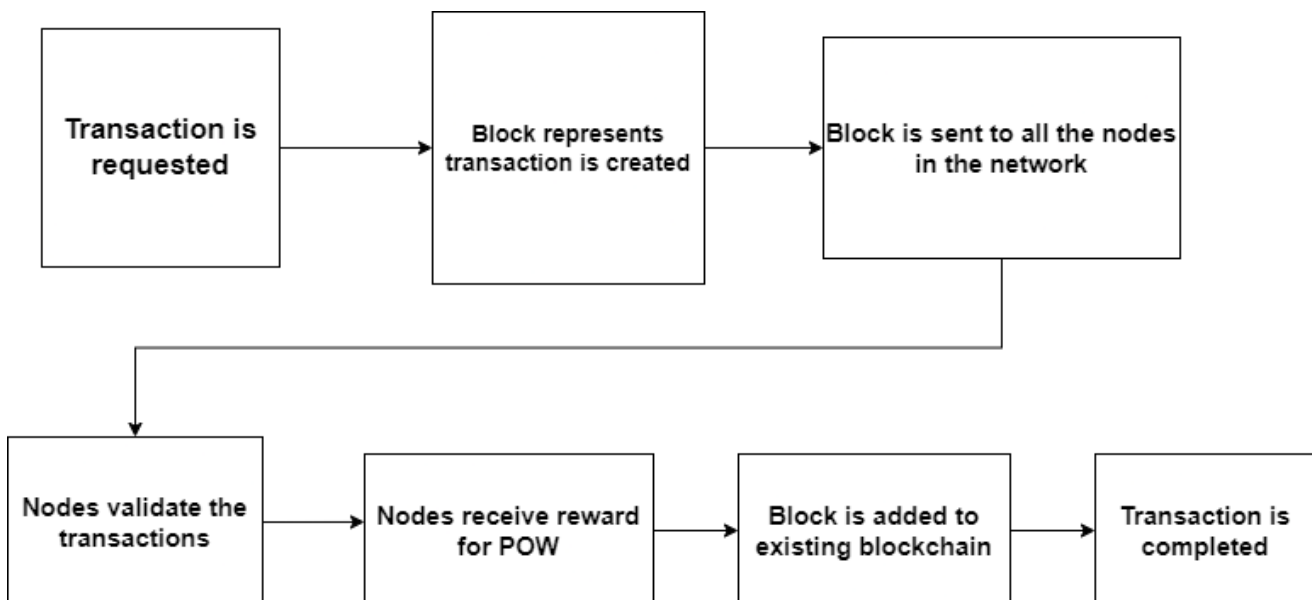
Traditional databases ar maintained by one organization, which organization has complete management of the information, together with the power to govern the hold on information, to censor otherwise valid changes to the information, or to feature information fraudulently. for many use cases, this is often not a retardant since the organization that maintains the information will therefore for its own profit, and thus has no motive to falsify the database's contents; but there are alternative use cases, like a money network, wherever the information being hold on is simply too sensitive and therefore the motive {to manipulate to management to govern} it's too engaging to permit any single organization to possess total control over the information. It can be warranted that the accountable organization would ne'er enact a dishonest amendment to the information there's still the likelihood that a hacker might break in and manipulate the information to their own ends.

III. TECHNOLOGICAL INFLUENCE

A. BLOCKCHAIN TECHNOLOGY

Block chain technology is a structure that stores transactional records in the form of blocks in several databases known as chain. These are stored in the network that is connected through peer – to – peer nodes. This kind of storage is typically referred to as a Digital Ledger.

Digital signature obtained from the owner is used to authorize each and every transaction. This prevents the tampering of transactions in the digital ledger as the information present is highly secure. The digital ledger is similar to a Google spreadsheet where the transactional records are stored with respect to the actual purchases where everyone can view the data but unable to corrupt it.





B. GANACHE

Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development that is used to develop, deploy and test the application developed in a safe and deterministic environment. With Ganache, it is possible to run our own local block chain. With Ganache, the application can be deployed and tested in a deterministic and safe environment.

C. METAMASK

MetaMask is a wallet that established interaction with Ethereum Blockchain. The wallet can be accessed through browser extension or using a mobile app. This in turn is used to interact with decentralized applications.

D. SOLIDITY

The highly prevalent block chain programming language being the Solidity helps in solving most of the problems faced by Block chain developers. It is a distributed computing platform that runs on the Ethereum Virtual Machine (EVM).

IV. PROPOSED WORK

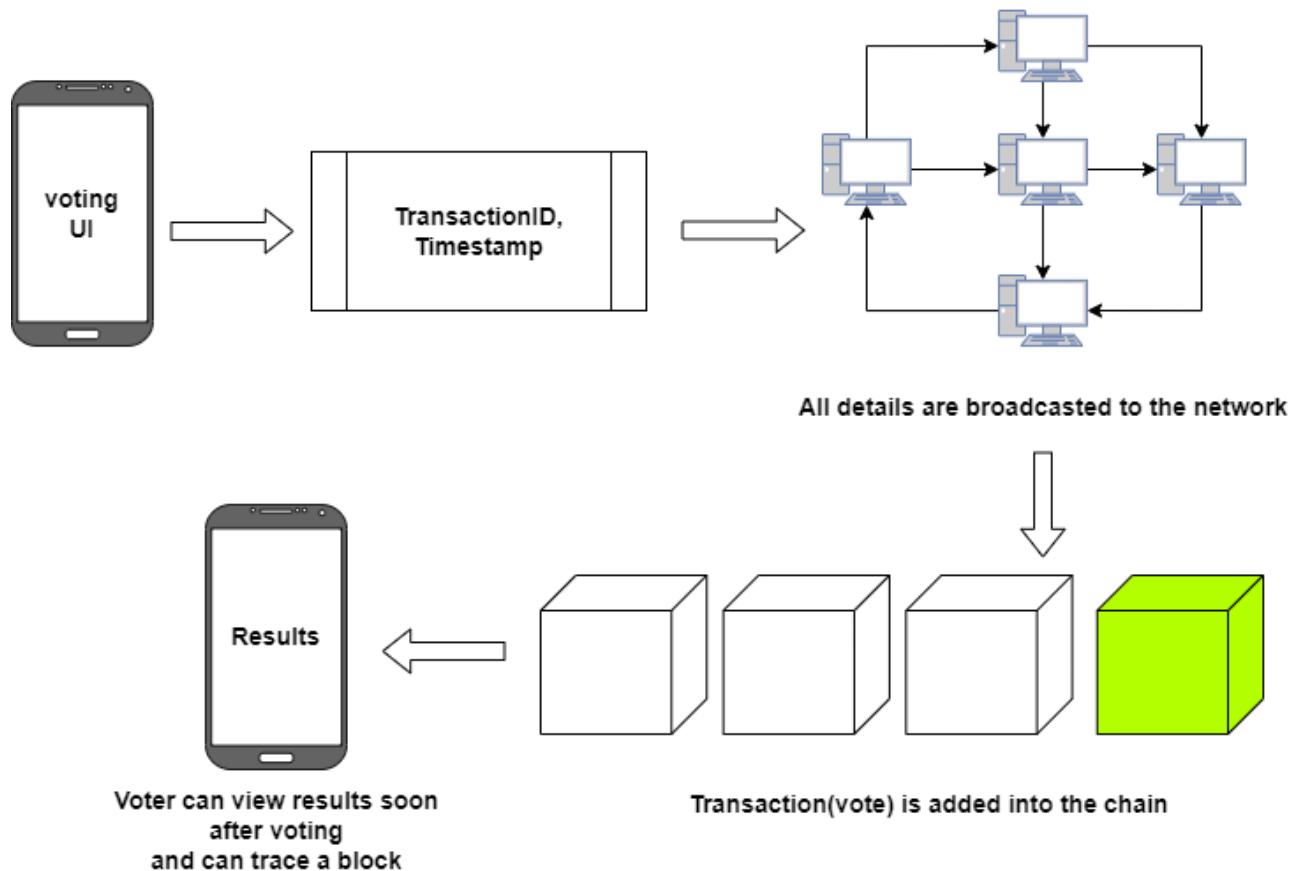


Fig. 1 Workflow diagram

The following figure shows the Login page of the e-Voting system project developed.

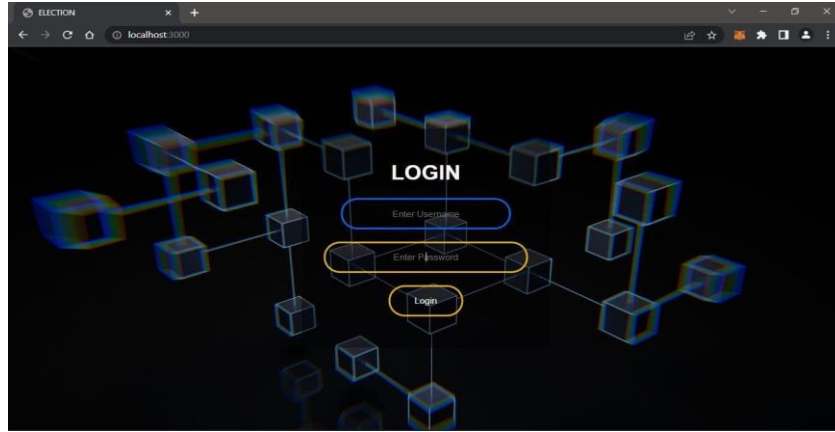


Fig.2 Login Page

The following figure displays the voting page where the individual can cast their vote.

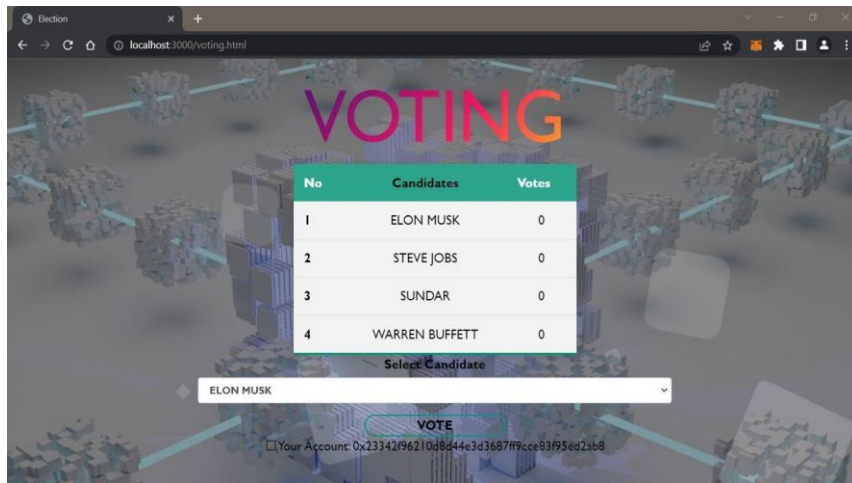


Fig. 3 voting page

The following image displays the process of voting like account details of the contestant, number of votes casted and the like.

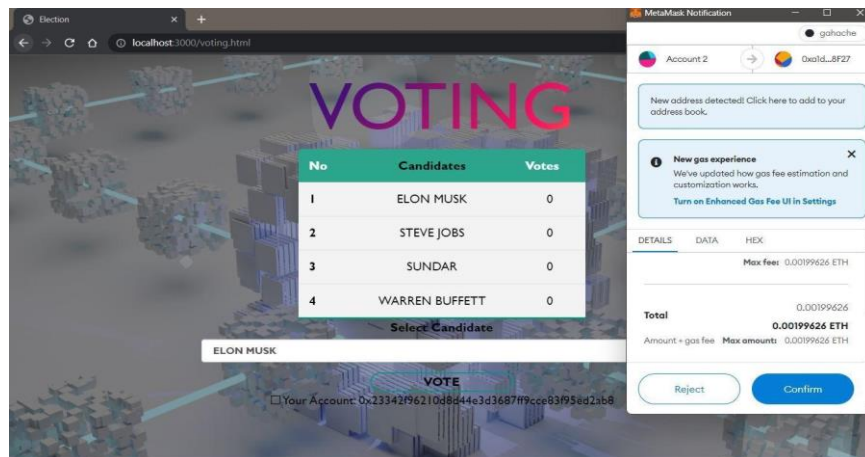


Fig. 4 voting process



The following figure displays the output showing the number of votes casted for each contestant.

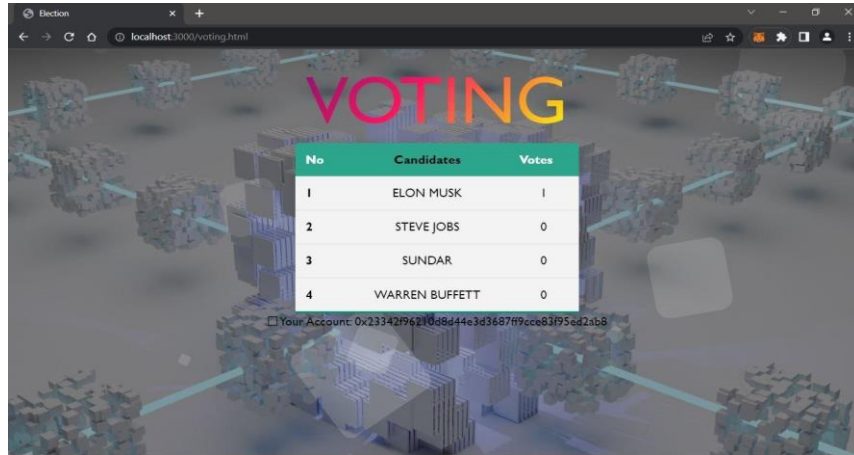


Fig. 4 Results page

V. CONCLUSION AND FUTURE WORK

A. CONCLUSION

The technology is improving Day by day in our day to day life but in some fields it still remains some. Thus the voting process is in a EVM method due to this method we need to spend a time and need to reach a place to vote. So it is best to vote in online in other hands it also has a disadvantage of hacking and fraud, so that we used a block chain technology it is immutable and cannot be manipulate or do any fraud and the transaction is transparent

B. FUTURE WORKS

- Creating a Voting portal by a user will be added
- UIDAI authentication will be used for more security
- Need to add chat box that interact with user
- UI and UX will be added for better user experience
- Auto successfully voted message will be send to the user mail

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. 335{348.
- [2]. Adida B. and Rivest, R. L. (2006). Scratch & 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.
- [3]. 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
- [4]. Workshop/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 using a trusted random number generator, in Proceedings of the 1st International Conference on E-voting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.
- [6]. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A., and Vora, P. (2008) Scantegrity: End-to-end voter-verifiable optical-scan voting, IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.
- [7]. R Sabitha, A Aruna, S Karthik, J Shanthini (2021), Enhanced model for fake image detection (EMFID) using convolutional neural networks with histogram and wavelet based feature extractions, Pattern Recognition Letters 152, 195-201.