E Voting System using Blockchain

Dr. M Sandhya Rani*[1], S Meghana[2], Vennapusa Bhavitha Reddy[3]

[1]Associate Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

[2,3]Student, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

ABSTRACT

Increasing digital technology has revolutionized the life of people. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline). General elections still use a centralized system, where in one organization manages it. Some of the problems that can occur in traditional electoral systems is with the organization that has full control over the database and system. It is possible to tamper with the database of considerable opportunities. Block chain technology is one of solutions; because it embraces a decentralized system and the entire database are owned by many users. Block chain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using block chain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, this will be a method based on a predetermined turn on the system for each node in the built of block chain.

Keywords: Security and Protection, Hardware, Online Information Services

I. INTRODUCTION

Lately, electronic voting systems have begun being used in many countries. Estonia was the first in the world to adopt an electronic voting system for its national elections [1]. Soon after, electronic voting was adopted by Switzerland for its state-wide elections [2], and by Norway for its council election [3]. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An e-Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on Tor to hide the identity of voters [4]. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control

different parts of the Internet which can allow them to identify or intercept votes.

II. LITERATURE SURVEY

Increasingly digital technology in the present helped many people lives. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from still widespread election with the conventional system (offline).Block chain technology is one of solutions, because it embracesa decentralized system and the entire database are owned by many users.[1]Bit coin introduces a revolutionary decentralized consensus mechanism. However, Bit coin-derived consensus mechanisms applied to public block chain are inadequate for the deployment scenarios of budding consortium block chain. We propose a new consensus algorithm, Proof of Vote (POV).The former guarantees the separation of voting right and executive right, which enhance the independence of bulter's role, so does the internal control system within the consortium. As for the latter, under the circumstance that at least Nc/2+1 commissioners are working effectively, our analysis shows that POV can guarantee the security, transaction? [2] There is no doubt that the revolutionary concept of the blockchain, which is the underlying technology behind the famous crypto currency Bitcoin and its successors, is triggering the start of a new era in the Internet and the online services. In this work, we have implemented and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language.[3]Block chain was first introduced by Satoshi Nakamoto (a pseudonym) , who proposed a peer to-peer payment system that allows cash transactions through the Internet without relying on trust or the need for a financial institution. Block chain is secure by design, and an example of a system with a high byzantine

failure tolerance.[4].Proof of stake protocol of block verification does not rely on excessive computations. It has been implemented for Ethereum and certain altcoins. Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proofof-stake protocols split stake blocks proportionally to the current wealth of miners. The idea behind Proof of Stake is that it may be more difficult for miners to acquire sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment.[5]

III. PROPOSED SYSTEM

The block chain technology used mostly works the same as the block chain technology contained in the E-voting system and focuses on database recording. The nodes involved in Block chain that have been used by Bitcoin are independently random and not counted. However, in this e-voting system a block chain permission is used, for nodes to be made the opposite of the Bitcoin system and the Node in question is a place of general election because the place of elections must be registered before the commencement of implementation, it must be clear the amount and the identity. This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process. This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once valid, then the database added with the data in the block. After the database update, the node will check

whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in block chain creation to avoid collision and ensure that all nodes into block chain. The submitted block contains the id node, the next id node as used as the token, timestamp, voting result, hash of the previous node, and the digital signature of the node.

Modules:

User

Block chain
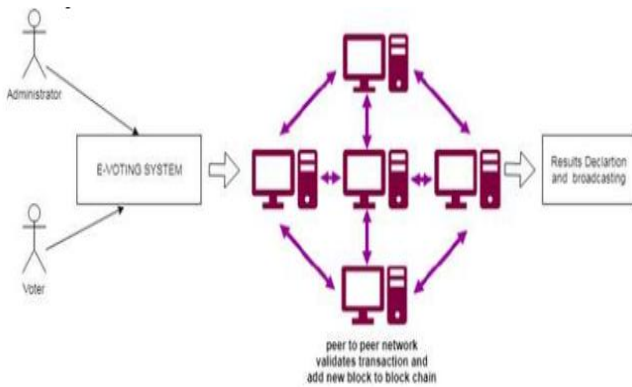
Visual Cryptography

Admin

Fig 1: System Architecture

Our e-Voting solution will include four main requirements that can be illustrated as shown below:

* Authentication: Only people already registered to vote can cast a vote. Our system will not support a registration process. Registration usually requires verification of certain information and documents to comply with current laws, which could not be done online in a secure manner. Therefore, the system should be able to verify voters' identities against a previously verified database, and then let them vote only once.

* Anonymity: The e-Voting system should not allow any links between voters' identities and ballots. The voter has to remain anonymous during and after the election.

* Accuracy: Votes must be accurate; every vote should be counted, and can't be changed, duplicated or removed.

* Verifiability: The system should be verifiable to make sure all votes are counted correctly. Beside the main requirement, our solution supports mobility, flexibility, and efficiency. However, we will limit this paper's discussion to the four main requirements.

IV. RESULTS AND DISCUSSION

Admin will create a voting instance by launching/deploying the system in a blockchain network (EVM), then create an election instance and start the election with the details of the election filled in (including candidates for voters to vote).Then the likely voters connect to the same blockchain network register to become a voter. Once the users successfully register, their respective details are sent/displayed in the admins' panel (i.e. verification page).The admin then will check if the registration information (blockchain account address, name, and phone number) is valid and matches with his record. If yes, then the admin approves the registered user making them eligible to take part and cast their respective vote in the election. The registered user (voter) following the approval from the admin casts their vote to the candidate of interest (from the voting page).After some time, depending on the scale of the election the admin ends the election. As that happens the voting is closed and the results are displayed announcing the winner at the top of the results page.

Here is the outline of the working process of our project in the form of architecture. We are also going to attach the screenshots of the working website to make it clear for the viewers of this paper.
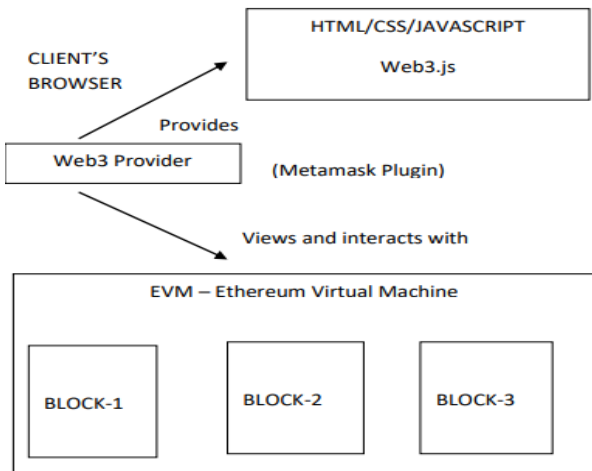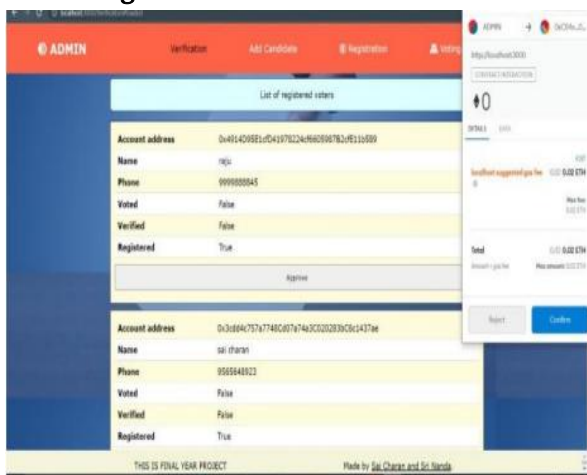
Fig 2. ACTUAL ARCHITECTURE

Fig 3 (Admin's view of the platform)

Fig 4 (Voter's view of the platform)

Fig 5 (Admin commencing election)
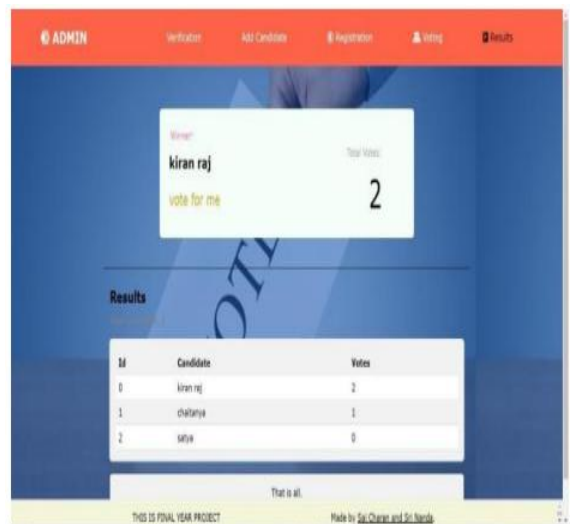

Fig 6 (End of election and results displayed)
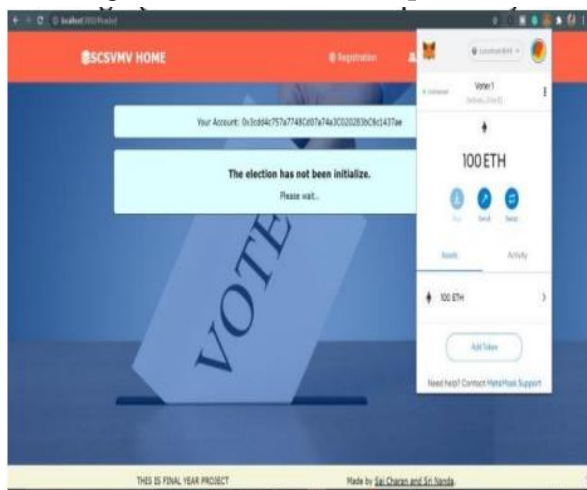
V. CONCLUSION

We have proposed an electronic voting system based on the Blockchain technology. The system is decentralized and does not rely on trust. Any registered voter will have the ability to vote using any device connected to the Internet. The Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it. We as well illustrated the limitations with our system, which will be addressed in future research papers.

VI. REFERENCES

[1]. Madise, U. Madise and T. Martens, "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world.",Electronic voting, 2nd International Workshop, Bregenz, Austria,(2006) August 2-4.

[2]. J. Gerlach and U. Grasser, "Three Case Studies from Switzerland: E-voting", Berkman Center Research Publication, (2009).

[3]. I. S. G. Stenerud and C. Bull, "When reality comes knocking Norwegian experiences with verifiable electronic voting", Electronic Voting. Vol. 205. (2012), pp. 21-33.

[4]. C. Meter and A. Schneider and M. Mauve, "Tor is not enough: Coercion in Remote Electronic Voting Systems. arXiv preprint. (2017).

[5]. D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communication of the ACM. Vol. 24(2). (1981), pp. 84-90.

[6]. T. ElGamal, "A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Info. Theory. Vol. 31. (1985), pp. 469-472.

[7]. S. Ibrahim and M. Kamat and M. Salleh and S. R. A. Aziz, "Secure E-Voting with Blind Signature", Proceeding of the 4th National Conference of Communication Technology, Johor, Malaysia, (2003) January 14-15.

[8]. J. Jan and Y. Chen and Y. Lin, "The Design of Protocol for e-Voting on the Internet", Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology, London, England, (2001) October 16-19.

[9]. D. L. Dill and A.D. Rubin, "E-Voting Security", Security and Privacy Magazine, Vol. 2(1). (2004), pp. 22-23.

[10]. D. Evans and N. Paul, "Election Security: Perception and Reality". IEEE Privacy Magazine, vol. 2(1). (2004), pp. 2-9.

Cite this article as :

Dr. M Sandhya Rani, S Meghana, Bhavitha, "E Voting System using Blockchain", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 5, pp.324-328, September-October-2022.