isrjournals

International Journal of Advanced Research in Electronics, Communication & Instrumentation Engineering and Development

Volume: 3 Issue: 1 Apr,2021,ISSN_NO: 2347 -7210

VOTING USING BLOCK CHAIN TECHNOLOGY

Mrs.V.NANAMMAL[1],J.AJAY KUMAR[2],R.HERISH KUMAR[3],S.JAISURIYA[4]

[1]Assistant Professor, [2] UG Scholar, [3] UG Scholar, [4] UG Scholar

[1,2,3,4] Department .of Electronic and communication Engineering, Jeppiaar Engineering College, Chennai-600 119.

***Abstract*—In this article, we propose Block chain is becoming the missing puzzle to solve many digital services problems these days. We propose a de-sign and implementation of a -based voting system that can be used in elections. we argue that our based voting system is more secure, reliable and it has the ability to protect voter privacy which will help boost the number of voters and their trust in the electoral system as well as reducing considerably the cost of national elections. compared to other state of the art -based voting systems is that it respects voter's privacy with a full transparency for auditing and user-friendly terminals, which will boost the confidence of people in the voting system and therefore increase the number of participants in the election.**

***Index Terms*—block chain technology, Ethereum smart contract, e-voting, , self-enforcing voting.**

I. INTRODUCTION

In a Blockchain, voting system, the voters cast their vote in a digital record of transactions. The name comes from its structure, in which individual records, called blocks, are linked together in single list, called a chain. Blockchains are used for recording transactions made with cryptocurrencies, such as Bitcoin, and have many other applications. Each transaction added to a blockchain is validated by multiple computers on the Internet. These systems, which are configured to monitor specific types of blockchain transactions, form a peer-to-peer network. They work together to ensure each transaction is valid before it is added to the blockchain. This decentralized network of computers ensures a single system cannot add invalid blocks to the chain.

When a new block is added to a blockchain, it is linked to the previous block using a cryptographic hash generated from the contents of the previous block. This ensures the chain is never broken and that each block is permanently recorded. It is also intentionally difficult to alter past transactions in blockchain since all the subsequent blocks must be altered first.

Blockchain is characterized by consensus, distributed computation, immutability, and authentication. Since blockchain is a budding technology, different types of applications require different types of blockchains. Permissionless or public blockchain does not have any control. Anyone can read or write into the network. At the same time, permissioned ledgers are restricted to authenticated users of the network. All blocks are encrypted by a private key and cannot be interpreted by anyone. Consortium blockchain are the combination of both the public and private blockchains, with the perspective of software architecture, the working model of blockchain.

II. EXISTING WORK

In most of the e-voting systems, trustworthy election authorities are required to preserve voter's privacy, to decrypt the vote and to compute the tally in a verifiable manner. Generally, threshold cryptography is used to distribute this trust among multiple tallying authorities; see, for example, Helios [1]. However, while using threshold cryptography, if the tallying authorities collude among themselves altogether, voter's privacy will be lost.

Several researchers have proposed e-voting systems based on blockchain. In Zhao and Chan propose a voting system using Bitcoin. In their voting system, random numbers and zero-knowledge proofs are used to hide the vote. In Tarasov and Tewari propose an e-voting system based on cryptocur- rency. In this system, a centralized trusted authority exists to coordinate the election. Tivi Follow my vote and The Blockchain Voting Machine] are Internet voting systems that use blockchain as a ballot box. These systems depend on trusted authorities to achieve voter's privacy. In Tivi, the trusted authority shuffles the encrypted votes before decrypting and computing the tally. In Follow my vote, the trusted authority obfuscates the link between a voter's identity and her voting key before the voter casts her vote. In our proposed protocol, the voter's privacy and the tally procedure do not depend on trusted election authorities. We implement the proposed protocol using smart contract in such a way that the Ethereum bockchain's con- sensus mechanism enforces the execution of the voting protocol. Recently, the Abu Dhabi Securities Exchange [33] has launched a blockchain-based voting service. In Estonia, blockchain-based voting systems [9] have been proposed for the internal elections of political parties and shareholder voting. The possibility of using blockchain in e-voting is also discussed in a report [9] by the Scientific Foresight Unit of the European Parliamentary Research Service. Recently, in [5], Bag *et al.* propose an end-to-end verifiable BlockChain count voting system. However,

isrjournals

International Journal of Advanced Research in Electronics, Communication & Instrumentation Engineering and Development

Volume: 3 Issue: 1 Apr,2021,ISSN_NO: 2347 -7210

their scheme is on a centralised setting where a central facility (i.e., a touch-screen voting machine) is used to directly record votes from voters. In such a setting, it is inevitable that the touch-screen machine learns the voter's choice. In this article, we propose the first self-tallying decentralized BlockChain count voting protocol, in which voters cast votes using their own devices in a distributed manner. No third-party entity can learn the voter's input unless all other voters are compromised (i.e., in a full-collusion attack). The first self-tallying voting protocol was proposed by Kiayias and Yung [38] for boardroom voting. Their protocol has the following three attractive features: it is self-tallying; it provides the maximum voter privacy;

III. PROPOSED SYSTEM

The proposed system consists the proposed protocol using smart contract in such a way that the Ethereum bock chain's consensus mechanism enforces the execution of the voting protocol. we propose a smart contract implementation of our protocol on Ethereum in order to enforce the execution of the voting protocol. We are using Ethereum since it can store and execute programs that are written as smart contracts

BLOCK DIAGRAM:

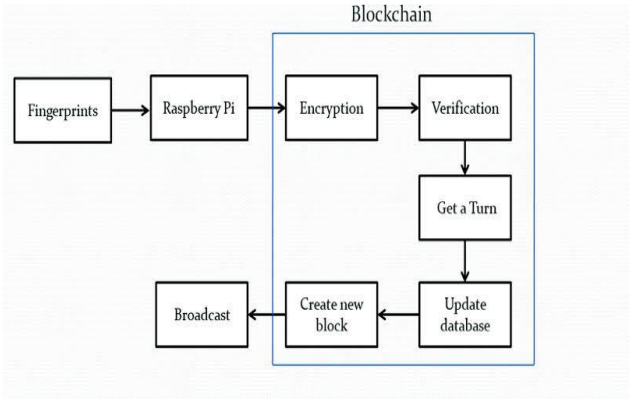

Fig.1 The block diagram of proposed system

In this system, we use RASPBERRY PI microcontroller which acts as brain of the system, because the entire system program instruction stored in it. Using Image In this system, we use RASPBERRY PI microcontroller which act as brain for the Authentication process, it will send the image of the fingerprint and after authentication, it will send the user to cast the vote. According to the user's data, their vote will update in the blockchain.

After casting the vote, it is encrypted and transfer the blockchain. After the voting process is completed, the encrypted data is stored in a secured server maintain by an organization.

and it is dispute-free. We discuss these properties in detail in a later section. Their protocol ex- ecutes in three rounds]. Hao, Ryan and Zieliński investigated the computation complexity and proposed the Open Vote Network (OV-Net) protocol [30]. Their protocol significantly improves computational complexity. In the first stage Processing, the image of the fingerprint is captured by a fingerprint sensor and is processed and the Second stage Authentication shows that it verify the type of user and is send to the controller.

Using these above steps we find out what type of user and whether are allowed to cast their vote. Besides when the user is verified, they are allowed to cast their vote to respective party.

The concept consists of two sections:

- Verification section
- Block chain section

VERIFICATION SECTION

Here in the verification section, using blockchain we proposed a new technique and it is composed of two stages:

- Processing
- Authentication

Processing- the image of the fingerprint is captured by a fingerprint sensor and is processed and the Second stage Authentication shows that it verify the type of user and is send to the controller.

Authentication- identify what type of user and whether are allowed to cast their vote. Besides when the user is verified, they are allowed to cast their vote to respective party

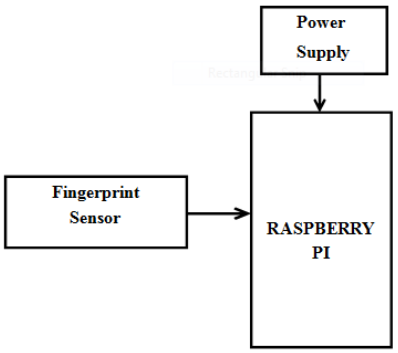

Fig.2 The block diagram of Verification Section

isrjournals

International Journal of Advanced Research in Electronics, Communication & Instrumentation Engineering and Development

Volume: 3 Issue: 1 Apr,2021,ISSN_NO: 2347 -7210

BLOCKCHAIN SECTION

In this Block chain section, where the final process takes place. The fingerprint sensor can scan the fingerprint data, to update in this section. The name and vote of the respective user updates can be switch over to this part. After voting the name and vote, can transfer the blockchain section using library function. In the section, the total vote is received using function and values are encrypted and stored in the block chain.

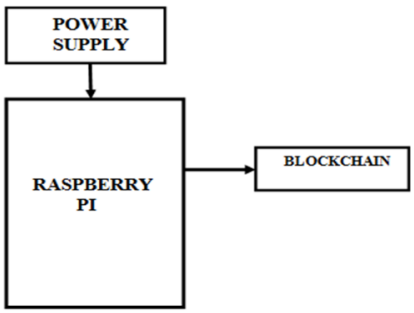

Fig. 3 The block diagram of Block Chain Section

WORKING

In this system, we use RASPBERRY PI microcontroller which acts as brain of the system, because the entire system program instruction stored in it. In this system, we use RASPBERRY PI microcontroller which act as brain for the Authentication process, it will send the image of the fingerprint and after authentication, it will send the user to cast the vote. According to the user's data, their vote will update in the blockchain.

After casting the vote, it is encrypted and transfer the blockchain. After the voting process is completed, the encrypted data is stored in a secured server maintain by an organization.

IV. RESULT AND DISCUSSION

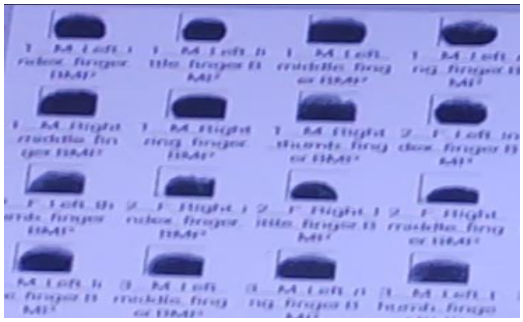

Fig .4 Sample Finger Print Data Set

The Blockchain count scheme is a ranked choice voting method in which voters rank candidates in order of preference. A score is associated with each rank. Let there are *k* candidates competing. open vote network [30], and general multi-party secure computation protocols.

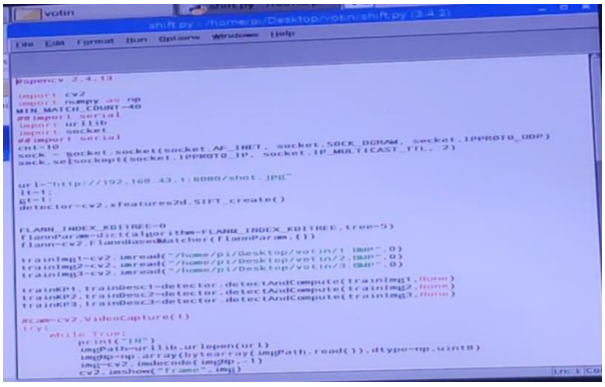

Fig. 5 Code for Verification Section

The above figure 4 and 5 takes place in the verification section which is shown in the figure 6. BlockChain count voting system. However, their scheme is on a centralised setting where a central facility (i.e., a touch-screen voting machine) is used to directly record votes from voters. In such a setting, it is inevitable that the touch-screen machine learns the voter's choice. In this article, we propose the first self-tallying decentralized BlockChain count voting protocol, in which voters cast votes using their own devices in a distributed manner. No third-party entity can learn the voter's input unless.

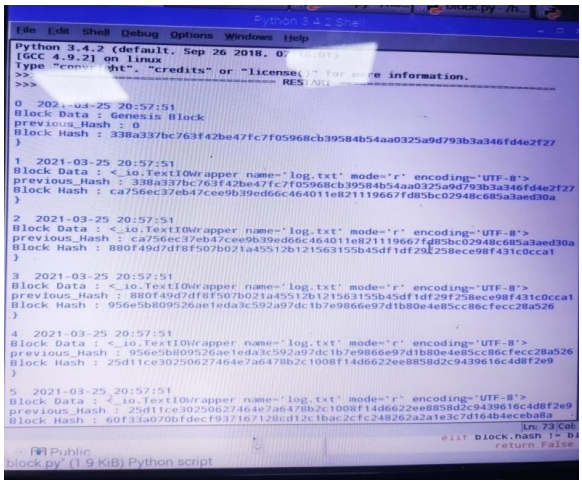

Fig .6 Voter's Detail in Block Chain

V. CONCLUSION AND FUTURE SCOPE

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions.

We have to introduced a unique, blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have outlined the systems architecture, the design, and a security analysis of the system. 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 today's scheme and offer new possibilities of transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. For countries of greater size, some measures must be taken to withhold greater throughput of transactions per second.

Our election scheme allows individual voters to vote at a voting district of their choosing while guaranteeing that each individual voters vote is counted from the correct district, which could potentially increase voter turnout.

REFERENCES

[1] B. Adida, "Helios: Web-based Open-audit Voting," in *Proc. 17th Conf. Secur. Symp.*, 2008, pp. 335–348.

[2] B. Adida *et al.*, "Electing a university president using open-audit voting: Analysis of real-world use of Helios," in *Proc. Conf. Electron. Voting Technol./Workshop Trustworthy Elections*, 2009, vol. 9, no. 10.

[3] B. Adida and R. L. Rivest, "Scratch & vote: Self-contained paper-based cryptographic voting," in *Proc. 5th ACM Workshop Privacy Electron. Soc.*, 2006, pp. 29–40.

[4] S. T. Ali and J. Murray, "An overview of end-to-end verifiable voting sys- tems," *Real-World Electronic Voting: Design, Analysis and Deployment*. Boca Raton, FL, USA: CRC Press, 2016, pp. 171–218.

[5] S. Bag, M. A. Azad, and F. Hao, "E2E verifiable BlockChain count voting system without tallying authorities," in *Proc. 14th Int. Conf. Availability, Rel. Secur.*, Aug. 2019, pp. 11:1–11:9.

[6] S. Bell *et al.*, "STAR-Vote: A secure, transparent, auditable, and reliable voting system," in *Proc. Electron. Voting Technol. Workshop/Workshop Trustworthy Elections*, Aug. 2013.

[7] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. Comput. Commun. Secur.*, 1993, pp. 62–73.

[8] D. Black, *The Theory of Committees and Elections*. Cambridge, U.K.: Cambridge Univ. Press, 1958.

[9] P. Boucher, "What if blockchain technology revolutionised vot-

[10] R. Bredereck, J. Chen, P. Faliszewski, A. Nichterlein, and R. Niedermeier, "Prices matter for the parameterized complexity of shift bribery," *Inf. Comput.*, vol. 251, no. C, pp. 140–164, Dec. 2016.

[11] M. A. Burgman *et al.*, "Voting systems for environmental decisions,"*Conservation Biol.*, vol. 28, no. 2, pp. 322–332, 2014.

[12] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups (extended abstract)," in *Proc. 17th Annu. Int. Cryptol. Conf. Adv. Cryptol.*, 1997, pp. 410–424.

[13] S. A. Chatzichristofis, K. Zagoris, Y. Boutalis, and A. Arampatzis, "A fuzzy rank-based late fusion method for image retrieval," in Advances in Multimedia Modeling, K. Schoeffmann, B. Merialdo, A. G. Hauptmann, C.-W. Ngo, Y. Andreopoulos, and C. Breiteneder, Eds. Berlin, Germany: Springer, 2012, pp. 463–472.

[14] D. Chaum *et al.*, "Scantegrity: End-to-end voter-verifiable optical- scan voting," *IEEE Secur. Privacy*, vol. 6, no. 3, pp. 40–46, May 2008.

[15] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," *IEEE Secur. Privacy*, vol. 2, no. 1, pp. 38–47, Jan./Feb. 2004.