Evoting Done Right Privacy and Transparency with Public Blockchain using Face Recognition

Chaitanya B [1], Revathy P [2], Gayatri G [3]

[1,2] Assistant Professor, Department of Computer Science and Engineering

[3] Assistant Professor, Department of Computer Science and Engineering

[1,2] Narsimha Reddy Engineering College,Kompally,Hyderabad,India.

[3] Malla Reddy College of Engineering and Technology,Kompally,Hyderabad,India.

ABSTRACT

The topic of e-voting systems is still at an early stage of development. We have chosen this domain not only for its recency but also because there are not many solutions that address problems of e-voting. Nowadays, popularity grows also in the development of e-Government. However, such a system is not feasible if basic services for citizens such as elections do not become electronic. "E-voting is one of the key public sectors that can be transformed by blockchain technology". Hand by hand with e-voting come also new challenges, which need to be addressed. One of them is e.g. securing the elections, which needs to be at least as safe as the classic voting systems with ballots. That is why we have decided to create safe elections in which voters do not have to worry about someone abusing the electoral system. In recent years blockchain is often mentioned as an example of secure technology used in an online environment. Our e-voting system uses blockchain to manage all election processes. Its main advantage is that there is no need for confidence in the centralized authority that created the elections. This authority cannot affect the election results in our system. Another challenge in e-voting is the lack of transparency in the functioning of the system, leading to a lack of confidence in

voters. This problem is solved by blockchain in a way of total transparency that allows everyone to see the stored data and processes such as how these data are handled. In the field of security, this technology is more suitable in every way than the classic e-voting platform without blockchain.

Keywords: 4leg 3 phase inverter, PI controller, NPC inverter.

1. INTRODUCTION

Some forms of voting have been here ever since. Mostly used form all over the world are paper ballots. Electronic voting schemes are being popular only in the last decade and they are still unsolved. E-voting schemes bring problems mainly regarding security, credibility, transparency, reliability, and functionality. Estonia is the pioneer in this field and may be considered the state of the art. But there are only a few solutions using blockchain. Blockchain can deliver an answer to all of the mentioned problems and furthermore bring some advantages such as immutability and decentralization. The main problems of technologies utilizing blockchain for e-voting are their focus on only one field or lack of testing and comparison. In this paper, we present a blockchain based e-voting platform, which can be used for any kind of voting. It is fully utilized by blockchain and all processes can be handled within it. After the start of the voting, the platform behaves as fully independent and decentralized without possibilities to affect the voting process. The data are fully transparent, but the identity of voters is secured by homomorphic encryption. We have tested and compared our solution in three different blockchains. The results show, that both public and private blockchains can be used with only a little difference in the speed. The key novelty of our solution is a fully decentralized management of e-voting

platform through blockchain, transparency of the whole process and at the same time security and privacy of the voters thanks to homomorphic encryption.

Literature survey:

"Voting Process with Block-chain Technology: Auditable Block-chain Voting System,"

There are various methods and approaches to electronic voting all around the world. Each is connected with different benefits and issues. One of the most important and prevalent problems is lack of auditing capabilities and system verification methods. Blockchain technology, which recently gained a lot of attention, can provide a solution to this issue. This paper presents Auditable Blockchain Voting System (ABVS), which describes e-voting processes and components of a supervised internet voting system that is audit and verification capable. ABVS achieves this through utilization of blockchain technology and voter-verified paper audit trail.

"Bitcoin: A Peer-to-Peer Electronic Cash System,"

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

"A Smart Contract for Boardroom Voting with Maximum Voter Privacy,"

We present the first implementation of a decentralized and self-tallying internet voting protocol with maximum voter privacy using the Blockchain. The Open Vote Network is suitable for boardroom elections and is written as a smart contract for Ethereum. Unlike previously proposed Blockchain e-voting protocols, this is the first implementation that does not rely on any trusted authority to compute the tally or to protect the voter's privacy. Instead, the Open Vote Network is a selftallying protocol, and each voter is in control of the privacy of their own vote such that it can only be breached by a full collusion involving all other voters. The execution of the protocol is enforced using the consensus mechanism that also secures the Ethereum blockchain. We tested the implementation on Ethereum's official test network to demonstrate its feasibility. Also, we provide a financial and computational breakdown of its execution cost.

"Efficient Fully Homomorphic Encryption from (Standard) LWE,"

We present a fully homomorphic encryption scheme that is based solely on the (standard) learning with errors (LWE) assumption. Applying known results on LWE, the security of our scheme is based on the worst-case hardness of "short vector problems" on arbitrary lattices. Our construction improves on previous works in two aspects: 1) we show that "somewhat homomorphic" encryption can be based on LWE, using a new re-linearization technique. In contrast, all previous schemes relied on complexity assumptions related to ideals in various rings. 2) We deviate from the "squashing paradigm" used in all previous works. We introduce a new dimension-modulus reduction technique, which shortens the ciphertexts and reduces the decryption complexity of our scheme, without introducing additional assumptions. Our scheme has very short ciphertexts and we therefore use it to construct an asymptotically efficient LWE-based single-server private information retrieval (PIR) protocol. The communication complexity of our protocol (in the public-key model) is k · polylog(k) + log |DB| bits per single-bit query (here, A; is a security parameter).

2. EXISTING SYSTEM

Some forms of voting have been here ever since. Mostly used form all over the world are paper ballots. Electronic voting schemes are being popular only in the last decade

and they are still unsolved. E-voting schemes bring problems mainly regarding security, credibility, transparency, reliability, and functionality. Estonia is the pioneer in this field and may be considered the state of the art. But there are only a few solutions using blockchain. Blockchain can deliver an answer to all of the mentioned problems and furthermore bring some advantages such as immutability and decentralization. The main problems of technologies utilizing blockchain for e-voting are their focus on only one field or lack of testing and comparison.

3. PROPOSED SYSTEM

In this paper, we present a blockchain based e-voting platform, which can be used for any kind of voting. It is fully utilized by blockchain and all processes can be handled within it. After the start of the voting, the platform behaves as fully independent and decentralized without possibilities to affect the voting process. The data are fully transparent, but the identity of voters is secured by homomorphic encryption. We have tested and compared our solution in three different blockchains. The results show, that both public and private blockchains can be used with only a little difference in the speed. The key novelty of our solution is a fully decentralized management of e-voting platform through blockchain, transparency of the whole process and at the same time security and privacy of the voters thanks to homomorphic encryption.

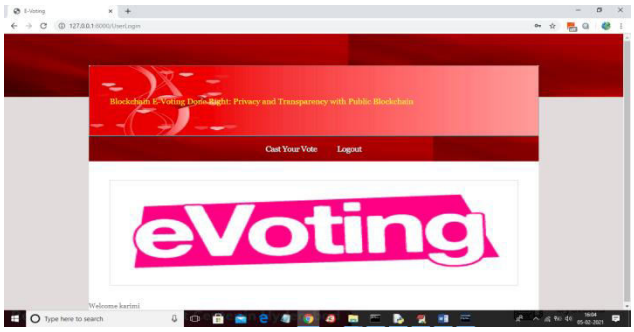
4. MODULES:

Admin module: This user responsible to add new party and candidate details and can view party details and vote count. Admin login to system by using username as ‘admin’ and password as ‘admin’.

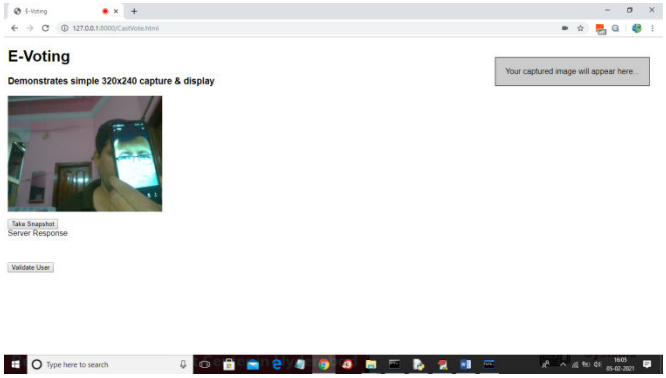
User Module: This user has to sign up with the application by using

username as his ID and then upload his face photo which capture from webcam. After registering user can go for login which validate user id and after successful login user can go for cast vote module which execute following functionality

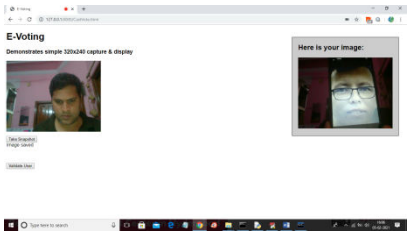
1. First user will be connected to his PC webcam and then image will be capture
2. Using OpenCV application will detect face and then using CNN application will predict user identify and if user identity matched with CNN predicted face then application will display all voting candidates list.
3. If user not casted vote then user can give vote to desire candidate by clicking link beside party name or candidate name.
4. Upon giving vote application will capture voter and candidate details and then encrypt the data and then store in Blockchain.



In above screen user can click on 'Cast Your Vote' link to get below webcam screen

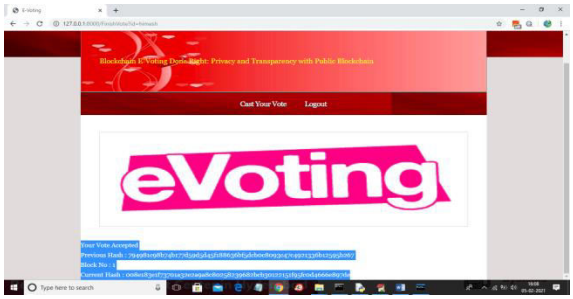


In above screen webcam is running and then by showing person face we need to click on 'Take Snapshot' button to capture his face

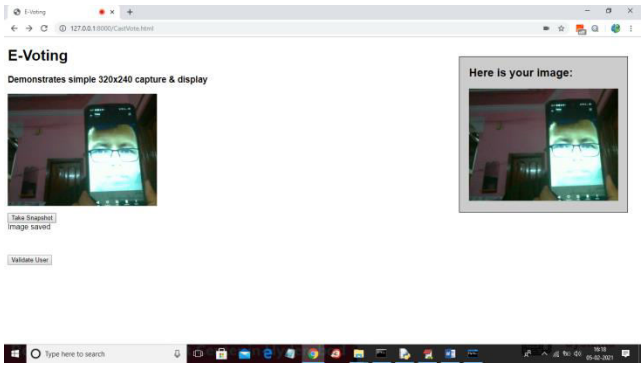


In above screen person faces is capture and now click on 'Validate User' button to validate user

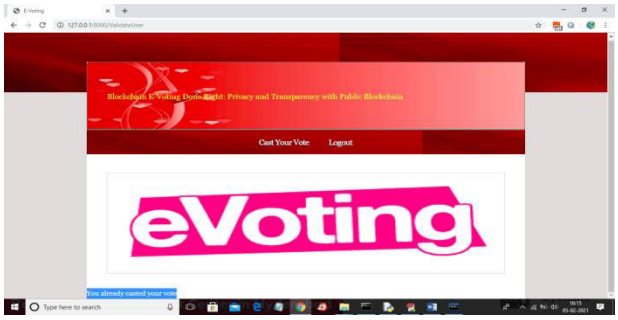
In above screen in blue colour you can see user is identified as 'azizullahkarimi' and then displaying list of candidates and now user can click on 'Click Here' option to cast his vote and to get below screen



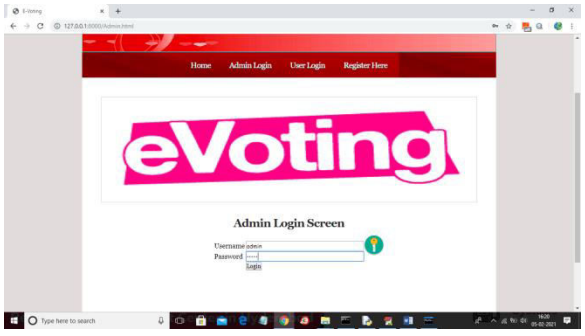
In above screen as this is the first vote so block will be added to Blockchain with block No as 1 and we can see Blockchain created a chain of blocks with previous and current hash code validation. Now try again with same user to cast vote



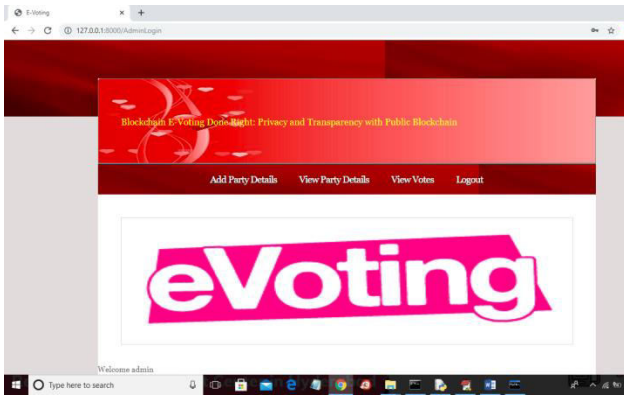
In above screen same user trying again and below is the result



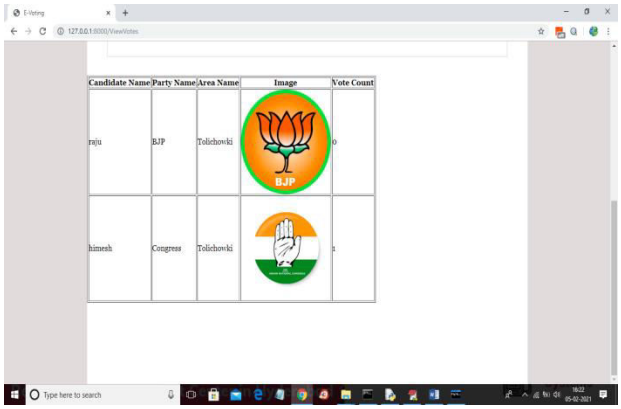
In above screen if same user try again then will get message as 'You already casted you vote' and now logout and login as 'admin' to get vote count



In above screen login as admin and after login will get below screen



In above screen admin can click on 'View Votes' link to get below screen



In above screen admin can view all vote counts.

5. CONCLUSION

Although we can see slight differences in network times, they are so negligible that public blockchain has more advantages in such an electoral system due to its openness of data and that anyone can watch them in the real time. A private blockchain is a bit faster, but it reduces the credibility of the whole system by being partially centralized because it only runs where the authority wants it. The table shows that the average times to add one person's voice are: Ganache 6.32 s (median 6.34 s), Hyper ledger Composer 6.05 s (median 6.04 s), and Ethereum Ropsten 17.75 s (median 17.93 s). These times are influenced by the used consensus algorithm and also by the block time.

REFERENCES

[1] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," IEEE Software, vol. 35, pp. 95-99, jul 2018.

[2] M. Pawlak, J. Guziur, and A. Poniszewska-Maranda, "Voting Processwith Blockchain Technology: Auditable Blockchain Voting System," inLecture Notes on Data Engineering and Communications Technologies, pp. 233-244, Springer, Cham, 2019.

[3] B. Singhal, G. Dhameja, and P. S. Panda, "How Blockchain Works," in Beginning Blockchain, pp. 31-148, Berkeley, CA: Apress, 2018.

[4] Agora, "Agora Whitepaper," 2018.

[5] R. Perper, "Sierra Leone is the first country to use blockchain duringan election - Business Insider," 2018.

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," tech.rep., 2008.

[7] G. Wood et al., "Ethereum: A secure decentralized generalized transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1-32, 2014.

[8] S. Landers, "Netvote: A Decentralized Voting Platform – Netvote Project Medium," 2018.

[9] P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," in Lecture Notes in Computer Science, ch. FCDS, pp. 357-375, Springer, Cham, 2017.

[10] Z. Brakerski and V. Vaikuntanathan, "Efficient Fully Homomorphic Encryption from (Standard) LWE,"SIAM Journal on Computing, vol. 43,pp. 831-871, jan 2014.

[11] O. Goldreich and Y. Oren, "Definitions and properties of zero knowledge proof systems," Journal of Cryptology, vol. 7, no. 1, pp. 1-32, 1994.