DECENTRALIZED ONLINE VOTING USING BLOCKCHAIN

Rajat Gupta

Student, Maharaja Agrasen Institute of Technology, Delhi, India

ABSTRACT

Voting is one of the most important events in a democratic country like India. Till now voting is done in offline mode where a voter goes to a polling booth and cast his vote in an EVM. But this system can be made online through a decentralized application that runs on top of the blockchain. Decentralized Online voting is the application that makes the whole voting system electronic and every voter can cast his/her ballot using his smartphone anywhere. Blockchain is the technology through which this can be achieved. Blockchain technology has cryptographic foundations which enable it to achieve resilient security solutions.

1. INTRODUCTION

A Blockchain resembles a data structure that maintains and shares all the transactions being executed through its genesis. It is a distributed decentralized database in which dynamic data gets stored which is completely secured from any external tampering and manipulation. It is nearly impossible to make a change in any data stored in the blockchain. A decentralized Online Voting application eases the method of voting. The decentralized application does not run/exist on a single computer instead it runs on a blockchain or P2P network, due to this property they are more secure and less prone to cyber-attacks and hacking. Using this application voters can cast his/her vote through online mode. The application uses the Ethereum network of blockchain which is one of the best options. There are various options available for blockchain networks like bitcoin, ethereum and we can choose any of them as each of them is equally secure.

2. FEASIBILITY STUDY

As the name explains itself, blockchain is a chain of blocks. Usually, each block contains transactions and a hash pointer, which serves as a link to the next block. This is the core technique for ensuring security in the network. It is impossible to delete any block or insert a new one in the chain because the network is designed in such a way that if the hash does not match, the operation cannot be completed. Whenever any transaction takes place on a blockchain's software, a block is created

corresponding to that transaction. A block of a transaction is known as a "node".

To attach the compiled block of transactions to the blockchain, a node must resolve a hash function of the block that satisfies certain mathematical conditions, although rules for block attaching can be different and depend on a respective concord algorithm, which is used in a particular blockchain. For a block to be included in a blockchain, a network agreement must be reached. It means that all blocks or network participants must confirm its authenticity. Depending on technical parameters, a block is included in a blockchain after a certain number of confirmations; however, it is being validated by all network participants, until everyone has an updated blockchain structure.

3. METHODOLOGY/PLANNING OF WORK

The voting protocol in a decentralized electronic voting system consists of the following steps:

1. Preparing a licit voter's list in a decentralized electronic identification system.
2. Generation of licit voters' wallets in a decentralized application system for online voting and result counting
3. Candidates registration in a decentralized application system for online voting and results counting.

4. Voters 'authentication in decentralized application system for online voting and results counting.
5. Voting in a decentralized application.
6. Counting of votes in a decentralized infrastructure and result declaration.

4. IMPLEMENTATION

This application consists of two layers:

1. **Frontend:** Frontend is done using HTML, CSS, and Javascript. Although improvisation is to be done using ReactJS.Till now the frontend is more of a basic design because the actual beauty of the application is in the backend. But there is always a scope for improvement hence ReactJS will be used to make UI design more attractive.

2. **Backend:** The backend Layer consists of several dependencies listed as follows:

    1. **NodeJS:** NodeJS is a cross-platform framework of javascript used to write server side code.

    2. **Solidity:** Solidity is the high-level programming language used to write smart contracts.

    3. **Ganache:** Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development. It is used to test the application on a local device.

    4. **Truffle:** Truffle is a development environment to build ethereum based applications.

Apart from these two layers, we have to use a crypto wallet for making transactions. Here we are using **Metamask** as a crypto wallet. Ganache provides some demo accounts with some amount of ethereum coins. Whenever a user casts his/her vote a certain(very small) amount of ethereum coin is deducted from the balance because casting a vote is a transaction in the blockchain network and each transaction has its cost therefore certain amount of balance is required in the user's wallet. Therefore to complete the transaction or depositing, withdrawing crypto coin requires an E-wallet hence Metamask is used.

5. DISCUSSION & FUTURE WORK

This concept requires some more secure and easy user authentication. Whenever an election gets conducted user needs to Sign up in the application so the method of signing up can be different like Aadhaar card number, Voter Id number along with biometric verification. So this decision is to be made so that it will be easy for common people to cast their ballot. Considering the diversity in a country like India where millions of people don't have access to the Internet and smartphones, we have to make this method reachable to them also. This can be done by some government volunteers who will create mass awareness and guide people on how to cast their votes.

6. CONCLUSION

The decentralized online voting application can be used as a medium to conduct any type of election whether it is government elections or some other purpose elections. It saves a lot of time and money for the country because all the expenses of conducting offline elections will be saved like appointing officers, cost of EVMs, Documentations, etc. Although It has some drawbacks like many people are unaware of technology and the Internet and many don't even have access to smartphones. So these kinds of things have to be considered before accepting this application for a purpose. Proper Authentication and Blockchain technology together makes the whole system very secure.

REFERENCES

1. Olusola, O., & Adesina, R. (2015). A Framework for Electronic Voting in Nigeria. International Journal of Computer Applications, 129(3), 12–16. https://doi.org/10.5120/ijca2015906786
2. Shuaibu, A., Mohammed, A., & Ume, A. (2017). A Framework for the Adoption of Electronic Voting System in Nigeria. International Journal of Advanced Research in Computer Science and Software Engineering, 7(3), 258–268. https://doi.org/10.23956/ijarcsse/V7I3/01310
3. Qadah, G. Z., & Taha, R. (2007). Electronic voting systems: Requirements, design, and implementation. Computer Standards & Interfaces, 29(3), 376–386. https://doi.org/10.1016/j.csi.2006.06.001
4. Khelifi, A., Grisi, Y., Soufi, D., Mohanad, D., & Shastry, P. V. S. (2013). M-Vote: A Reliable and Highly Secure Mobile Voting System. 2013 Palestinian International Conference on Information and Communication Technology, 90–98. https://doi.org/10.1109/PICICT.2013.25
5. Ayo, C. K., Ekong, U. O., Ikhu-omoregbe, N. A., & Ekong, V. E. (2007). M-voting implementation: The issues and trends. 1–5. Retrieved from http://www.academia.edu/download/3258019/EEE4041.pdf
6. Ekong, O. U., & Ekong, E. V. (2010). M-Voting: A Panacea for Enhanced E- Participation. Asian Journal of Information Technology, 9(2), 111–116. https://doi.org/10.3923/ajit.2010.111.116