Blockchain in Voting System

*Introduction*

Through new technologies such as blockchain, the accessibility and structure of voting has been transformed. Our team has designed and implemented a blockchain in order to to demonstrate the benefits of using one in a voting system. Throughout our work we showcase the security, framework, and future possibilities when blockchain is used in a voting process, specifically how votes are counted and stored. Several factors such as electoral system, popular votes or issues with a two party system were not in the scope with our project and therefore not considered. Rather, we built a system to demonstrate how voter information can be stored, retrieved, and secured. In addition, we also hope to improve the confidence of voters that their votes are in fact recorded securely, correctly, and remain protected.

*Our Blockchain Architecture*

We decided to utilize the distributed network capability of blockchain along with the aggregation associated with traditional voting. There are three network tiers, one each at the local, constituency and national level. Nodes at the local level represent the polling stations and can communicate with other nodes in the same constituency. Similarly, state level nodes would have direct connectivity to few selected local nodes based on location and can communicate with other state level nodes. The same applies for national level nodes as well. To minimize the complexity in our project, we decided to focus on local level nodes only. For our project, we implemented a two step approach to digitize the voting process. In step one, for voter registrations we created a blockchain, called “voter registration chain” and similarly, another distinct blockchain, “voting chain”, was used to store user’s vote at the constituency level. For the details of each node, please refer to Section 1 in Appendix.

Before any election that were to to use our blockchain, a voter interesting in casting a ballot would be notified to register to vote. Once the voter was registered, a government assigned miner would add the voter’s information to a block in the voter registration chain. While doing so, the system internally assigns a unique verifier, using SHA-256 hashing, to the voter. These unique verifiers are what would be used to restrict unregistered voters from casting their vote on election day. A block is added to the voter registration chain in each of the below cases:

1. New voter’s details are verified against the government database and if found eligible to vote, a government assigned miner would add the voter’s info to a block in the chain.
2. Once the voter casts his/her vote on election day, another block with the user’s information and “status = voted” is added to the chain.

On election day, whenever a voter logs in to the portal to cast their vote, the system will verify the user’s eligibility to vote by checking against the voter registration chain. In the backend, if the user is already registered and user’s status is not “voted”, then the system will allow the user to cast their vote. If not, then the user will get an appropriate error message. If eligible, a block with “status = voted” will be added to the voter registration chain and user’s vote detail (with just the vote and unique verifier) will be passed on as a transaction to the second blockchain i.e. the voting chain. Even though the transaction is created on a specific constituency code, it is available to all nodes at the same constituency level, via a peer-to-peer network, for miners to mine it. A government assigned miner would mine the blocks with vote details and add them to the voting chain. The constituency nodes would periodically run a consensus resolving algorithm to stay up to date with other nodes in the same constituency. It is important to note that there are two blockchains, one which tells us if a user is authorized to vote and other which stores the contents of the user’s vote. By implementing two distinct blockchain in a multi-tiered approach, we achieve anonymity as the voting chain will only have a unique verifier, generated by SHA-256, and the vote. In the future if a user wants to verify their vote, they can do so by using their ID and name. The system will internally generate the unique verifier by passing on user details to SHA-256, and find a match in the voting chain.

For a visual representation of our blockchain process please refer to **Diagram 1.**

*Improvements*

While developing our blockchain there were some components we acknowledged that would need to be addressed before this new technology could be implemented on a national scale.

* With more time, we would have liked to implement a user interface that would allow users to conveniently register their votes in our blockchain.
* Voter encryption was not implemented in our system. This is required so that user details and their vote are kept anonymous.
* Ideally, we would restrict voters from voting outside of the state of residence because each state has unique rules and requirements for state citizens to be eligible to vote.
* Understanding/acknowledging the legal methods for communication used by the federal government.
* Improving the proof-of-work mechanism to take into account the issues of soft-fork and difficulty of proof-of-work.

*Examples of Current Applications in Modern World*

The country of Estonia is perhaps the best example of a nation who is adopting advanced technologies and blockchain methods. Estonia is working hard to fully implement an e-voting system in which both e-residents and nationals can cast votes in company shareholders meeting both securely and remotely. Similarly, in the Middle East, Abu Dhabi has recently announced the use of blockchain in the stock exchange for different stakeholders to not only observe but also participate in votes for their annual meetings.[[1]](#footnote-0)

*Conclusion*

Blockchain is a revolutionary technology that has the potential to transform the way voting is conducting in any democracy, through its security, ability for remote use, transparency, and the fact that it could give voters more confidence in the system. We have only worked through a small fraction of addressing and solving this fundamental issue, however through future collaboration and worldwide adoptions we are all a few steps closer to a more efficient and effective voting process.

Works Cited/Appendix

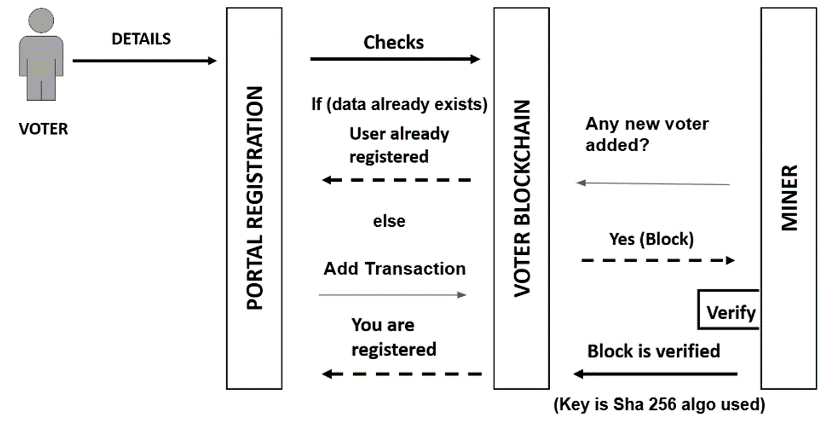
Walt, Vivienne. “Is This Tiny European Nation a Preview of Our Tech Future?” *Fortune*, 27 Apr. 2017, fortune.com/2017/04/27/estonia-digital-life-tech-startups/.

**Section 1:** <http://34.212.33.143:5000/view_chain> (Voter Registration chain)

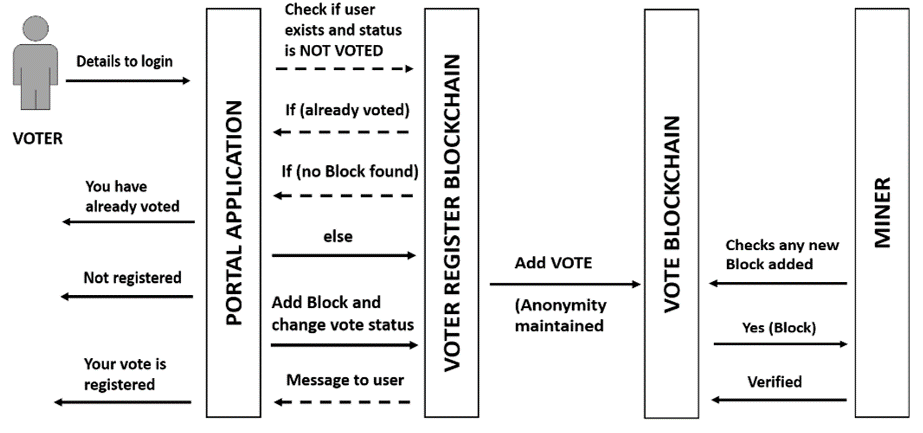
<http://34.212.33.143:5001/view_chain> (Voting Chain Node 1)

<http://34.212.33.143:5002/view_chain> (Voting Chain Node 2)

<http://34.212.33.143:5003/view_chain> (Voting Chain Node 3)

**Diagram 1: Blockchain Architecture **

Voter Registration Chain



Voting Chain

1. fortune.com/2017/04/27/estonia-digital-life-tech-startups/ [↑](#footnote-ref-0)