CENG 489 Term Project

Blockchain Based E-Voting System

Çağdaş Fil

2093839

Berkant Bayraktar

2098796

Problem Statement

The purpose of this project is to implement the digital voting system using blockchain technology.

These days, many countries, including our country, holds paper-based election. Taking advantage of modern technology, changing elections from paper-based to electronics has become a necessity these days. We need to keep up with the technology in this regard. Therefore, elections that uses e-voting should be held instead of traditional paper-based elections.

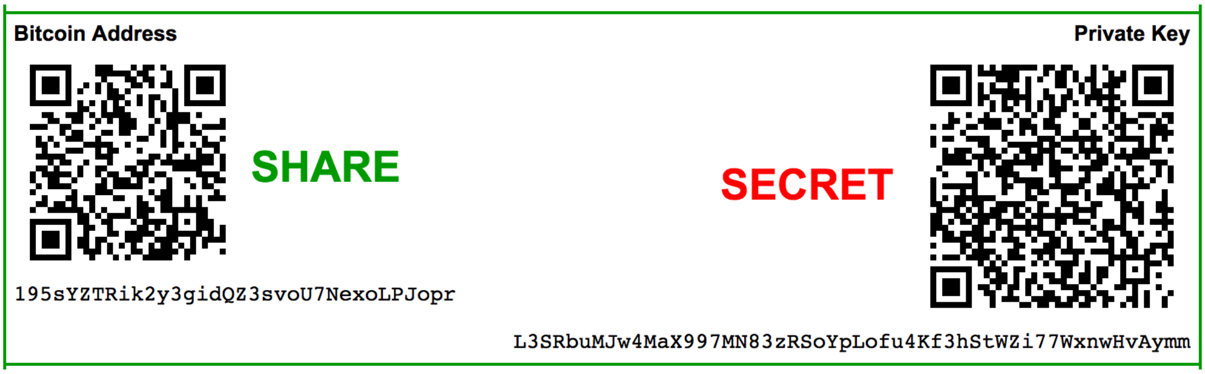
One of the biggest concerns of e-voting system is whether the system is completely secure or not. Most of these concerns are overcome by block-chain technology. Thus, e-voting systems that includes block-chain technology are both secure and practical.

Proposed Approach

We aimed to use blockchain technology in elections to make them in a more secure way. For this purpose, we prepared a web-based application that provides two functionalities. One of them is for voting, other one is for tracking results. The purpose is that making both voting operation and tracking the results very easy. Anyone with an internet connection can vote from wherever they want. For the people who are not capable of accessing internet, there should be some voting stations where people use their votes. Apart from reducing huge amount of cost, this voting system provides voters a reliable and simultaneous source for results. People no longer need to follow news agencies and be doubtful about which one is correct.

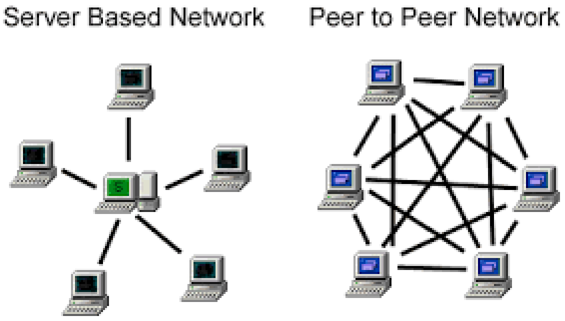
Our proposed approach has similarities to cryptocurrencies which are blockchain-based. Both voters and parties can be considered as wallet. For parties, a random private key is generated. Then, public key is extracted from private key and the private key is wiped out. Votes given to a party cannot be deleted or undone in any way. Public keys of the parties are available for everyone. Just like cryptocurrency transaction, a vote can be signed to a party by identifying it with its public key.

Every voter in the system has a unique private key. This private key is used for voting operation. In our application, the private key should be entered to the provided box for voting. Since these keys are long strings, a better solution can be used for entering the key like scanning QR code etc. Every voter should be provided one vote to use. A central account like official election board can distribute a vote for every voter, similar to sending a coin to everyone's wallet in cryptocurrency scenario.


Bitcoin Address
SHARE
195sYZTRik2y3gidQZ3svoU7NexoLPJopr
Private Key
SECRET
L3SRbuMJw4MaX997MN83zRSoYpLofu4Kf3hStWZi77WxnwHvAymm

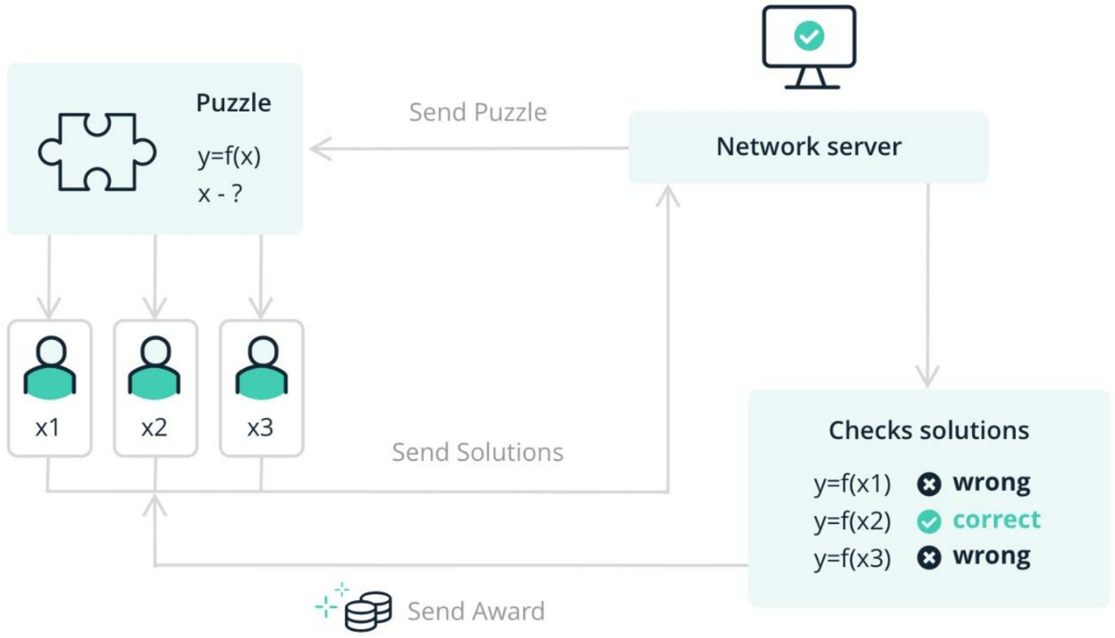
Everyone that uses the application can access the results immediately. Blocks of the blockchain are generated in very small time. In Bitcoin, creation of a block takes approximately 10 minutes. In our implementation, we decreased this time to seconds. However, how much time to create a block can be adjusted in our implementation. This is related with the difficulty of the solving a kind of math problem. In the implementation, we represented this value with a value named difficulty. The way of calculating results is similar to showing the balance of an account in cryptocurrency. The public key of a party is accessible so checking how many votes a party have resembles checking balance of a given public key.

The power of the blockchain comes from its decentralized structure. Central control over the system brings some security problems. On the other hand, decentralization makes the process transparent. The data is stored across its peer-to-peer network. It has no central point of fault. Blockchain uses public-key cryptography (public/private key like address/password). Votes can be considered as transaction from an address (public key) to another address. In general, the data stored in blockchain-based system is considered incorruptible.



In a decentralized system, there is an important component, which is the nodes. Nodes are the components that store blockchain. Main data is replicated and stored over all nodes in the system. New blocks are generated by mining and distributed over the network. In this approach, nobody has precedence over other participants in network. The trust to the system increases as nodes in the network increases. In our approach, we thought that government can provide computational power for increasing number of the nodes in the system to make it more secure. Also, anyone can be a node for the system because it is open for everyone. It strongly decreases the probability of the %51 attack. Small block creation time also helps to prevent %51 attack.

There are some concerns like creating blocks fast and spamming the blockchain, tampering with the blocks in the chain or taking control of the blockchain by creating the longest chain. All these problems are solved with proof-of-work. It is done by creating a computational work to prevent abuse. We implemented proof-of-work by requiring a specific number of zeros on the beginning of the hash. The number of the zeros is also named as difficulty. Difficulty can determine the amount of time to create a new block. Since the hash of the block is created by the data that should not change. We placed a value named nonce to blockchain. The nonce value is increasing until a valid hash is found. Finding a hash that satisfies the difficulty is also called as mining.

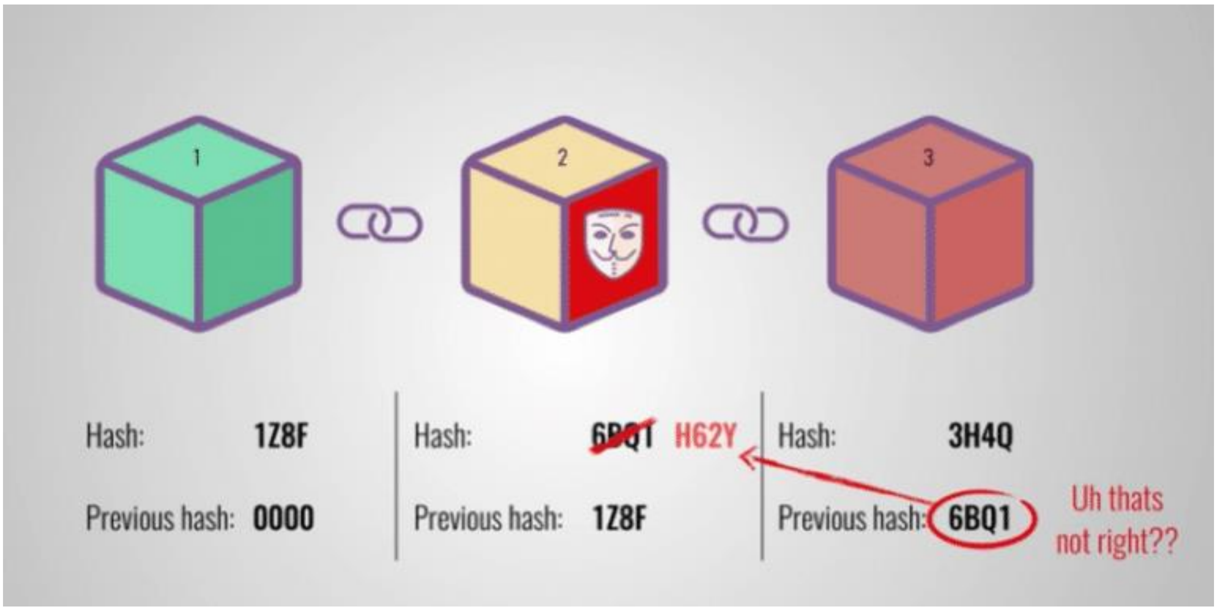


In cryptocurrency implementations, miners are rewarded with some coin. In our situation, rewarding is not possible (like rewarding the miner with more vote). Mining operation should be supported by the government. Also, voters can do mining voluntarily to help processing the votes. All votes are collected as pending until a block is created. Pending votes forms the data section of the newly created block.

Experiment Results

We tested our application by using votes and displaying results. In voting operation, votes are created successfully and listed in pending votes. Then, a valid block is created and added to the chain in the desired amount of time. We examined the data in blocks. The data consists of valid votes and it is trackable. Total votes of a party calculated correctly by using the data in the blocks. Results page of the application displays the correct results.

Our implementation is similar to Bitcoin implementation. Currently, Bitcoin has the largest volume in cryptocurrencies. Bitcoin is being used in all over the world. It is considered as reliable by many authorities and is still standing. There has not been any security leak until now. It shows that blockchain can be used in elections to make them more secure.



We tried to tamper with the data in the blockchain. However, the system denied the temperance and secured itself. We used methods in the blockchain implementation to test the validation of the chain. Whenever we tried to tamper with the data, the system alerted that the blockchain is invalid.

Conclusion

We tried to implement a voting system that uses blockchain technology to make it more secure and transparent. Also, it can reduce the cost of the elections enormously. There can be some improvements in our system.

One of the problems in our implementation is that there is a private key for every voter. The key is in a long string format. It is very hard to keep it in mind. This private key should be in voter’s responsibility. The key can be stolen so it can be problematic because of the irreversible structure of the blockchain. Also, the key is entered as string in our implementation. This phase can be improved like scanning QR code or by using a special magnetic card etc. To sum up, authentication of the system can be improved.

Another way to improve our implementation is that our system still needs some centralized control. Generating a private key for voters and giving them one vote right to use is somehow conflicting with the philosophy of the blockchain system. By solving this situation, the system can be made more decentralized.

Reference

- https://en.wikipedia.org/wiki/Blockchain
- https://www.savjee.be/2017/09/Implementing-proof-of-work-javascript-blockchain/
- https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html
- https://en.wikipedia.org/wiki/Proof_of_work
- https://bitcoin.org/bitcoin.pdf