Original scientific paper
Received: 2022-03-15
Accepted: 2022-04-07

BLOCKCHAIN–BASED E–VOTING SYSTEM

Maris PAVIČEVIĆ, RIT Croatia, mxp3742@rit.edu

Abstract

To create a reliable, strong e- voting system with high security, credibility, transparency, reliability and functionality, the best solution is to base it on a blockchain technology which would support all the mentioned components.

E-voting system will be based on the private blockchain which will allow only a selected number of verified participants to join. Only verified participants will be able to make transactions. Because of that, validation is required, and it will be implemented through the network operators or by the network's precisely defined set protocol.

The mentioned private blockchain will control who has permission to participate in the network, execute the consensus protocol which determines voting rights, and finally maintain the shared ledger. The most common role the majority users will have is a voter role, whose only authority is to give a vote in the selected voting category. The only role which should have the right to edit or delete certain entries on the blockchain would be the operator or the owner but considering that the votes should not be edited or deleted, there will not be a role with that authority. On the other hand, there will be a creator role, which will have authority to create new voting lists and set the conditions which voters have to follow and respect, but it will not have any direct impact on the blockchain.

Private blockchain on which this system will be based on, is a distributed ledger that operates as a secure, closed database, which is not decentralized (in comparison with a public one which is decentralized) and it is grounded on the cryptography concepts.

Key words: blockchain, e-voting, ledger, decentralized.

1. Introduction

1.1. Keep up with the times

Nowadays, technology is becoming the most crucial and important tool on which the world 'relies'. Application development makes a lot of things more efficient and less time consuming. The already existing example of it would be online banking; it is way easier and faster to perform a transaction or to pay the bills via online banking instead of going to the bank and losing a big amount of time by waiting in lines.

Same as online banking, a quality, well organized e-voting system would highly benefit every

country for the same specific reason. Also, e-voting would be more credible if a sum of votes would be transparent all the time (of course, without showing specific details regarding the votes), in comparison with the paper – based voting system in which citizens never knew if the votes were summed up properly.

1.2. Solution to the current problem

The main problem which must be solved is an unreliable, untrustworthy counting of votes, which has a big possibility to happen during a paper – based voting in which citizens haven't got any proof that all votes have been counted properly. All that makes the old-fashioned voting principle extremely untrustworthy.

The most efficient way by which this problem can be solved would be by virtualizing our votes, or, in other words, by switching up to the blockchain based e-voting system. The e-voting system would provide to all of its users to verify their votes and to track information about votes-counting. This way, every single voter would benefit from the new voting method. All of them would rely on the highly secure system by which the blockchain works, instead of being in continuous doubt if the votes have been counted honestly and properly.

Not to mention that the online voting system would not be time consuming as the old way of voting, as well as it would be very cost-efficient in comparison to it.

Simple e-voting schemes can bring problems regarding security, credibility, transparency, reliability, and functionality; but blockchain can deliver an answer to all of the mentioned problems and furthermore bring some advantages such as immutability and decentralization (Košťál, Bencel, Ries, Kotuliak, 2019). Blockchain technology would solve all the potential problems and risks mentioned above. E-voting system would be reliable and secure for all of its users.

1.3. Potential benefits

The movement from paper-based voting system to electronic system brings new enhancements such as real time counting, instant result, environment friendly, transparent, anonymity, less error and decentralization (Singh, Chatterjee 2019). And those are just a few benefits when it comes to the e-voting.

Instead of being in doubt if a particular person counted all the votes properly during the paper-based voting, in e-voting voters would trust specifically to the blockchain technology which has no ability to be biased, which will ensure a highly credible and secure virtual voting environment. E-voting reduces the cost and the time which used to be consumed by using traditional voting (Al-madani, Gaikwad, Mahale, Ahmed, 2020). Voters would not have further need to go to the voting places, to wait in lines and lose their time.

E-voting would not just replace paper-based voting, but it would enhance voting quality as well. All the votes would be verified, and users would have an ability to count all the votes, or simply to see the sum of votes which were previously counted by program, not a person. By that way, the complete system becomes more convenient and reliable.

It would be time saving, as well as cost-efficient if it is taken into consideration that there is no further need for travel and waiting in lines to vote.

2. E-voting Implementation

There are specific blockchain networks which can be used to build solutions of their own, as well as there are tools that can help them in that process (Hijfte, 2020). It also must be known that blockchain is fool-proof technology and what is once written is not easy to change forcefully. This feature of blockchain makes it perfect for voting. By casting votes as transactions, a blockchain which keeps track of the tallies of the votes can be created. This way, everyone can agree on the final count because they can count the votes themselves, and because of the blockchain audit trail, they can verify that no votes were changed or removed, and no illegitimate votes were added (Banafa, 2020).

2.1. Blockchain

E-voting system should not be built as a centralized web application primarily because if we store its data (votes) inside the database, they can be completely changed or deleted entirely. Also, all of the code (especially one related to the election rules are in danger) can be changed/destroyed. The ideal environment for this system would be a decentralized one, on the blockchain, which will ensure that all votes are counted once, that they can't be changed, and that the field which contains the most votes wins the election.

In a decentralized application, the network is decentralized (it is peer to peer), data is decentralized because it is shared across the devices over the network, and code is decentralized because it is shared across devices over the network.

On the blockchain, data is distributed on the peer-to-peer nodes which talk to each other (it is decentralized), instead of laying on a central server. Data that is shared across to blockchain contains bundles of records, blocks, which are chained together and create a public ledger (it represents data on the blockchain). All nodes across the network work together in order to ensure that all data on the public ledger remains secure and unchanged. By that way, every time when a vote is given, the voter's account sends a transaction, and the vote goes to the exact candidate and it is recorded properly. All the data is shared across the blockchain, and all the nodes talk to each other, so we consider it as a database and network at the same time.

Blockchain technology is sometimes represented as a long DNA chain, periodically increasing in size when information related to new transactions is added. Transactions are grouped in blocks (where the name "blockchain" comes from), which are sorted in a sequential way with each block linked to the previous one. The chain is maintained by a network of nodes, which verify the validity of transactions and add them to new blocks in a process called mining (Gatteschi, Lamberti, Demartini, Pranteda, Santamaria, 2018).

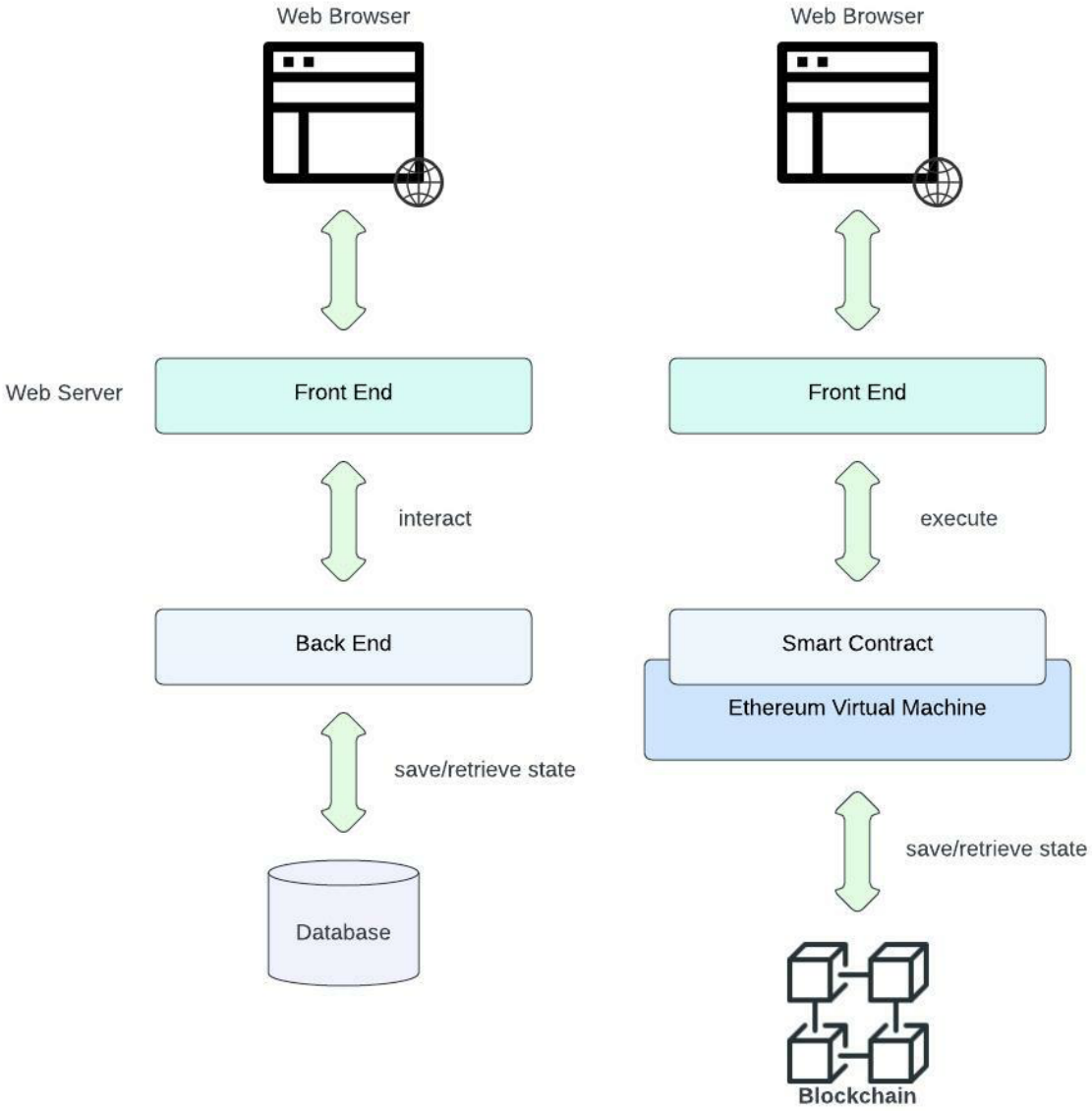

Figure1: Traditional Web Application VS DAPP (Mahdi Farnaghi Ali Mansourian, 2020)

2.2. Code

Code on the blockchain is shared and unchangeable. Etherium allows us to write code that we can deploy to the blockchain, which will be executed by the nodes. This will be the principle of how the code which manages all the election rules will be written and executed. All the code will be secured and unchangeable, which also supports the fact that rules of our election won't change.

Code of decentralized application is based on the smart contract. Etherium also allows us to write code which is executed on the Ethereum virtual machine with smart contracts (here the business logic of the application relies: reading and writing data, transferring value, executing business logic). Smart contract represents a kind of agreement which ensures that votes will be counted once, that

the votes can't be changed and that the most votes win the election.

Most blockchains are, at their core, massively distributed and publicly accessible databases; therefore, beyond ensuring that the data they store does not, in and of itself, betray user privacy, any research program that seeks to fully address blockchain privacy must additionally consider (at the very least) privacy for two fundamental types of transactions: reading data from and writing data to a blockchain (Henry, Herzberg, Aniket 2018).

A client-side application will be written in JavaScript, which will not be connected to the web server, but to the blockchain. The code on the decentralized application will be built by the smart contract (written in Solidity) which will be compiled and deployed to the blockchain. Accounts on the network will be allowed to use the application and participate/vote in the election.

2.3. Project Objectives

- Credibility
- Transparency
- Reliability
- Functionality
- Decentralization
- Time - saving
- Cost – efficient

E-voting system must have credibility when it comes to verifying the votes.

Blockchain is fool-proof technology and what is once written is not easy to change forcefully. This feature of blockchain makes it perfect for voting. By casting votes as transactions, a blockchain which keeps track of the tallies of the votes can be created. This way, users can agree on the final count because they can count the votes themselves, and because of the blockchain audit trail, they can verify that no votes were changed or removed, and no illegitimate votes were added (Banafa, 2020).

Transparency would be achieved by making counted votes visible to the users. Every user would be able to see the sum of the votes, or count it individually, but details regarding votes (users' data as names) would not be visible. By that way, privacy of every voter would be achieved, and the number of votes would be transparent.

All the votes would be counted by a program, and not by a person, which prevents wrong voting results and bias.

Functionality of the e-voting system would rely on the blockchain, which would have a main role in security and verification of voting data.

Also, blockchain provides a decentralized model that makes the network Reliable, safe, flexible, and able to support real-time services (Al-madani, Gaikwad, Mahale, Ahmed, 2020).

When it comes to the time and cost efficiency, e-voting would benefit all the voters. There is no further need to travel and wait in lines when it comes to voting.

2.4. Improvements

The potential improvements on this project would be working on the user registration segment. The registration environment has to be highly secured; each account created must be unique and assigned to the one and only specific user. There should not exist a possibility for one person to create more than one account. Also, there should not exist the possibility for multiple persons to have one user account either. Each account has to strictly and in detail define its user.

These improvements are classified as additional work which will be developed in the future, while the focus of the current project is specifically on the voting segment.

3. Conclusion

This project represents a logical solution to the current voting problems by giving special importance to the security, credibility, transparency, reliability and functionality of the voting system. Also it solves the problem regarding the time and cost of the elections, for both; voters and voting organizations. While the primary focus of this project is based on the voting connected to the elections; other voting types can also be performed as well as organization voting, school voting etc. A large proportion of the population in the developing world can benefit from blockchain (Kshetri, Voas, 2018). By focusing specifically on e-voting, that voting system can serve not just for the government purposes as elections, but for all the other voting types as voting in schools, society organization voting etc.

The future work and improvements on this project are possible and will be focused on developing an even more secure environment by focusing on users' (voters') registration which should also support security and credibility of each user, with preventing the possibility of fraud and counterfeiting.

References

Al-madani, A. M., Gaikwad, A. T., Mahale, V., & Ahmed, Z. A. T. (2020). Decentralized E-voting system based on Smart Contract by using Blockchain Technology. In 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC) (pp. 176-180). IEEE. https://ieeexplore.ieee.org/document/9299581

Banafa, A. (2020). Blockchain Technology and Applications. In River Publishers. IEEE. https://ieeexplore.ieee.org/book/9218853

Farnaghi, M., Mansourlan, A., (2020). Blockchain, an enabling technology for transparent and accountable decentralized public participatory GIS In Research Gate. Elsevier. https://doi.org/10.1016/j.cities.2020.102850

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain or Not to Blockchain: That Is the Question. In IT Professional (Vol. 20, pp. 62-74). IEEE. https://ieeexplore.ieee.org/document/8338007

Henry, R., Herzberg, A., & Kate, A. (2018). Blockchain Access Privacy: Challenges and Directions. In IEEE Security & Privacy (Vol. 16, pp. 38-45). IEEE. https://ieeexplore.ieee.org/document/8425613

Košt'ál, K., Bencel, R., Ries, M., & Kotuliak, I. (2019). Blockchain E-Voting Right: Privacy and Transparency with Public Blockchain. In 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS) (pp. 592-595). IEEE. https://ieeexplore.ieee.org/document/9040770

Kshetri, N., & Voas, J. (2018). Blockchain in Developing Countries. In IT Professional (Vol. 2, pp. 11-14). IEEE. https://ieeexplore.ieee.org/document/8338009

Singh, A., & Chatterjee, K. (2018). SecEVS: Secure Electronic Voting System Using Blockchain Technology. In 2018 International Conference on Computing, Power and Communication Technologies (GUCON) (pp. 863-867). IEEE. https://ieeexplore.ieee.org/document/8675008