AGM Voting System using Ethereum's Blockchain

Name: Sultan Ahmed Ali Alkaabi

Email ID: sultanalkaabi61110@gmail.com

Phone: +968 99723242

Abstract

Electronic voting can be provided by end to end verifiability as depending of voters if they can verify the votes as were suitably counted and get correctly of their results on the election. There were many potential electronic voting systems build with cartelized systems. In this proposal we present electronic voting solution to Muscat Clearing and Depository Company that is built by Ethereum platform to use all features of smart contracts that enable to provide the rules close to election ballots. While these ballots can be both universally and independently maintain and verifiable necessary rules and standards on the blockchain which is immutability. These can achieve more benefit of centralized systems which keep voters with more privacy and security.

Introduction

Current E-voting systems can be built by serious designs flaw that are centralized designing, which mean third party control the system that includes all of database and monitor the tools to authenticate the voting results. However, lack of independently verifiable systems when the voters try to mark their ballot to vote, and they should put their trust voting with correct organization to be counted and recorded. This make them difficult when lack of independently verifiable for centralized output to get more trustworthiness as required from all voters, that possibly limits voter participations, and also could cast doubt as to publish election outcome. [1]

There are two types of existing Electronic Voting two; one is to use specific machines at polling stations, other hand the ballot paper and casting the vote via Internet. Previous tends regarding to Direct Recording Electronic that can normally display the ballot option with screen to be activated and updated via voters and then the records of voting keeping on the memory process the next steps of electronic voting. Though, several electronics face some problems of how can modify all applications and possibly to insert malicious code with security issue. The voting on the Internet, could face privacy issues, the voting under duress or corruption and voter should feel the system is very robust security to trust them. [2]

In this report we plan to design end to end verifiable technology as built on e Blockchain and use Ethereum platform. This system will allow the voters to register on Ethereum address then can be added the list permission addresses on smart contract. When the ballot start, a voter can modify allocation of his/her vote via smart contract until ballot ending. Regarding to Ethereum nature of smart contracts, the voter can prove and ensure their election is in robust security as no votes have been modified when the ballots over. Everyone can confirm number of their votes users via querying that written on smart contract with certain addresses that are added to smart contract. So, validity all votes will be correct and not modifying.

Ethereum platform give us to deploy decentralized applications with no 3rd party. The decentralized application has many purpose to do on other use case, such as peer-to-peer payment. The benefit of decentralized systems like blockchain are not been controlled via any individuals or central system. Because the blockchain technology is immutability which mean 3rd party cannot change or modify the data Also the other benefit of blockchain technology is no central failure point for Dapps which run all nodes via the network. Also the most importing benefit to use blockchain technology on electronic voting that using secured hashing cryptography to give the applications robust protected against any malicious attacks or fraudulent activities. And keep zero downtime the voting to be up and switched on all the period of voting. [3]

Electronic voting design

In this report, we propose end to end verifiable solution of electronic voting to build the on Ethereum Blockchain platform and our design is as following bellow:

A) Ballot: 1) The ballots on the election are designed depend the size of voters as will decide upon. 2) All ballot will be provided with smart contract to Ethereum blockchain of voting options. Solidity is programming language to write smart contract

B) verification voters before election: 1) The voter will register remotely after provide valid IDs 2) External registrars can generate via user id that is used by log in the voting system and these user IDs is then tangled with any correct ballots voters.

C) Registration: 1) All voter can log into voting system by user ID that directly change login.

2) All voters then will register voting via Online system for all ballots as eligible for.

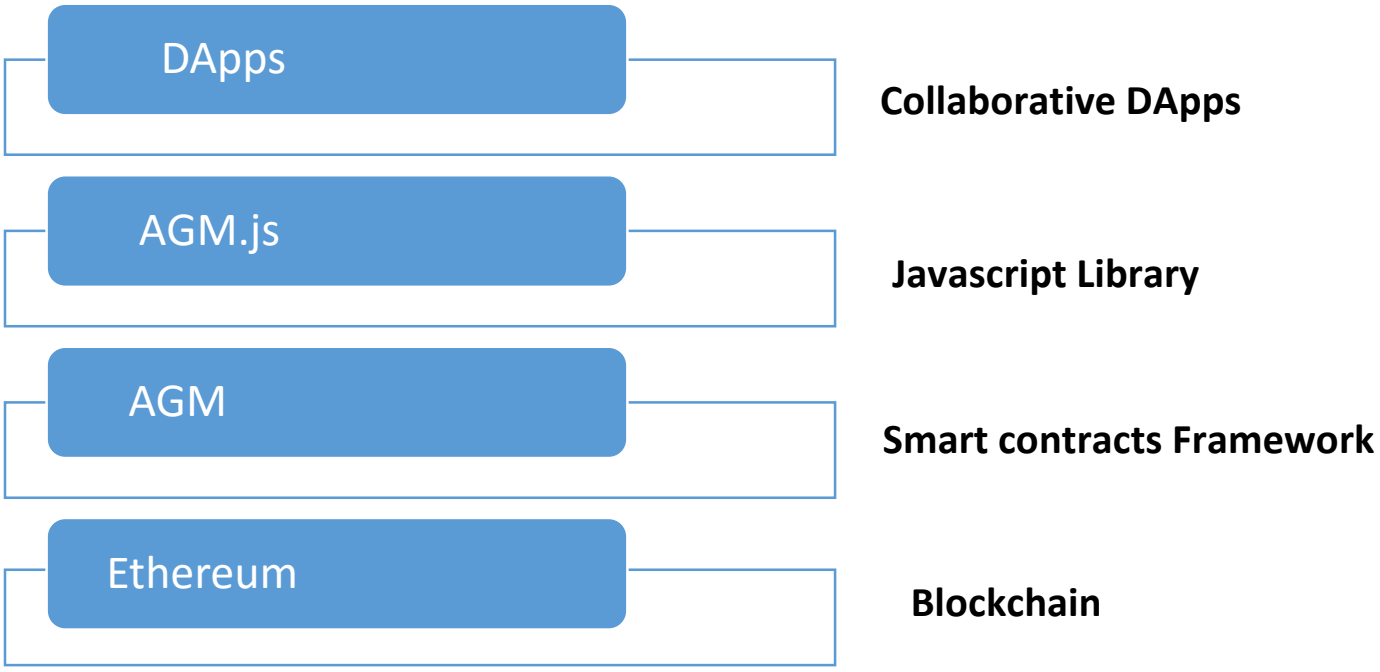
3) unique address of Ethereum will generate and validate to only linking with correct user ID.

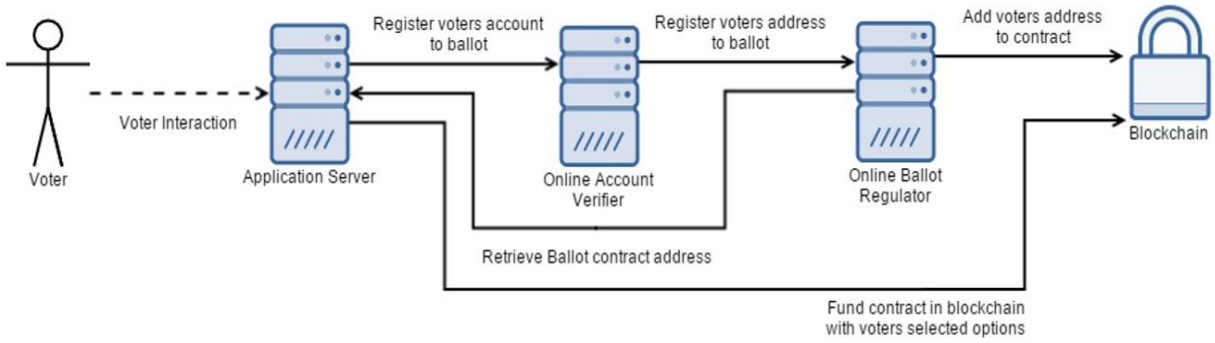
4) The address of users will add into the ballots as written on smart contract

5) The address will fund enough Ether with all voters to count their vote.

D) Voting: 1) Once the voters decide to cast of their vote they will present interface mirror on option on smart contract. 2) When voters are selecting the options, smart contract will fund the voters to be selected options and the voter's choice will be immutably filling via blockchain that should be verifiable by every user.

E) Election result: When an election end, no more votes can add or delete any candidate as design of smart contract framework.





References

[1] Moses, L. B., Goré, R., Levy, R., Pattinson, D., & Tiwari, M. , "No More Excuses: Automated Synthesis of Practical and Verifiable Vote-Counting Programs for Complex Voting Schemes," *In International Joint Conference on Electronic Voting,* pp. 66-83, 2017.

[2] Cortier, V., Dragan, C. C., Dupressoir, F., & Warinschi, B, "Machine-checked proofs for electronic voting: privacy and verifiability for Belenios," *In 2018 IEEE 31st Computer Security Foundations Symposium (CSF),* pp. 298-312, 2018.

[3] Ernest, A., Hourt, N., & Larimer, D, "Blockchain electronic voting system and method. U.S. Patent Application," *15/298,177,* 2017.