Blockchain based E-voting using Smart Contract

Kazi Sadia, Rajib Kumar Paul and Md. Masuduzzaman
American International University-Bangladesh
Email: gazirisha@gmail.com,krajib60@gmail.com,masud.prince@aiub.edu

Background

This protocol proposes a fully decentralization e-voting system based on the blockchain technology and using smart contract. This protocol integrates the blockchain paradigm and notion of the smart contract into the e-voting system to deal with security issues, accuracy and voters' participation during the vote. The protocol results in a transparent, non-editable and independently verifiable procedure that discards all the intended fraudulent activities occurring during the election process. Also, this proposed protocol emphasizes on all the issues of e-voting based on blockchain that were previously discussed in other related papers.

Blockchain is the distributed peer-to-peer network that works under the consensus of the majority of the participants within the system. The "Proof of Work" makes it hard for the hackers to edit or add malicious blocks to the network. E-voting reduces the issues of the traditional voting system such as-invalid ballots, lack of privacy and transparency, time consumption and greater involvement of third party. Also, the exhaustion of the voters is reduced as voters no longer has to continue with the tiring phases of voting. The smart contract is an executable code that runs on the blockchain to trigger actions to take place when pre-defined conditions are met. Smart contract facilitates the work reducing the need of acceptance of the third party in order to continue with a task. The concept of smart contract is utilized to prevent the involvement of third-party completely ensuring complete decentralization. Also, random decisions for voting are generated that helps prevention of coercion.

Motivation and Problem Formulation

Secure and healthy elections play a vital role behind the development of a country and the welfare of citizens. Thus, elections must be carried out effectively and efficiently. Elections these days are very less secured and buying votes is a common issue. Manual election process is a time consuming activity and also there is no guarantee of hundred percent accuracy. Human errors are common issues in elections. In this paper, blockchain and smart contract helps the process of election to work as per desired to resolve these issues. Blockchain technology these days is a very interesting and attractive topic that has already taken over or disrupted various industries. It has been used in cases of tracking of important data or transactions. Since, the votes of the voters are very important data, any sort of issue might result or impact the process. Thus, we can use the blockchain to take over the election process to develop a transparent, reliable, controlled protocol. The figure below illustrates the basic functionalities of the protocol as an overview.

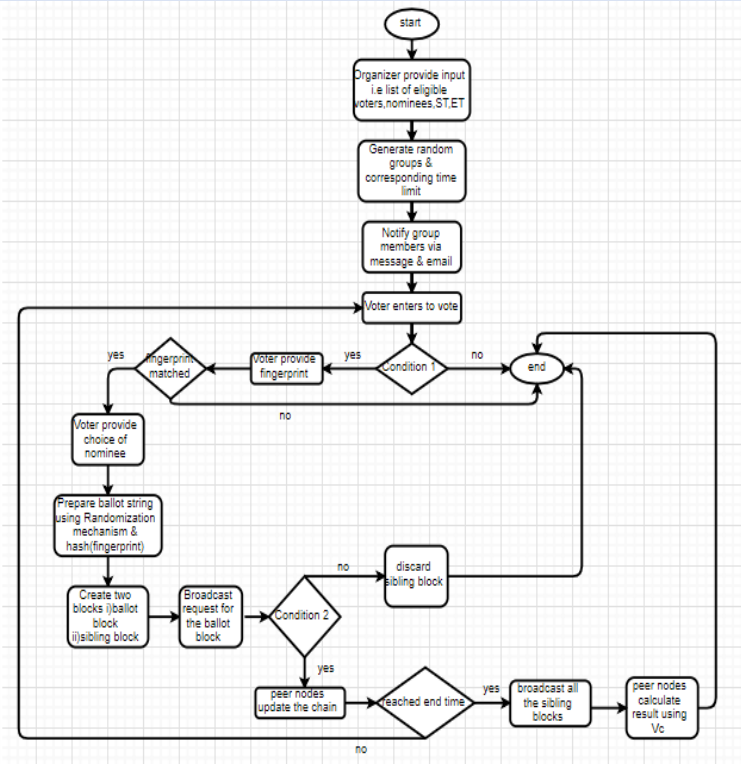

start
Organizer provide input i.e list of eligible voters,nominees,ST,ET
Generate random groups & corresponding time limit
Notify group members via message & email
Voter enters to vote
Condition 1
yes
no
end
Voter provide fingerprint
fingerprint matched
yes
no
Voter provide choice of nominee
Prepare ballot string using Randomization mechanism & hash(fingerprint)
Create two blocks i)ballot block ii)sibling block
Broadcast request for the ballot block
Condition 2
no
discard sibling block
yes
peer nodes update the chain
reached end time
yes
no
broadcast all the sibling blocks
peer nodes calculate result using Vc

Fig 1.1: Flowchart representation of the functionalities

Condition 1-Verify whether the voter is in the group X and the flag of X is true (flag true → X is currently specified for voting). Also, check whether the voter is in the eligibility list or not.

Condition 2- Mathematical computation (proof of work) is done. Also, verify whether the voter has casted vote previously or not and check the ballot is in correct format or not.

NOTE: Choice of nominee is hidden in the ballot string. The arrangement of the choice is hidden in the variable Vc, the arrangement is prepared by random number generation. Thus, nobody has any idea of the user's choice until the end of the election.

Proposed Methodology

Pre-voting phase:

The organizer is the actor responsible for collecting the list of the eligible voters and nominee based on the desired condition (if any). The list of the voters should contain voter's name, fingerprint and any other information based on the direction of the election commission. Organizer provides the list of eligible voters, nominees, start date-time and end date-time as an input on the genesis block. Genesis block is the parent block of the blockchain. The program (code) is previously integrated within the blockchain. On reaching the start date-time, the code is executed, and corresponding activities are performed. Voters are grouped randomly, and random time is generated for each groups. Voters of specific groups are notified via email and message; a time limit is set for each group. The flag remains true during the time limit of the group. No one is allowed to vote after the flag becomes false i.e. the time limit exceeds. The flag becomes false automatically once all the voters within the group is done with their voting.

Voting Phase:

As the voter approaches to vote providing his/her name (public key of the voter), it is verified (within the code) whether the voter is in the group with a flag value of true and the voter is in the eligibility list. On verifying, the voter is to provide his/her fingerprint (private key of the voter) as a need of verification that no other people other than the voter is casting his/her vote. The fingerprint is matched with the one provided in the eligibility list, the fingerprint sensor is used to figure out the coordinates. The coordinates are then matched, if it matches then according to the figure 1.2, the binary value of the coordinates is obtained. The hash of the binary value is basically the unique voter identification in the ballot within the block.

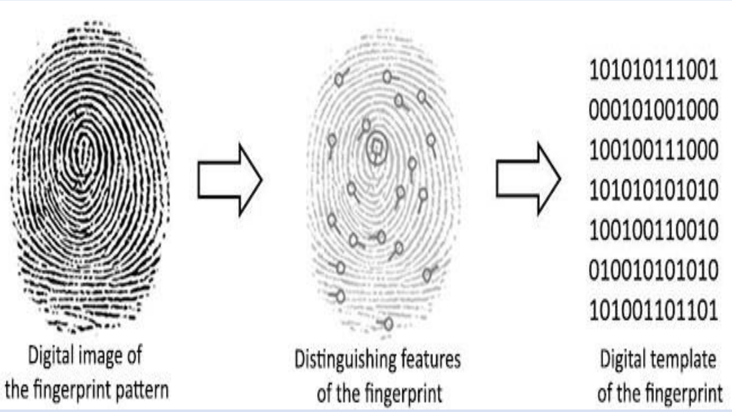
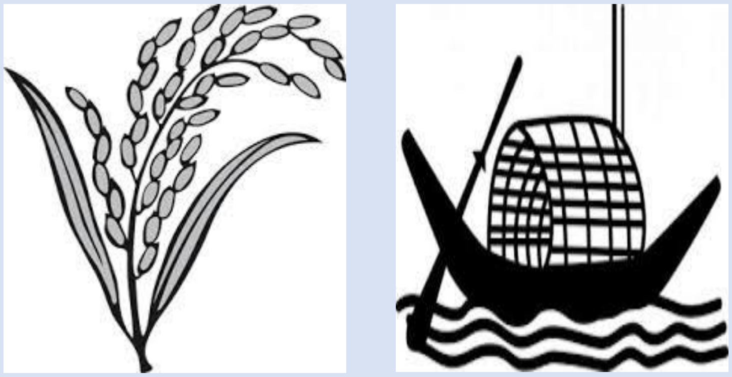

101010111001
000101001000
100100111000
101010101010
100100110010
010010101010
101001101101
Digital image of the fingerprint pattern
Distinguishing features of the fingerprint
Digital template of the fingerprint

Fig 1.2: Formation of the binary value of fingerprints

The nominees are represented by their representative logo, the logos have a binary value which is basically selected and worked with when chosen. Fig 1.3 shows an example of the representation. The number of 1's and 0's in the value must be same otherwise it is possible to guess the choice of nominee in the ballot string. If the representation does not remain consistent then increase the number of bits in order to get different representation for equal numbers of 0's and 1's. Example- Three bits with two 1's and a 0 will have representations – 110,011,101 so three logos can be represented by these.



Binary Value → 1010 Binary Value → 1100

Fig 1.3: Binary representation of nominee logos

The voter selects his/her choice of nominee and the ballot is ready to be prepared. A ballot is designed to have a ballot number in it. The ballot consists of the voter →hash (fingerprint binary) and the ballot string. The ballot string is prepared by the execution of a function inside the code. The ballot string has two sub-strings, choice string and the random string. The choice string consists of the nominee choice hidden within other values. The random string is randomly generated 0/1 values. The ballot string is prepared in two phases, the following are:

NOTE: The total number of bits has no restriction. 16-bit is just an example. Greater number of bits is secured as chances of similar generation of numbers decreases.

Consider a 16-bit ballot string of which 8 bits are choice string-the red ones and 8 bits are random string- the black ones. The random string is integrated to ensure differentiation of each ballot string.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

i) If n bits are representing each logo then n random numbers are generated from 0-7, the binary value of the logo is arranged in the generated random value indexes of the ballot string i.e.

Number of bits representing each logo→4
Random numbers→ 4,5,7,1 (4)→Vc→opening value
Nominee choice →binary value of logo→1100

0				1	1		0								
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

ii) Generate another number between 1/0. Fill that number in the other four indexes. Example-1

0	1	1	1	1	1	1	0								
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

iii) Generate random numbers randomly from 1/0 and put on the indexes (8-15) suppose, 11001010

0	1	1	1	1	1	1	0	1	1	0	0	1	0	1	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

The ballot string is prepared, and the choice is hidden inside the string. The choice is recognized by the Vc only. One block is created containing the ballot and another sibling block is created that consists of the voter→hash (fingerprint binary), the ballot number of the broadcasted one and the opening value.

As the voter casts the vote i.e. broadcast the ballot containing block, the peer nodes start to work for the proof of work for the block. The one completing earlier then also verifies whether the voter has casted vote earlier and whether the ballot is in correct format. After verification, the ballot contained block is added in the blockchain and peer nodes verifies and updates their block. Majority is taken in consideration. The sibling block is not broadcasted at the voting phase. This not broadcasting issue is pre-defined earlier in the code.

Experimentation and/or Theoretical

Following are the security analysis related with the protocol:

i) Voter's privacy: Voter's fingerprint's hash is the only information that is kept in the block broadcasted so attacker has no knowledge about it. No one is aware of others choice, so no unfair means takes place. Also, voters cast vote randomly (dependent upon code executed) so the one intended to manipulate fails on this. Moreover, fingerprint is the most secure metadata of a person and hash function (SHA-256) cannot be backtracked and is the most secure.

ii) Ballot forgery: Ballots checked by the peer nodes and no third party involved. Thus, no chance of any fraudulent activity. Ballots casted by unfair means are rejected by the whole network. Majority is taken into consideration so is not possible to manipulate the majority.

iii) Accuracy: Results are calculated by the peer nodes therefore accuracy is ensured; the results are completely visible. Blocks cannot be edited or deleted once broadcasted so no probability of lost vote or change vote. The whole election takes place sequentially by the execution of codes.

iv) Choice privacy: Voter's choice is randomized to avoid recognition. Choice recognition can be a threat for the voter so securing the choice is a mandatory task. Also, Vc of each ballot is broadcasted at the end. An earlier representation of the choices would have an impact and the progress of the election will be exposed and might be influenced by any means. Also, the number of 0's and 1's is always kept same for every representation of nominee/logo due to avoid chances of predicting the choice. Furthermore, number of bits are increased when various representation is not possible.

v) Ballot separation: Ballots consisting of same choice string is separated by the random string and the random number generated within the choice string.

vi) Coercion prevention: It is prevented as attacker has no knowledge about when the voter will vote. Voters are selected randomly, anyone other than the voter has no knowledge about their timing, so manipulation is tough.

vii) Double votes: Voters are checked if they have voted before or not before broadcasting any block. This is again ensured by the peer nodes within the system. Every single node verifies each vote before updating the chain so voting more than once is prohibited and the initial verifications are done by the code itself.

viii) Transparency: Every action take place under the blockchain, peer nodes verify and monitor the process. Everything is open and verifiable by the citizens of the nation. No authority is in control.

ix) Complete decentralization: No third party are related with any of the processes once the voting starts. The peer nodes are the ones playing the roles of the third party. Moreover, the program specifies each action accordingly so no need of third party.

x) Network load: Groups are formed in such a way that it does not arise the problem of network issues and time limit should also be adjusted so that voters will be able to cast their vote.

Findings

The followings are the expected findings that are suggested:

i) Fully decentralization without a single third party involvement once the election starts.

ii) Transparency in every actions performed, peer nodes and the codes verify every actions.

iii) Voter's choice kept encoded so has no possibility of threat and exposure of election progress.

iv) Counter are the voters or peer nodes themselves so no chance of frauds and unfair means. Thus, accuracy and reliability is obtained.

v) Non-eligible are discarded at the beginning. Double votes are also discarded therefore, unfair means are reduced.

vi) Prevention of coercion is obtained as attackers/people working for any of the nominees cannot buy votes/manipulate/force voters due to the technique of randomly voting in groups.

vii) Individually verifiable as each voter can verify whether his/her vote is added on the block or not.

viii) Voters themselves know about their identity, others are unaware about it, so voters remain anonymous.

Transparency and prevention of coercion are obtained together considering all the other necessities are fulfilled.

Conclusion and Future Work

This protocol uses the potential of blockchain technology in combination with the smart contract concept to figure out an easier, secured, efficient mechanism without the involvement of any third party. It would have been nice if the protocol could have been discussed in more detail. Any technique other than the providing of fingerprint while voting is highly appreciated and would help making the process easier. The security issues must be taken in consideration.

References

[1] Yi Liu and Qi Wang, "An E-voting Protocol Based on Blockchain"

[2] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy"

[3] Antony Lewis, "A Gentle Introduction To Blockchain Technology"

[4] Maher Alharby, and Aad van Moorsel1, "BLOCKCHAIN-BASED SMART CONTRACTS : A SYSTEMATIC MAPPING STUDY "

[5] "General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia"

[6] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"

[7] Michael Crosby ,Nachiappan , Pradan Pattanayak , Sanjeev Verma , Vignesh Kalyanaraman , "BlockChain Technology: Beyond Bitcoin"