A Competent and Accurate BlockChain based E-Voting System on Liquid Democracy

1st Samika Kashyap
dept. of Computer Science and Engineering
SRM Institute of Science and Technology
Kattankulathur, Tamil Nadu, India
samikakashyap_yogendra@srmuniv.edu.in

2nd Dr. A Jeyasekar
Associate Prof., Dept. of Computer Science and Engineering
SRM Institute of Science and Technology
Kattankulathur, Tamil Nadu, India
jeyaseka@srmuniv.edu.in

***Abstract*—In order to avoid the demerits of Direct Democracy (DD) and Representative Democracy (RD), recently a democratic reform called Liquid Democracy (LD) was introduced which is a combination of DD and RD that gives the people full decisional control either by voting directly or by entrusting their voting power to a representative for some political ideologies or bills. Our work attempts to study the democratic models based on accuracy and competence parameters. Further a liquid democracy voting protocol is proposed and implemented on a block chain based distributed ledger which is capable of fighting attacks of integrity and non- repudiation while ensuring authenticity of the votes. This system would be transparent thus ensuring people about the legitimacy of their delegation of votes and direct votes. This is a big step up from the current existing system of EVM's that do not guarantee this level of security.**

***Index Terms*—Liquid Democracy, Blockchain, Authentication , Security, Delegative voting**

I. Introduction

Democracy was literally defined as "Rule by people", a system that allows the people to express their preferences. To solve the limitations of DD [1] and RD [2], recently a democratic reform called Liquid Democracy (LD) was introduced [3]. Blockchain is the perfect technology stack that can be used to implement Liquid Democracy. The paper explores the competency and accuracy of a Liquid Democracy model with other democratic models through extensive research. Green-Armytage [4] had constructed an argument in the favor of delegative democracy stating that the proposed delegative democracy algorithmically. Kahng et al. [5], discussed the mathematical approach to liquid democracy and pointed out its superiority to other democratic models. From the above mentioned works it is safe to say that Liquid democracy provides better competency and accuracy as compared to other democratic models.

II. Proposed work

A. Design Requirements

The entities required in the election process with their associated user roles are discussed below

978-1-7281-7091-6/20/$31.00 ©2020 IEEE

- Ballot : This contains the list of all the votes submitted by the voters in favour of a chosen proposal for a given election.
- Proposals : This is a structure or a promise that makes up the criteria on which the votes will be casted.

User roles are:

- Administrator : They are responsible for invocation of the proposal or smart contract.
- ProposalMakers : ProposalMakers are leaders that submit their proposals in the form of a contract as a promise for a given election.
- Individuals : These are people with lesser knowledge of the topic of election that delegate their voting power to representatives.
- Representatives : These are people that are well versed with the topic of election. They all have a voting weight assigned to them that is in proportion to the number individuals that have delegated their votes to them.

B. Liquid Democracy voting Protocol

The paper has proposed a *LiquidDemocracyVoting* Protocol which is a four round protocol. A description of the liquid democracy network is a graph [4], where all voters $(v_1, v_2...v_n)$ constitute a list of eligible participant in the election and each participant has the following information:
k_r : their private or reserved key , known only to them.
k_u : their public key

1) Round 1: Administrator publishes the following information on a common board : Set of eligible proposal makers P where, $P = \{P_1, P_2..P_n\}$ and a set of voters V.

2) Round 2: Each interested proposal maker P_i broadcasts their public key k_{up} and non-interactive zero knowledge proof NIZKPk_{rp} [6] to prove knowledge of k_r as a source of authentication to the administrator. P_i then submits their proposal signed by k_r. These proposals should be stored in a secured and tamper proof manner. All members in the system can access these proposals and all of them are involved in the verification of the identity of P_i.

3) Round 3: Voters authenticate themselves by broadcasting their public k_{uv} and submitting a NIZKP k_{rv}. Voters then register to a particular ballot using k_r as their signature. Each voter verifies the signature and stores the information securely regarding all the other voters.

4) Round 4: Voters then delegate their votes to other voters or vote independently on a proposal. Each voter's action is signed using $k_{rv}$and the validity of this is checked by all members present. Each member also stores a record of all the actions made to overcome the lack of trust in the system. After verifying all the actions and the identities a final tally of the votes is done collectively by the entire system, ensuring that there no center place of complete control. The distributed and decentralized behaviour of the *LiquidDemocracyVoting* makes it ideal to be implemented over blockchain. Ethereum's private blockchain has been used to implement this protocol.

III. Blockchain Implementation of LiquidDemocracyVoting protocol

For each user role, a different view using HTML and javascript have been created, which provides users a browser interface for all election related interactions. The protocol is executed in 5 stages. An outline of it is presented in "Fig. 1". Two scripts coded in JavaScript, one script for html connections and one for migrations, as well as an HTML page have been created created. This system assumes that the roles described above that use this system all have either a virtual wallet like Metamask or are running an Ethereum node to interact with our Blockchain based platform. The implementation utilizes the Ethereum's Web3 framework, this provides already built in features and functionalities for managing transactions. There is a single smart contract written in Ethereum's Solidity language called Ballot.sol, it implements the proposal submission, delegation of votes followed by voting and then finally the tallying processes, through its different stages. The use of timers is implemented for marking the commencement and finish of a stage.

IV. Performance Analysis

The above implementation was also deployed on the Ropsten Test network for Gas Cost Estimation Analysis. A test network was selected for performance analysis as this would mimic the system after its maturity thus providing more accurate result sets. We sent around 150 transactions on this and observed variations in gas cost while increasing the number of proposals. A general positive trend of very slight increase in gas cost was observed with increasing proposal count. This can be further visualized in the graph "Fig. 2"

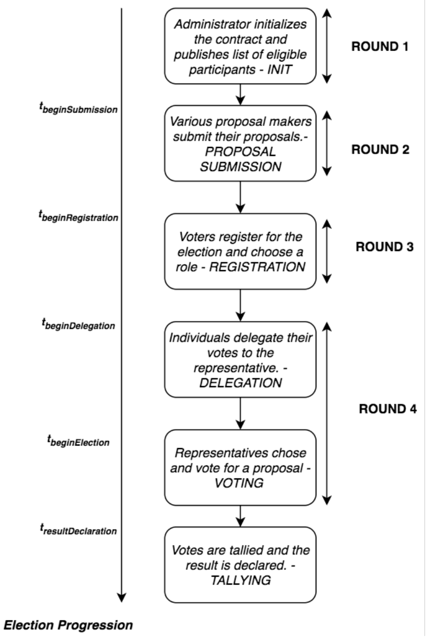
Administrator initializes the contract and publishes list of eligible participants - INIT
ROUND 1
$t_{beginSubmission}$
Various proposal makers submit their proposals.- PROPOSAL SUBMISSION
ROUND 2
$t_{beginRegistration}$
Voters register for the election and choose a role - REGISTRATION
ROUND 3
$t_{beginDelegation}$
Individuals delegate their votes to the representative. - DELEGATION
ROUND 4
$t_{beginElection}$
Representatives chose and vote for a proposal - VOTING
$t_{resultDeclaration}$
Votes are tallied and the result is declared. - TALLYING
Election Progression

Fig. 1. Stages and Election Progression of LiquidDemocracyVoting Protocol

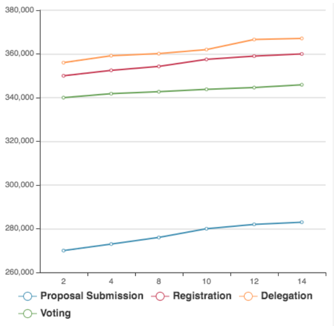

Fig. 2. Gas Cost Analysis With Increasing Proposal Count

V. Conclusion

In today's democratic system,there is, in fact, no practical way to hold representatives accountable in real time when they fail to keep their electoral promises. If only there was a system to automatically force them to step down, or to at least pay a price, for blatant dereliction of the representative's duties. Liquid democracy and Blockchain technology make this possible and this paper has proposed a feasible implementation of it. A liquid democracy protocol was proposed, which can be applied to any voting system and further a block chain based implementation was designed as a proof of concept which is capable of providing the integrity and non-repudiation that is imperative to the current practices of electoral systems. This is a step towards incorporating accountability and trust which has been missing from our voting system and electoral democracy since the beginning of time.

References

[1] Budge, Ian. "Direct and representative democracy: Are they necessarily opposed?." Representation 42.1 (2006): 1-12.
[2] Christoff, Zoé, and Davide Grossi. "Binary voting with delegable proxy: An analysis of liquid democracy." arXiv preprint arXiv:1707.08741 (2017).
[3] Ford, Bryan Alexander. Delegative democracy. No. REP_WORK. 2002.
[4] Green-Armytage, James. "Direct voting and proxy voting." Constitutional Political Economy 26.2 (2015): 190-220.
[5] Kahng, Anson, Simon Mackenzie, and Ariel D. Procaccia. "Liquid democracy: An algorithmic perspective." Thirty-Second AAAI Conference on Artificial Intelligence. 2018.
[6] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. M. Odlyzko, editor, Crypto'86, volume 263 of LNCS, pages 186–194. Springer, 1987.