AN E-VOTING PROTOCOL BASED ON BLOCKCHAIN

By

Sourav Mandol

Roll: 1607044

&

Suman Mia

Roll: 1607045

Supervisor:

Dr. Kazi Md. Rokibul Alam

Professor

Department of Computer Science and Engineering

Khulna University of Engineering and Technology.

Signature

Department of Computer Science and Engineering

Khulna University of Engineering and Technology

Khulna 9203, Bangladesh

1. Introduction

Blockchain based E-voting technology provides a platform for creating a highly secure, decentralized, anonymized, yet auditable chain of voting, used presently in cryptocurrency systems.

To understand electronic voting, it is convenient to consider four basic steps in an election process: **ballot composition**, in which voters make choices; **ballot casting**, in which voters submit their ballots; **ballot recording**, in which a system records the submitted ballots; and **tabulation**, in which votes are counted.

In comparison with the traditional paper-based voting, remote e-voting is environmentally friendly, real-time counting and processing, less error-prone. Meanwhile, as the time and efforts to vote decrease, the overall voter turnout may increase [5]. The concept of electronic voting appeared in 1981. In nearly forty years of development, security and privacy have always been the focus of electronic voting research. Aiming at the security of electronic voting, many researchers propose a large number of secure electronic voting schemes using various technologies such as informatics and cryptography.

2. Related Works

There has been a lot of work on remote e-voting protocols using cryptographic tools. In some case trusted third party was involved for casting and counting votes. However, a powerful TTP may also become the vulnerable spot of the whole system. A few efforts have been made to combine an e-voting protocol with the blockchain paradigm to design a voting protocol without a TTP, which provides anonymity and verifiability as well [1]. Zhao and Chan proposed a voting protocol [6] in 2015, which introduces a reward/penalty scheme for correct or incorrect behaviors of voters. Although the protocol has some limitations, this is the first attempt to combine e-voting with blockchain. Mukherjee, Prodipta Promit proposed a Hyperledger fabric-based e-voting system in 2020[2]. But they have some privacy issues for voter about the voting information.

3. Motivation

Blockchain is distributed, immutable, incontrovertible, public/private/permissioned ledger. That's why this technology gives these following extra features:

No Failure: Ledger used by blockchain exists in many different locations. So, no single point of failure in the maintenance/vote counting of the distributed ledger.

Distributed Control: There is always a distributed control over who can append new vote to the ledger.

Prevent Tempering: Any proposed "new block" to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.

Mining & Consensus: A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger**.**

Dependability: Guaranteed by the cryptographic algorithms and the practical consensus mechanisms of blockchain, the protocol protects the voting procedure against dishonest behaviors and attacks.

4. Objectives

Our proposal is not to change the whole voting system but integrating these new following features with the voting system-

- **Decreasing the dependency on TTP (Trusted Third party):** And coming up with a flexible, feasible voting mechanism to satisfy almost all the main requirements of normal voting system.
- **Auditability:** As the whole process will be recorded on blockchain.

- **Anonymity:** Only voters can know the information of their own vote.
- **Transparency:** Due to the transparency of blockchain, the whole procedure is open to the public. This leads to more fairness and validity.
- **Individual Verifiability:** Each voter is able to verify individual voting procedure, e.g., whether his/her ballot has been cast and recorded successfully, counted in the final tally, etc.

5. Required Security Tools

In this session we introduce our following three main techniques used in our protocol-

- **Blockchain Based Network** (For transparent and decentralized network)
    - Hyperledger Fabric
- **Blind Signature** (preserve voters' choices during the election.)
- **Consensus Mechanism** (For getting final feedback)
    - Proof of Authority (POA)

6. Methodology

6.1 Hyperledger Fabric

We proposed Hyperledger Fabric as FAAS (Framework As A Service). This faas contains these 3 following stages:

- Hyper-ledger Fabric Framework
- Micro-services Layer
- RESTful APIs Layer

Hyperledger Fabric is intended as a foundation for developing applications or solutions with a modular architecture. Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play.

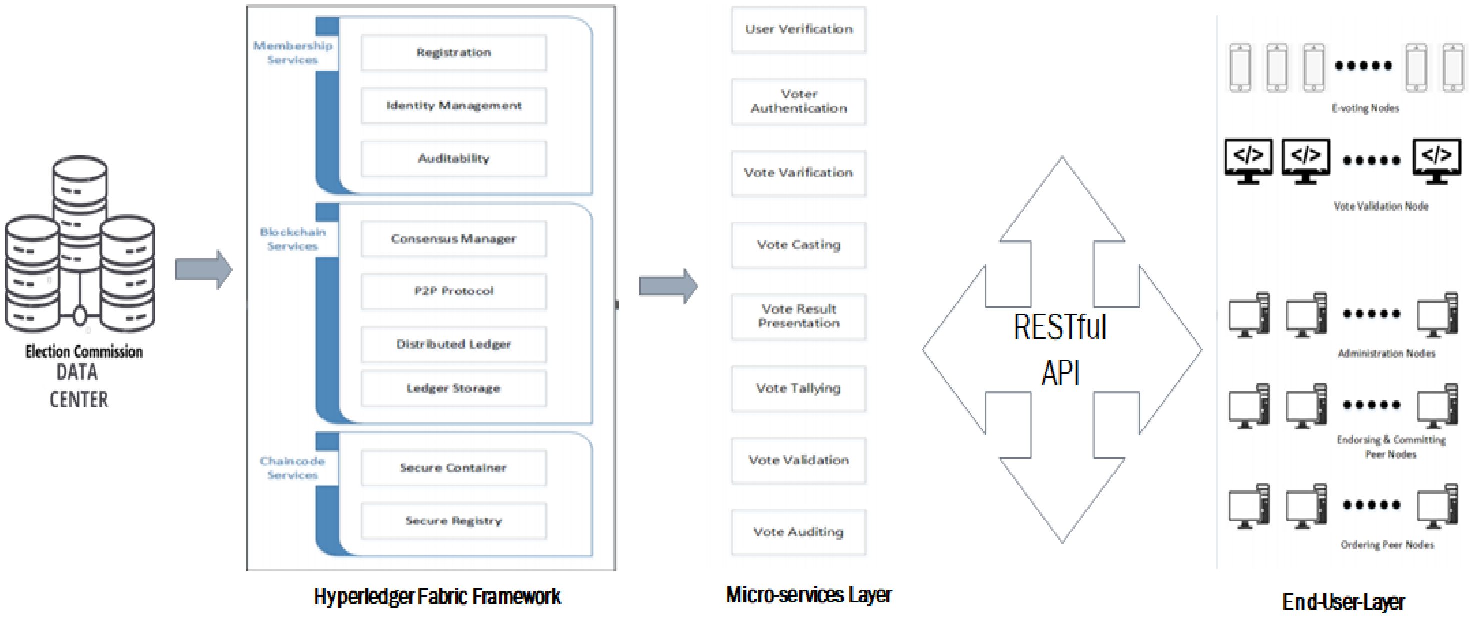

Fig. 1. A top level architectural design of a E-voting system using Hyper-ledger Fabric based Framework as a Service (FaaS).

6.1(A) Hyperledger Fabric Framework

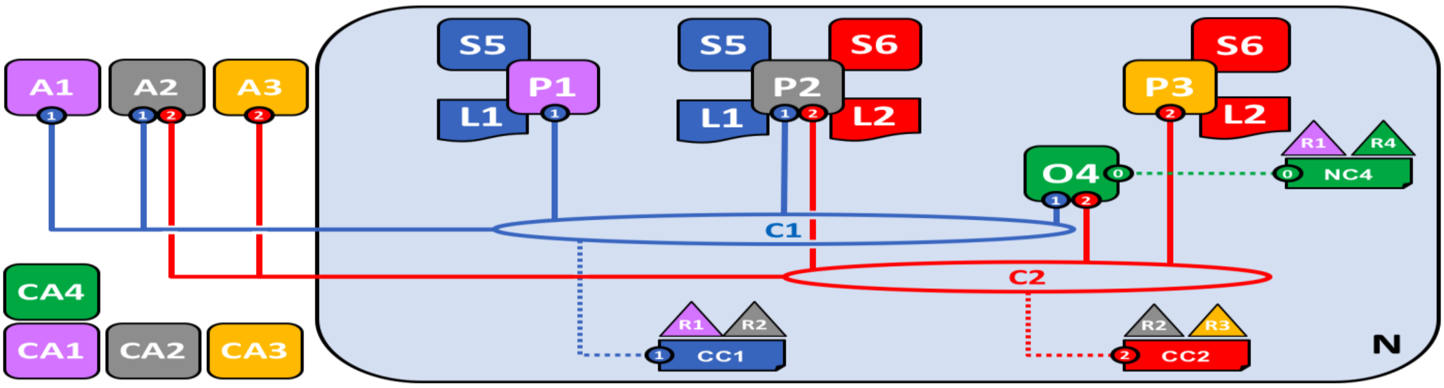

Fig.2: Hyperledger fabric Framework

This is the foundation which makes the e-voting solution possible, with the use of Hyper-ledger Fabric. Hyper-ledger Fabric is a blockchain framework implementation which enables the development of blockchain information system solutions by using a modular architecture approach.

6.1(B) Micro-services Layer

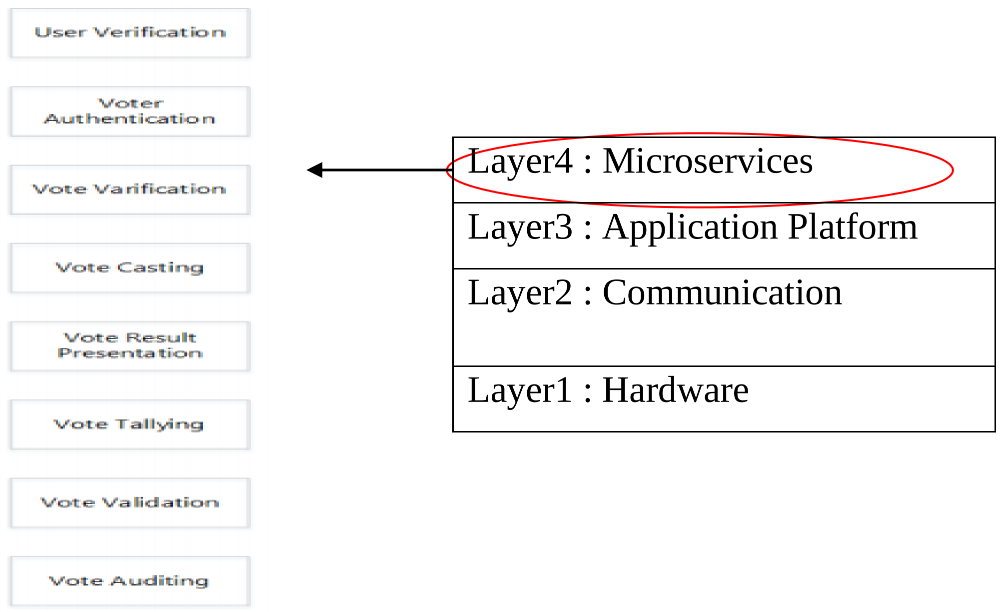

Fig.3: Micro-services Layer

These services perform by heading into a general objective together. These services are inter-related, but they are not inter-depended. They enable all the access to services is governed through access control and permissions determined by the responsibilities of each node type.

6.1(C) RESTful APIs Layer

Representational state transfer (REST) is a software architectural style that defines a set of constraints to be used for creating Web services. It enables the end-user-layer.

Fig.4: RESTful APIs layer

6.2 Blind Signature

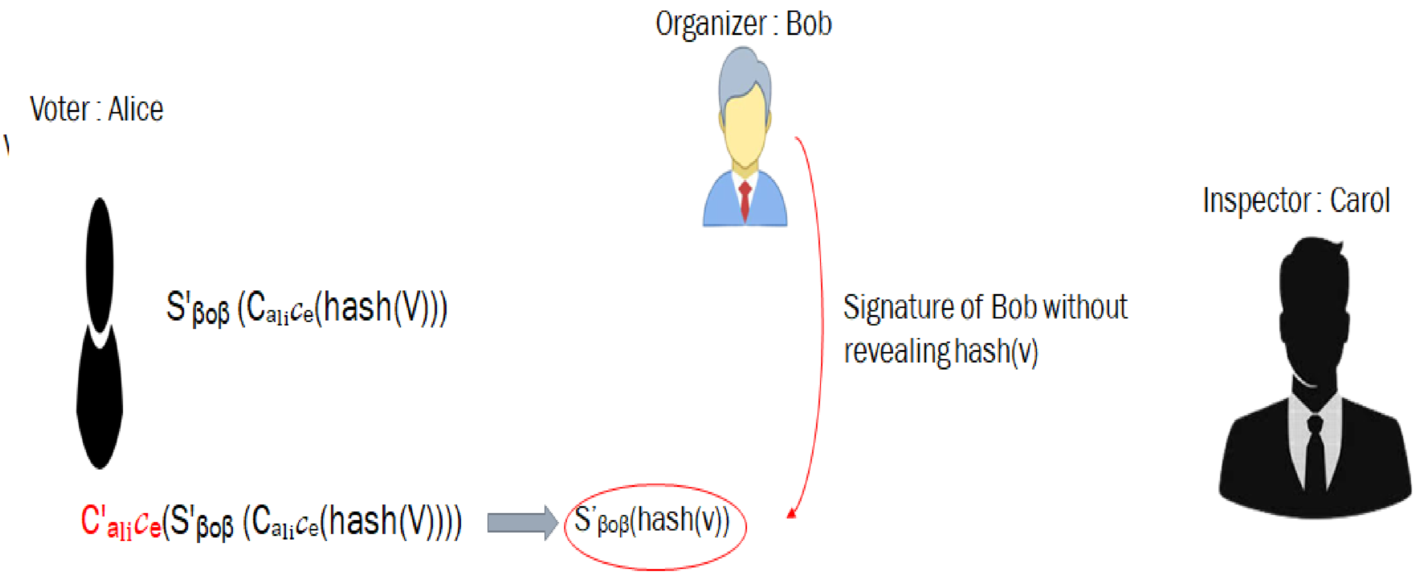

Fig.5: Organizers Signature Without Revealing Vote Information

The signing procedure is presented as follows:

1. Alice sends C_{alice}(hash(V)) to Bob.
2. Bob receives C_{alice}(hash(V)) and signs it using $S'_{\beta o\beta}$ to obtain $S'_{\beta o\beta}$ (C_{alice}(hash(V))). Then he sends $S'_{\beta o\beta}$(C_{alice}(hash(V))) to Alice.
3. Alice uses C'_{alice} to obtain $S'_{\beta o\beta}$(hash(v)) according to C'_{alice}($S'_{\beta o\beta}$ (C_{alice}(hash(V)))) = $S'_{\beta o\beta}$(hash(v)).

Thus, Alice gets the sign without revealing his vote information.

Following the steps above, Alice also gets sign of Carol (Inspector).

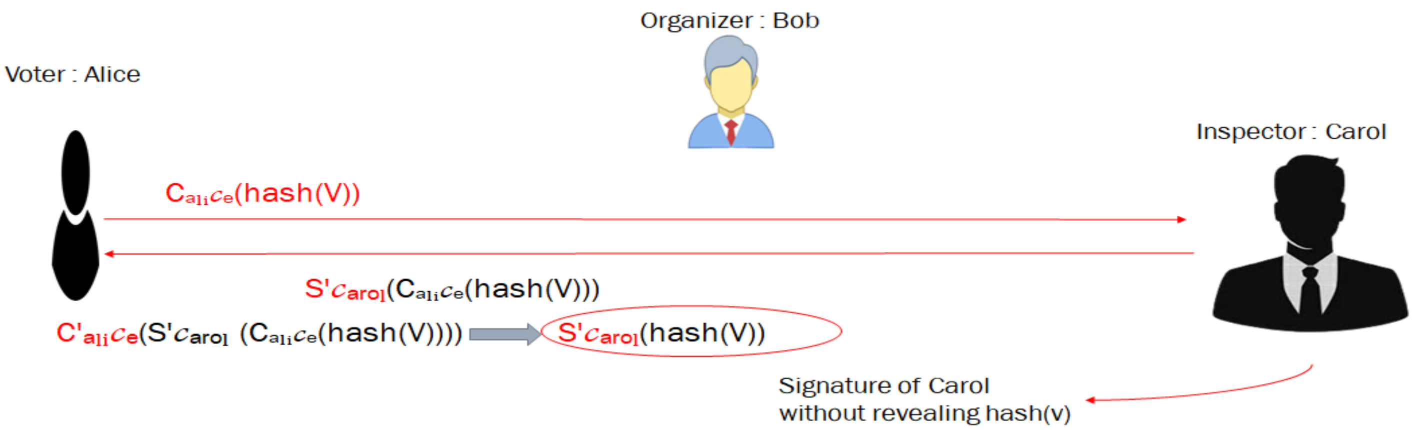

Fig.6: Inspectors Signature Without Revealing Vote Information

So, without revealing voters choice voter can make themselves approved by the organizer and inspector. Thus, the privacy of voters preserved.

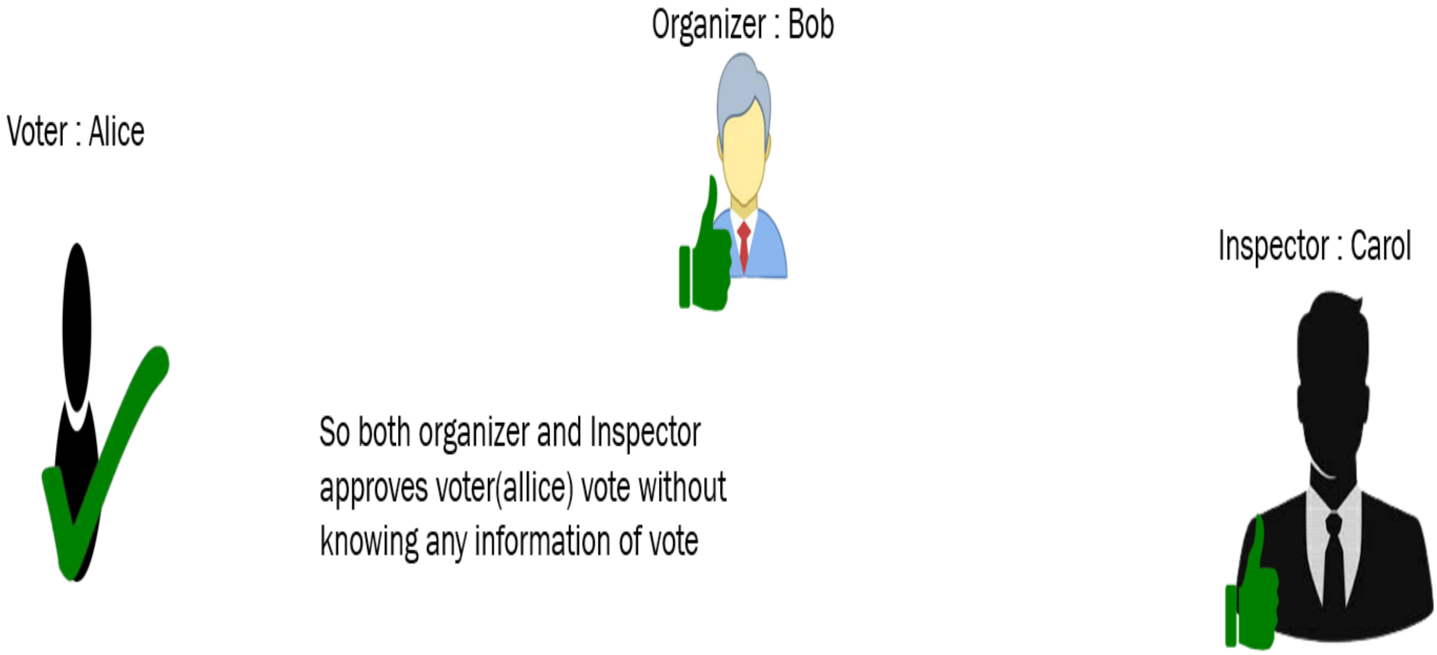

Fig.7: Approval for Voter Without knowing Voters Choice

6.3 Consensus Mechanism

6.3(A) Proof of Authority (POA):

The Proof of Authority model relies on a limited number of block validators and this is what makes it a highly scalable system. Blocks and transactions are verified by pre-approved participants, who act as moderators of the system.

7.Proposed Voting Stages

We Propose these two following stages of voting-

- Vote casting Stage
- Post Voting Stage

7.1Vote Casting Stage

Voting Stage defines how voters will give their vote and how they will be approved without revealing their voting information. Proposed Voting stage block diagram is given below:

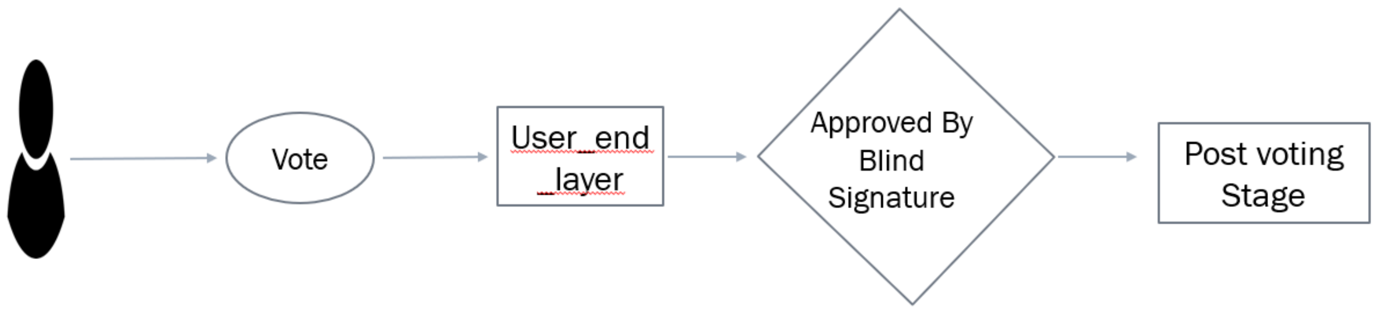

Fig.8: Block diagram of Voting Casting Stage

7.2 Post Voting Stage

Input: All Ballots

Output: All valid Ballots & Result

1: for each b ∈ Ballots do

2: if isCorrectF ormat(b) & hasAllSignature(b) &

isCastOnT ime(b) & hasNotBeenCounted(b)

then-

3: ValidBallots ← ValidBallots ∪ {b}

4: end if

5: end for

8. Challenges

Ballot Collision:

Ballots are identified by the choice code and the random string in the voting string. If it happens that different voters produce the same string, a collision occurs and one of the two ballots will be invalid. According to the Birthday Attack, for 128-bit voting strings, the probability that collisions occur is less than 10−18.

Resisting Coercion:

Voters can be forces by politically to cast their vote for a fixed candidate. Then it's quite impossible to make a neutral election.

References

[1] Liu, Yi, and Qi Wang. "An E-voting Protocol Based on Blockchain." *IACR Cryptol. ePrint Arch.* 2017 (2017).

[2] Mukherjee, Prodipta Promit, et al. "A Hyper-ledger Fabric Framework as a Service for Improved Quality E-voting System." *2020 IEEE Region 10 Symposium (TENSYMP)*. IEEE, 2020.

[3] Ma, Xiaoyu, et al. "A Blockchain Voting System Based on the Feedback Mechanism and Wilson Score." Information 11.12 (2020).

[4] Khan, Kashif Mehboob, Junaid Arshad, and Muhammad Mubashir Khan. "Secure digital voting system based on blockchain technology." *International Journal of Electronic Government Research (IJEGR)* 14.1 (2018): 53-62.

[5] Carter, L., B´elanger, F.: Internet voting and political participation: an empirical comparison of technological and political factors. DATA BASE 43(3) (2012) 26–46

[6] Zhao, Z., Chan, T.H.: How to vote privately using bitcoin. In Qing, S., Okamoto, E., Kim, K., Liu, D., eds.: Information and Communications Security - 17th International Conference, ICICS 2015, Beijing, China, December 9-11, 2015, Revised Selected Papers. Volume 9543 of Lecture Notes in Computer Science., Springer (2015) 82–96