Decentralized E-voting using the Blockchain

Mahmudun Nabi

Department of Computer Science
University of Calgary

Outline

UNIVERSITY OF CALGARY

- Questions
- E-voting
- Problem and Motivation
- Our Goal and Approach
- Literature Review
- Implementation
- Security and Cost Analysis
- Conclusion and Future work

Questions

UNIVERSITY OF CALGARY

1. What are the basic security requirements of an e-voting system?

2. How smart contract execution (in Ethereum blockchain) guarantees that the result of the voting protocol is correct without relying on any trusted third party (i.e., tallying authority)?

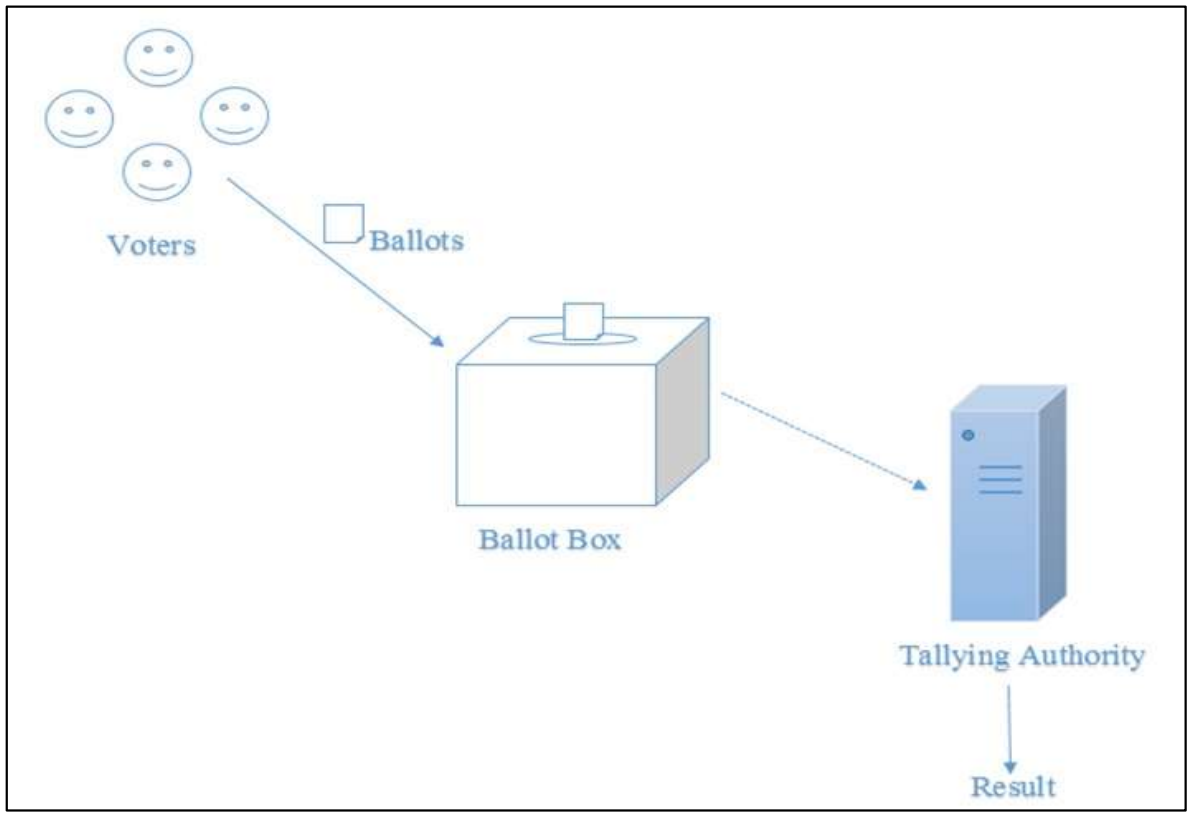
3. How blockchain technology provides decentralization for an e-voting protocol?

What is E-voting?

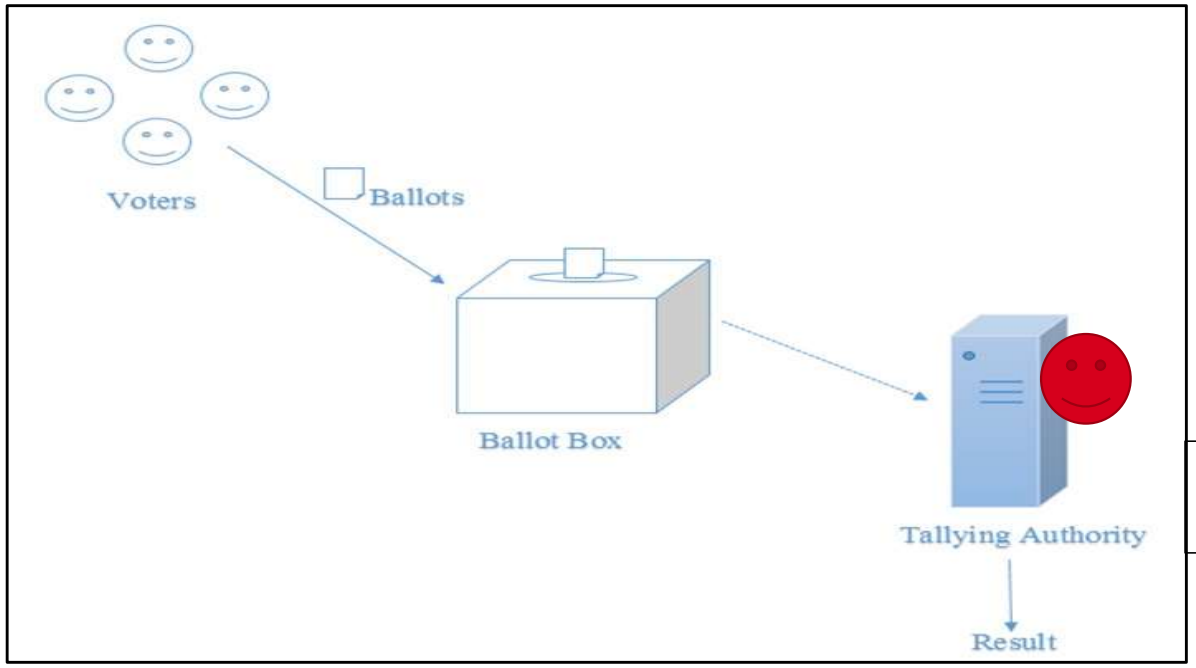
UNIVERSITY OF CALGARY

- Using Computers to organize elections
  - Voting machines in polling stations
  - Remote voting on the internet
- More convenient
  - For voters: vote from home, or abroad
  - For authorities: easier to record and tally votes
- Many protocol have been proposed:
  - Helios [B. Adida, 2008], Voatz[P. Chaido et al., 2016] …
- But of course:
  - Need to ensure voting protocols are secure

E-voting



Problem of E-voting



- Dishonest Tallying Authority
  - Can publish false result

➢ **What does it mean for a voting protocol to be secure?**

E-voting security requirements

UNIVERSITY OF CALGARY

- **Privacy**
  - No one should know who I voted for.
- **Transparency** and **Verifiability**
  - Each step of the election process should be open to all.
  - Everyone can ensure that the votes are counted correctly.
- **Trusted Entity**
  - Trustworthy authority for computing tally correctly.

Other requirements:

- *Eligibility*
  - Only eligible voters should be allowed to vote

Our Goal

UNIVERSITY OF CALGARY

- Existing e-voting systems (such as Helios) assume tallying authorities (TAs) as trusted individuals to perform the tallying operation.
  - TAs might collude and tamper the election result.

- Analyze e-voting systems that support:
  - **End-to-End (E2E) verifiability**
    - Every voter should be able to verify whether his/her vote is posted and counted correctly
  - **Correctness of Tallied Result**
    - Without depending on any trusted third party as tallying authorities

Our Approach

UNIVERSITY OF CALGARY

- Decentralized e-voting using the Blockchain:
  - Decentralized election setting:
    - Voters are responsible for coordinating the communication among themselves.
  - Blockchain:
    - As a public bulletin board
    - For public verifiability
- Analyze blockchain based e-voting schemes.
- Implement an e-voting protocol using Ethereum blockchain for a specific case
  - Analyze the security requirements for this case
  - Compare costs with existing schemes for this case

Ethereum and Smart contract

UNIVERSITY OF CALGARY

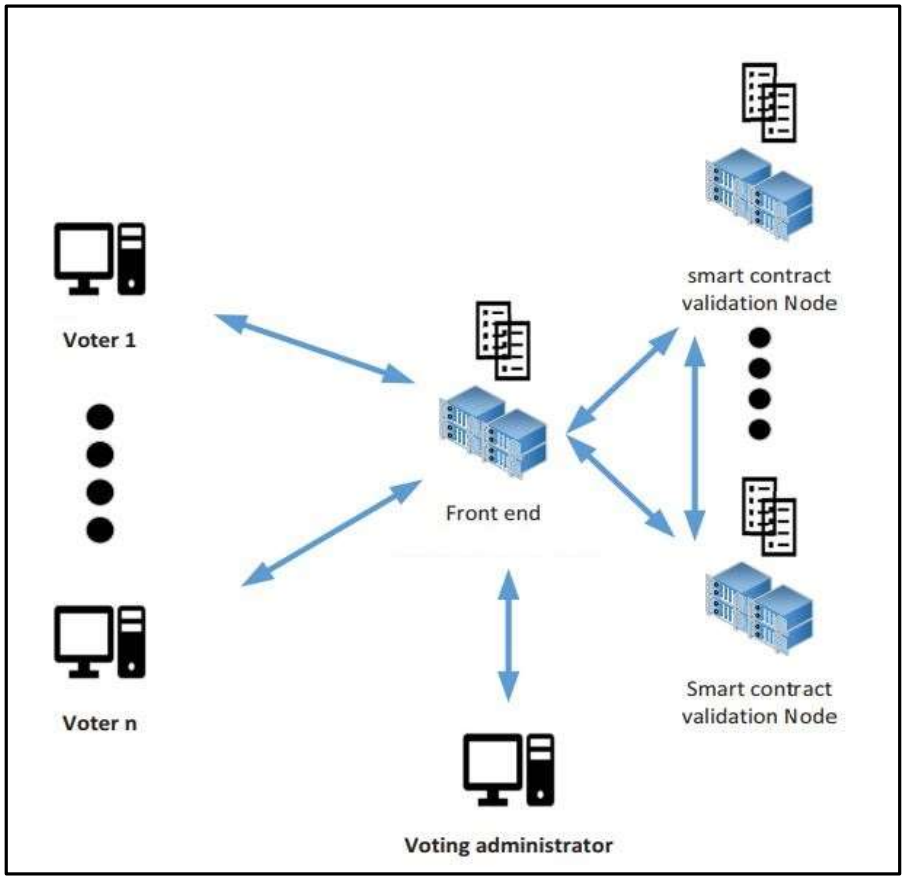
- Ethereum:
  - An open source, decentralized computing platform

- Smart contract:
  - Computer program that is stored and running on the blockchain.
  - The code is executed by the consensus peers.
  - The correctness of execution is guaranteed by the consensus protocol of the blockchain.

E-voting using Smart Contract

General Idea

- Smart contracts as a TTP with the goal of ensuring correctness of Tallied Result.



Picture source: Yu, Bin, et al. "Platform-independent secure blockchain-based voting system." *International Conference on Information Security*. Springer, Cham, 2018.

E-voting Using Blockchain

Related Works

UNIVERSITY OF CALGARY

- **Paper 1** – A Smart Contract for Boardroom Voting with Maximum Voter Privacy [P. McCorry et al.(2017)]

- **Paper 2** - Towards Secure E-Voting Using Ethereum Blockchain [E. Yavuz et al. (2018)]

- **Paper 3** – E-Voting with Blockchain: An E-Voting Protocol with decentralization and Voter Privacy [F.S. Hardwick et al. (2018)]

A Smart Contract for Boardroom Voting with Maximum Voter Privacy

UNIVERSITY OF CALGARY

- Proposed by Patrick McCorry, Siamak F. Shahandashti and Feng Hao in 2017.

- The primary goal of this work
  - Implement decentralized and self-tallying e-voting protocol
  - Use smart contract to perform vote cast and counting.
  - Supports voters privacy.

- Implements **Open Vote Network**, an e-voting protocol.
  - Self-tallying protocol
  - Public communication

How it Works?

UNIVERSITY OF CALGARY

- **Entities:**

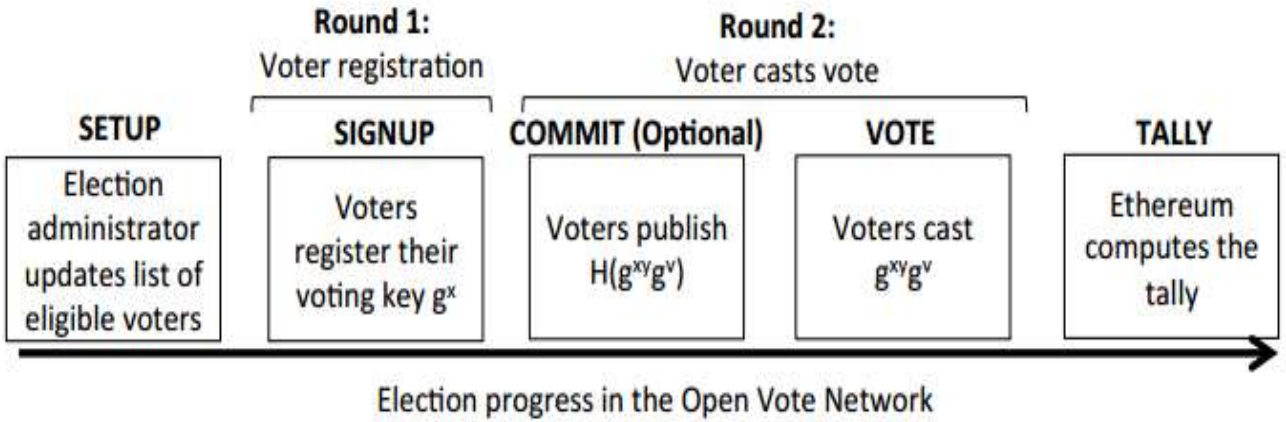
- **Election Administrator**
  - Deploy e-voting smart contracts.
  - Initiate e-voting environment
  - Determine list of eligible voters.

- **Voter**
  - Registers
  - Casts vote
  - *Count votes*

- **Observer**
  - Observes the election process
  - Can count votes

- **Round One :**
  - Setup
  - Signup

- **Round two**
  - Commit
  - Vote
  - Tally



Security Analysis

UNIVERSITY OF CALGARY

- Satisfies
  - Public Verifiability
  - Privacy
  - Self-tallying
    - Anyone can compute the tally.
- Issue:
  - Requires all the registered voters to finish the vote. If there is one of the registered voters does not finish the voting, the tally calculation cannot be performed.

Towards Secure E-Voting Using Ethereum Blockchain

UNIVERSITY OF CALGARY

- Proposed by E. Yavuz, A. K. Koc, U. C. Cabuk and G. Dalkilic in 2018.

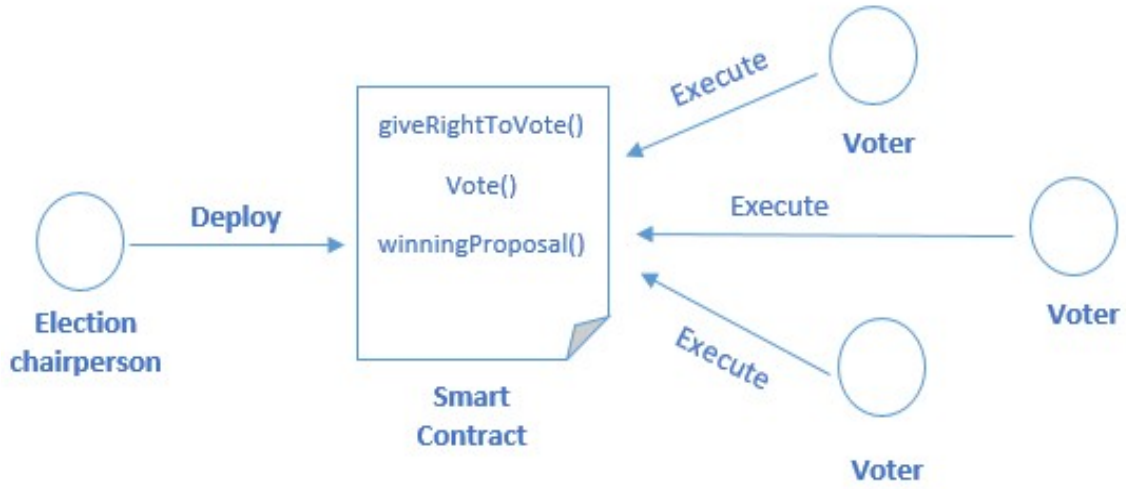
- The primary goal of this work
  - Implement small scale e-voting system
  - Use smart contract to perform vote cast and counting.

How it works?

- Election chairperson
  - Initiated e-voting environment
  - Deployed e-voting smart contract

- Voter
  - E-voting registration
  - Cast votes

- **Phases of e-voting system**
  - Initialization Phase
  - Registration Phase
  - Voting Phase
  - Vote Counting Phase



Security Analysis

UNIVERSITY OF CALGARY

- Satisfies
  - Eligibility
  - Transparency
  - Individual verifiability
- Does not satisfy
  - Personal Authentication
  - Privacy

E-Voting with Blockchain: An E-Voting Protocol with decentralization and Voter Privacy

UNIVERSITY OF CALGARY

- Proposed by Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis in 2018.

- The primary goal of this work
  - Utilize blockchain as a transparent ballot box.
  - Develop a e-voting protocol that satisfies
    - A degree of decentralization
    - Voting alteration mechanism

What are the entities?

UNIVERSITY OF CALGARY

- Election administrator
  - Initiated e-voting environment
  - Deployed e-voting smart contract

- Voter
  - E-voting registration
  - Cast votes
  - Count votes

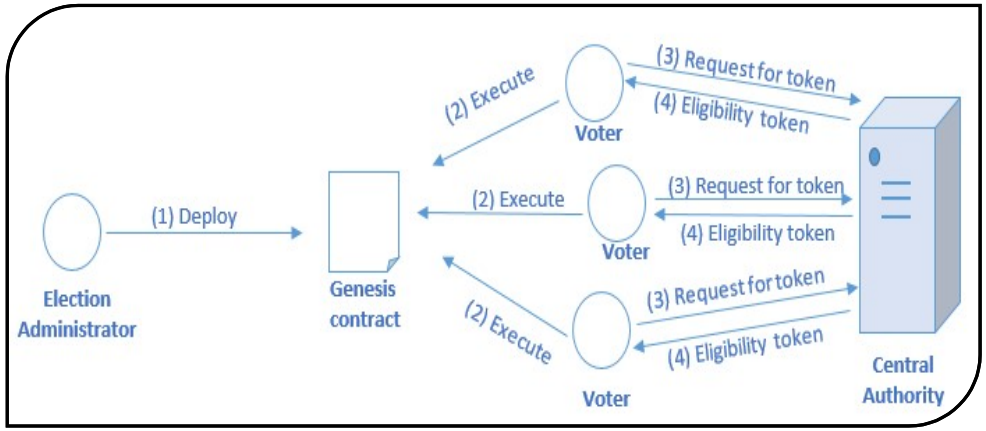
- Central authority (a trusted third party)
  - Assures voters' eligible
  - Authenticates eligible voters'
  - Ensures voters' privacy

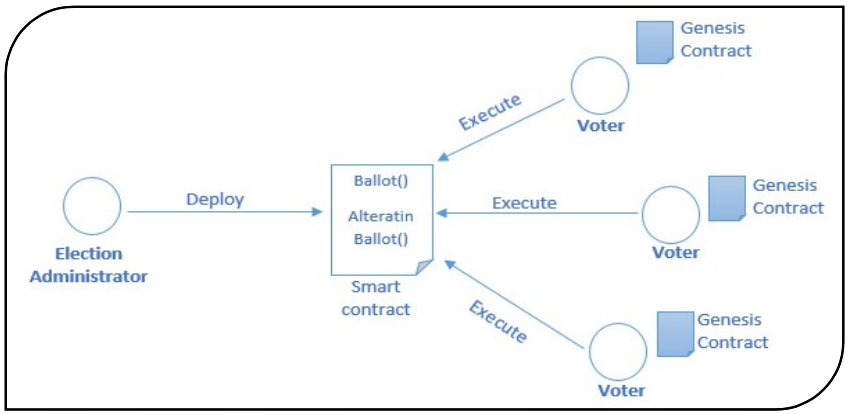
How it works?

- This paper considered two round voting protocol

- **Phase One:**
  - Initialization Phase
  - Preparation Phase

- **Phase Two**
  - Voting Phase
  - Counting Phase





Security Analysis

UNIVERSITY OF CALGARY

- Satisfies
  - Eligibility
  - Individual verifiability
- Does not satisfy
  - privacy
  - Complete Trustworthy (CA may break the trust)

UNIVERSITY OF CALGARY

Implementation and Results

Implementation

UNIVERSITY OF CALGARY

- Extend Boradroom voting [P. McCorry et al.] to *multiple candidates* voting option.

Setup:

- Blockchain: Ethereum
- Smart contract Language: Solidity
- Tools used:
  - Truffle: Smart contract development environment.
  - Ganache: Blockchain for Ethereum development.

The voting protocol

- **Entities**:
  - Voting Administrator
  - Voter(s)
  - Smart Contract as Tallying Authority

The voting process has following steps:

- **Setup**
  - Election administrator creates a new election by providing all information about the election.
    - List of eligible voters
    - **List of Candidates**
    - Custom Parameters: Vote duration, registration duration etc.
- **Registration**
  - Each voter registers with their public key.
- **Voting**
  - Each eligible voter submits her encrypted vote.
- **Tally**
  - Smart contract does the tallying and anyone can get the tallied result.

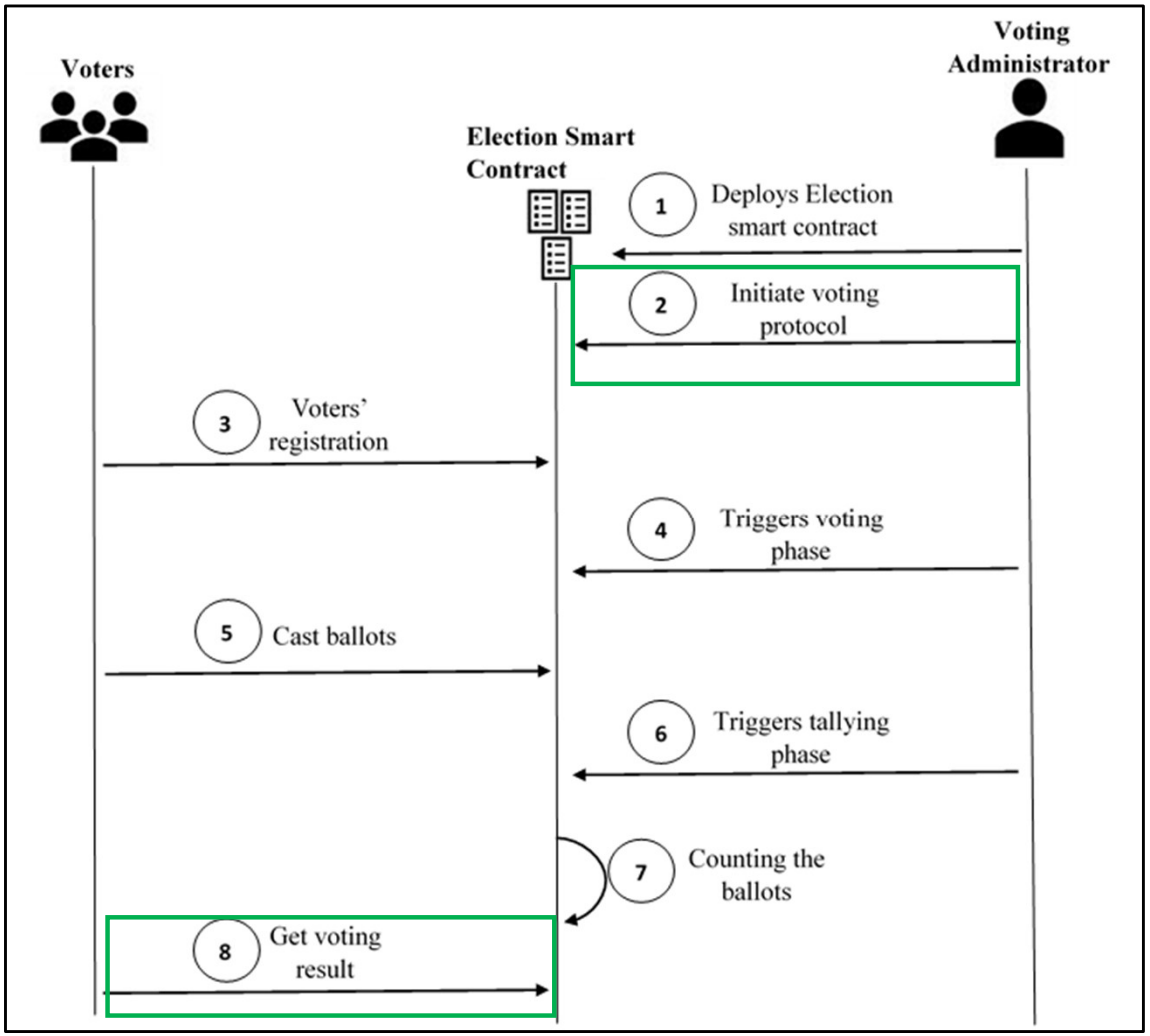


Figure: The voting protocol diagram

Abstract Election Smart Contract

UNIVERSITY OF CALGARY

```
pragma solidity ^0.4.10;
import "ECCMath library";
import "Secp256k1 library";
contract Election{
        constructor ();
        function setEligibleVoter(address[] addr) onlyOwner ;
        function addCandidate(string memory _name) ownerOnly;
        function beginSignUp (string _electionName, uint _electionDuration)  onlyOwner;
        function register(uint xG, uint vG, uint z);
        function finishRegistrationPhase()  onlyOwner;
        function submitVote(uint[2] y, uint _vr, string _CandidateName) ;
        function computeTally() inState(State.VOTE) onlyOwner;
        function getResult() returns (string);
        function verifyZKP(uint xG, uint vG, uint z) returns (bool);
}
```

Security Analysis

UNIVERSITY OF CALGARY

- **Privacy**
  - Vote is hidden since each voters submit her ElGamal encrypted vote to the smart contract.
- **Transparency and Verifiability**
  - Everyone interested in the election can openly access the related information via Ethereum blockchain (i.e., public bulletin board).
  - The voter can verify that their vote has been recorded as cast by inspecting the Blockchain and decrypting their vote using their secret key.
- **Trusted Authority and correctness of result**
  - Voting protocol is implemented as a smart contract.
  - It is executed by all the Ethereum nodes.
  - This execution can be seen as execution by a trusted global machine.
  - Correctness of execution is guaranteed by the consensus protocol of the Ethereum blockchain.

Cost Analysis

UNIVERSITY OF CALGARY

Paper	Extension of P. McCorry et al. [2017]		E. Yavuz et al. [2018]	
Phases	(Execution cost in Gas)	(Execution cost in $)	(Execution cost in Gas)	(Execution cost in $)
Initialization	5245676	$1.51	971949	$0.27992
Registration	743458	$0.21411	168355	$0.04848
Vote	532016	$0.1527	27218	$0.00783
Tally	642790	$0.18	0	0
Total Cost:	7163940	$2.056	1167522	$0.33624

Election contract creation	4414334
setEligibleVoter	21387
addCandidate	74628
initialize	104774

Ballot contract creation	944839
addCandidate	27110

Summary

UNIVERSITY OF CALGARY

- What Achieved:
  - *Decentralization*
    - Blockchain provides an authenticated broadcast channel (i.e., underlying peer-to-peer network) for casting the vote, which are necessary in a decentralized e-voting protocol to support coordination amongst voters
    - Using smart contract as tallying authority any voter can perform the tally computation without relying on any central authority.

- Challenges:
  - Voter authentication
  - Large scale implementation

Conclusion and Future work

UNIVERSITY OF CALGARY

- E-voting:
  - Addressed the security concerns of e-voting protocol.
  - Discussed how blockchain technology satisfies these security concerns by providing decentralization and correctness guarantee without relying on any trusted third party.

- Issues not addressed/Future work:
  - Coercion resistance

References

[1] McCorry, Patrick, Siamak F. Shahandashti, and Feng Hao. *A smart contract for boardroom voting with maximum voter privacy*.InternationalConference on Financial Cryptography and Data Security. Springer, Cham, 2017.

[2] Yavuz, Emre, et al. *Towards secure e-voting using ethereum blockchain*. 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018.

[3] Hardwick, Freya Sheer, et al. *E-Voting with blockchain: an E-Voting protocol with decentralisation and voter privacy*. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018.

[4] Hao, Feng, Peter YA Ryan, and Piotr Zieli´ nski. *Anonymous voting by two-round public discussion.* IET Information Security 4.2 (2010): 62-67.

[5] Hj´ almarsson, Fririk ., et al. *Blockchain-based e-voting system*. 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018.

[6] Hanifatunnisa, Rifa, and Budi Rahardjo. *Blockchain based e-voting recording system desig*." 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). IEEE,2017.

[7] Hertig, Alyssa. *The First Bitcoin Voting Machine Is On Its Way*. Motherboard Vice, Nov (2015).

[8] Adida, Ben. *Helios: Web-based Open-Audit Voting.* USENIX security symposium. Vol. 17. 2008.

[9] Kiayias, Aggelos, and Moti Yung. *Self-tallying elections and perfect ballot secrecy*. International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2002.

UNIVERSITY OF CALGARY

Thanks