Voting Systems and Blockchain

Comps Co., Ltd.
Yoshikazu Nishimura

Requirements for Voting Confidentiality

The following are two requirements for maintaining the confidentiality of voting.

- Anonymity of voters
- Confidentiality of results in progress

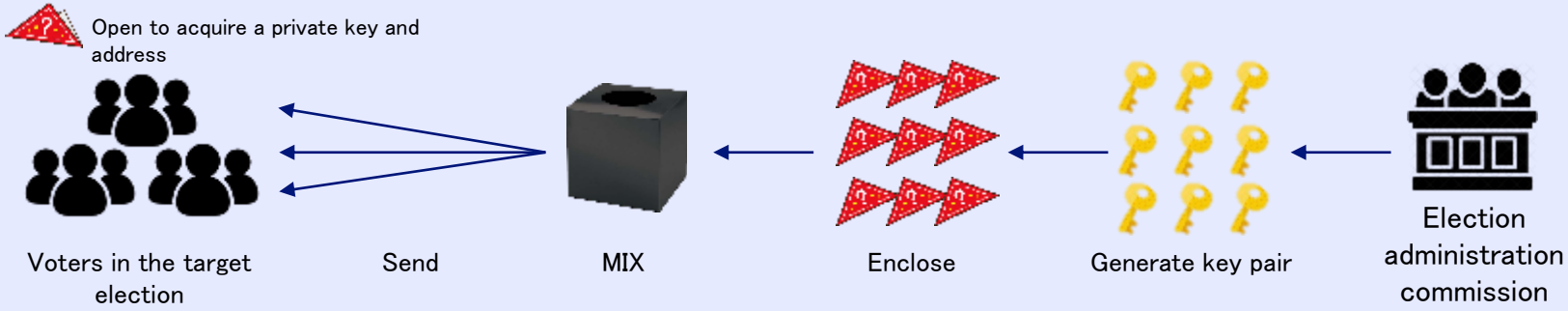
	Open Vote Network	C.R.E.A.M
Anonymity of voters	○	○※
Confidentiality of results in progress	○	△

Anonymity of voters

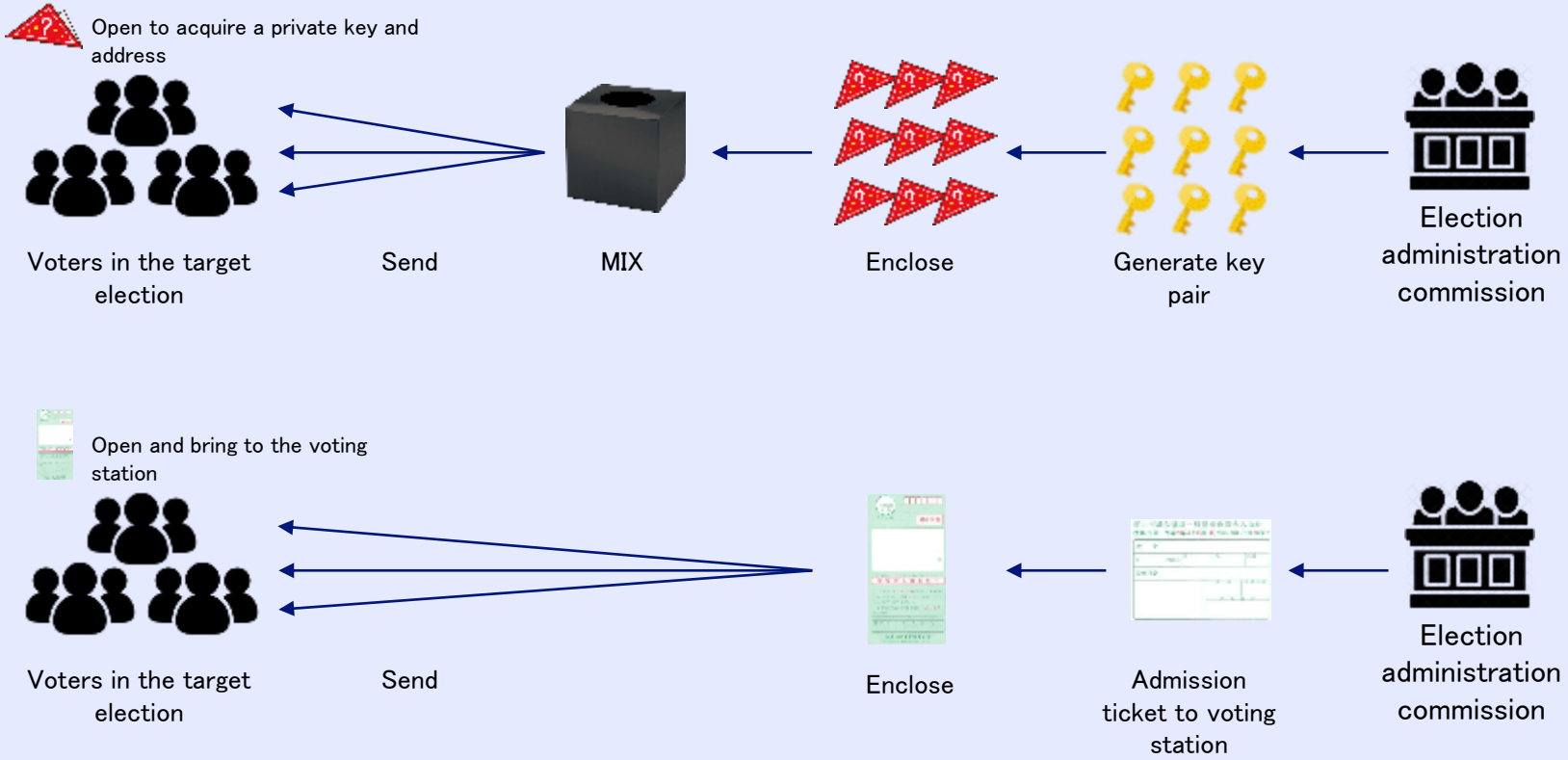
Although achieving anonymity (anonymous addresses) on blockchain is ideal, is it cost-effective? (Cost : economic costs and calculation volume)

[Proposal]

When considering anonymity for names, is it possible to achieve this anonymity by ensuring not to link blockchain addresses with personal information?



Anonymity of voters



If an anonymous voting ticket can be distributed only to voters following confirmation of identity, this is sufficient.

Confidentiality of results in progress

Confidentiality of results in progress (voting confidentiality requirement 2) can be achieved with just a commit/reveal scheme.

Voters in the target election

reveal value = 1 vote for Candidate A

hash

commit value = 171190d7dbb5bf35

Election administration commission

Since signature address and individuals cannot be determined, the requirements for anonymous voting are cleared.

By comparing signature address with the voter list, the voter determination requirement is cleared.

Since commit value alone is insufficient to determine which candidate voters voted for, the requirement for anonymity during the voting process is cleared.

Voting smart contract

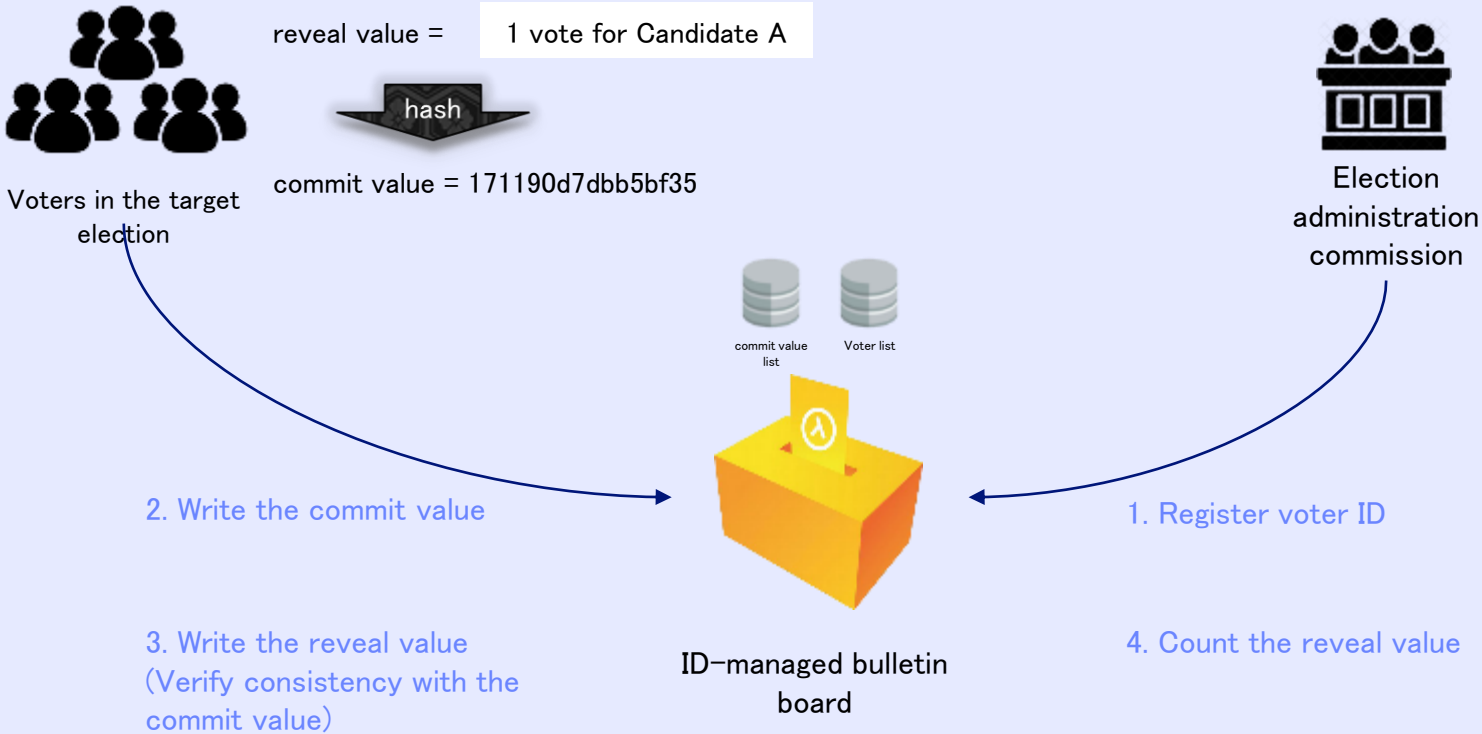
1. Register voter addresses

4. Count the reveal value

Confidentiality during the voting process

Confidentiality during the voting process (voting confidentiality requirement 2) can be achieved with just a commit/reveal scheme.

A commit/reveal system on its own can be achieved without the use of blockchain.



Requirements for Voting Confidentiality

The following are three requirements for maintaining the confidentiality of voting.

- Voter anonymity (individual anonymity)
- Voter anonymity (address anonymity)
- Confidentiality in the voting process

	Commit/Reveal	Open Vote Network	C.R.E.A.M
Individual anonymity	○	○	○※
Address anonymity	×	○	○※
Confidentiality of results in progress	○	○	△

Gas cost for the Open Vote Network

Entity: Transaction	Cost in Gas	Cost in $
A: VoteCon	3,779,963	0.83
A: CryptoCon	2,435,848	0.54
A: Eligible	2,153,461	0.47
A: Begin Signup	234,984	0.05
V: Register	763,118	0.17
A: Begin Election	3,085,449	0.68
V: Commit	70,112	0.02
V: Vote	2,490,412	0.55
A: Tally	746,485	0.16
Administrator Total	12,436,190	2.74
Voter Total	3,323,642	0.73
Election Total	145,381,858	31.98

Table 1. A breakdown of the costs for 40 participants using the Open Vote Network. We have approximated the cost in USD ($) using the conversion rate of 1 ether = $11 and the gas price of 0.00000002 ether which are the real world costs in November 2016. Also, we have identified the cost for the election administrator 'A' and the voter 'V'.

For voting by 40 people:

- Voter: 0.16 ETH (around 6,750 JPY)
- Admin: 0.62 ETH (around 26,000 JPY)

*Assuming gasPrice = 50 Gwei.

Gas cost for an Open Vote Network

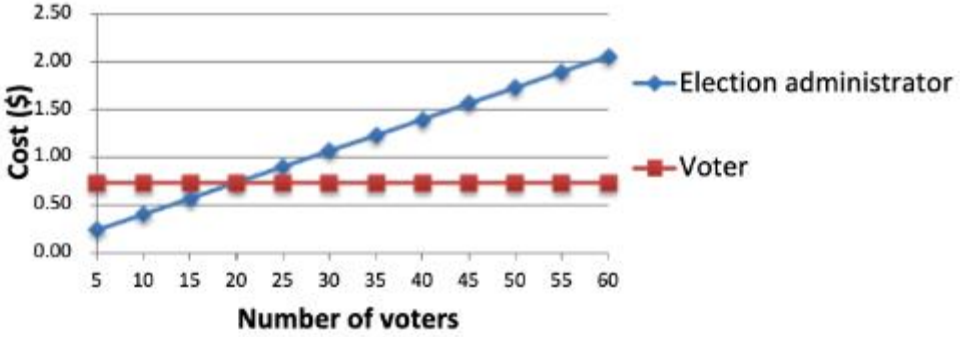


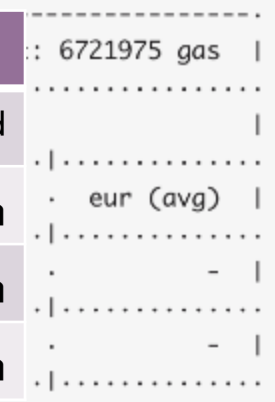
Fig. 3. The average cost for the election administrator and the voter based on the number of voters participating in the election.

The cost for voters is 0.16 ETH (around 6,750 JPY) regardless of the number of voters.
Admin cost rises in a linear fashion. For a 5,000-person (village mayoral election level) scale, cost is 77.5 ETH (3.1 million JPY).

*Assuming gasPrice = 50 Gwei.

Gas cost for C.R.E.A.M.

Action	Actor	Gas	Gas ETH	JPY
deploy	Admin	Unverified	Unverified	Unverified
mint/transfer	Admin	50,000	0.0025 ETH	100 yen
deposit	Voter	380,350	0.0190 ETH	760 yen
withdraw	Voter	369,018	0.0185 ETH	740 yen



For a 5,000-person (village mayoral election level) scope :

- Voter cost = 1,500 JPY
- Admin cost = 500,000 JPY (*If call as Bulk, this may be slightly cheaper.)

Simple Commit/Reveal Scheme

```
pragma solidity ^0.6.6;

contract CommitRevealBallot {
  address public admin;
  uint256[] public candidates = [0,1];
  mapping (address => uint256) public voters; // 1: Registered, 2: Voted
  mapping (bytes32 => uint256) public commits; // 1: Committed, 2: Revealed
  mapping (uint256 => uint256) public voteCount;

  constructor() public {
    admin = msg.sender;
  }

  function addVoter(address _voter) external {
    require(msg.sender == admin);
    voters[_voter] = 1;
  }

  function commit(bytes32 _commit) external {
    require(voters[msg.sender] == 1);
    require(commits[_commit] == 0);
    voters[msg.sender] = 2; // Voted
    commits[_commit] = 1; // Committed
  }

  function reveal(uint256 _reveal, bytes32 _commit) public {
    require(_commit == keccak256(abi.encodePacked(_reveal)));
    require(commits[_commit] == 1);
    uint256 vote = _reveal % candidates.length;
    voteCount[vote]++;
    commits[_commit] = 2; // Revealed
  }
}
```

Gas cost for a simple Commit/Reveal Scheme

Action	Actor	Gas	Gas ETH	JPY
deploy	Admin	426,946	0.0213 ETH	854 yen
addVoter	Admin	42,706	0.0022 ETH	86 yen
commit	Voter	42,852	0.0022 ETH	86 yen
reveal	Voter	49,952	0.0025 ETH	100 yen

For a 5,000-person (village mayoral election level) scope :

- Voter cost = 186 JPY
- Admin cost = 427,914 JPY (*If call as Bulk, this may be slightly cheaper.)

CommitRevealBallotLight

```
pragma solidity ^0.6.6;

contract CommitRevealBallotLight {
  mapping (bytes32 => address) public commits;

  event Voted(address indexed _voter, uint256 _vote);

  function commit(bytes32 _commit) external {
    commits[_commit] = msg.sender;
  }

  function reveal(uint256 _reveal, bytes32 _commit) public {
    require(_commit == keccak256(abi.encodePacked(_reveal)));
    emit Voted(commits[_commit], _reveal);
  }
}
```

Action	Actor	Gas	Gas ETH	JPY
deploy	Admin	194,281	0.0097 ETH	388 yen
commit	Voter	42,770	0.0021 ETH	86 yen
reveal	Voter	24,493	0.0012 ETH	49 yen

Use blockchain as a minimal ledger
Count via executing an event off-chain

CommitRevealBallotLight

```
pragma solidity ^0.6.6;

contract CommitRevealBallotSuperLight {
  function commit(bytes32 _commit) external {
    // Do nothing
  }

  function reveal(uint256 _reveal, bytes32 _commit) public {
    // Do nothing
  }
}
```

Action	Actor	Gas	Gas ETH	JPY
deploy	Admin	91,443	0.0046 ETH	195 yen
commit	Voter	21,752	0.0011 ETH	47 yen
reveal	Voter	21,911	0.0011 ETH	47 yen

Use blockchain as a minimal ledger
Count via verification and tally using Calldata