投票システムとブロックチェーン

株式会社コンプス情報技術研究社
西村 祥一

秘密投票の要件

秘密投票の要件には以下の2つが存在すると考える

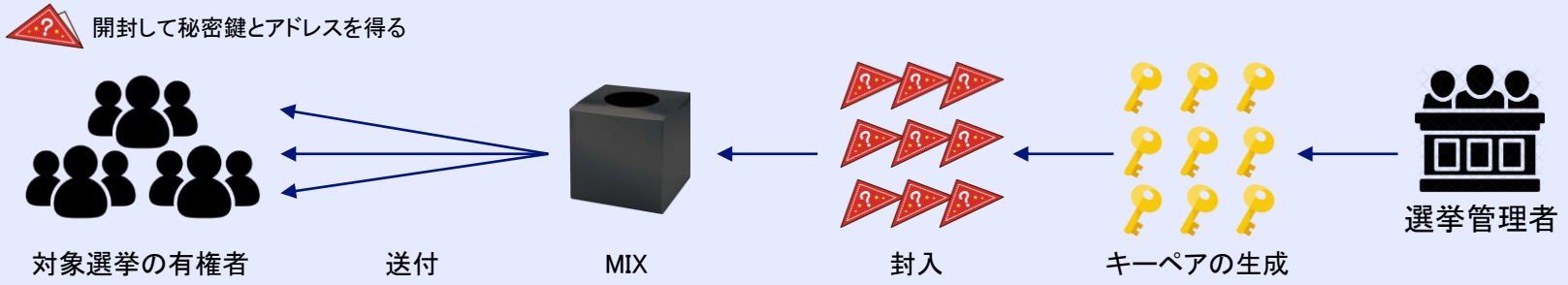
- 投票者の匿名性
- 投票途中経過の秘匿性

	Open Vote Network	C.R.E.A.M
投票者の匿名性	○	○※
途中経過の秘匿性	○	△

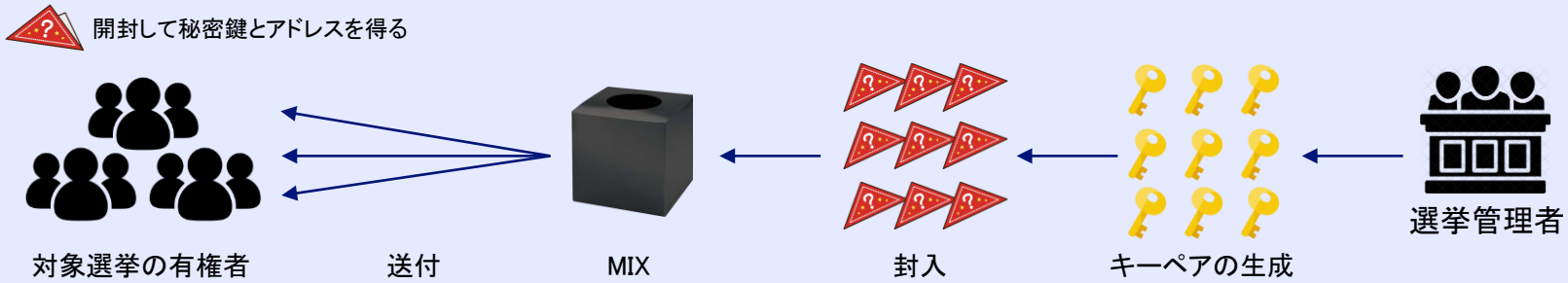
投票者の匿名性

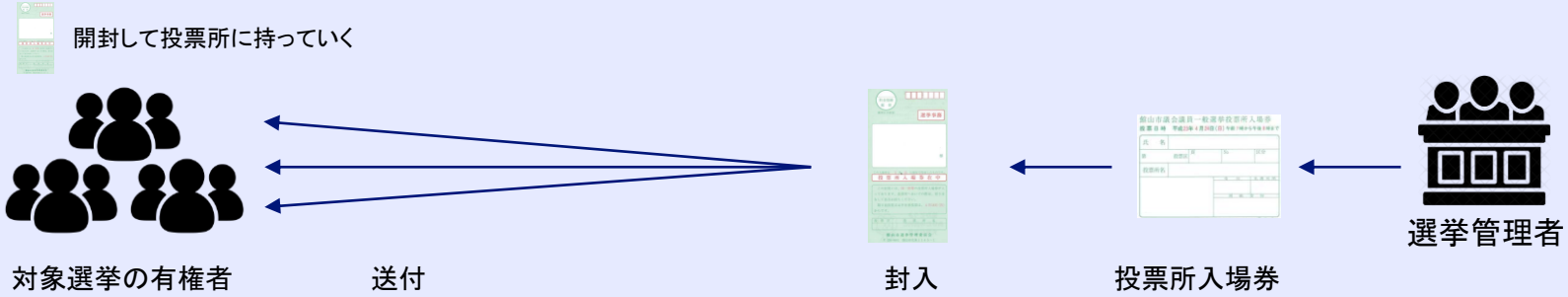
ブロックチェーン上での匿名性（anonymity: 匿アドレス性）を実現することは理想だが、コスト対効果はどうか。（コスト：経済的コスト、計算量）

[提案]
匿”名”性を考えた場合に、ブロックチェーン上のアドレスと本人性の紐付けができないことをもって匿名性ということは可能か？



投票者の匿名性





本人性が確認された上で、無記名の投票券（権）を有権者のみに配布できれば良い

途中経過の秘匿性

途中経過の秘匿性（秘密投票要件2）は commit/reveal 方式だけで実現できる

対象選挙の有権者

reveal 値 = 候補Aに1票

hash

commit 値 = 171190d7dbb5bf35

選挙管理者

署名アドレスと個人の特定はできないため匿名投票の要件をクリア

署名アドレスを有権者リストと照合することで有権判定要件をクリア

commit 値のみではどの候補に投票したかわからないため途中経過の秘匿性要件をクリア

投票スマートコントラクト

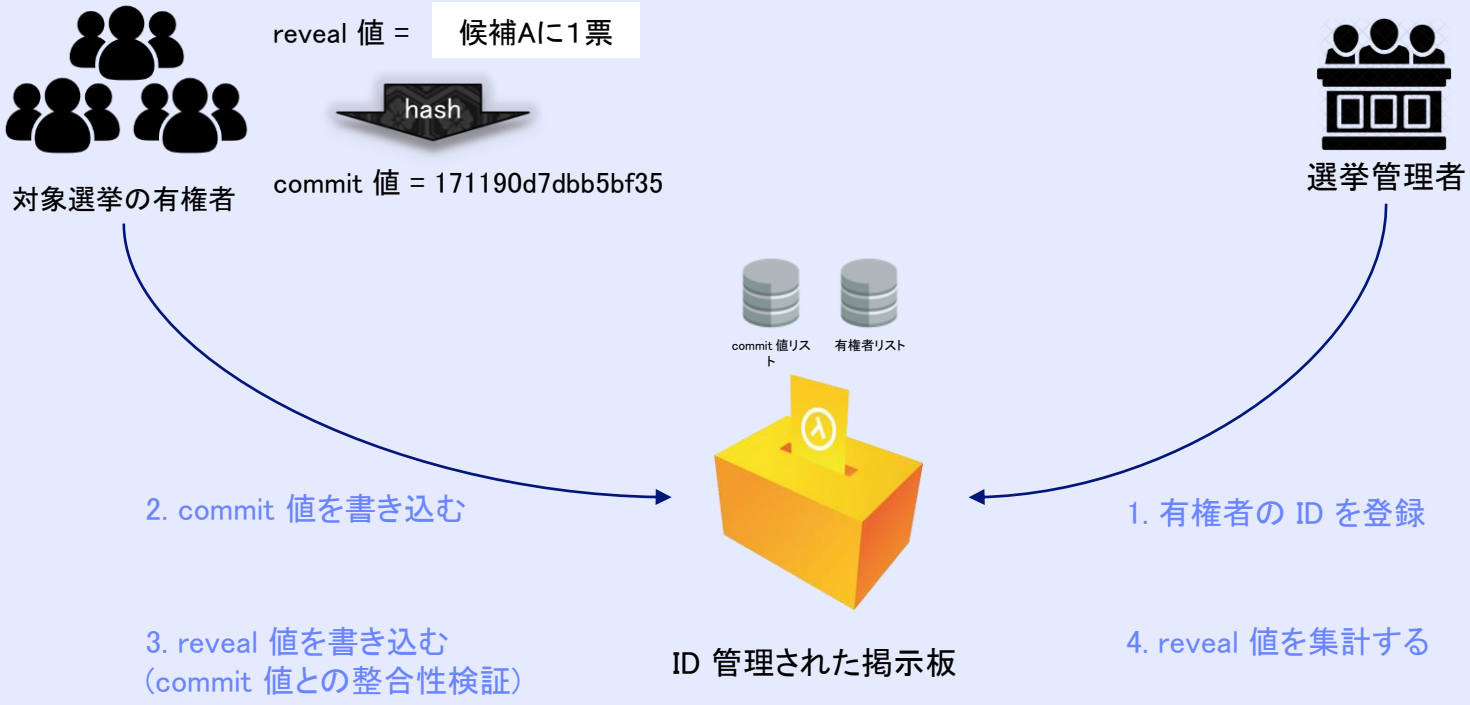
1. 有権者のアドレスを登録

4. reveal 値を集計する

途中経過の秘匿性

途中経過の秘匿性（秘密投票要件2）は commit/reveal 方式だけで実現できる

commit/reveal 方式自体はブロックチェーンがなくても実現できる



秘密投票の要件

秘密投票の要件には以下の2つが存在すると考える

- 投票者の匿名性（個人の匿名性）
- 投票者の匿名性（アドレスの匿名性）
- 投票途中経過の秘匿性

	Commit/Reveal	Open Vote Network	C.R.E.A.M
個人の匿名性	○	○	○※
アドレス匿名性	×	○	○※
途中経過の秘匿性	○	○	△

Open Vote Network の Gas コスト

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'.

40人の投票で、

- 投票者：0.16 ETH（6,750円くらい）
- 管理者：0.62 ETH（26,000円くらい）

※ gasPrice = 50 Gwei 想定

Open Vote Network の Gas コスト

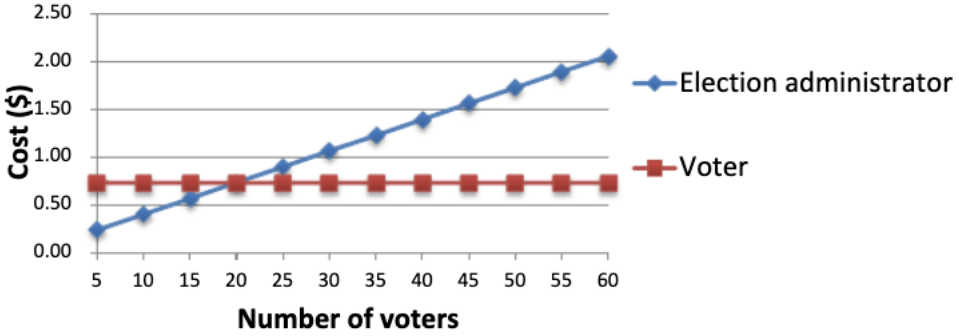


Fig. 3. The average cost for the election administrator and the voter based on the number of voters participating in the election.

Voter のコストは投票人数に関わらず 0.16 ETH（6,750円くらい）
Admin のコストは線形に上がる。5,000人（村長選挙）規模で 77.5 ETH（310万円）

※ gasPrice = 50 Gwei 想定

CREAM の Gas コスト

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

```
: 6721975 gas  |
               |
· eur (avg)  |
·          -  |
·          -  |
```

5,000人（村長選挙）規模で

- Voter のコスト　=　1,500円
- Admin のコスト　=　500,000円（※ Bulk で呼べばちょっと安くなるかも…）

単純 Commit/Reveal 方式

```
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
  }
}
```

単純 Commit/Reveal 方式の Gas コスト

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

5,000人（村長選挙）規模で

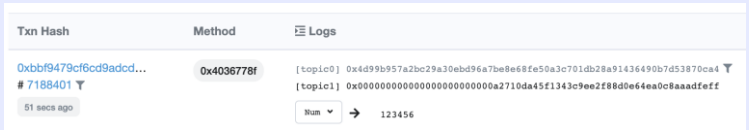
- Voter のコスト　=　186円
- Admin のコスト　=　427,914円（※ Bulk で呼べばちょっと安くなるかも…）

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円
commit	Voter	42,770	0.0021 ETH	86円
reveal	Voter	24,493	0.0012 ETH	49円

ブロックチェーンを最小限の台帳として使用する
集計は Event をオフチェーンで行う



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円
commit	Voter	21,752	0.0011 ETH	47円
reveal	Voter	21,911	0.0011 ETH	47円

ブロックチェーンを最小限の台帳として使用する
集計は Calldata を検証・集計して行う