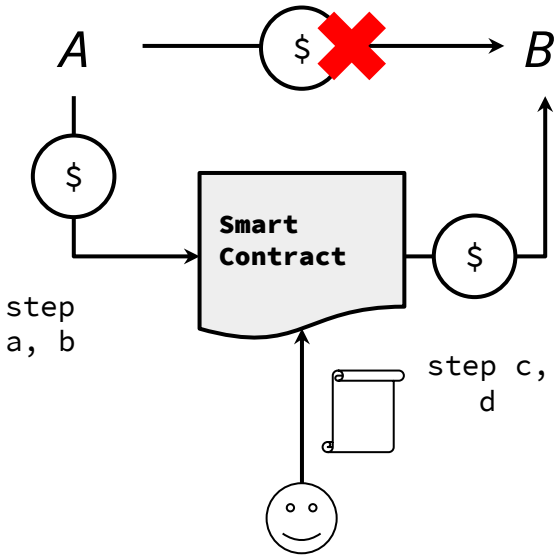
Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

about CREAM?

- https://github.com/couger-inc/cream
- Anonymous Voting using ERC(20/721) coins
- Summary of Voting steps (version 1.0)
  a. Reception phase
  b. Voting contract accepted coin deposit
  c. Call the Voting contract from a non-deposit account (or relayer) and withdraw to a different account
  d. Manage withdraw history on the contract side to prevent double spending



Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

Anonymity

- ❏ Offer proof of commitment at the time of deposit
- ❏ If verification is confirmed as true, deposited coins can be withdrawn (transferred)
- ❏ Issuing tx is possible for only who know the commitment
  - ❏ It is acceptable to verify using an account other than the account used for deposit
- ❏ Tx sender of coin: because “**from**” is always the contact address, it is possible to keep it secret information regarding who voted for whom during voting.

Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

setup ①

- Let $\mathbb{B} = \{0, 1\}$
- Let e be for the pairing arithmetic operation used in the SNARK proof and defined against a group of prime numbers q
- Let $H_1 : \mathbb{B} \to \mathbb{Z}_p$ be the Pedersen hash function, let $H_2 : (\mathbb{Z}_p, \mathbb{Z}_p) \to \mathbb{Z}_p$ be the MiMC hash function
- Let τ be a Merkle tree of any height (16 for example). The non-leaf nodes hash the left and right by H_2
- Let $O(\tau, \iota)$ be the path of the Merkle tree τ represented by the root hash R with the index τ

Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

setup ②

- Let the value of k in $k \in \mathbb{B}^{248}$ be the *nullifier*, *let* the value of r in $r \in \mathbb{B}^{248}$ be the *secret*
- Let B be the candidate's Ethereum address
- Let $S[R,h,B,f,t]$ be the following knowledge description using the public values R, h, B, f, t
  : $S[R,h,B,f,t]$ = {if and only if $h = H_1(k)$ and knows where the value of O at the known position ι for the know the path of $k,r \in \mathbb{B}^{248}$, $\iota \in \mathbb{B}^{16}$, $O \in \mathbb{Z}_p$ of ^{16}R of $H_2(k||r)$}
  - f = Fee for going via the relayer node
  - t = relayer node address
  - h = known as the *nullifier hash*

Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

setup ③

- Let $D = (d_p, d_v)$ be the key pair for zk-SNARK proof verification for S created by the trusted setup
- Proof: Prove$(d_p, \tau, \iota, B, f, t) \rightarrow P$
- Verification: Verify(d_v, P, R, h, B, f, t)

Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

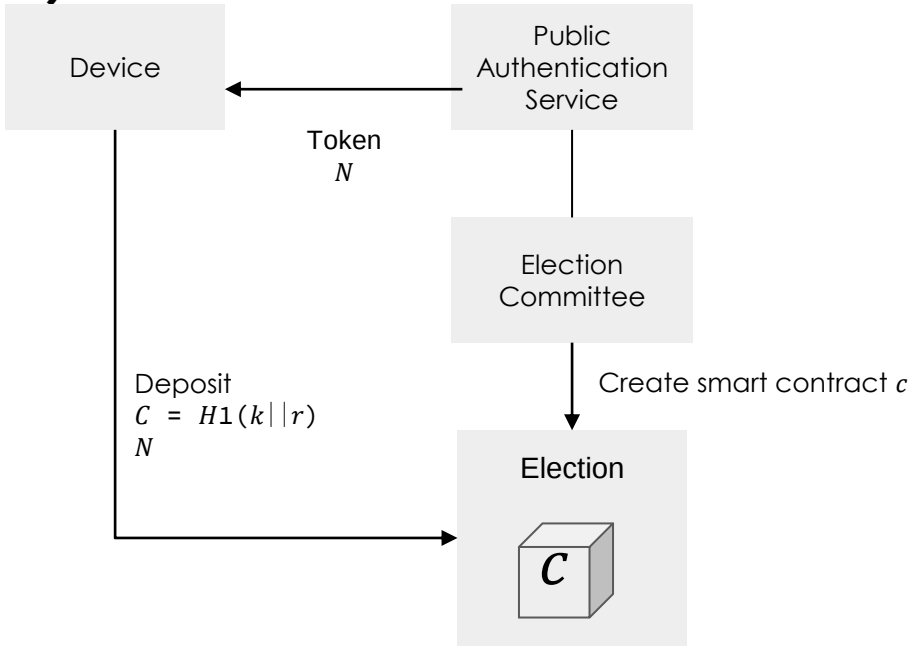
deposit (reception)

- Randomly generate $k, r \in \mathbb{B}^{248}$, calculate $C = H_1(k||r)$
- Send N amount of coins to smart contract c along with C
  - At this time C is an unsigned 256-bit integer
- If there is space on the Merkle tree, c accepts the transaction then adds C to the Merkle tree as a non-zero value

Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

deposit (reception)



Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

withdraw (Voting)

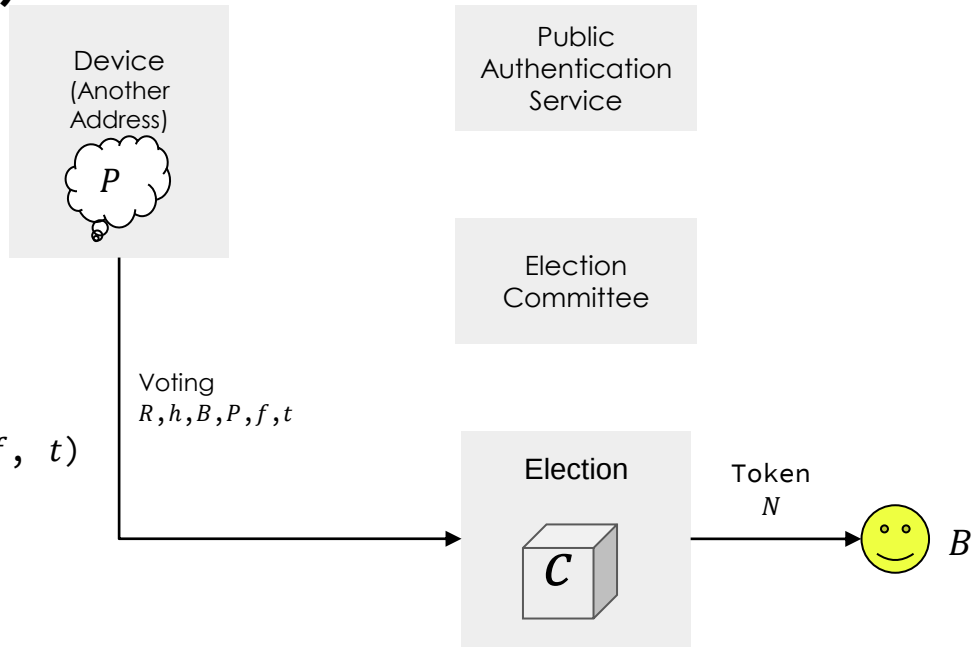
- ❑ Select Candidate B
  - ❑ Select the fee for relayer $f \leq N$ (optional)
- ❑ Select root R from the options stored in the smart contract and calculate the path $O(\iota)$ ending in R
- ❑ Calculate $h = H_1(k)$ which is the *nullifier hashed value*
- ❑ Create Proof P by calling up d_p in Prove function
- ❑ Execute *withdraw* using one of the following methods:
  - ❑ send a transaction to c with R, h, B, f, t, P
  - ❑ send a transaction request to relayer with R, h, B, f, t, P to c
- ❑ After this has been completed, map h to the mapping variable L in $L[h]$ = true

Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

withdraw (Voting)

R = Root
h = $H_1(k)$
B = Candidate address
P = Prove(d_p, τ, ι, B, f, t)



Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

Prevention of Double Voting

- Contract c saves and stores R in past array n = 100
- The most up to date Merkle tree t saves and stores the value of the node on the most recently added leaf-to-root path as well as the one required to calculate the next route.
- The mapping variable shall be L, map h with the success of *withdraw*, and verify $L[h] \neq true$ when the *withdraw* function is called.

Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

Tasks

- ❑ When using the Ethereum mainnet
  - ❑ Will voters have to pay for gas?
  - ❑ When using relayer, is it reliable? (Risk of SPOF)
- ❑ Configuration when voting result isn't be disclosed (i.e using batch process) until the end of voting period
  - ❑ Who will do this?
  - ❑ Can it be trusted?
  - ❑ Staking, etc?
- ❑ Is it possible to certify voting results are accurate?

Is the Confidentiality Protocol Cream Adaptable to Internet Voting?

ETHTerakoya

V2 implementation

- Layer2, Migration to Operator Model
  - **Pros**
    - Gas cost reduction
    - Increase in Tps
    - Tx batch processing → concealing interim progress
    - Multiple votes within the voting period → conspiracy prevention (MACI)
  - **Cons**
    - Perfect Operator(s) trust model → Can this be decentralized?