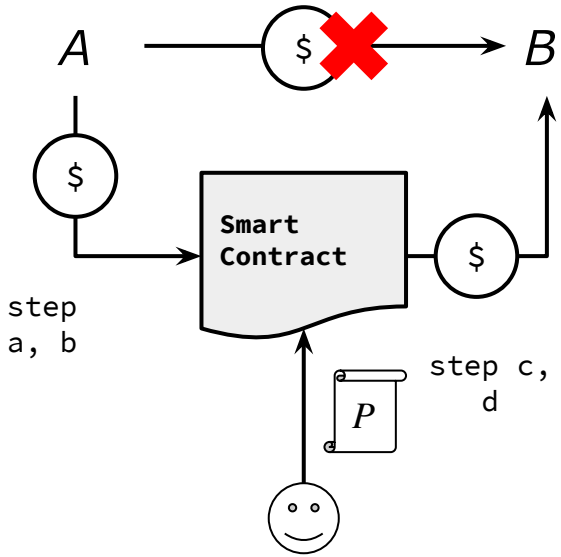
秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

about CREAM？

- https://github.com/couger-inc/cream
- ERC(20/721)コインを使った匿名投票
- 投票ステップ概要 (version 1.0)
  a. 受付フェーズ
  b. 投票コントラクトがコインの depositを受入
  c. デポジット時以外のアカウント（もしくはリレイヤー）から投票コントラクトを呼び出し、別のアカウントへwithdrawする
  d. コントラクト側でwithdrawの履歴を管理し、二重投票防止



秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

anonimity

- deposit時のcommitmentを証明する
- 証明がtrueならdepositされたコインをwithdraw(transfer)できる
- tx発行はcommitmentを知っている人なら誰でも可能
  - つまりdepositとは別のアカウントから証明をする事ができる
- コインの送信元:fromは常にコントラクトアドレスなので、誰が誰へ投票したのかは秘匿化する事ができる

秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

setup ①

- $\mathbb{B} = \{0, 1\}$とする
- e をSNARK証明で使用されるペアリング演算、素数 q の群に対して定義されるものとする
- $H_1 : \mathbb{B} \to \mathbb{Z}_p$ をPedersenハッシュ関数とし、$H_2 : (\mathbb{Z}_p, \mathbb{Z}_p) \to \mathbb{Z}_p$ をMiMCハッシュ関数とする
- τ 任意の高さ（16）のマークル木とし、リーフではないノードは左右の子供を H_2 でハッシュ化する
- $O(\tau, \iota)$ をインデックス ι を持つルートハッシュ R で表されるマークル木 τ のパスとする

秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

setup ②

- ❏ $k \in \mathbb{B}^{248}$ の値 k を*nullifier*とし、$r \in \mathbb{B}^{248}$ の値 r を*secret*とする
- ❏ B を候補者のEthereum addressとする
- ❏ $S[R,\hbar,B,f,t]$ を公開値 R, $\hbar$, B, f, t をもつ次の知識の記述とする

  : $S[R,\hbar,B,f,t] = \{\hbar = H_1(k)$ かつ O の値がポジション ι での $H_2(k||r)$の R へのパスとなる $k,r \in \mathbb{B}^{248}$, $\iota \in {}^{16}\mathbb{B}$, $O \in {}^{16}\mathbb{Z}_p$ を知っている$\}$

  - ❏ f = リレイヤーノードを経由した際の手数料
  - ❏ t = リレイヤーノードのアドレス
  - ❏ $\hbar$ = *nullifier hash*と呼ぶ

秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

setup ③

- $D = (d_p, d_v)$ を信頼された設定手順（trusted setup）を使って作成された S のzk-SNARK証明検証鍵ペアとする
- 証明：$\mathtt{Prove}(d_p, \tau, \iota, B, f, t) \rightarrow P$
- 検証：$\mathtt{Verify}(d_v, P, R, \hbar, B, f, t)$

秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

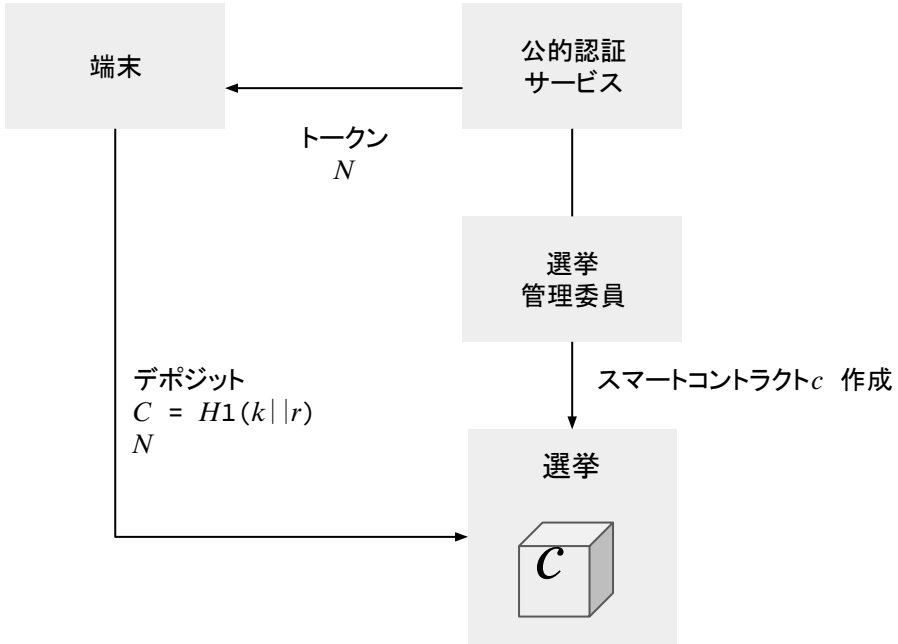
deposit（受付）

- $k, r \in \mathbb{B}^{248}$ をランダムに生成し、$C = H_1(k||r)$ を計算する
- コイン N 量をスマートコントラクト c へ C と共に送金する
  - この時 C は符号なし256ビット整数
- マークル木に空きが有れば c はトランザクションを受入れ、C をマークル木にゼロではない値として追加する

秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

deposit（受付）



秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

`withdraw`（投票）

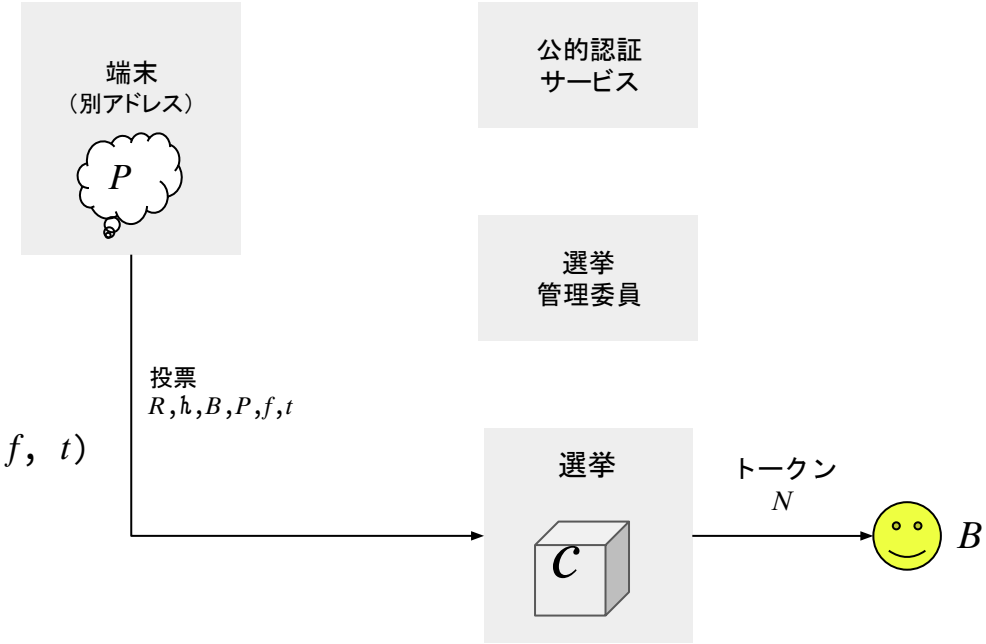
- ❏ 候補者 B を選択
  - ❏ リレイヤーへの手数料 $f \leq N$ を選択（オプション）
- ❏ スマートコントラクトに格納されているものの中からルート R を選択し、R で終わるパス$O(\iota)$を計算する
- ❏ *nullifier hash* 値である $\hbar = H_1(k)$ を計算する
- ❏ 証明 P を Prove関数に d_p を呼び作成する
- ❏ 以下の方法のどちらかで*withdraw*を実行する：
  - ❏ トランザクションを R，$\hbar$，B，f，t，P と共に c へ送る
  - ❏ リレイヤーへトランザクションリクエストを R，$\hbar$，B，f，t，P と共に c へ送る
- ❏ 実行後、$\hbar$ を c 上のマッピング変数 L へ $L[\hbar]$ = trueをマップする

秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

withdraw（投票）

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



秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

二重投票の防止

- コントラクト c は配列に過去 $n = 100$ 個の R を保管する
- 最新のマークル木 t は、最後に追加されたリーフからルートまでのパス上のノードの値を格納し、次のルートを計算するのに必要なノードの値を格納する
- マッピング変数 L とし、*withdraw*が成功した h をマップし、withdraw関数が呼ばれる際に $L[h] \neq true$ を検証する

秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

課題

- Ethereum mainnetを使う場合
  - gasを投票者が支払うのか？
  - リレイヤーを使う場合、信頼できるのか？（SPOFになる可能性）
- 投票終了まで投票結果を表示しない（バッチ処理を行う）場合の構成
  - 誰が行う？
  - 信頼できるか？
  - ステーキングなど？
- 投票の結果の保証はできるのか？

秘匿化プロトコルCreamはインターネット投票に適応可能か？

ETHTerakoya

V2実装

- Layer2, Operatorモデルへ移行
  - **Pros**
    - Gas費用削減
    - Tps増加
    - Txバッチ処理 → 途中経過の非公開
    - 期限内の複数回投票 → 共謀防止(MACI)
  - **Cons**
    - 完全Operator(s)信頼モデル → 分散化できる？