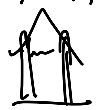
Ecash

Thursday, November 16, 2017 12:34 PM

Anonymous Credentials

Issuing Authority



Alice

{"name": Alice
"DoB": 12/1/89
"SSN": XXX-XX-XXXX
"City": Orlando
"publickey": pkey
}

Signed by Authority σ

credentials

Alice → Web Service

authenticate session

"only users 18 years or older"

ZK { (credential, σ) : VerifySig(σ, credential, $pkey_{Authority}$)
- pkey,
- name,

credential.DoB < ($Today - 18 years)

credential.name = name }

Building a currency application using a bulletin board.

Starting point:	Bulletin Board	Piazza
- Anyone can post/view	✓	✓
- Append-only - no deletions - timestamps	✓	X
- Authentication	X	✓

Goal: Currency application "fair"

- Starts with a fixed initial allocation.
- You can send money to someone else
- No theft, - money conserved

...

A "pay", Bob, $2 →

$F_{currency}$ ← initial allocation

```
Bal := { Alice : $10,
         Bob : $10,
         ... }

on pay($X, R) from S:
  assert Bal[S] ≥ $X
  Bal[S] -= $X
  Bal[R] += $X
  leak ~~...~~ to A
```

→ "You have money!" $X to B

A

1. Simple Accounts

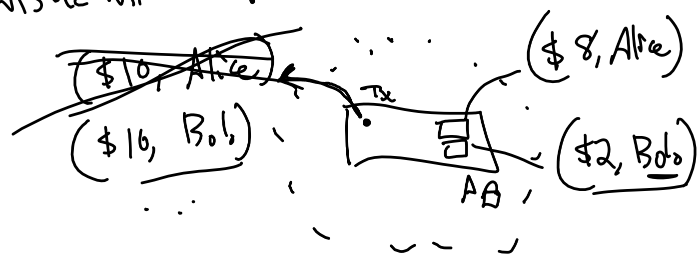
```
Bulletin Board
Bal = { Alice, ...
        Bob, ...
tx1
tx...
```

"Send $X from A to B"
- signed by A

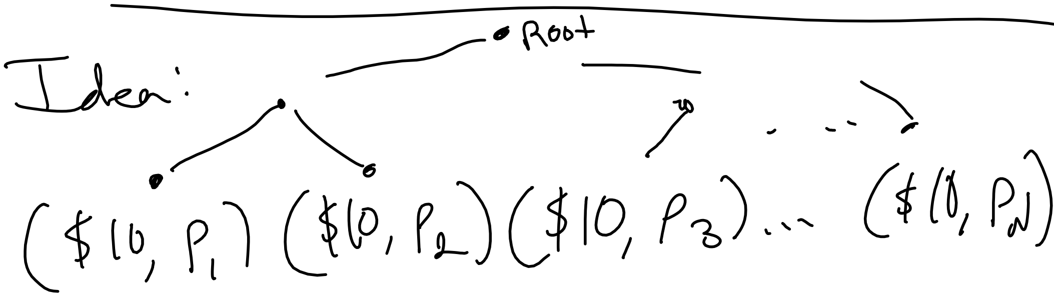
- post signed msg's to BB
- everyone can replay tx and checks
  - signature is valid
  - account balance sufficient

  otherwise ignore

2. Transaction Graph



3. Idea:



Spend one of the coins w/o revealing which.

$m := (\$10, B)$

$$\mathrm{SoK}[m]\{(x): P_1 = g^x \text{ OR } P_2 = g^x \dots \text{ OR } P_N = g^x\}$$

— Problem 1: double spends

Solution: "Key Image" $\underline{I(P) = \underline{prf_x}(P)}$ where $x = \log_g P$

$$\mathrm{SoK}[m]\{(x): (\underline{P_1} = g^x \text{ and } \underline{I} = prf_x(P_1)) \text{ OR } (\underline{P_2} = g^x \text{ and } I = prf_x(P_2)) \dots\}$$

$P_1, \dots P_N$, I

— Discard transaction if I is already used.

— Problem 2: Efficiency.

proofs are $O(N)$ for N coins

merkle branch

$$\mathrm{SoK}[m]\{(x, \underline{P}, \pi) : \text{and } I = prf_x(P)$$

$$\underline{P} = g^x, \quad \underline{\text{MerkleVerify}(\underline{\text{ROOT}}, (P, \$10), \pi) = 1}\}$$

root, leaf, branch

ROOT, I,

merkle root over $(P_1, \$X), \dots (P_N, \$X)$

Now only $O(\log N)$ elements.

— Problem 3: Amounts are the same!

$(P_1, \$10), (P_2, \$8) \dots$

Solution: Pedersen Commitments

$(P_1, C_1), \dots (P_N, C_N)$

$m := (P_{new}, C_{new})$ $\quad \$X$

$\mathrm{SoK}[m]\{(X, P, \pi, r, r_{new}): \$X, r$

ZK(...) (...) $C = g\ h$

$\text{Merkle}^{\text{verify}}_{@}\left((R, C) \ldots\right)$

$$C = g^{\underline{\$X}} h^{r}$$

and $$C_{new} = g^{\underline{\$X}} h^{r_{new}}$$

$$\sum_{i \in In} \$X_i = \sum_{i \in out} \$X_i$$

— Problem 4: Interaction for each payment

Idea: Derived public key