Anonymous Credentials

Issuing Authority

Alice

credentials

Web Service

authenticate session

"only users 18 years old"

ZK \{(credential, c) : VerifySeq((credential, pkx, Authority))

Credential.DOB < (Today - 18 years)

Credential.name = name

Building a Currency application

Using a bulletin board.

StrengthPoint: Bulletin Board

- Anyone can post/rev ✓ ✓
- Access only ✓ x
  - no X X
  - no threats X ✓
- Authentication x ✓

Goal: Currency application

- Starts with a fixed initial allocation ✓ ✓
- You can send money to someone else ✓ ✓
- No theft ✓ ✓
- money conserved ✓ ✓
1. Simple Accounts

- Billboards:
  - Bob: $10
  - Alice: $10

- Transaction:
  - $X from A to B
  - Signed by A

- Post-signed msg to BB
- Everyone can replay tx and check
- Signature is valid
- Account balance serves
- Otherwise ignored

2. Transaction Graph

   ($10, Alice)  
   ($10, Bob)  
   ($2, Bob)  

2. Idea:

   ($10, A) ($10, B) ($10, C) ... ($10, P)

   Spend one of the coins /o re-encoding which:

   \[ m := ($10, B) \]
\[ \text{SoK}^{-1} (x) : \quad P_i = g^x \\
\text{or} \quad \text{P}_2 = g^x \\
\text{or} \quad \text{P}_n = g^{x_n} \]

- Problem: Double spends
- Solution: "Key Image" \( I(P) = \text{prf}_x(P) \) where \( x = \log P \)

\[ \text{SoK}^{-1} (x) : \begin{cases} 
(P_1 = g^x \text{ and } I = \text{prf}_x(P_1)) \\
\text{or} \quad (P_2 = g^x \text{ and } I = \text{prf}_x(P_2)) \\
\text{or} \quad \ldots 
\end{cases} \]

- Discard transaction if \( I \) is headers used.

- Problem 2: Efficiency
- Proofs are \( O(N) \) for \( N \) ashs

\[ \text{SoK}^{-1} (x) : \quad \text{Merkle hash} \quad \text{root I, P} = g^x \]

\[ \text{Merkle Roots} (\text{root}, (\text{P}, 10), X) = Y \]

\[ \text{Now only } O(\log N) \text{ elements.} \]

- Problem 3: Amounts are hashes

\[ (P_1, 10), (P_2, 8), \ldots \]

Solution: Pedersen commitments

\[ (P_1, C_1), \ldots (P_n, C_n) \]

\[ \text{xi} = (\text{key}, C_n) \]

\[ < 1 \subseteq \text{m} \subseteq (x, P, M, r, \text{root}) \text{, } x \text{, i, r} \]
\[ C = g \cdot h \]
\[ C = g^{x\cdot h} \]
\[ C_{\text{new}} = g^{x_{\text{new}} h} \]

\[ \sum_{i \in \text{In}} x_i = \sum_{i \in \text{Out}} x_i \]

---

**Problem 4:** Interaction for each payment

**Idea:** Denoted publicly