MIT Connection Science

Identities & Permission-Groups for Blockchains

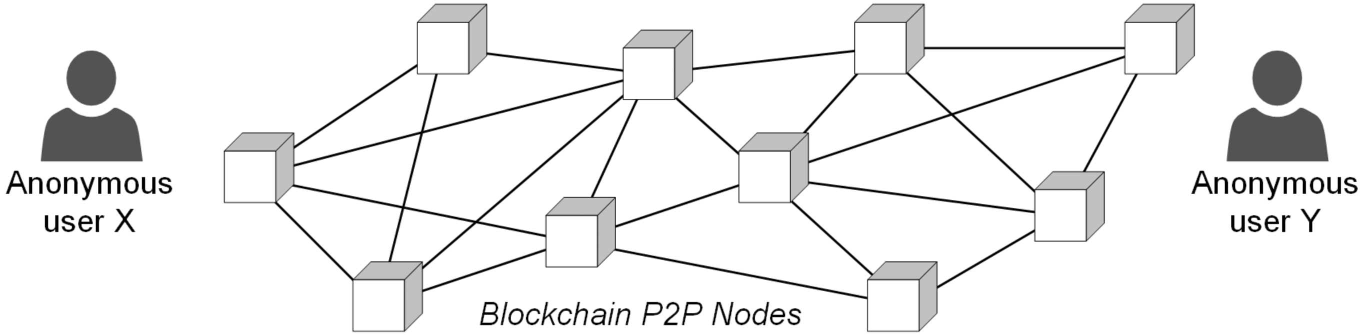
Overview of MIT ChainAnchor Project

Thomas Hardjono & Alex (Sandy) Pentland
MIT Connection Science

February 2016

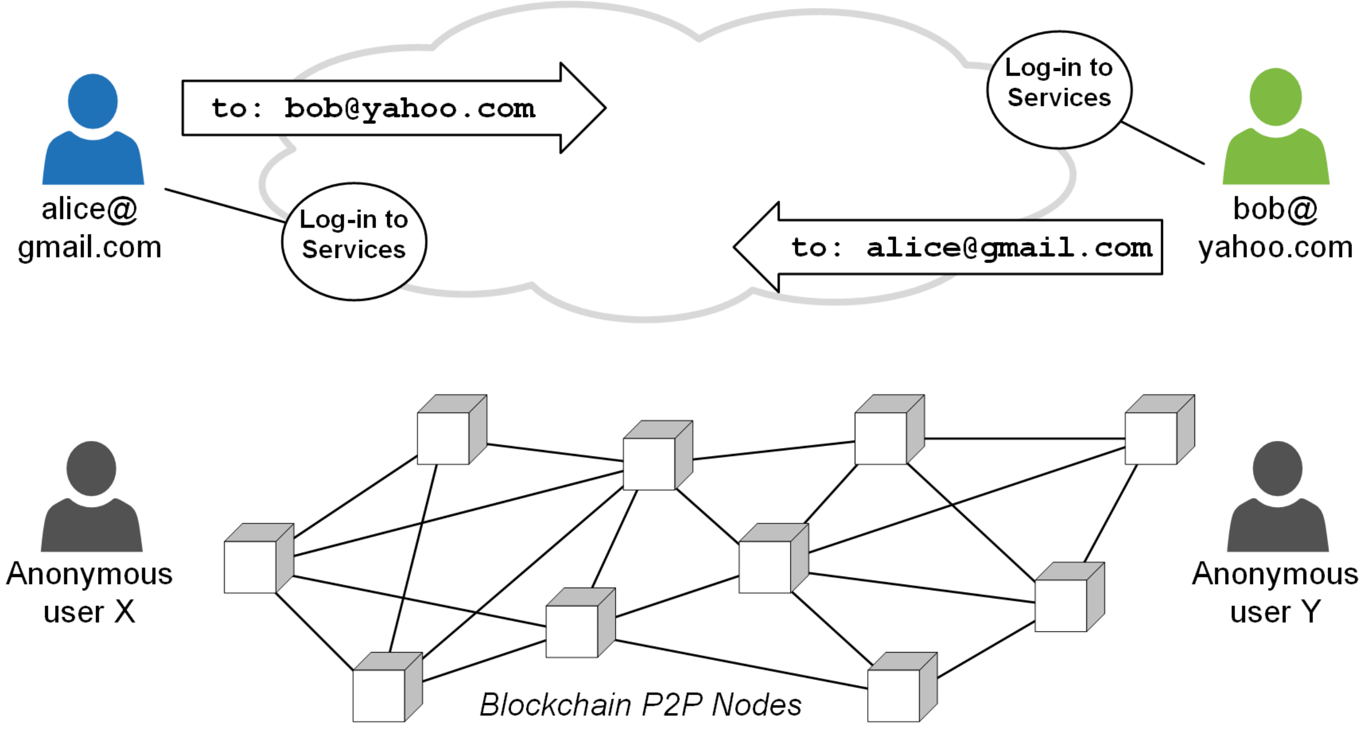
Current “Identities” in Bitcoin

- Entities known only by their public-key
- Self-created (”self-asserted”)
- Entities addressable only within Bitcoin
- Purposed solely for currency transactions

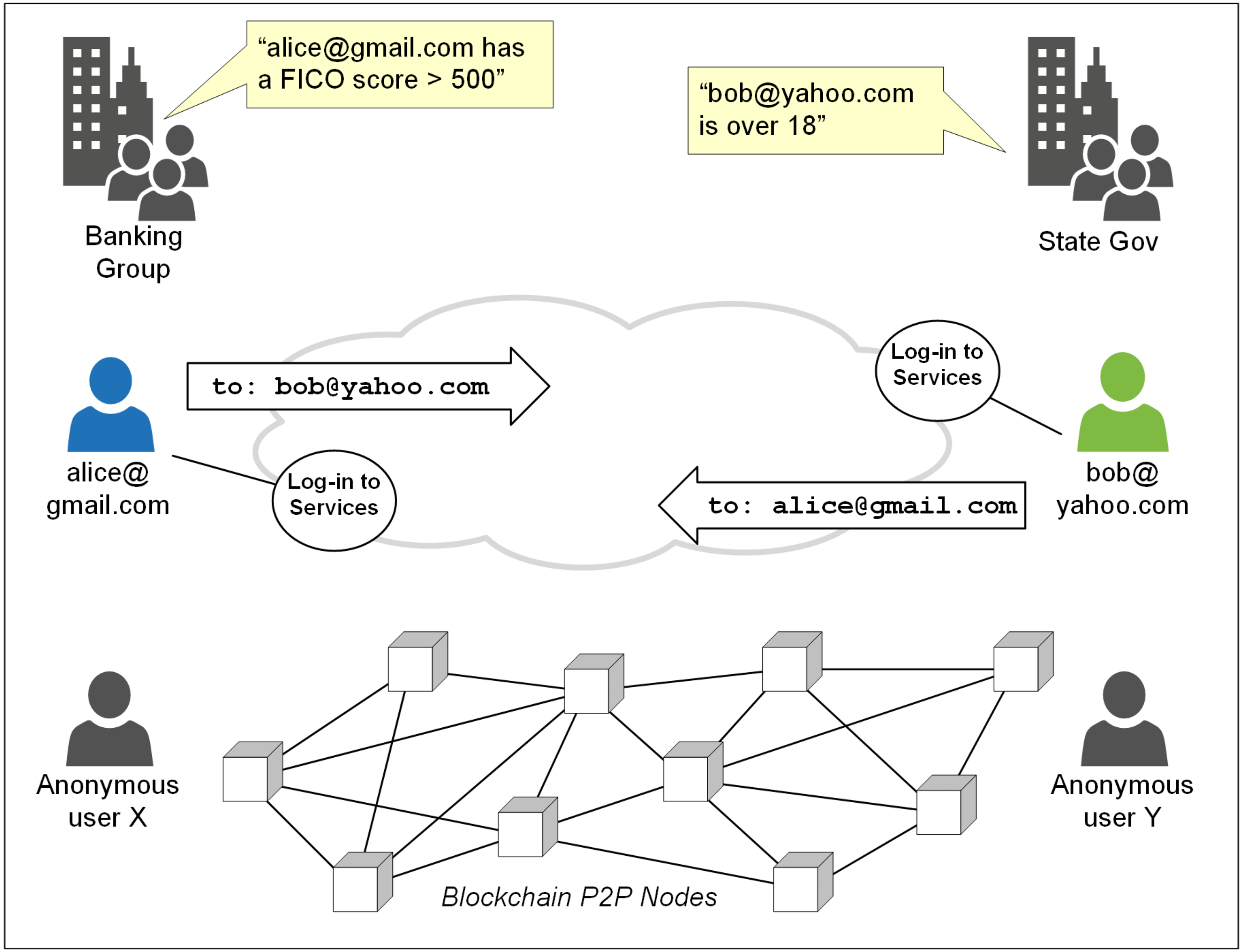


Digital Identities Today

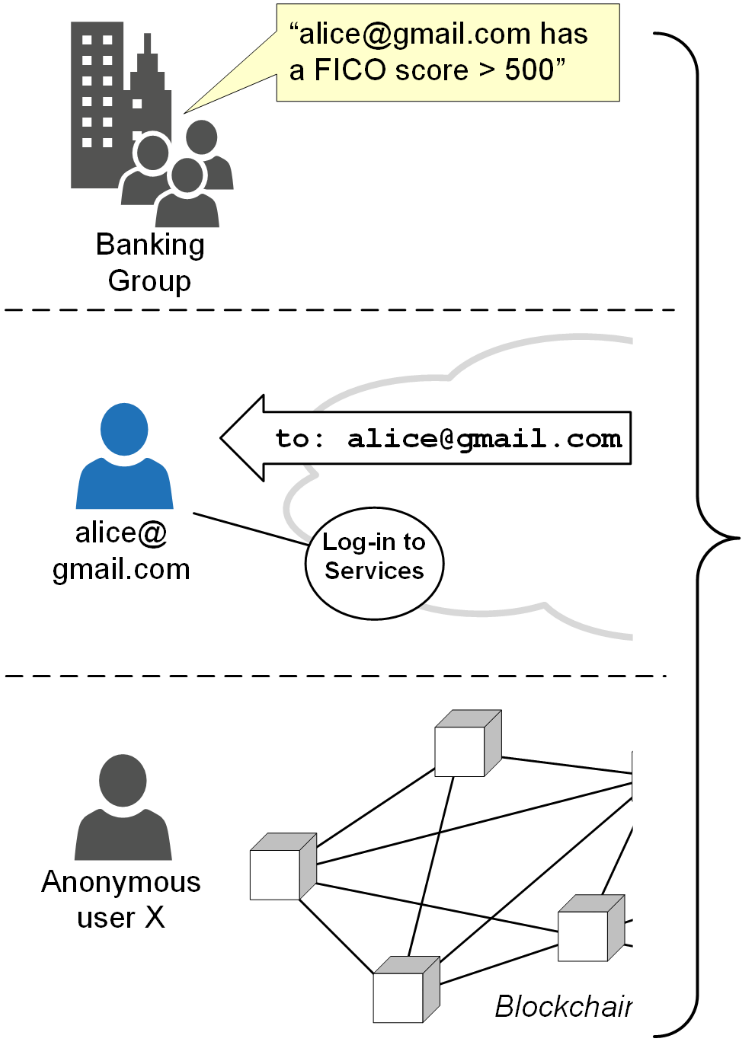
- Issued by Identity Providers (IdP)
- Addressable & routable globally (cf. DNS)
- Primary “identity” for accessing services



Attributes & Attribute Authorities



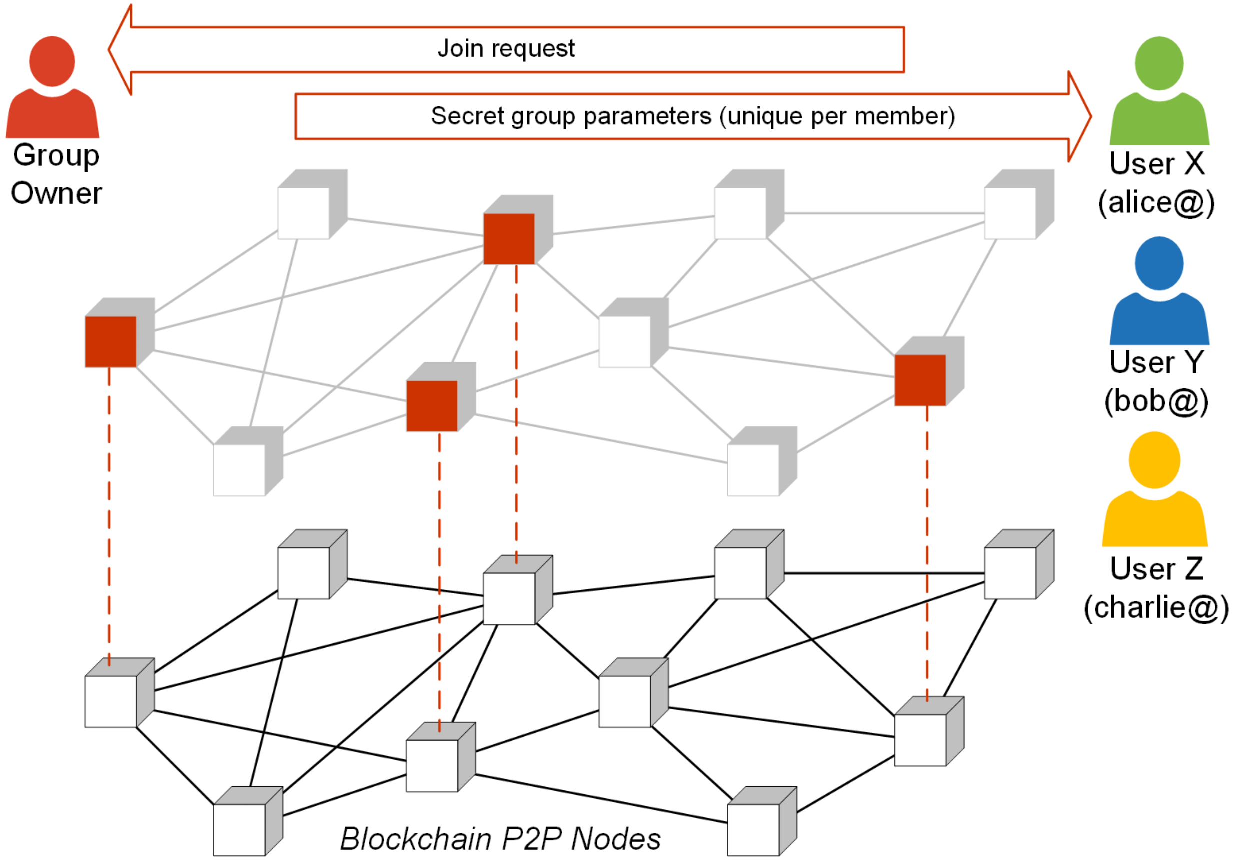
Challenge: Which Alice & Which Attributes



How to:

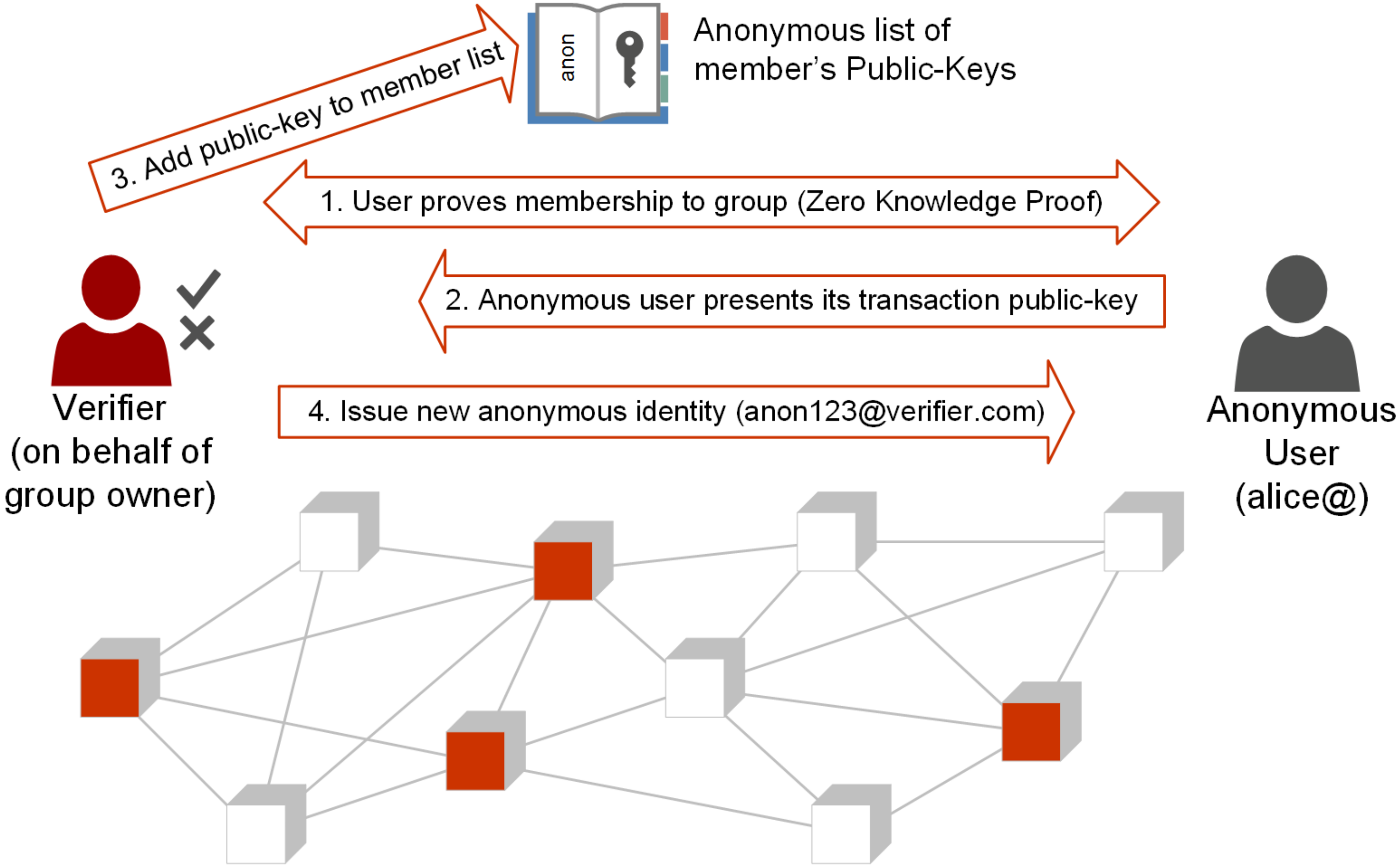
- "Link" identities across layers - preserving privacy
- Option to remain anonymous but verifiable
- Option to disclose an anonymous identity – without affecting other owned identities
- Bind attributes to anonymous identity with verifiable truthfulness

ChainAnchor: Permission Groups



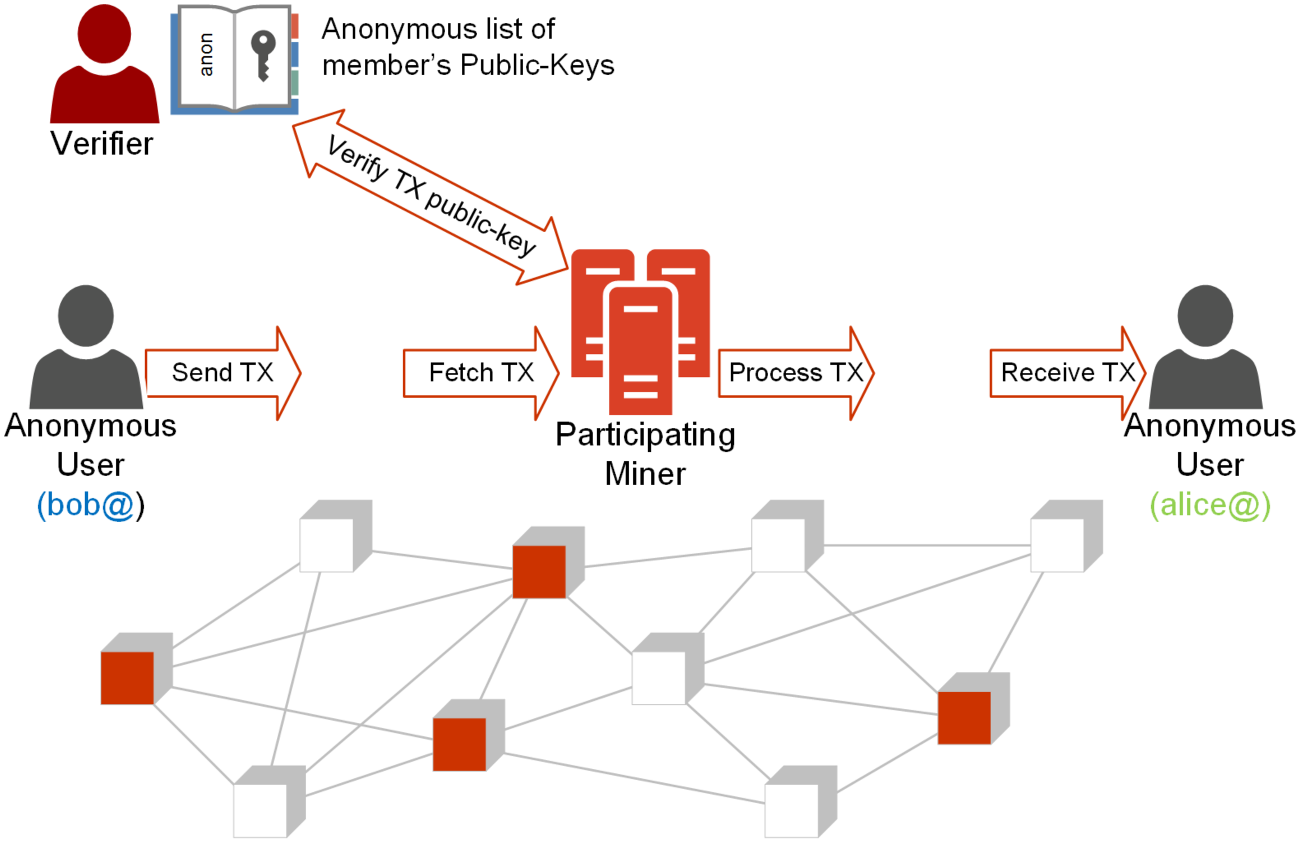
- Permission Group = Logical group of entities sharing a common blockchain
- Group Owner initially knows true identity of members
- Each member is given unique secret keying material & parameters
- Each member “blinds” keying material and then operates anonymously

Proving Membership (Anonymously)


3. Add public-key to member list
anon
Anonymous list of member's Public-Keys
1. User proves membership to group (Zero Knowledge Proof)
2. Anonymous user presents its transaction public-key
4. Issue new anonymous identity (anon123@verifier.com)
Verifier (on behalf of group owner)
Anonymous User (alice@)

- Member switches to anonymous & ``blinds'' secret keying material
- Member runs Zero-Knowledge Proof (ZKP) protocol with Verifier
- Member generates public-key pair, and Verifier adds pubkey to member's list
- From Step-2 onwards, user is anonymous to Group-Owner & Verifier

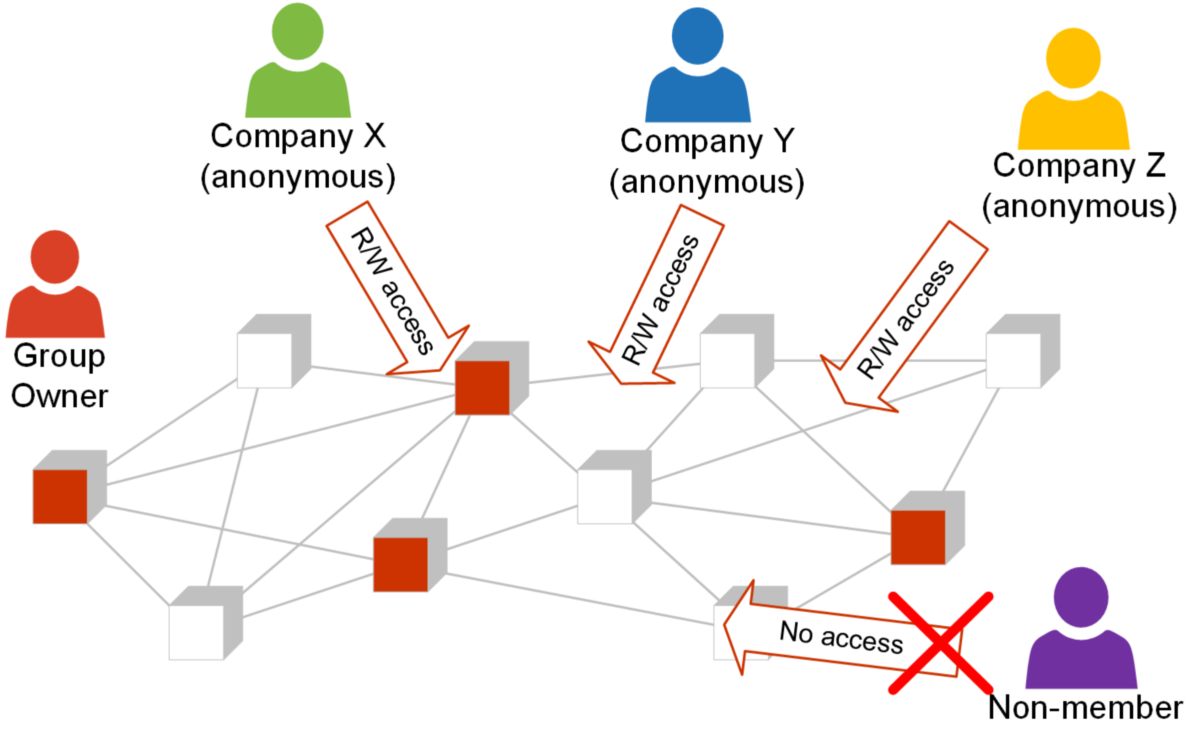
Filtering for Members' Transactions



- Participating miner chooses to process only members' transactions
- Miner looks-up anon list of members' public-keys prior to processing
- Miner can also remain anonymous by running ZKP protocol with Verifier
- Miner gets higher reward for participating – payout from Group-Owner

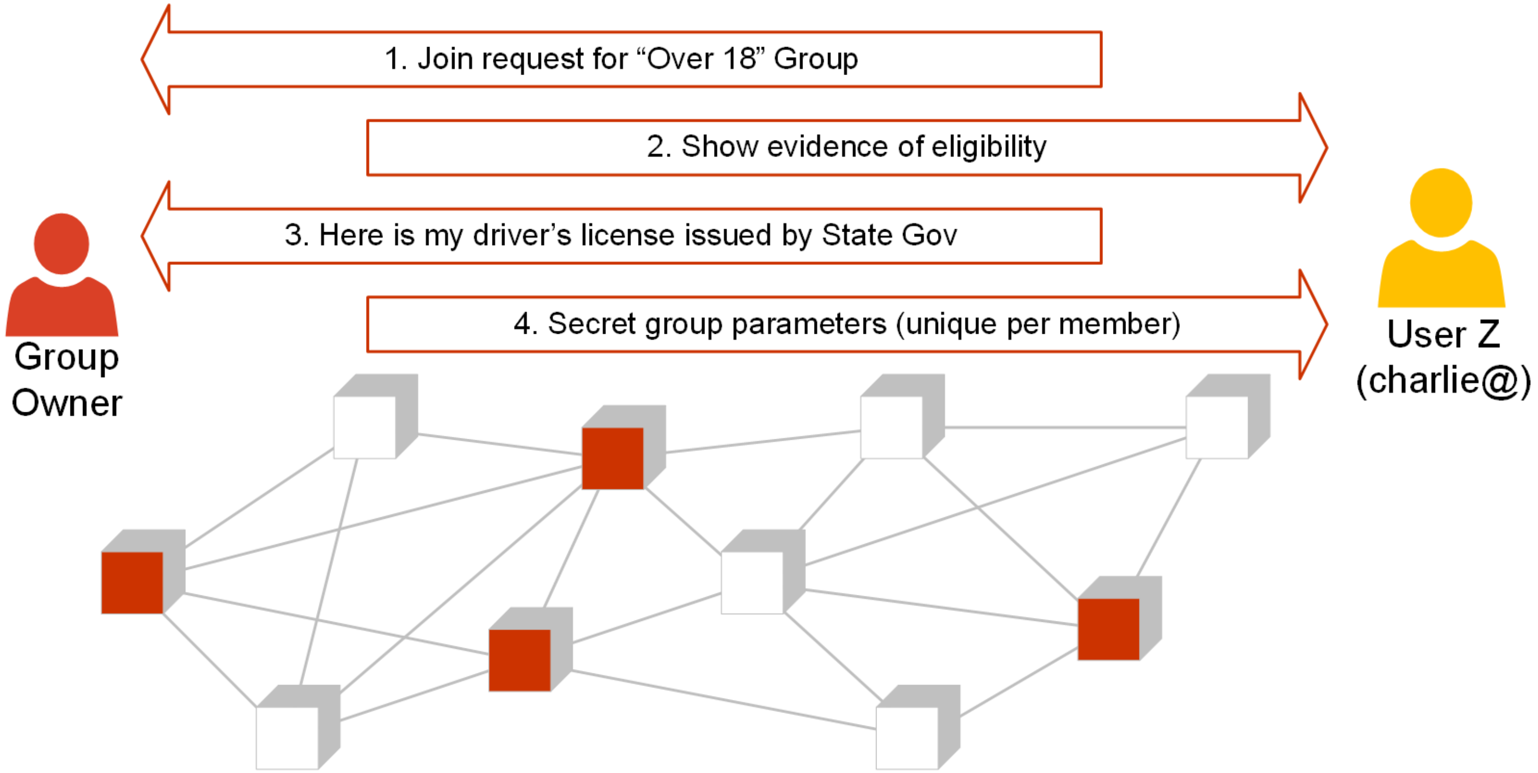
ChainAnchor: Use-Cases

Use Case #1: Competing Entities Sharing a Common Ledger



- ChainAnchor Group implements membership to shared blockchain
- Competing entities remain anonymous to one another
- Optional disclosure of identity when challenged (e.g. regulatory needs)
- Read/Write or Read-only access to shared blockchain

Use Case #2: Attribute Groups



1. Join request for “Over 18” Group

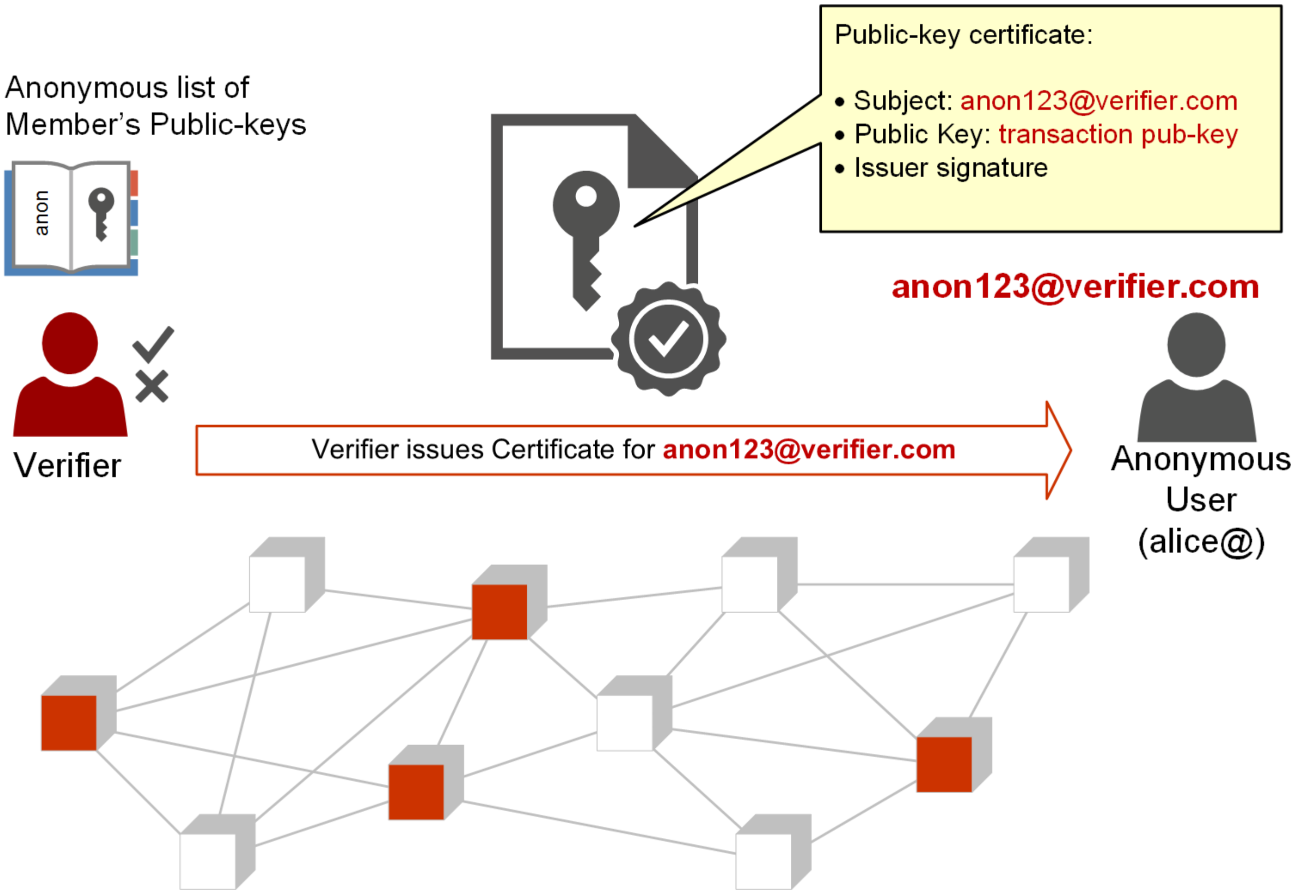
2. Show evidence of eligibility

3. Here is my driver’s license issued by State Gov

4. Secret group parameters (unique per member)

- Membership expresses possession of attributes (e.g. “Over 18” group)
- User must show evidence of eligibility (e.g. driver’s license)
- Evidence issued by external Attribute Authority
- User switches to anonymous mode after obtaining secret params.

Use-Case #3: Certificate for Anonymous Identity



Anonymous list of Member's Public-keys

Public-key certificate:

- Subject: anon123@verifier.com
- Public Key: transaction pub-key
- Issuer signature

anon123@verifier.com

Verifier

Verifier issues Certificate for **anon123@verifier.com**

Anonymous User (alice@)

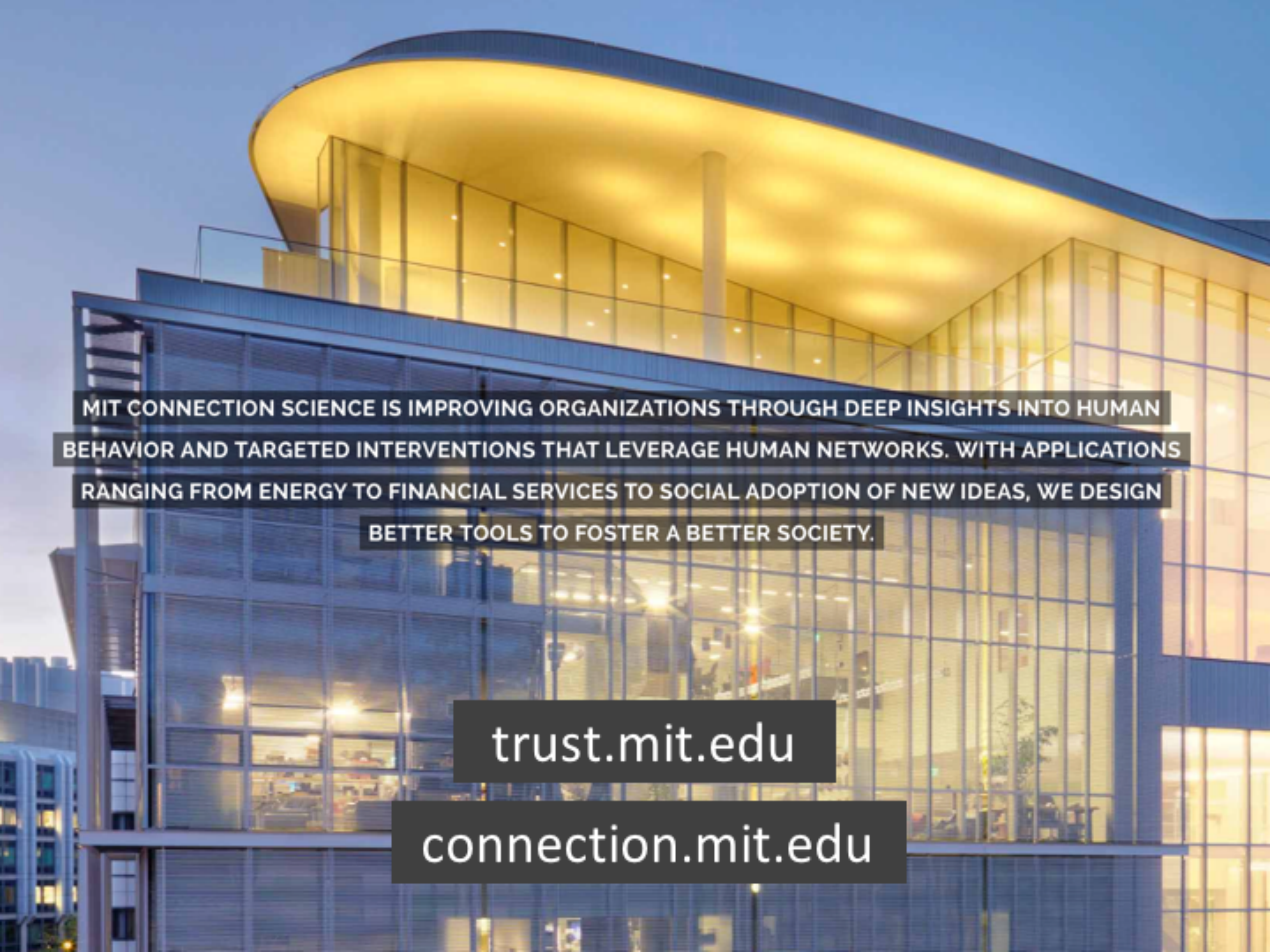
- Verifier becomes a Certificate Authority (or Registration Authority)
- Certificate contain anonymous identity & transaction public-key
- Certificate, identity & public-key usable outside blockchain

Use-Case #4: “AML-Friendly” Currency Circulation

- ChainAnchor group implements controls over currency circulation
- Group Owner disburses currency to members only
- Members can transact only within group
- Spending limit per transaction (per time duration)
- Miners verify membership of originator & recipient
  - TX with unknown originator/recipient are dropped
  - TX which violate spending limit are dropped
- Option to disclosed pubkey/address upon legal challenge – but without affecting other pubkeys
  - Property of ZKP protocol
- Can be “overlayed” atop Bitcoin

Contact

hardjono@media.mit.edu
sandy@media.mit.edu



MIT CONNECTION SCIENCE IS IMPROVING ORGANIZATIONS THROUGH DEEP INSIGHTS INTO HUMAN BEHAVIOR AND TARGETED INTERVENTIONS THAT LEVERAGE HUMAN NETWORKS. WITH APPLICATIONS RANGING FROM ENERGY TO FINANCIAL SERVICES TO SOCIAL ADOPTION OF NEW IDEAS, WE DESIGN BETTER TOOLS TO FOSTER A BETTER SOCIETY.

trust.mit.edu

connection.mit.edu