BLOCKCHAIN COMMONS

EDGE IDENTIFIERS & CRYPTOGRAPHIC CLIQUES

CHRISTOPHER ALLEN

PGP: `FDA6C78E`

- Internet Cryptography Pioneer
  - Co-editor & co-author – IETF TLS 1.0 protocol
- Decentralized Identity Architect
  - Co-organizer – ID 2020 (UN Summit on Digital Identity)
  - Co-author, –W3C Decentralized Identifiers 1.0
  - Founder – #RebootingWebOfTrust Workshops
  - W3C Invited Expert – DID 1.1 and Verifiable Credentials 1.1 Working Group
- Principal Architect, Executive Director – Blockchain Commons

WHAT IS BLOCKCHAIN COMMONS?

- We are a community that brings together stakeholders to collaboratively build open & interoperable, secure & compassionate infrastructure.
- We design decentralized solutions where everyone wins.
- We are a neutral “not-for-profit” that enables people to control their own digital destiny.

THE SINGLE SIGNATURE PARADIGM

- A Traditional Model for Identity
  - One private key
  - One public key
  - One identifier

THE SINGLE SIGNATURE PARADIGM

- But It Has Its **Dangers**
  - Single Point of Compromise
  - Single Point of Failure
  - Key Fragility & Bitrot
  - Side-Channel Attacks
  - Key Rotation Limitations

NOT THEORETICAL

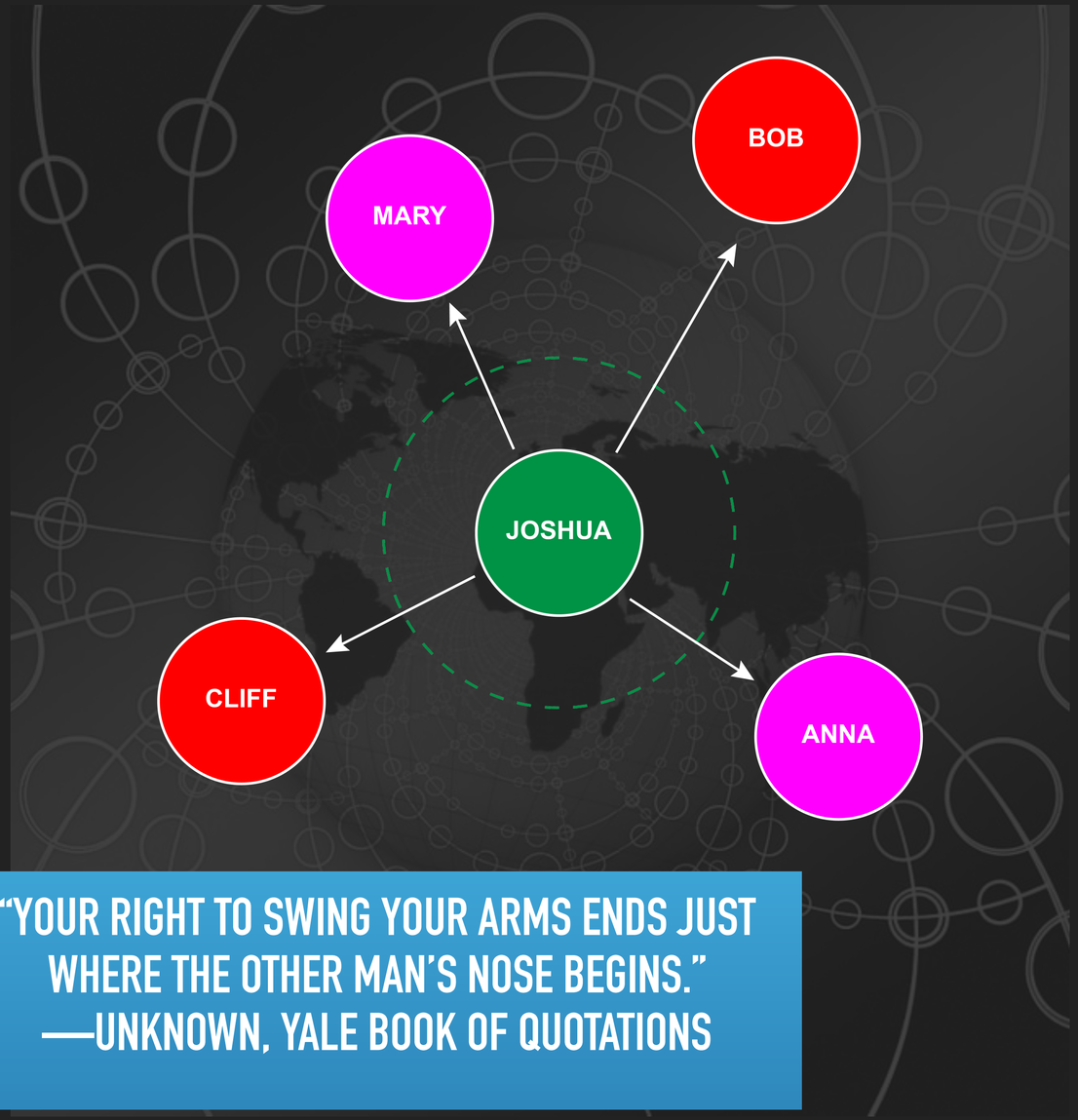
- From our ***#SmartCustody*** book (1999)
  28 Adversaries of Keys:
  - **Loss by Acts of God:** Death / Incapacitation; Denial of Access; Disaster
  - **Loss by Computer Error:** Bitrot; Systemic Key Compromise
  - **Loss by Crime, Theft:** Institutional Theft; Internal Theft; Network Attack, Personal; Network Attack, Systemic; Physical Theft, Casual; Physical Theft, Sophisticated; Social Engineering; Supply-Chain Attack
  - **Loss by Crime, Other Attacks:** Blackmail; Coercion; Non-Financially Motivated; Terrorist/Mob;
  - **Loss by Government:** Legal Forfeiture; Nation State Actor
  - **Loss by Mistakes:** Convenience; Key Fragility; Process Fatigue; Transaction Error; User Error;
  - **Privacy Related:** Censorship; Correlation; Loss of Fungibility

A NEW MODEL FOR IDENTIFIERS

WHAT IF IDENTITY WAS BASED ON RELATIONSHIPS?

RELATIONSHIPS & SSI

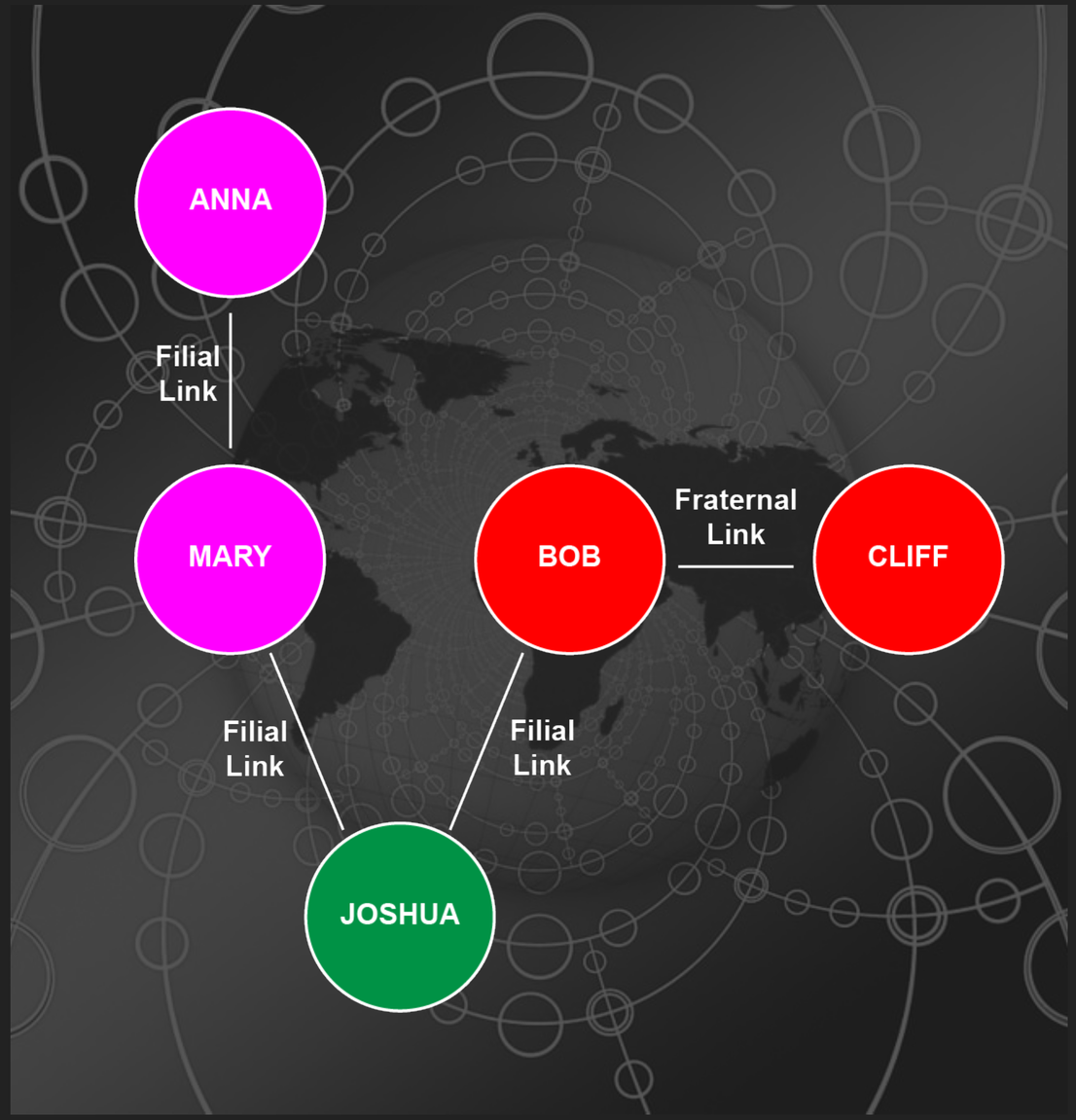
- Self-Sovereign Identity was always about relationships
  - You control your identity
  - You don’t control the network!
- Support human dignity



“YOUR RIGHT TO SWING YOUR ARMS ENDS JUST WHERE THE OTHER MAN’S NOSE BEGINS.”
—UNKNOWN, YALE BOOK OF QUOTATIONS

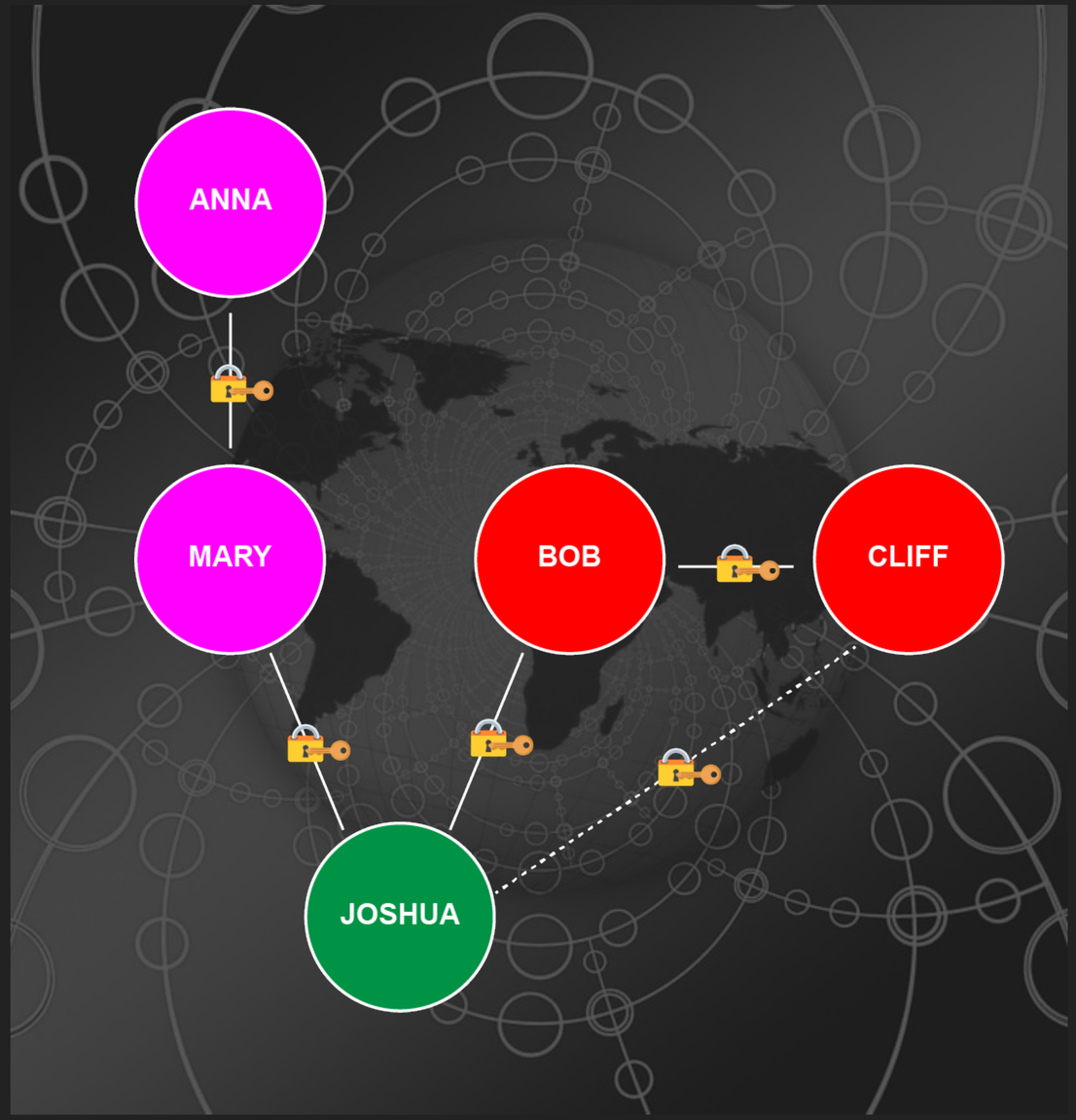
RELATIONAL EDGE IDENTITY

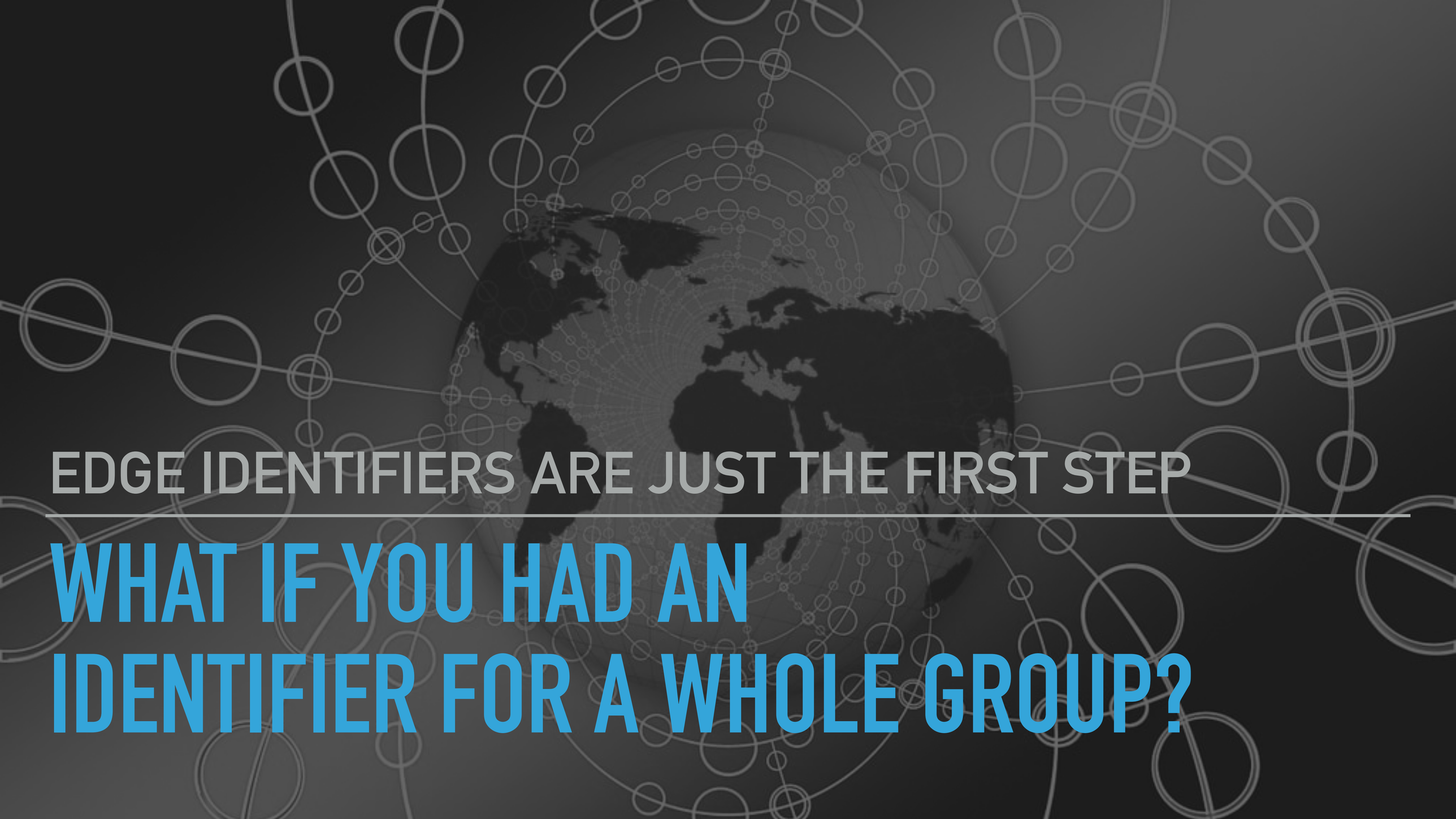
- Identity is actually decentralized
  - It can be viewed as relationships
  - Relational “edges” define connections
- These edges are the “membranes”
  - A **membrane** supports selective information exchange between entities
    - *(Thanks Living Systems Theory!)*
  - See also: *Local Names*, *Pet Names*



RELATIONAL EDGES & SCHNORR

- Schnorr gives us the power to create these **relational edges**
- Two entities create a key pair together
  - Each party contributes a secret
  - But key only exists in a cryptographic “fog”
  - Multisigs are the same size as single sig
- Group public key is an edge identifier
- Group “fog” private key allows for joint signature



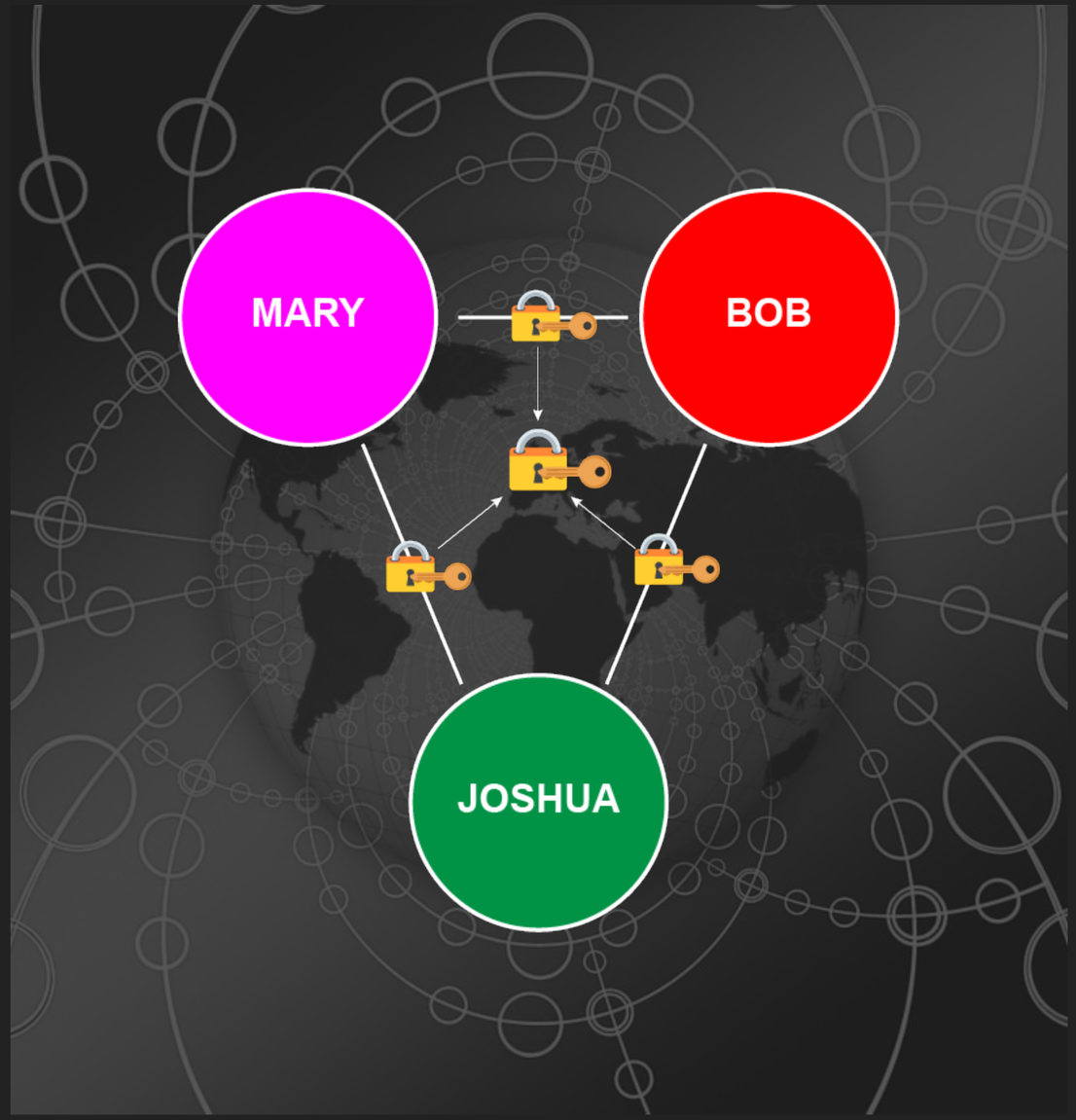


EDGE IDENTIFIERS ARE JUST THE FIRST STEP

WHAT IF YOU HAD AN IDENTIFIER FOR A WHOLE GROUP?

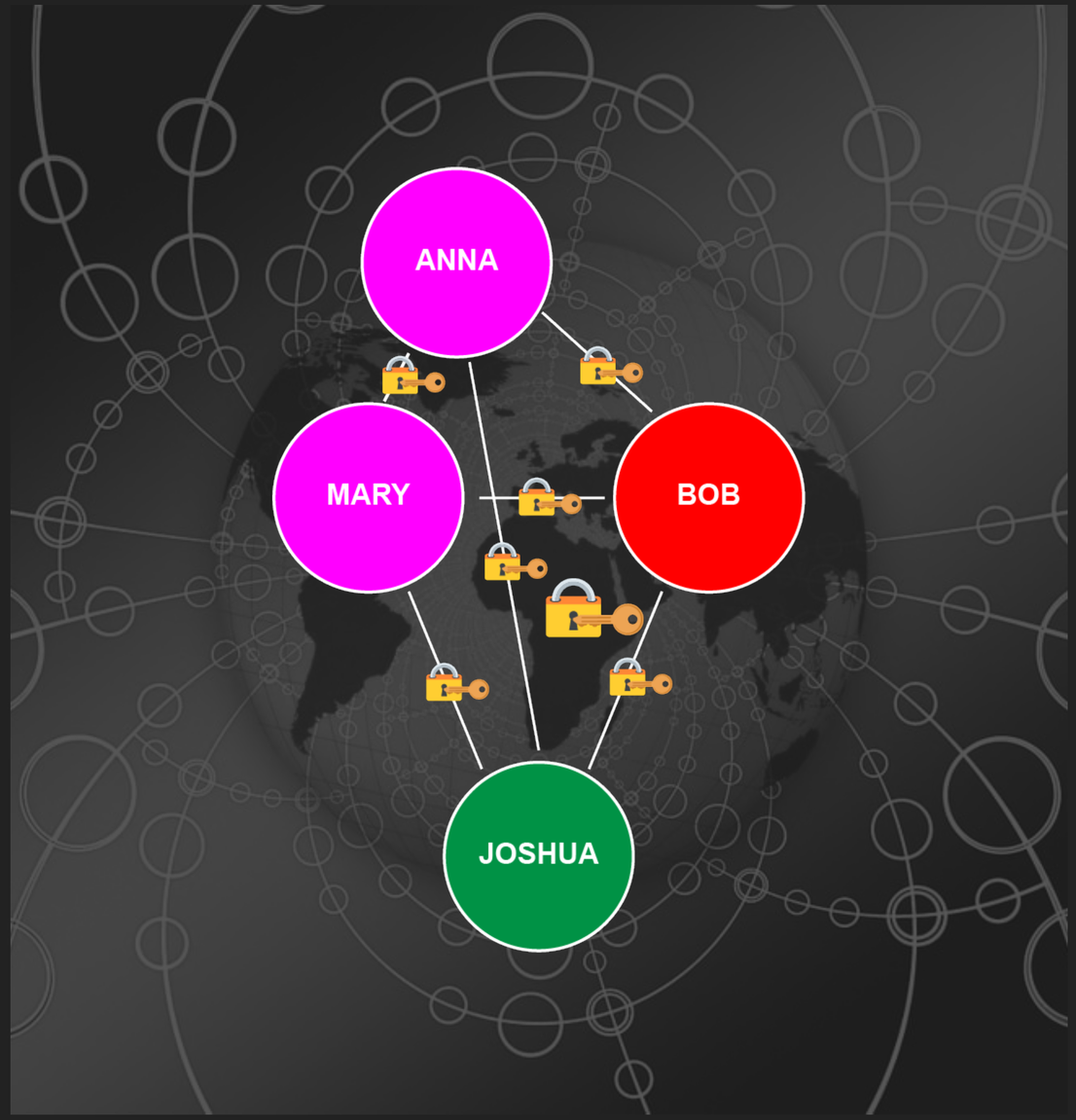
CLOSED CLIQUES

- Cryptographic clique
  - Simplest form is a **“triadic”** clique
- Edge identifier between every pair of entities
- Edge keys together create clique key
- Group public key identifies the clique
- Group private key is for joint decisions & signatures



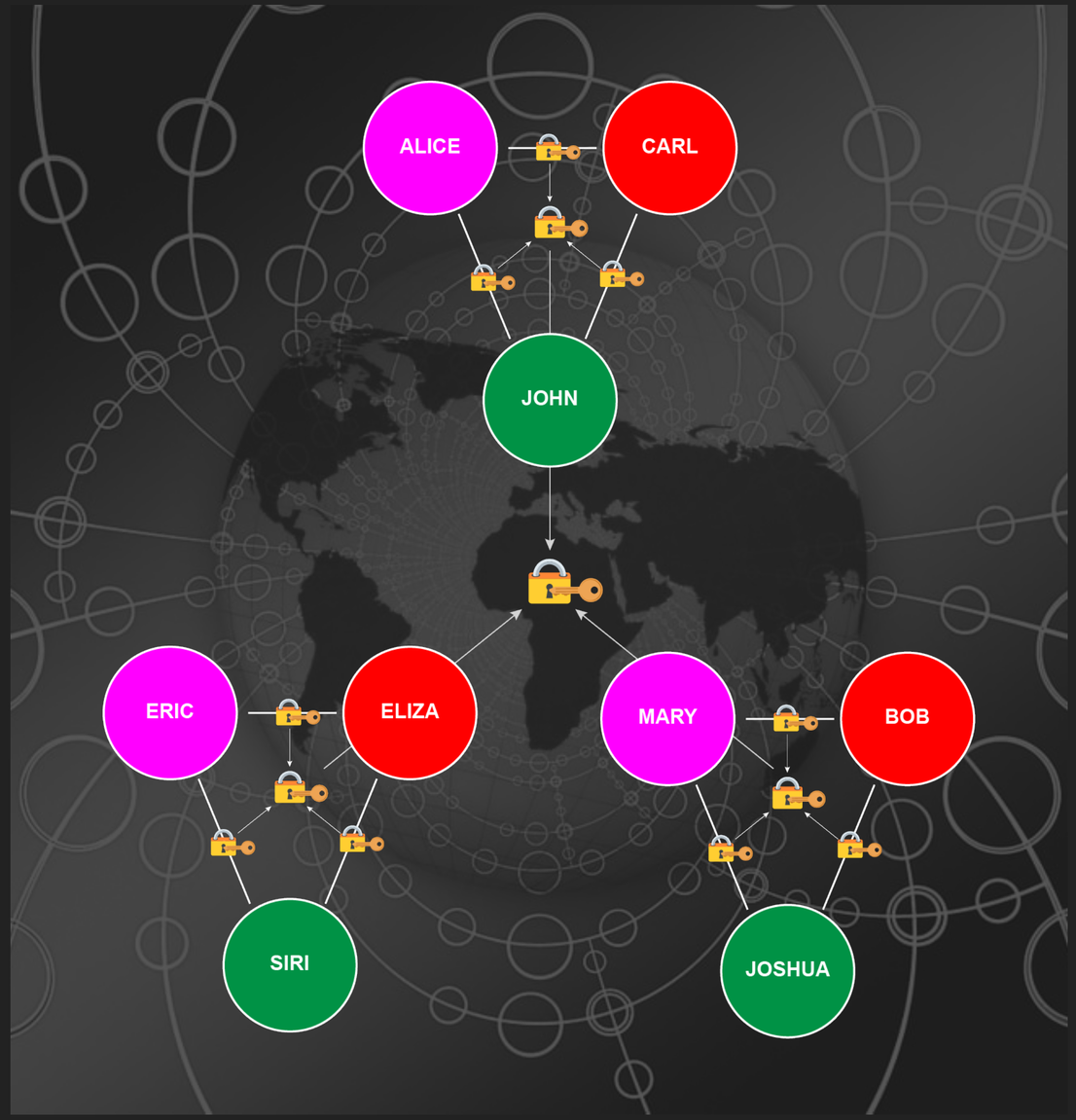
HIGHER ORDER CLIQUES

- Triadic cliques are simplest form
- Higher order cliques are possible
  - n nodes
  - (n*(n-1))/2 edges
- The more members, the **harder to close** graph!



CLIQUES OF CLIQUES

- Cliques are **recursive**!
- Instead of entities being edges …
  - They could be other cliques!
- This creates a clique of cliques



THE PURPOSE OF THE EXERCISE

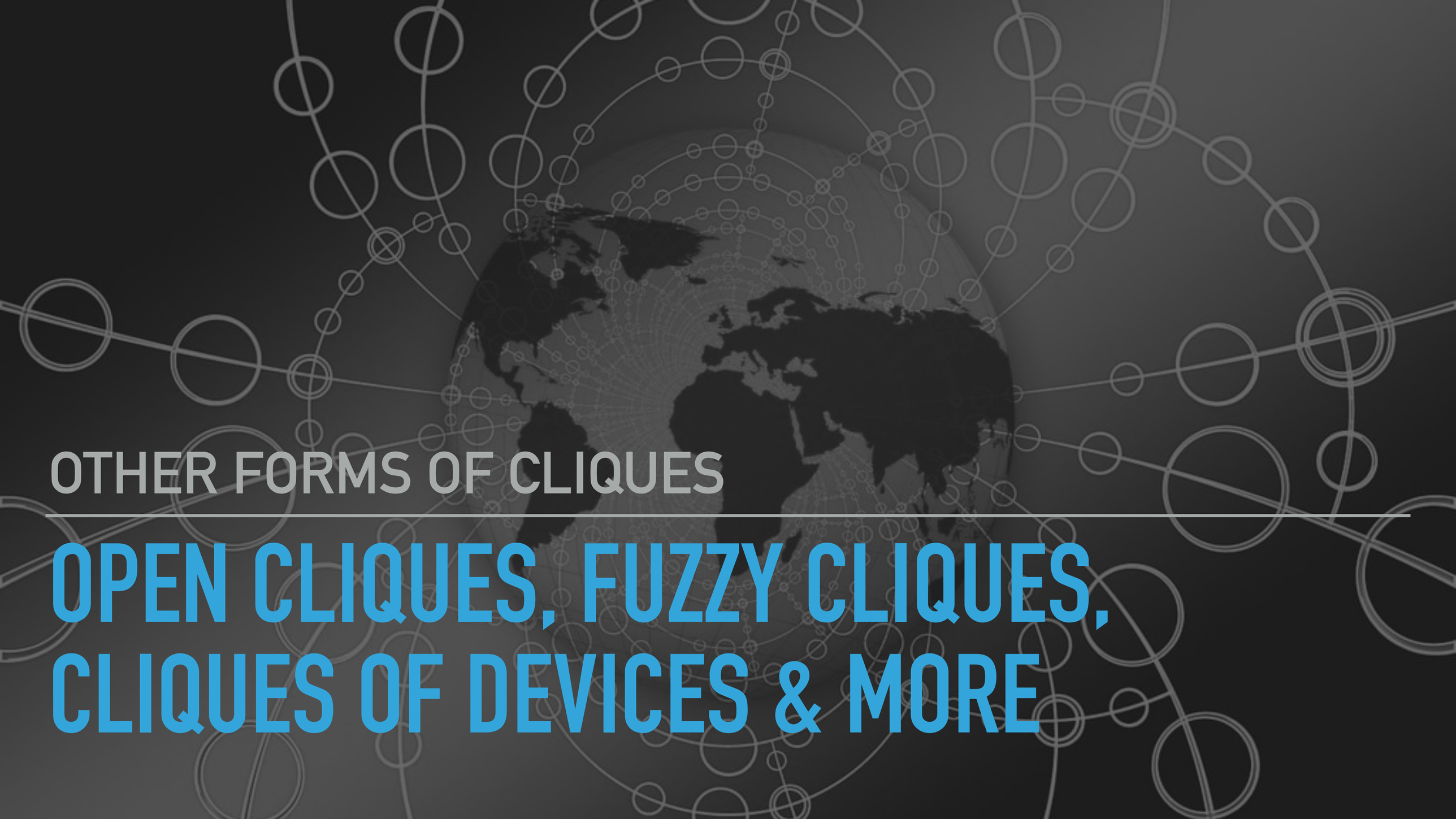
WHAT ARE THE ADVANTAGES OF EDGE IDENTIFIERS & CLIQUES?

CLIQUE IDENTIFIER SUPER POWERS

1. **Decentralized Identity Management.** Peer-based identity creation.
2. **Identity Validation.** Peer-based identity authentication.
3. **SPOC/SPOF Resilience.** Distributed control guards against compromise & failure.
4. **Secret Group Decision Making.** Decisions are secure, distributed, irrevocable, and coercion-resistant
5. **Enhanced Privacy.** MuSig Taproot trees & FROST both can increase privacy.

CLIQUE IDENTIFIER DRAWBACKS

1. **Technological Complexity.** Depends on multi signing Schnorr tech.
2. **Multisigning Takes Time.** No instant gratification!
3. **A New Paradigm.** Requires more study.

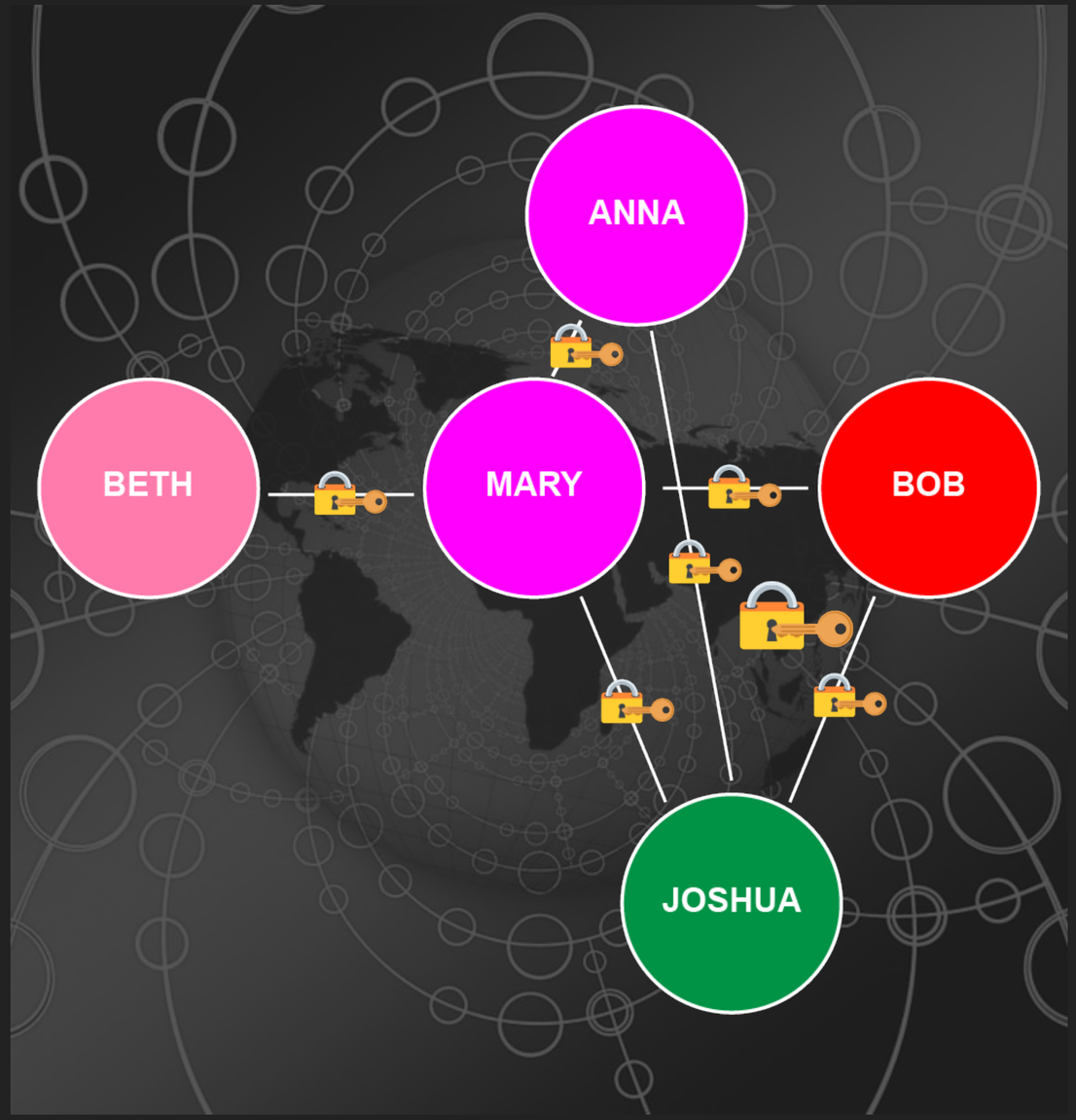


OTHER FORMS OF CLIQUES

OPEN CLIQUES, FUZZY CLIQUES, CLIQUES OF DEVICES & MORE

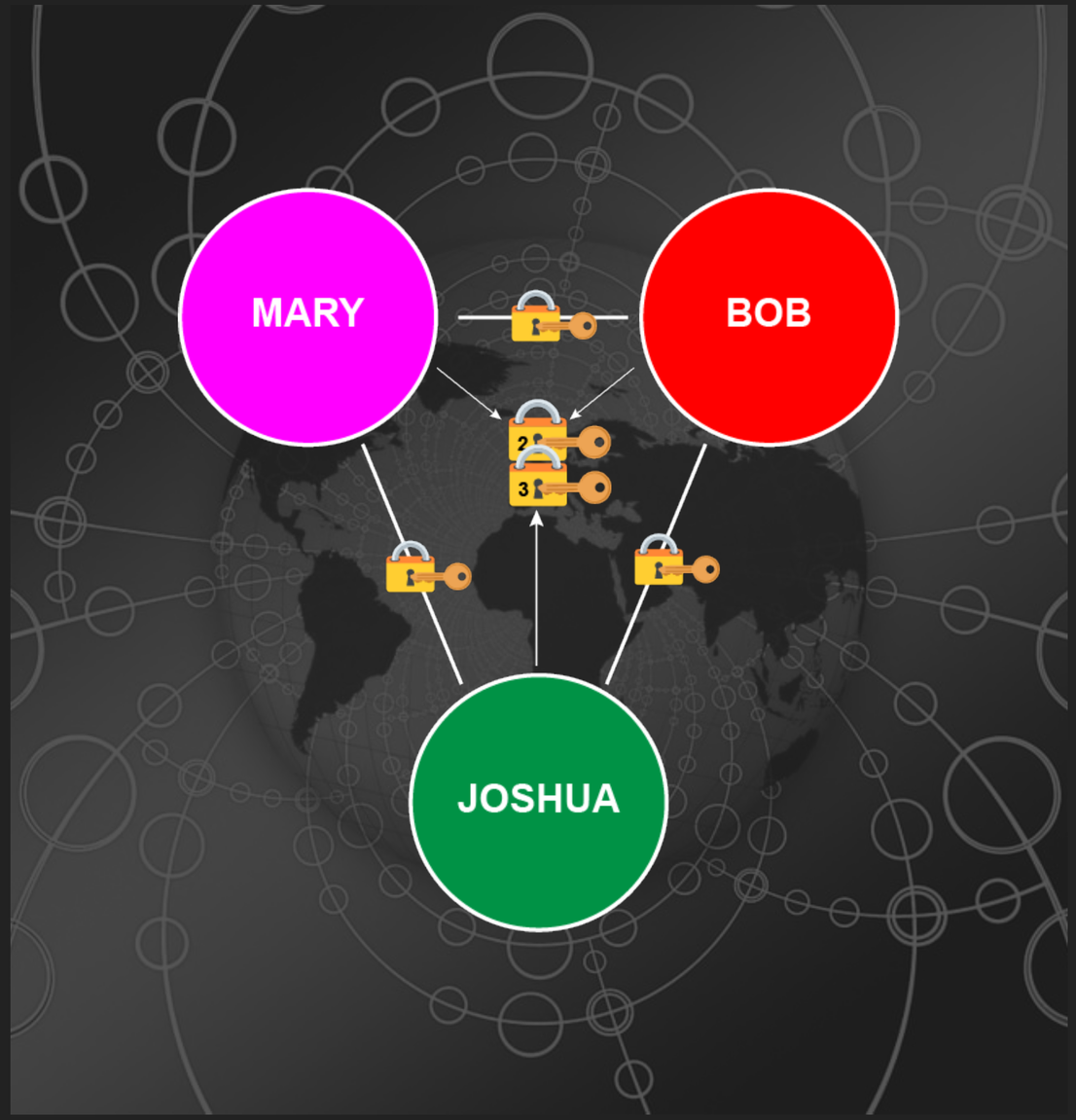
OPEN CLIQUES

- Cliques don’t have to be closed
  - Not everything is connected!
- Open cliques support realistic relationships
  - Can evolve & change
- Lose some graph-analysis advantages
- But lots of **new possibilities**



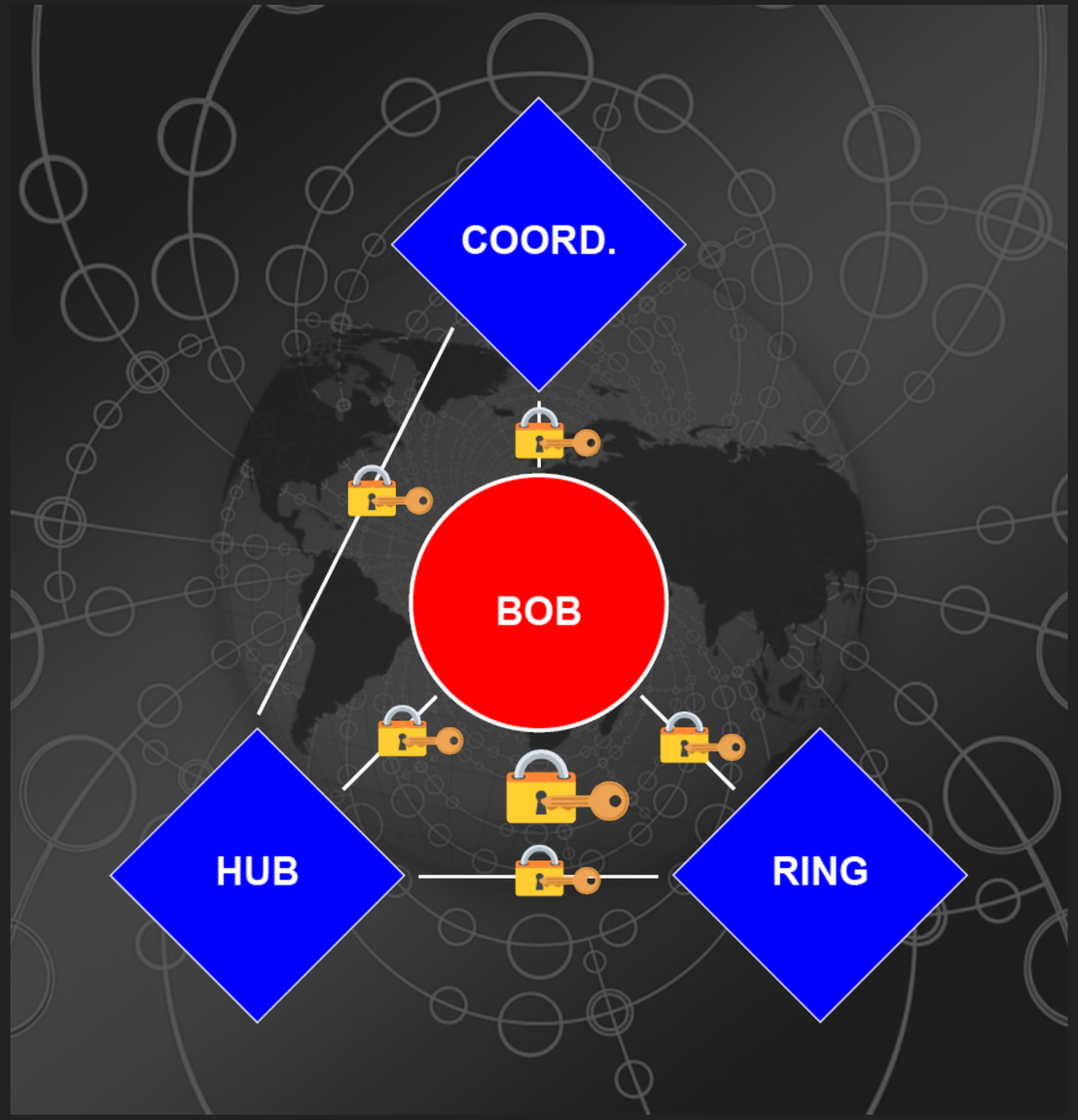
FUZZY CLIQUES

- **FROST** is one of the options for Schnorr
  - It has unique advantages
  - Can create Fuzzy Cliques
- Allows threshold signing
  - Just some members of clique
  - You don’t even know who!



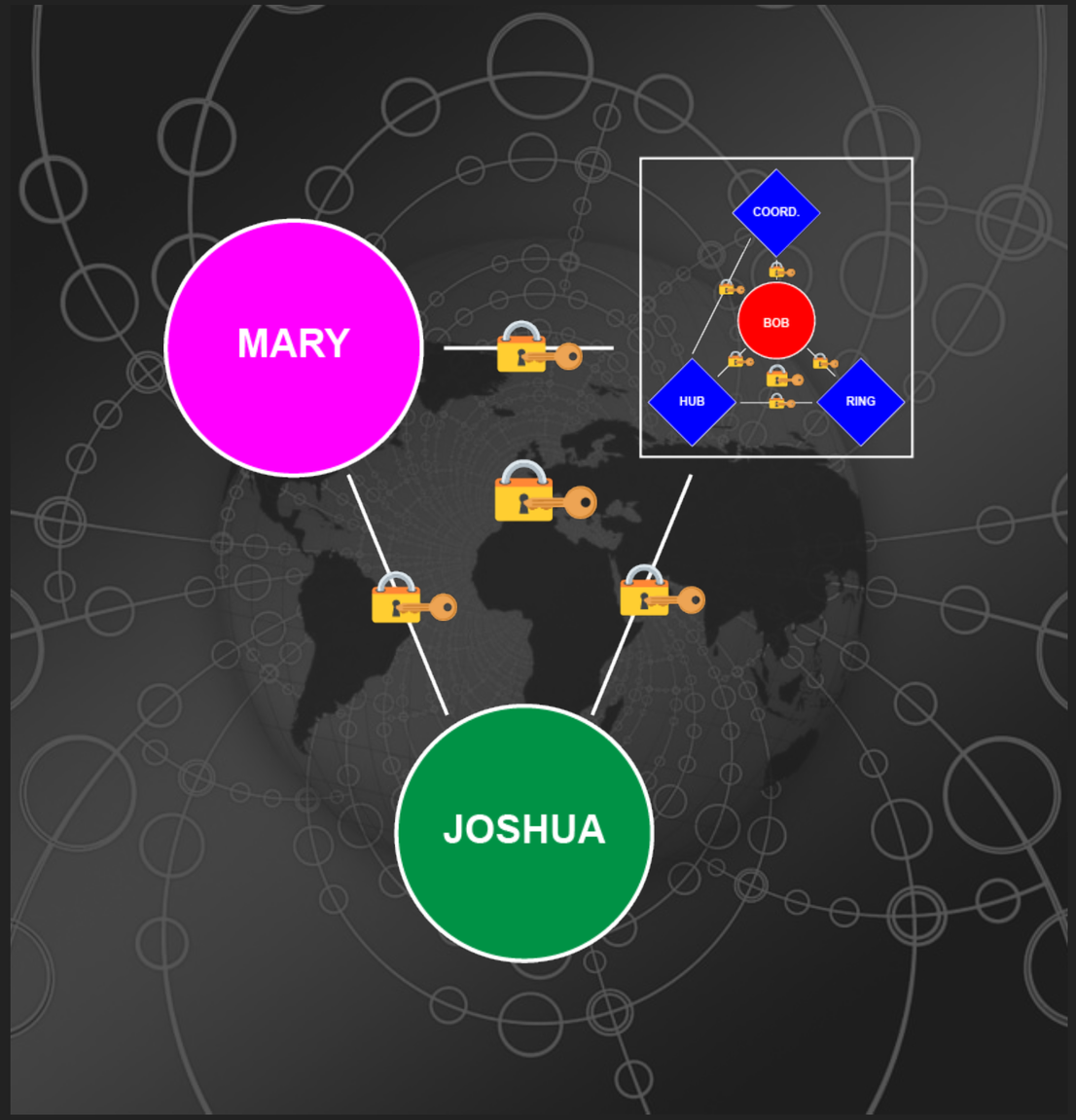
CLIQUES WITH DEVICES

- The entities in cliques don’t have to be people
  - **Devices** can be parts of cliques
  - **Devices** can form their own cliques
  - **Devices** together might form an identity!



CLIQUES OF CLIQUES WITH DEVICES

- Due to the recursive power of cliques
  - Bob's node is no longer a Single Point of Failure
  - The possibilities are **endless**!



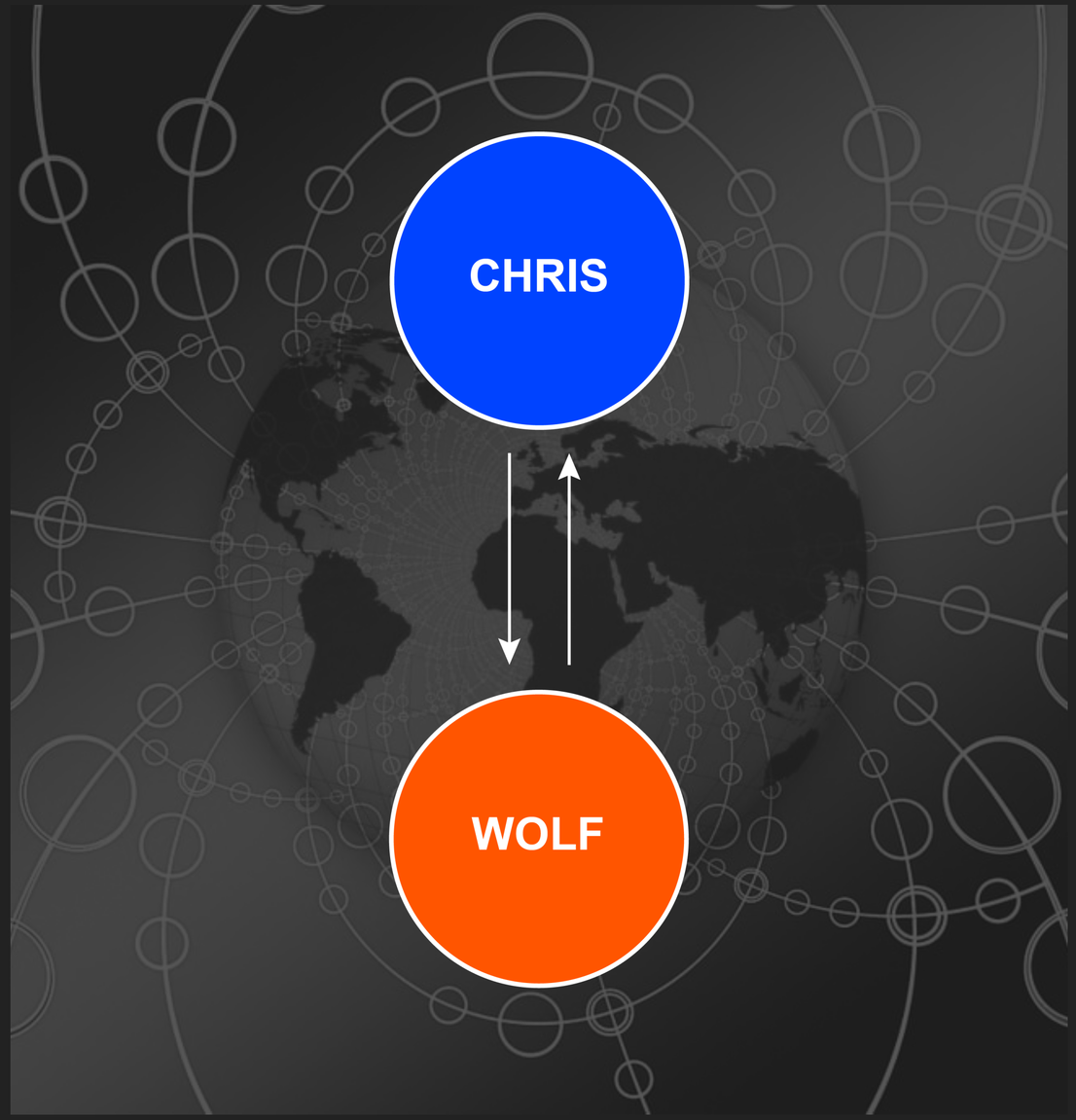
IMPLICATIONS FOR IDENTITY

// Classic `FOAF` peer claims

```
{ XID(ChristopherA) [
    ‘credential’: ‘knows’ [
        'key': PublicKeyBase
        'who': XID(Wolf) ]
] } [
    'verifiedBy': Signature
]

{ XID(Wolf) [
    ‘credential’: ‘knows’ [
        'key': PublicKeyBase
        'who': XID(ChristopherA) ]
] } [
    'verifiedBy': Signature
]
```

// We can infer these are `peers`, but can’t prove it

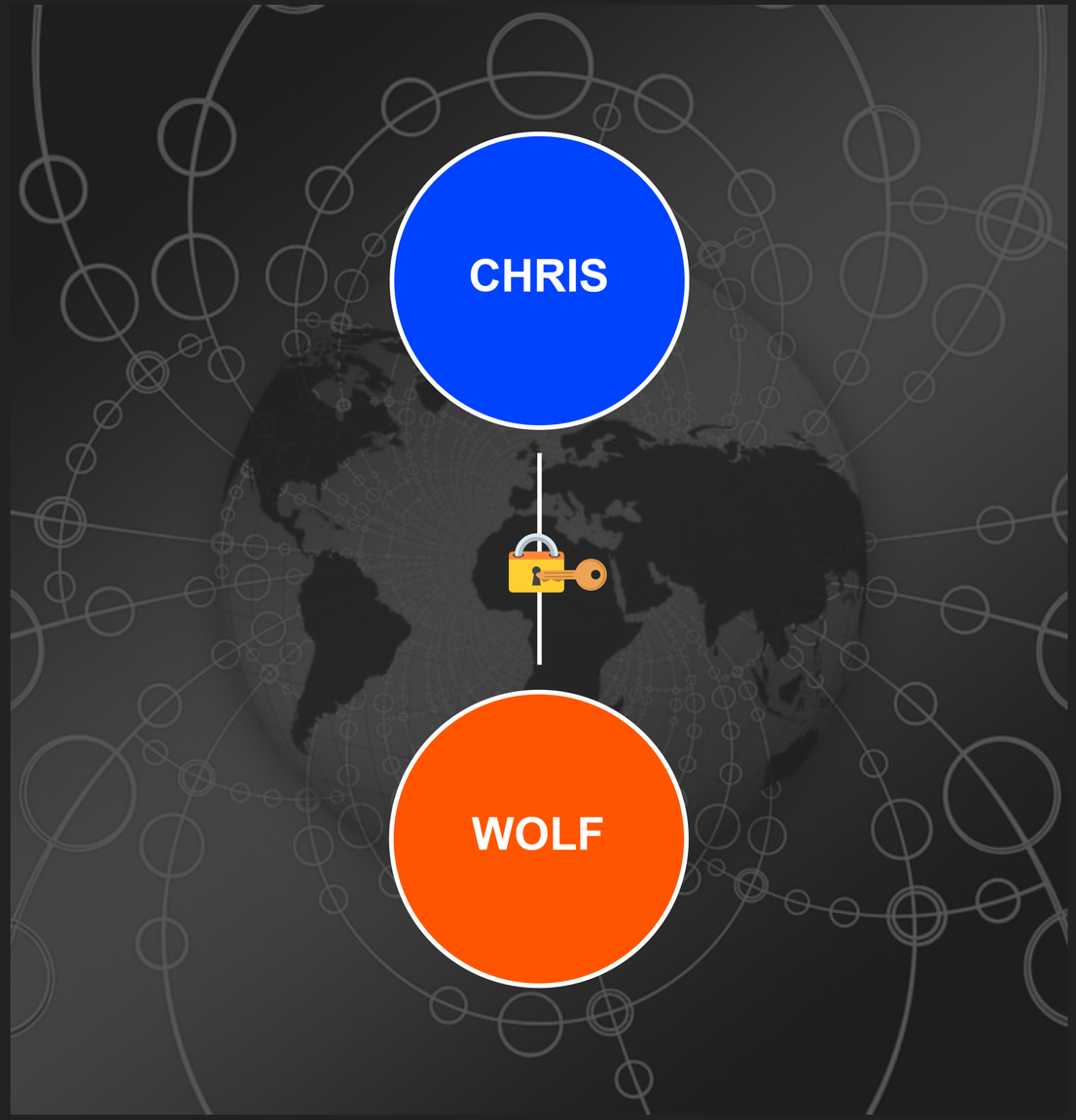


EDGE CREDENTIAL

// …re-envisioned as an VC-style Edge credential:

```
{ XID(CwEdgeIdentifier) [
    'credential': 'peerGroup' [
        'peer': XID(ChristopherA)
        'peer': XID(Wolf)
        'key': PublicKeyBase
] ] } [
    'verifiedBy': Signature
]
```

// With an Edge, we can prove they are 'peers' by aggregating the PublicKey in PublicKeyBase of both XIDs, and then comparing it to the this Edge Credential's PublicKeyBase

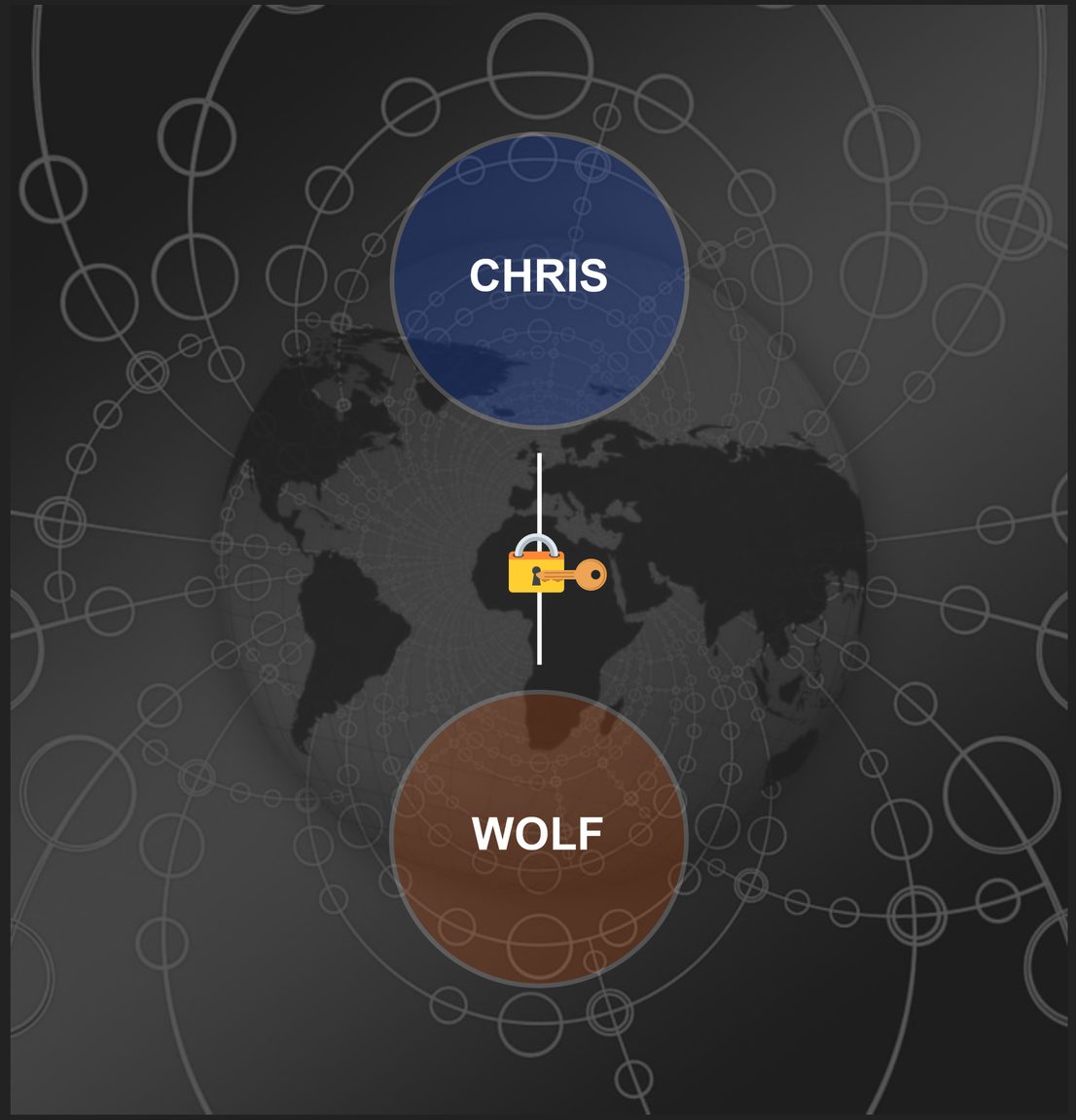


CLAIM PRIVACY VIA ELISION

// …with other credentials, we don't need to reveal this is a group claim:

```
{ XID(CwEdgeIdentifier) [
    'credential': 'peerGroup' [
      "homepage": "https://edge.com"
      'key': PublicKeyBase
      ELIDED (2)
] ] } [
    'verifiedBy': Signature
]
```

// But if needed, we can reveal the ELIDED sub-envelope prove this signed by an Edge.



FINAL NOTES

- Single signature paradigm is not enough!
- We need relational identifiers for peers & groups
  - That's what edge identifiers & cliques do
- Closed, nested, open, fuzzy, or device cliques
  - There are many exotic possibilities!
- There are many interesting challenges
  - *(and opportunities!)*
  - …too express the richness of this paradigm!

“Edge Identifiers & Cliques”

https://www.blockchaincommons.com/musings/musings-cliques-1/

CHRISTOPHER ALLEN

@ChristopherA

ChristopherA@LifeWithAlacrity.com

@BlockchainComns company/blockchain-commons

“Advocating for the creation of open, interoperable, secure & compassionate digital infrastructure to enable people to control their own digital destiny and to maintain their human dignity online”

EDGE ASSERTION

```
// …re-envisioned as an Edge assertion:
{  {   XID(CwEdgeIdentifier) [
          'assertions': 'peerGroup' [
             'peer': XID(ChristopherA)
             'peer': XID(Wolf)
          ]
          'key': PublicKeyBase
       ]
    } [
       'declaredBy': XID(CwEdgeIdentifier)
    ]
} [
    'verifiedBy': Signature
]
// With an Edge, we can prove they are 'peers' by aggregating
the PublicKey in PublicKeyBase of both XIDs, and then
comparing it to the this Edge Assertion's PublicKeyBase
```