Sovereign Individual System (SIS): Own Your Server and ID

An Autonomous Digital Platform for Sovereign Individuals

Ying.Liu@csulb.edu

Facts

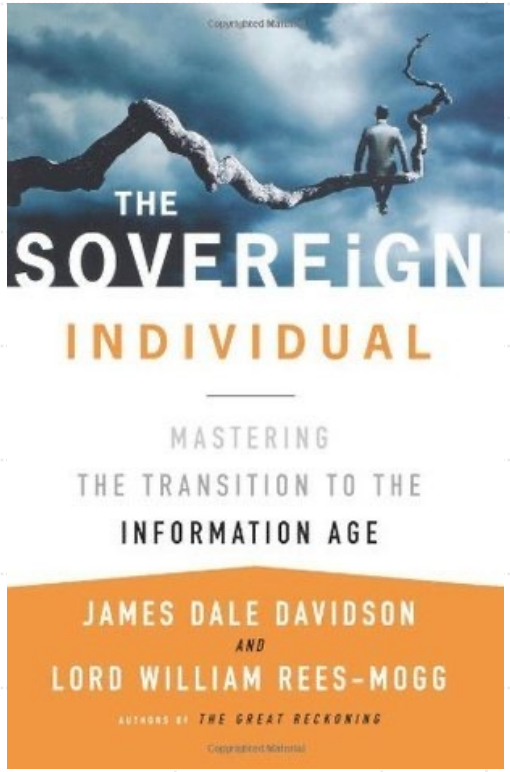
- Truly decentralized and autonomous
- No company/government/blockchain
- No dependency on DNS or any Internet infrastructure
- Not for profit
- Still an early stage design

Sovereign Definition

- For people and nation-state (Cambridge English Dictionary https://dictionary.cambridge.org/dictionary/english/sovereign)
  - *having the highest power or being completely independent.*
- For the digital world (this research)
  - *having the highest power and being completely independent.*

The Future Institution

- Prediction: Sovereign Individual is the institution of information age (1997)
  - Individuals use digital currency
  - Individual mental capital is the most valuable assets
  - Individuals decide the place to live/work and tax
- Sovereign individual applications/products
  - PGP email
  - Git and the creation of Linux
  - Cryptocurrency and DEFI
- “On the dimension of technology, the conflicts has two poles: AI and crypto. … If AI is communist, crypto is libertarian” – Preface by Peter Thiel



Digital Challenges (Why SIS)

- Sovereign conflicts between individual and nation-state
  - Privacy
  - Free expression
  - Fiat currency and digital account: privacy, access, and seigniorage (inflation)
- Sovereign conflicts among nation-states
  - National security concerns: TikTok
  - Inconsistent policies: EU GDPR
- Sovereign conflicts between individual and service providers
  - Privacy
  - Deny of service/access
  - Data ownership
- Too much noise or false information

Sources of Challenges

- No sovereign digital assets
- No sovereign digital identity
- No decentralized autonomous applications
- No control of sent/received information

The First Principle: Own Your Server and ID (OYSI)

No sovereign digital assets: Own your server

- Computer
- Storage
- Network

Store your ID in your server that represents the required digital resources that

- Available
- Reliable
- Scalable

Feasibility of OYSI

- Cheap, reliable and scalable digital assets
  - Cloud computing is cheap, reliable and scalable on demand
  - Virtual computers (firecracker) restart in 0.2 seconds
  - Safe runtimes for extensions in WASM
- Sovereign ID
  - Public-private key pairs
  - Key management
    - Biometric key access and recovery (it is safe because of OYSI)
    - Multiparty key recovery

SIS Solution

No sovereign digital identity: Own your identity
- Safe
- Easy to use
- East to recover

No decentralized autonomous applications: Autonomous/decentralized applications
- Open source
- Safe (isolated)
- Trustable (authenticated)

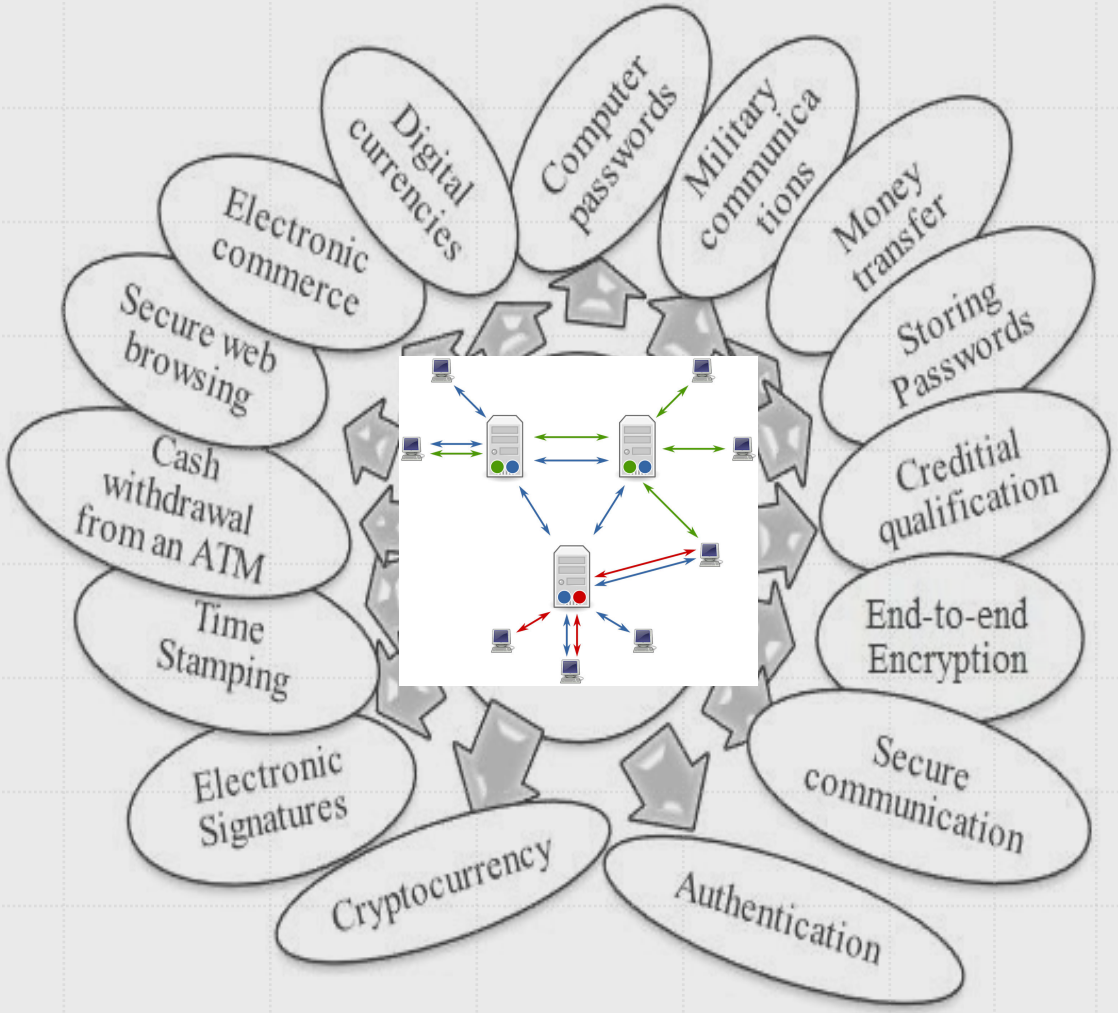
No control of sent/received information: pull-based communication protocol
- End to end security
- Authenticated message
- Pull-based protocol

Foundation of SIS

Central Theorem in Cryptography

“any function you'd like to compute, that you can compute with a trusted authority, you can also do without a trusted authority”.

source: Dan Boneh
https://www.coursera.org/learn/crypto/lecture/ubmLN/what-is-cryptography



Source: https://www.researchgate.net/figure/Applications-of-cryptography_fig3_344949733

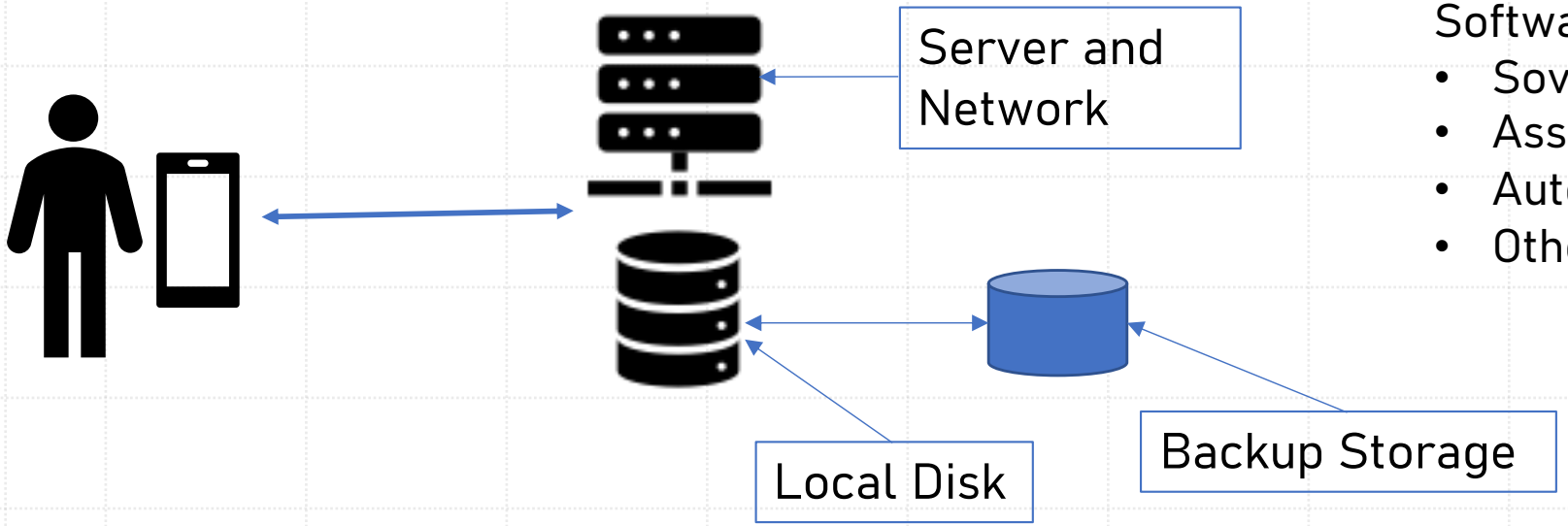
Sovereign Individual System (SIS)

- Sovereign Individual
  - Self-owned computation, storage, and communication
  - Self-sovereign identity：public key
  - Self-controlled, autonomous, optionally signed digital assists: messages, blogs, web sites,,,
- Group of Sovereign Individuals
  - Web of trust or hierarchical trust: group/organization
  - Organization-owned private network, End-to-End secure communication
  - Consensus-based applications: currency, DAO
  - Collaboration applications: payments, events,,,

SIS: the Platform

Client: smart phone, PC, Pad
Function: UI and offline access

Server: computer, storage, network
Function: reliable and scalable digital assets



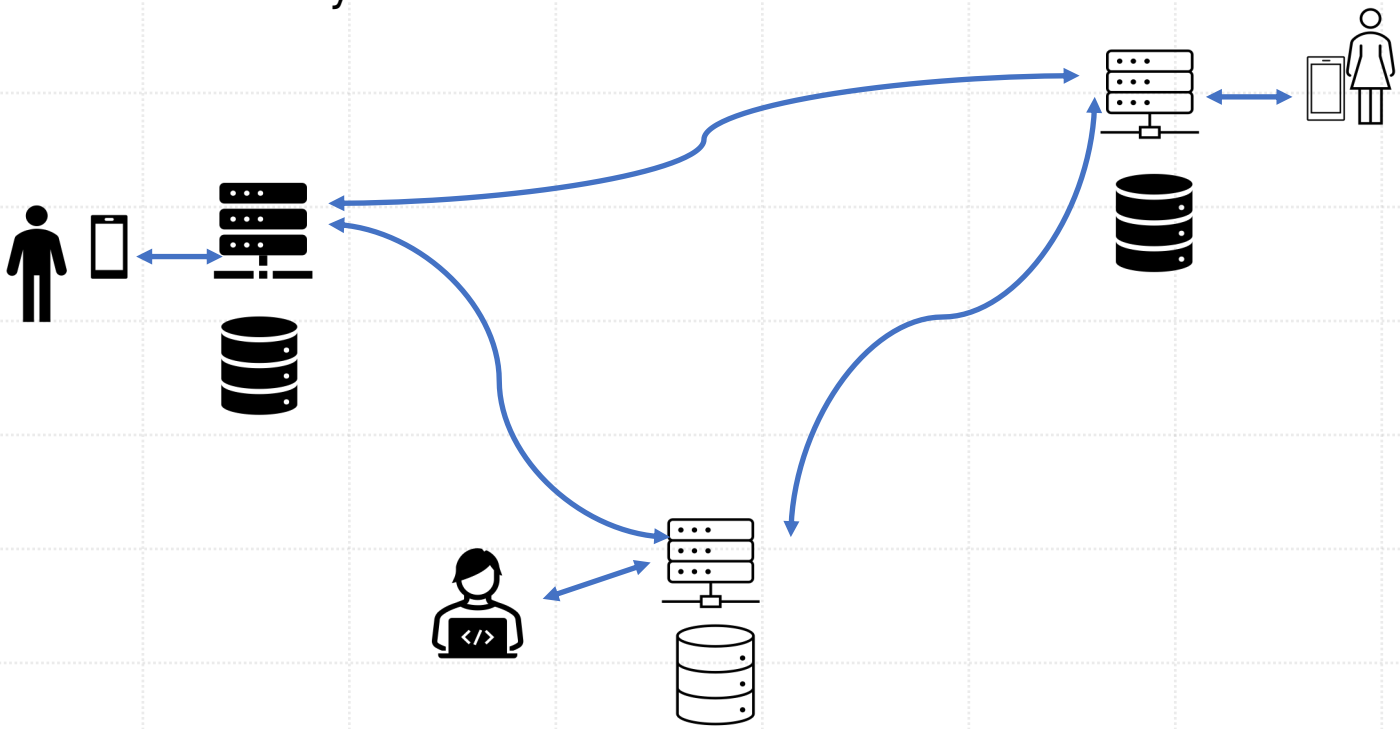
Software
- Sovereign id
- Asset management
- Autonomous applications
- Other app clients

SIS Network

- Three Types
  - everyone brings a server
  - no servers
  - some bring servers
- Network protocol
  - Routing is based on two-tier ID: Self-sovereign ID -> Data Name -> Named Data
  - Two types of trust: web of trust (direct and transitive) and hierarchical trust (DNS, organization etc.)
  - Pull communication protocol for named data

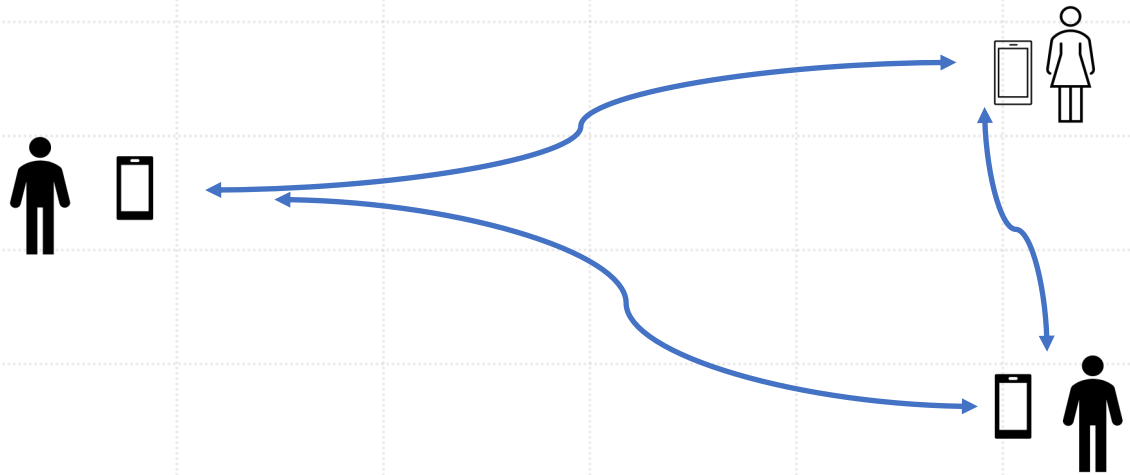
Network Type (1): everyone brings a server

- Pros: reliable service, simple protocol
- Cons: cost and redundancy



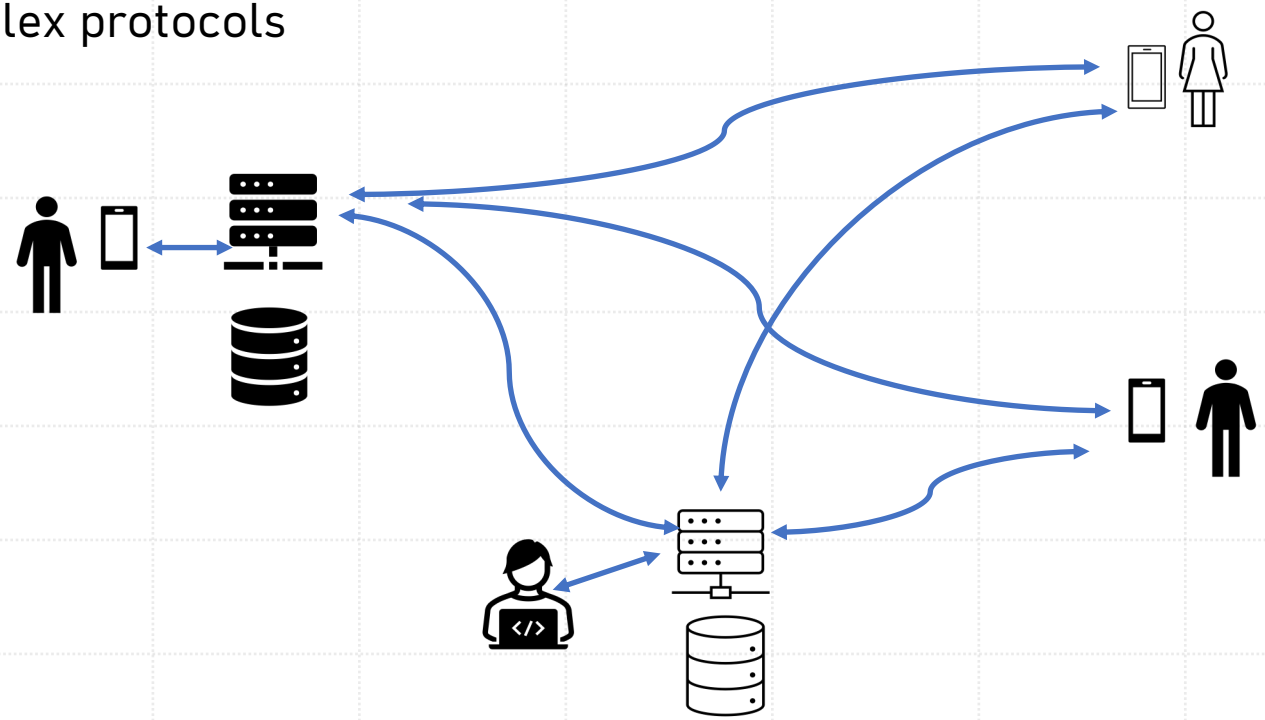
Network Type (2): no servers

- Example: Smart Phone Ad Hoc Network (SPAN) 。
- Pros: direct communication with device WIFI or Bluetooth (Firechat) 。
- Cons: unreliable, uncommon



Network Type (3): some bring servers

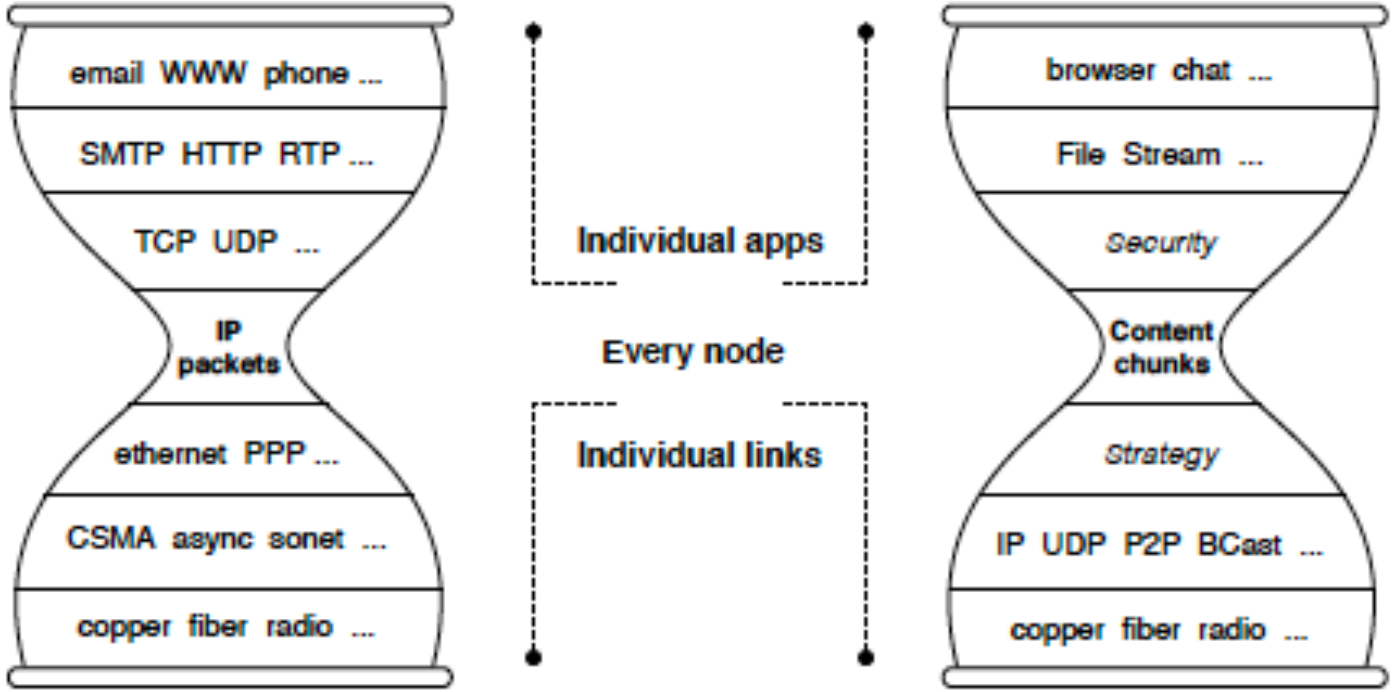
- It is the network type for most applications
- Pros: flexibility and economy
- Cons: complex protocols



Two Types of Network Protocols

- Internet-based: customized Matrix protocol (https://matrix.org/)
  - Mature and ready-to-use
  - Compatible
- Named data networking (https://named-data.net/)
  - ID-name binding
  - Decentralized, independent overlay networks
  - More efficient with name-based cache, pull protocol and multicasting
  - More than 10 years R&D

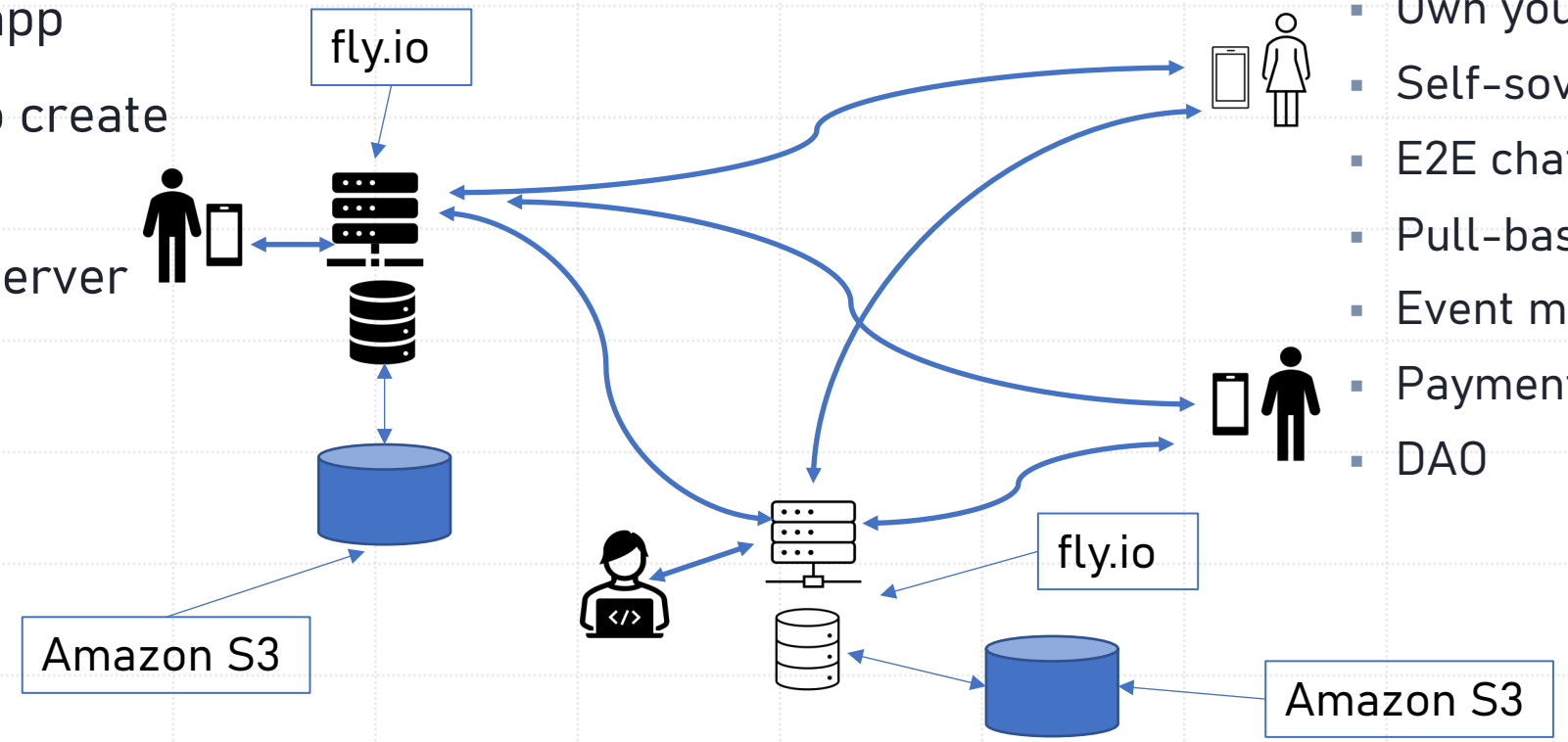
An Overlay Network



An Example App: Sovereign Individual Chat (SiChat)

Use

- Download an app
- Simple click to create a chat server
- Matrix client-server protocol
- Web of trust



Features

- Own your chat server
- Self-sovereign ID
- E2E chat messages
- Pull-based group chat
- Event management
- Payment
- DAO

Evolution

- Centralized
- Federated
- User-centric
- Self-sovereign identity / DID
- Sovereign Individual System: ID and more
  - System
  - Trust model
  - Network

Contributions

- Own your server and ID
  - *Autonomous: self-sovereign ID is not enough, SI needs a system (computation, storage and network) to have the highest power and be completely independent*
  - ID management: easy, safe and reliable biometric key recovery
- SIS network
  - Trust on sovereign ID (web of trust or hierarchical trust)
  - Scalable E2E security and authentication: cryptocurrency and DAO
  - Ready to try: efficient decentralized NDN protocols