Frequency

Encrypted by Default

The Evolution of Data Control in Decentralized Networks

Web3 Summit 2025

What is Data Control?

What is data control?

- Create
- Read
- Update
- Delete

What is data control?

- Create
- Read
- Update
- Delete
- = CRUD!

Different for different data

- Financial
- Health/Healthcare Data
- Broadcast Communications
- Personal Communications
- Metadata

Data control in decentralized systems

- Create
- Read
- Update
- Delete

Data control in decentralized systems

- Create
  - Authorship validation
- Read
- Update
- Delete

Data control in decentralized systems

- Create
  - Authorship validation
- Read
- Update
  - Logic
- Delete

Data control in decentralized systems

- Create
  - Authorship validation
- Read
- Update
  - Logic
- Delete
  - State: Logic
  - History: Tombstones

Data control in decentralized systems

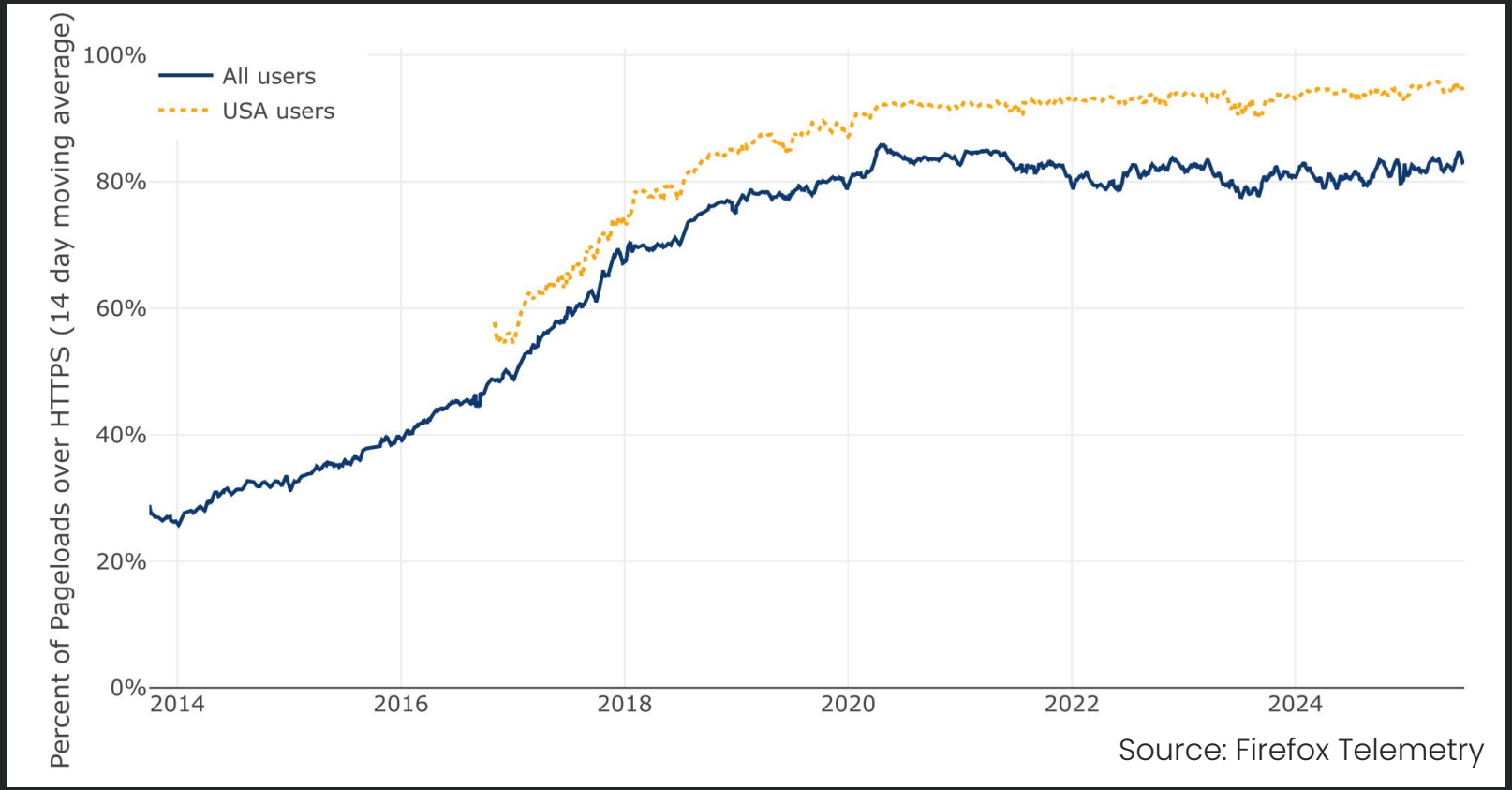
- Create
  - Authorship validation
- **Read**
  - **Public**
- Update
  - Logic
- Delete
  - State: Logic
  - History: Tombstones

History

How did the internet develop data control?

- Physical Access Controls
- User Access Controls
- Encrypted Communication
- Encrypted Data

The Great Encrypting of the Internet



How did the internet develop data control?

- Physical Access Controls
- User Access Controls
- Encrypted Communication
- Encrypted Data

What about Blockchain?

Etherscan Shows All

TRANSACTIONS (24H)	PENDING TRANSACTIONS (LAST 1H)	TOTAL TRANSACTION FEE (24H)	AVG. TRANSACTION FEE (24H)
1,230,437 (3.71%)	85,289 (Average)	179.21 ETH (2.54%)	0.48 USD (12.00%)

More than 2,880,595,108 transactions found
(Showing the last 500k records)

Download Page Data | First | Page 1 of 10000 | Last

Transaction Hash	Method	Block	Age	From	To	Amount	Txn Fee
0xf5b3866e9fa...	Transfer	22869510	12 secs ago	quasarbuilder	Stader Labs: Permi...	0.015460747 ETH	0.00005025
0x30ca83b8c1...	0x4a004205	22869510	12 secs ago	0x00000000...514D94f4a	0xa7AAbd7F...87aFcc8B8	0 ETH	0.00035866
0xda842a1c2c...	Transfer	22869510	12 secs ago	0xD0d1b57A...7c159F576	0x7908d07D...5F4E28965	0.002715735 ETH	0.00003559
0x78a5aefb0e6...	Transfer	22869510	12 secs ago	0x59891E6b...1Ae6628c1	0x9998baCF...c92643077	0.000160351 ETH	0.00003559
0xb7c4304d1e...	Transfer	22869510	12 secs ago	0x721eb111...a80CF34a9	Circle: USDC Token	0 ETH	0.00006838
0x36f6bf015b3...	Transfer	22869510	12 secs ago	FixedFloat 1	Pepe: PEPE Token	0 ETH	0.00010249
0x5a3a9fb820d...	Approve	22869510	12 secs ago	0x33ec4E86...9693dd884	Tether: USDT Stabl...	0 ETH	0.00008287
0xb372222b98...	Add Sequenc...	22869510	12 secs ago	0x74a0d46B...1c7DaBf3C	0x85eC1b91...901040b59	0 ETH	0.00017381

The Present

Where are we today, the good

- Most Internet sites use SSL
- Device encryption common
- p2p encryption common and promoted
- Sensitive data often encrypted at rest
- Encryption is easier than ever
- Newer tools (TEE, zk-proofs)

Where are we today, the bad

- Blockchain... Still mostly public
- web2 and web3 applications leaks personal data
- Users are not well educated

Privacy on Frequency

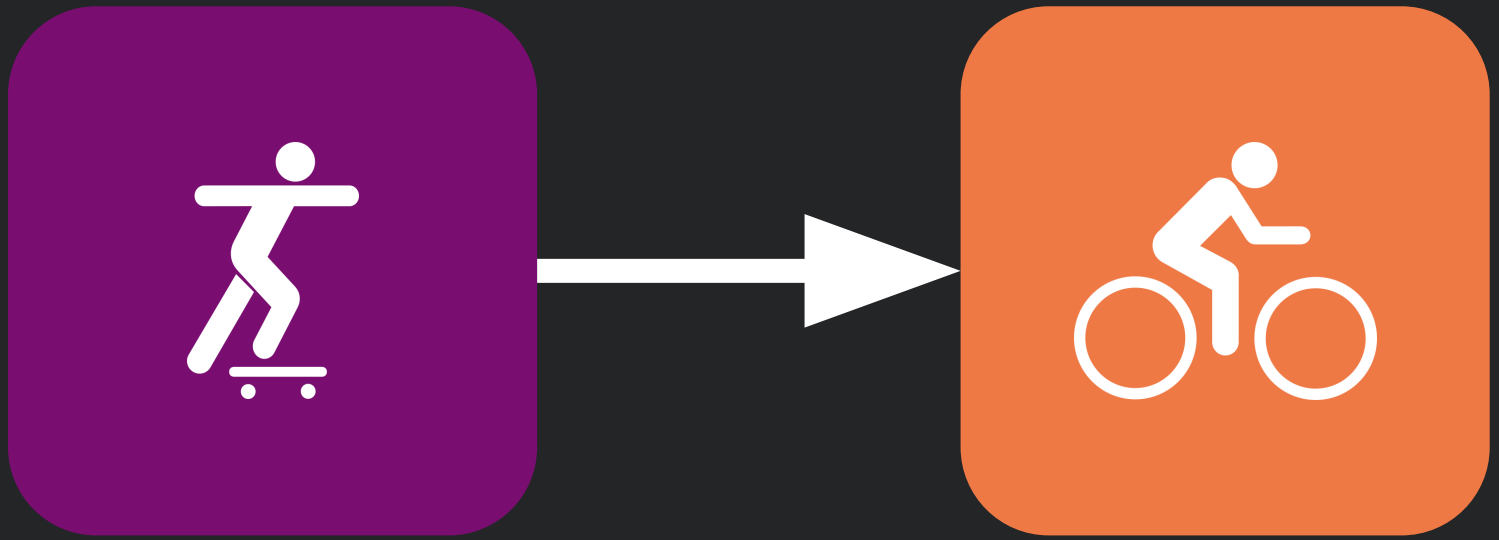
Why social graph privacy?

- Your social connections are yours
- Permission to read is permission to exploit
- Social connections expose a lot of information
- Users need to be able to trust decentralized social

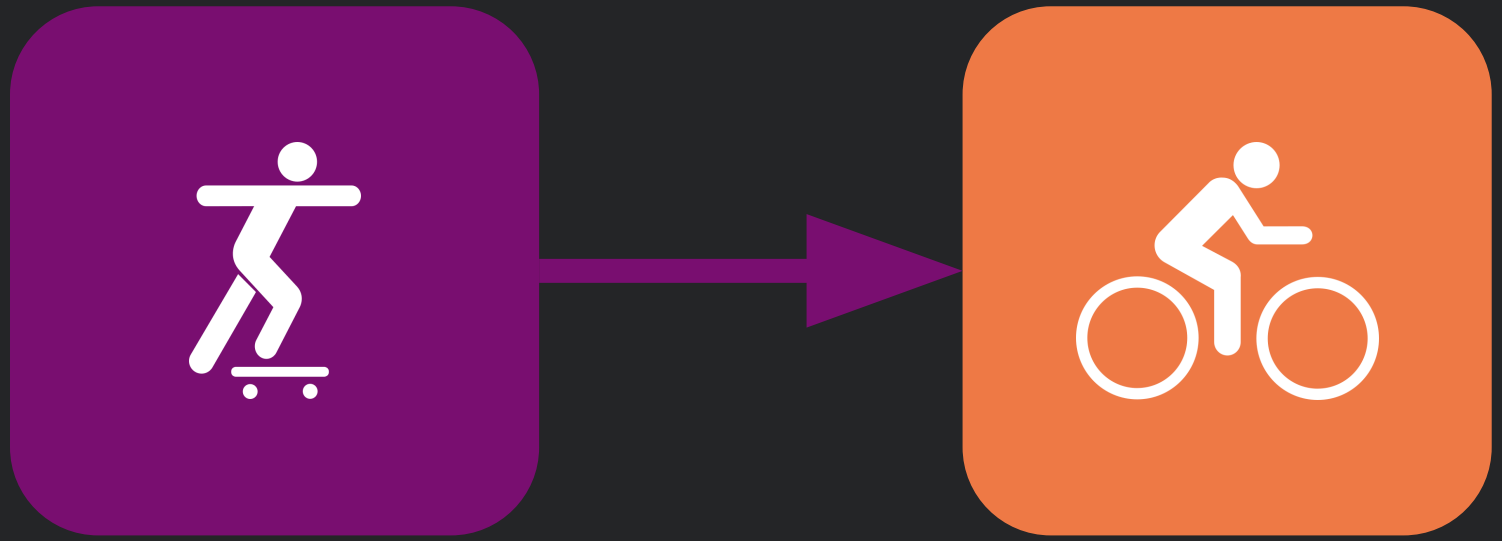
Some of the problems we faced

- How do we approach the shared ownership nature of connections?

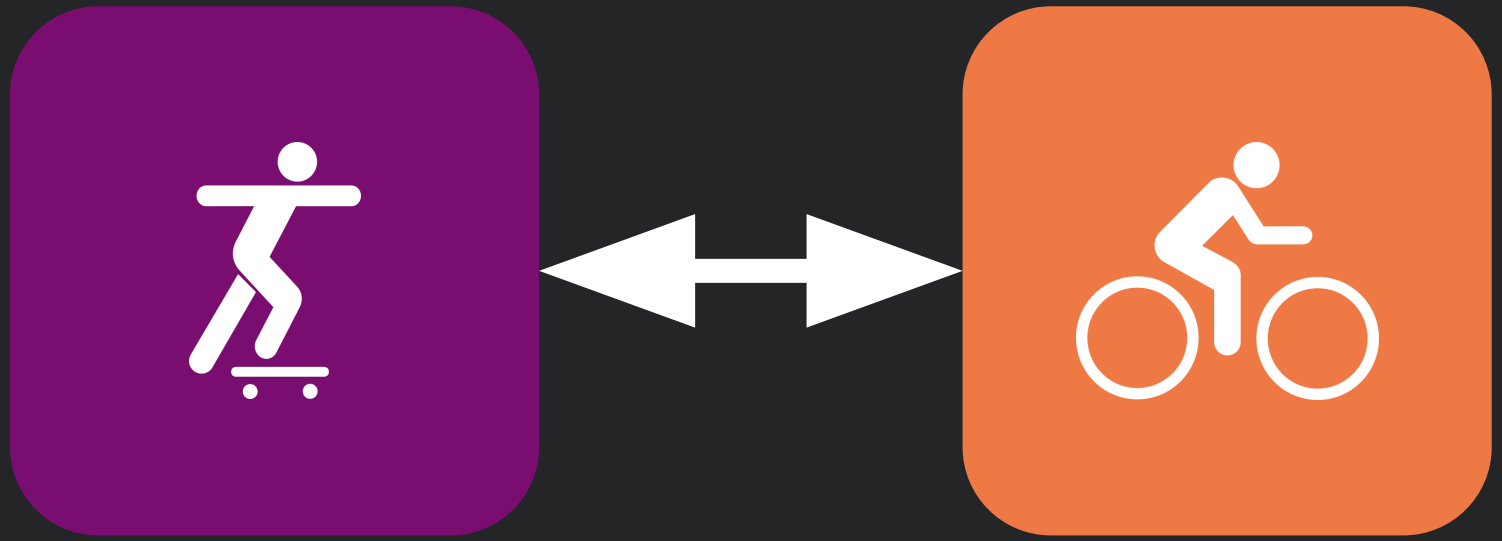
Unidirectional aka “Follows”



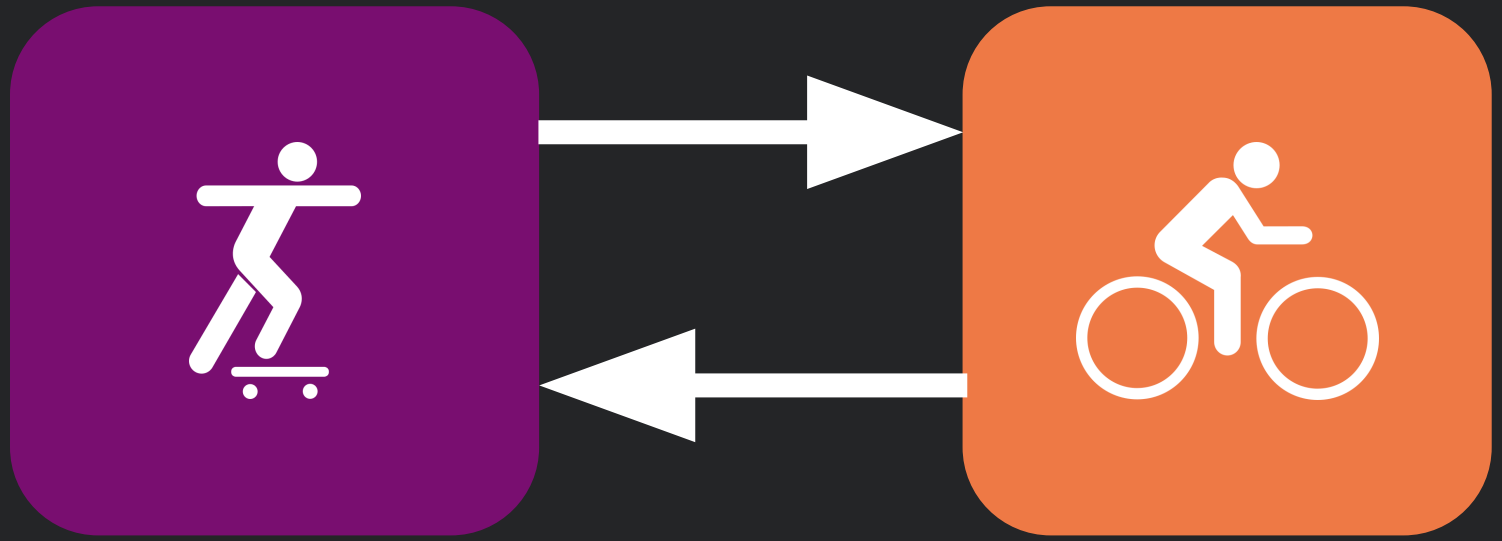
Unidirectional aka “Follows”



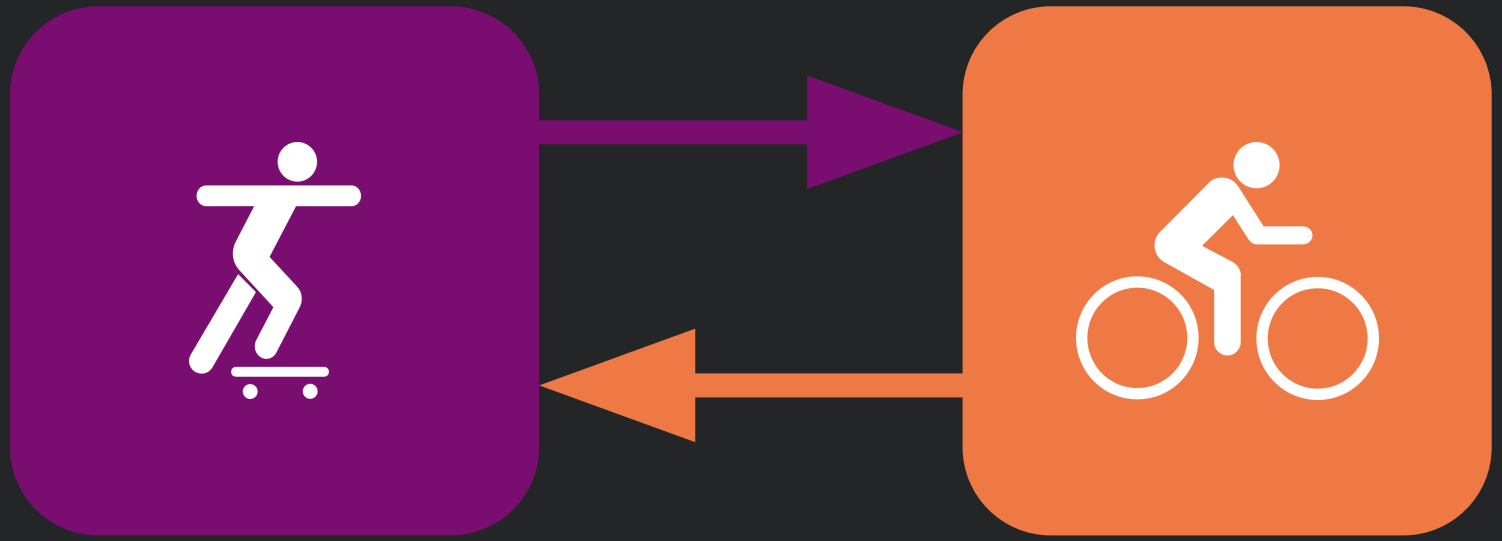
Bidirectional aka “Friends”



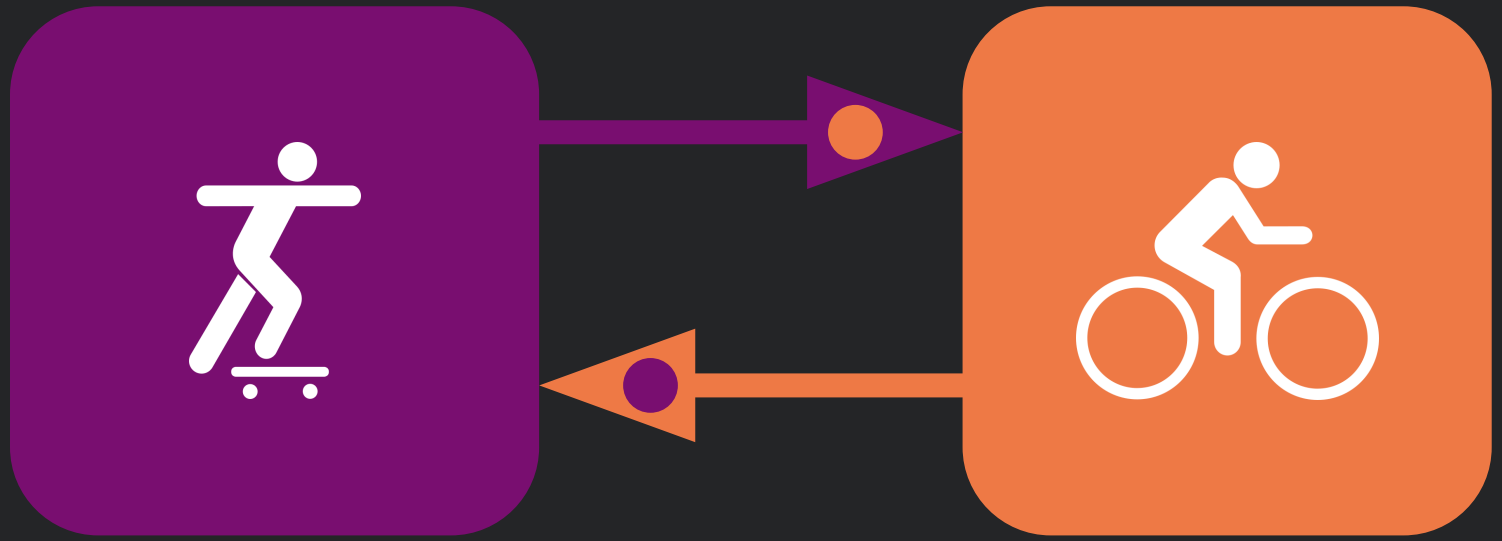
Bidirectional aka “Friends”



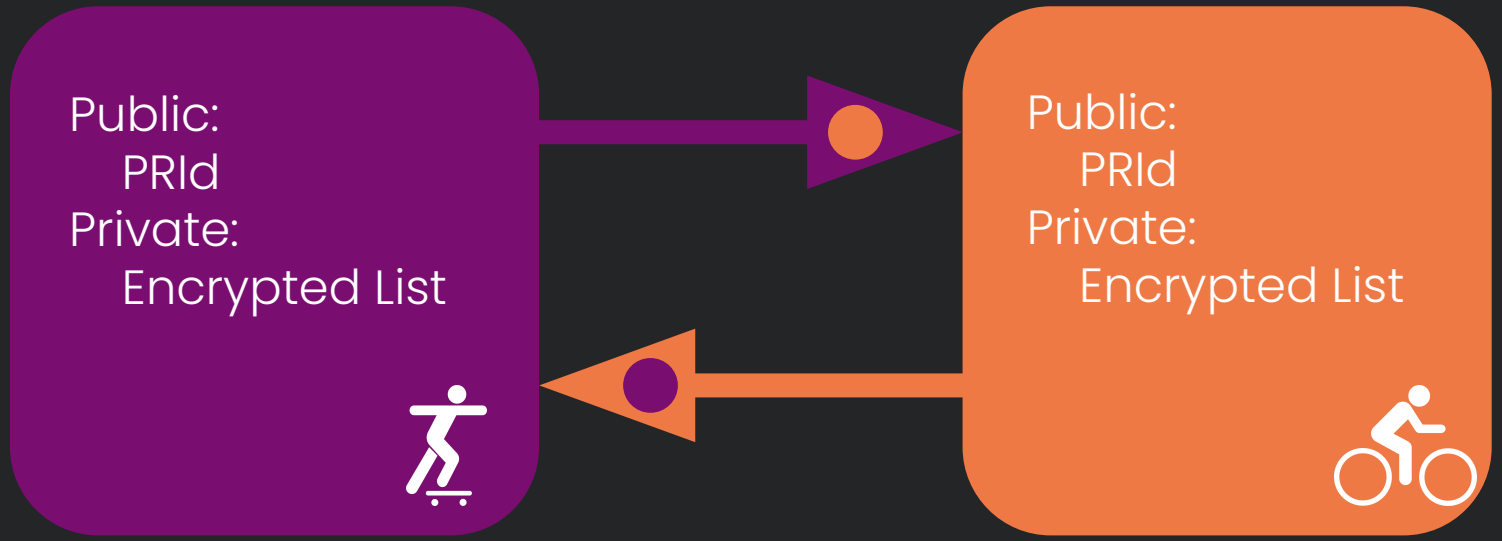
Bidirectional aka “Friends”



Bidirectional aka “Friends”

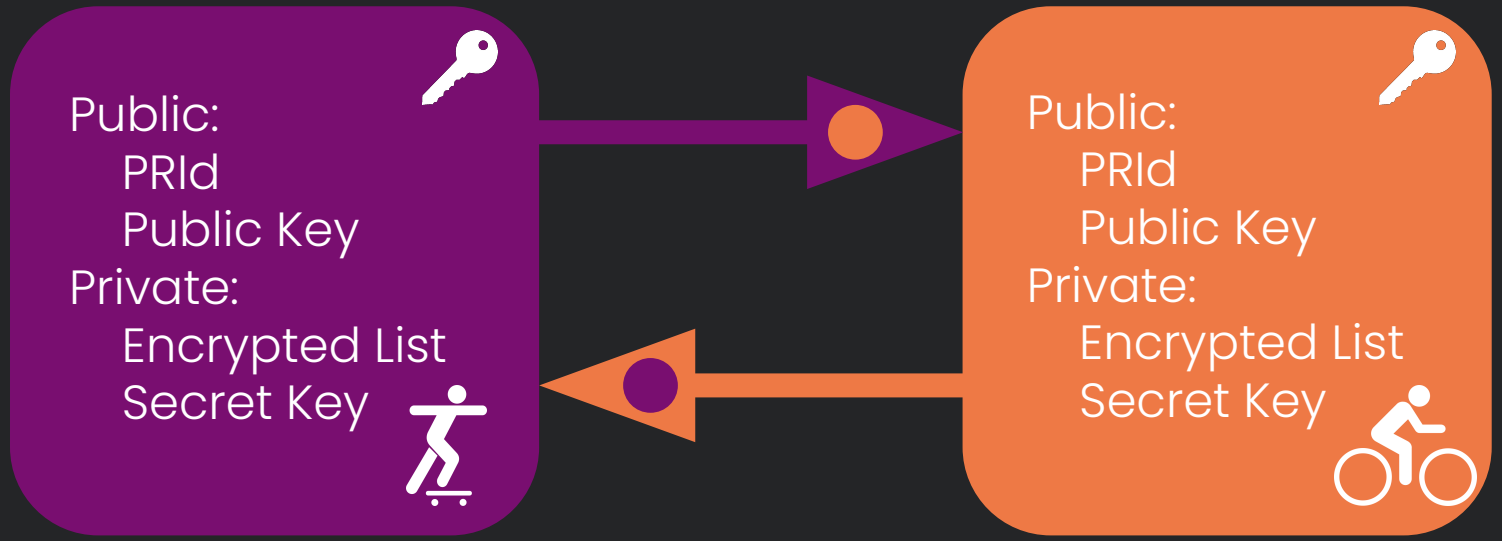


Bidirectional aka “Friends”



PRId: Pseudonymous Relationship Identifier

Bidirectional aka “Friends”



PRId: Pseudonymous Relationship Identifier

PRId: Pseudonymous Relationship Identifier

$$\text{Root\_Shared\_Secret}_{AB} \leftarrow \text{ECDH}(\ \text{Bob}_{public}\ \text{Alice}_{secret}\ )$$

$$\begin{aligned}
&\text{Alice->Bob Context Secret}_{A\to B\ Ctx} \leftarrow \text{Blake2b256}(\\
&\quad \text{key} = \text{Root_Shared_Secret}_{AB}\\
&\quad \text{salt} = \text{Id}_{Bob}\\
&\quad \text{personal} = \text{"PRIdCtx0"})
\end{aligned}$$

$$\begin{aligned}
&\text{Alice->Bob PRId} \leftarrow \text{XSalsa20}(\\
&\quad \text{message} = \text{Id}_{Bob}\\
&\quad \text{key} = \text{Secret}_{A\to B\ Ctx}\\
&\quad \text{nonce} = \text{Padded_24_Bytes_LE}(\ \text{Id}_{Alice}\ )\ )
\end{aligned}$$

Source: https://spec.dsnp.org/DSNP/Types/PRId.html

Some of the problems we faced

- How do we approach the shared ownership nature of connections?
- How can we store this much data?

Data Storage

- Minimize the data
- Compress the data before encryption
- Chunk (paginate) the data
- Place the data in child trees
- Require the storage in state
- Remove (eventually) historical states

Some of the problems we faced

- How do we approach the shared ownership nature of connections?
- How can we store this much data?
- Where do we store and how do we rotate the private key?

Key Management & Communication

- Wallet encryption key storage for now
- SIWF standard extending EIP-4361 and CAIP-122
  - Defines communication of Verified Credentials and signed payloads for permissions
- Rotation results in “lazy” access updating

Some of the problems we faced

- How do we approach the shared ownership nature of connections?
- How can we store this much data?
- Where do we store and how do we rotate the private key?
- Is e2e encryption possible for this data?

End to End Encryption?

- Trust in the client
- Services provided
- Limits with shared data

End to End Encryption?

- Trust in the client
- Services provided
- Limits with shared data
- Result: Application level trust

Tangent Alert: Information Theory

We can offer *choice* in who to trust, *limit* the amount of trust required required, and control some of the *consequences* of broken trust.

The Future

Threshold Cryptography

- **What**: Nodes that together can provide cryptographic actions
- **Imagine**: Users only needed to worry about proof of permission instead of key management
- **Status**: Viable Now
- **Potential Limit**: Collusion and Sybil Attacks

Homomorphic Encryption

- **What**: Calculation and transformations on encrypted data
- **Imagine**: Applications can be information blind while still providing services
- **Status**: Slow & expensive
- **Potential Limit**: May never be fast enough for some operations and could leak significant metadata

Passkey Encryption

- **What**: PRF extension to WebAuthn
- **Imagine**: Devices provide on-device encryption primitives to applications
- **Status**: Limited support
- **Potential Limits**:
  - Trust in the passkey systems and the application
  - Sandboxed to the application

Quantum Everything

- **What**: Quantum-safe cryptography
- **Imagine**: Quantum computing still allows for cryptography
- **Status**: Working, but more expensive
- **Potential Limit**: Theoretical safety, take care with storage

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence…

Universal Declaration of Human Rights: Article 12

Thank you

www.frequency.xyz

---

www.dsnp.org