DECENTRALIZED IDENTITY

The Element DID Method: Sidetree, Ethereum & IPFS

Orie Steele

Cofounder & CTO @ Transmute

twitter.com/OR13b
github.com/OR13

SSIMeetup objectives

1. Empower global SSI communities
2. Open to everyone interested in SSI
3. All content is shared with CC BY SA

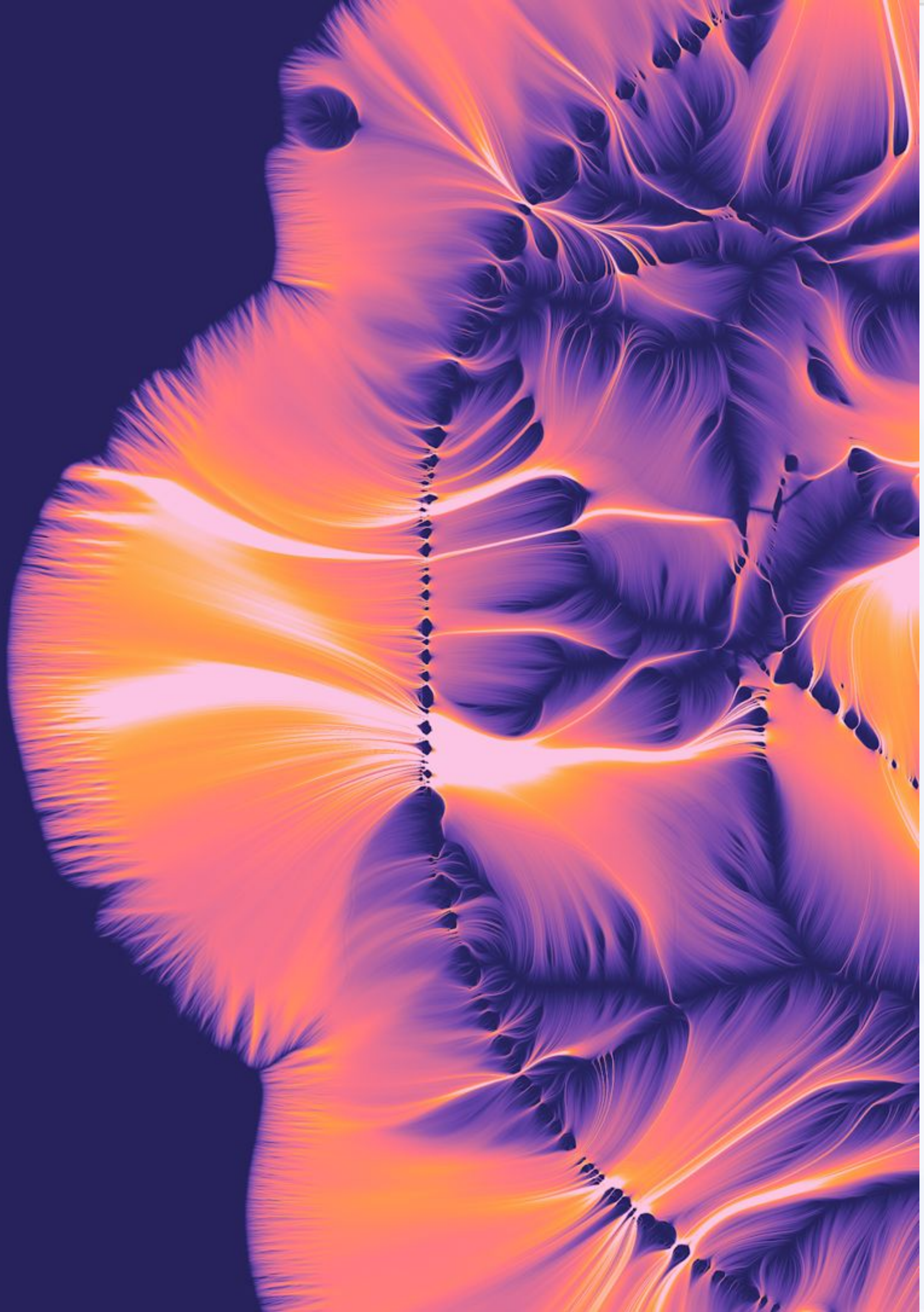
Alex Preukschat @SSIMeetup @AlexPreukschat
Coordinating Node SSIMeetup.org

ABSTRACT

Orie Steele is Cofounder and CTO of Transmute, a company developing IAM and Verifiable Credential solutions that integrate Decentralized Identity for Enterprises.

He has a BS in Cyber Security and MS in Computer Science from Stevens Institute of Technology where he studied social network malware and botnets between 2007-2012. He was an early engineer at Patient IO, a Techstars backed startup acquired by Athena Health in 2016, where he helped develop and secure a care coordination platform that connected nurses and patients.

In this talk, Orie will discuss the history of the Element DID Method, how it leverages the same Sidetree Protocol that is used by ION on the Bitcoin Network. He'll introduce the motivation for Element and ION, and then walk through the core components of developing a working DID System, including topics such as wallets, signing, did resolution, key revocation, and decentralization.



MOTIVATION

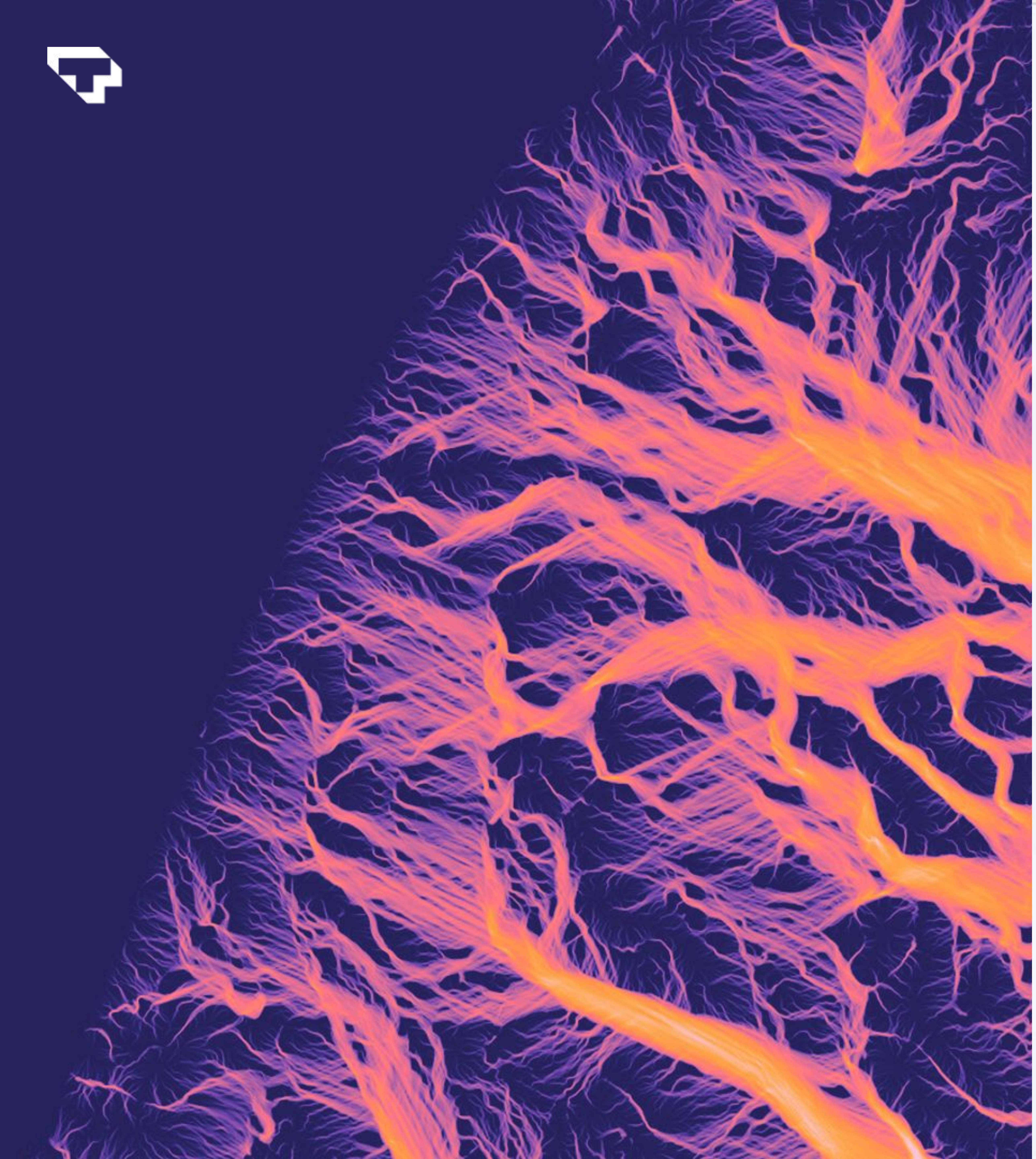
- BTCR / ETHR focused on SSI, but lacked batching, causing challenges for throughput and cost.
- We’ve learned how to leverage centralization better.
- DID Methods contain a lot of duplication, can we share a common protocol?
- Supply Chain, IoT, FinTech & AdTech have some use cases for DIDs that need more scale to support.

SIDETREE

- Ledger agnostic protocol for anchoring batches of signed JSON Patch Operations resulting in a DPKI CRDT.

- Batching supports higher throughput & lower cost, but paranoid users can still anchor themselves.

- Open Source Apache-2 Implementations for Bitcoin & Ethereum supported by the Linux Foundation.

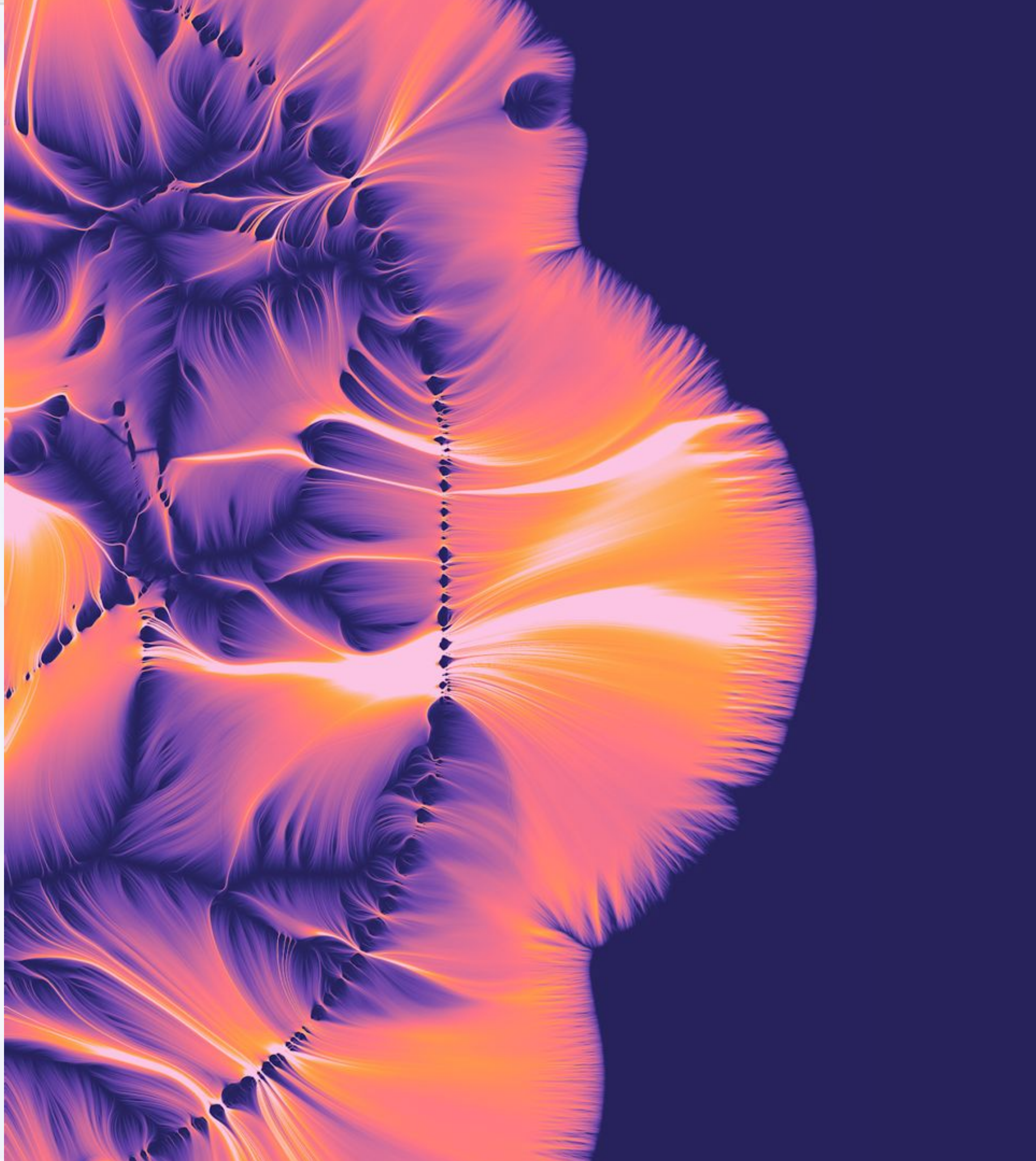


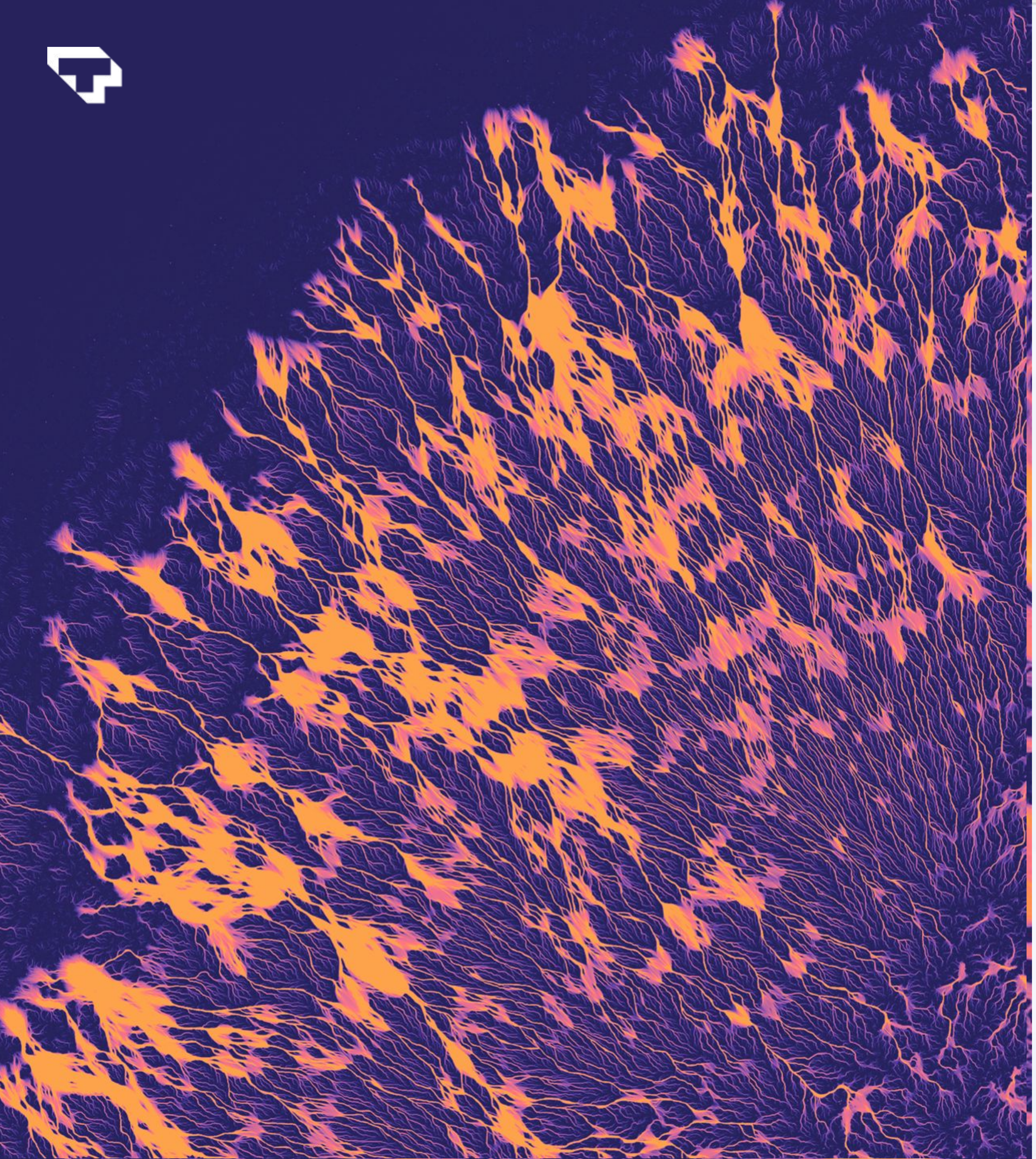
ELEMENT

- DApp / Light Node first approach, with a wink toward paranoid users.
- Client and Server UI Support, we want user driven development ASAP.
- Lerna monorepo of javascript modules and project.
- Slightly more functional than object oriented.
- Live testnet Progressive Web Application.

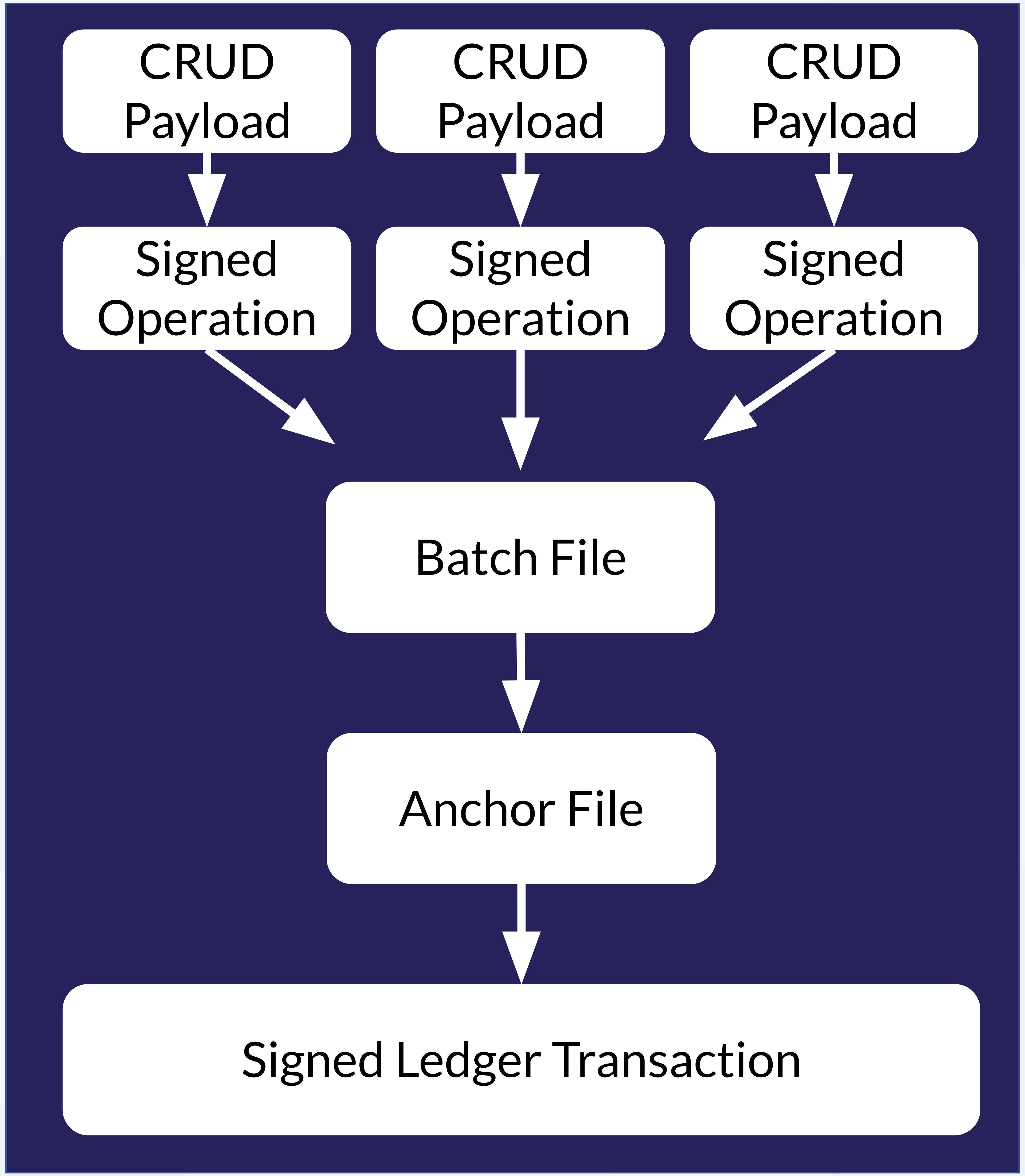
WALLET

- Hardware, Mobile, Web, API, Trusted Execution Environment?
- JWS vs JSON-LD Signatures, the case for JSON-LD.
- Shamir, Recovery and Usability.
  Not all keys need to be in the same place!





ANCHORING

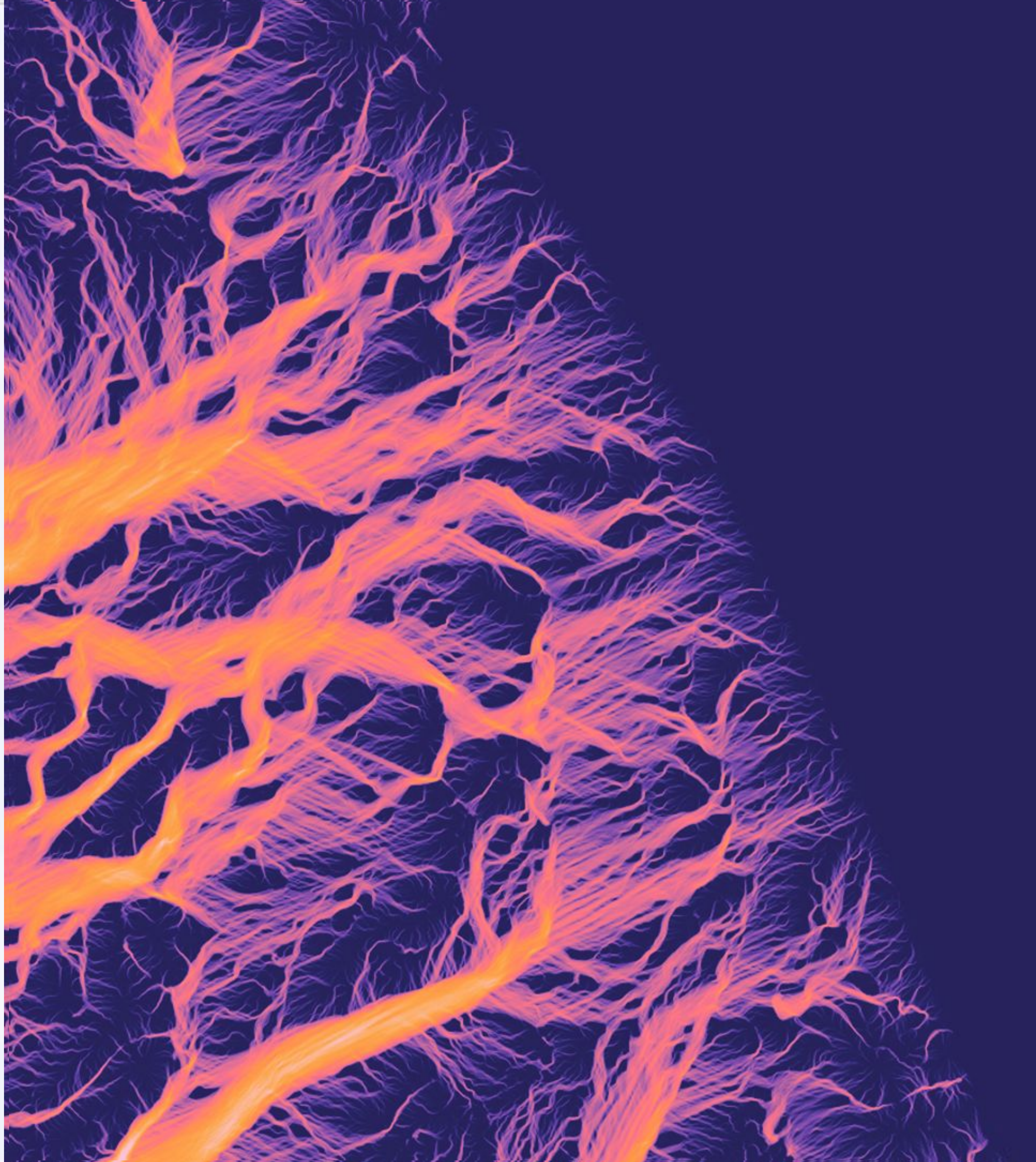

CRUD Payload
CRUD Payload
CRUD Payload
Signed Operation
Signed Operation
Signed Operation
Batch File
Anchor File
Signed Ledger Transaction

RESOLUTION

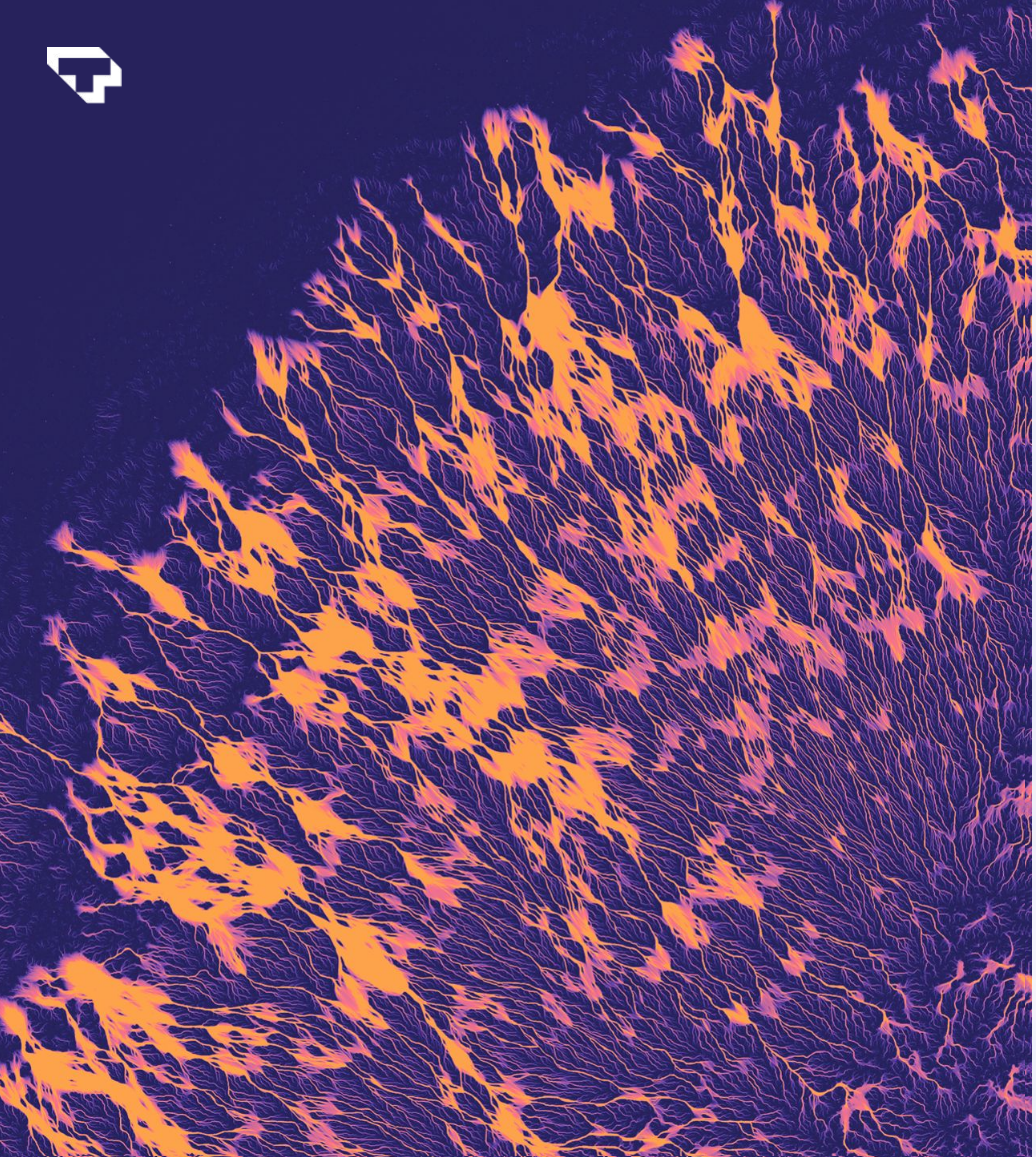
- A kind of reverse anchoring:
  ledger -> anchor -> batch -> operation **=>**
  did document

- Data Poisoning, Spam and Errors:
  How do trusted nodes handle bad data?

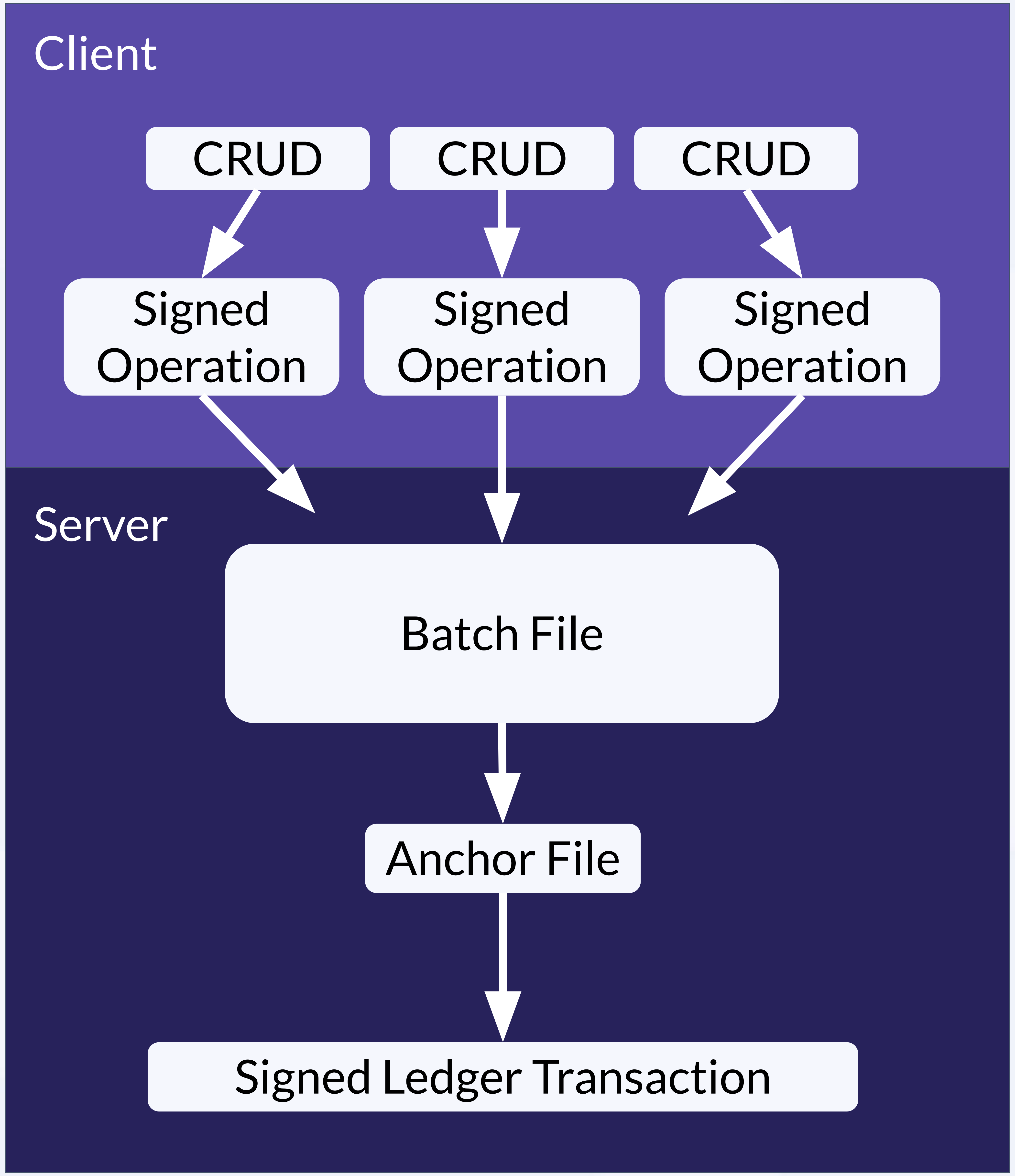
- Why resolve a DID?
  Signature Verification, Service Endpoints
  and the Future of SSI.



SIMEETUP Self-Sovereign Identity



ANCHORING


Client
CRUD
CRUD
CRUD
Signed Operation
Signed Operation
Signed Operation
Server
Batch File
Anchor File
Signed Ledger Transaction

ELEMENT DEMO

DECENTRALIZED IDENTITY

The Element DID Method: Sidetree, Ethereum & IPFS

Orie Steele

Cofounder & CTO @ Transmute

twitter.com/OR13b
github.com/OR13