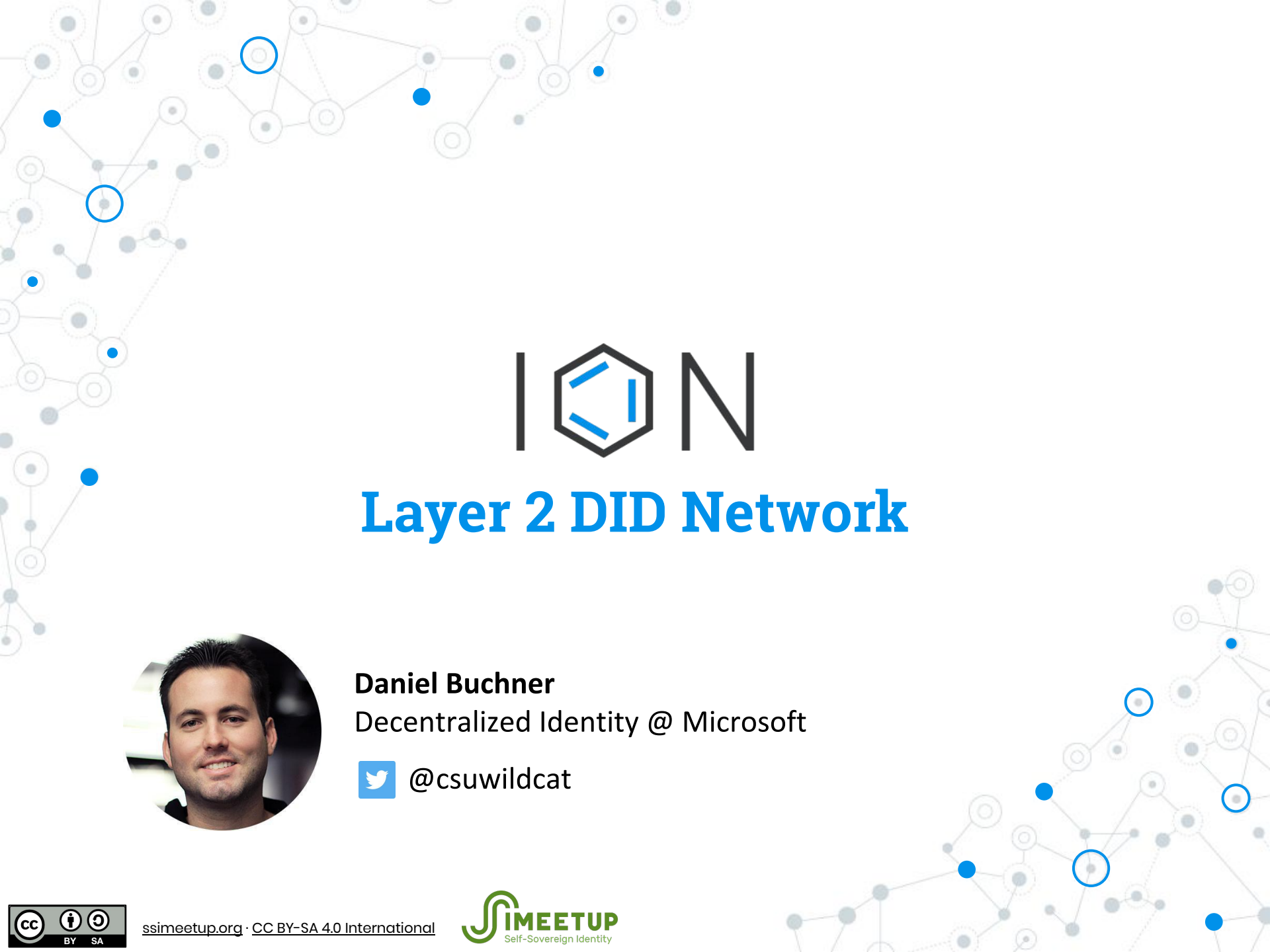


Layer 2 DID Network

Daniel Buchner
Decentralized Identity @ Microsoft

@csuwildcat

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

SSIMeetup.org

1.

The Scaling Trilema

Creating secure, decentralized systems that run at world-scale

Three critical components:

Decentralization

Without this property, many proposed solutions do not deliver sufficiently differentiated benefit over those built using traditional systems.

Scalability

If decentralized systems (i.e. blockchains, DLTs) are to deliver on the benefits they promise, they must support billions of participating entities.

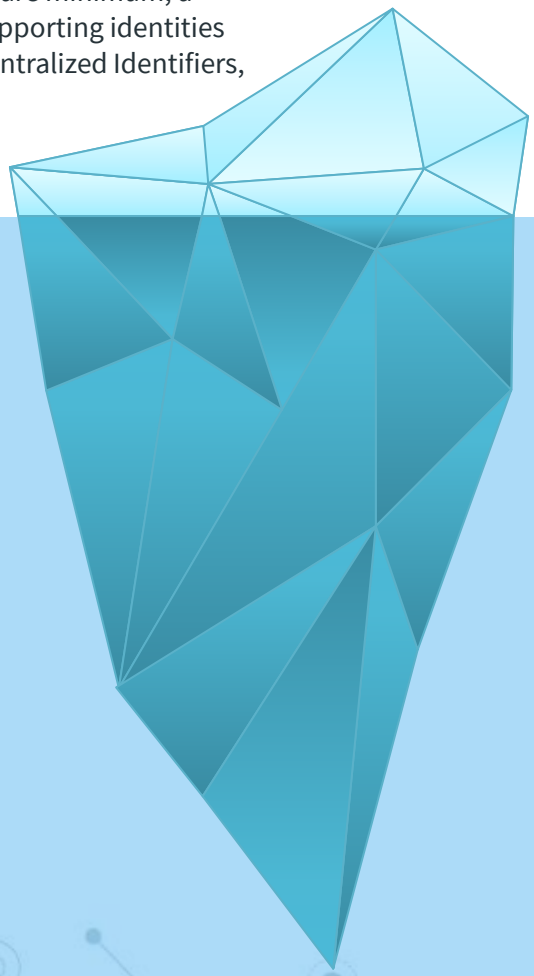
Security

These systems must achieve decentralization at global scale, while maintaining a high level of security.

The Scale of Decentralized Identity:

Human Identity

There are 7.5 billion humans on Earth currently. At bare minimum, a decentralized identity system must be capable of supporting identities for all of them. Each person may have multiple Decentralized Identifiers, each requiring their own PKI lineage.



Identity of All Things.

Human identity is just the tip of the iceberg – there is an entire world containing hundreds of billions of devices, machines, apps, and other entities, both tangible and virtual.

Requirements for DPKI:

- Global, immutable, append-only log
- No central providers or authorities
- Censorship and tamper resistant

Key Realization

Identifiers and PKI do not suffer from the same double spend problem money does, because DIDs do not need to be transferred between parties like assets. However, you must still prevent double issuance and ensure all parties on the DID network can derive a single deterministic PKI state for an identifier.

How might these differences in requirements affect how we approach the architecture of a DID network?

2.

Technical Overview

Architecture and Protocol Details

What is ION?

ION is a public, permissionless, decentralized DID overlay network that runs on Bitcoin, and leverages a deterministic DPKI protocol, called Sidetree.

Technical Assumptions:

No secondary consensus required

ION nodes do not require a secondary consensus system to derive the correct PKI state of IDs.

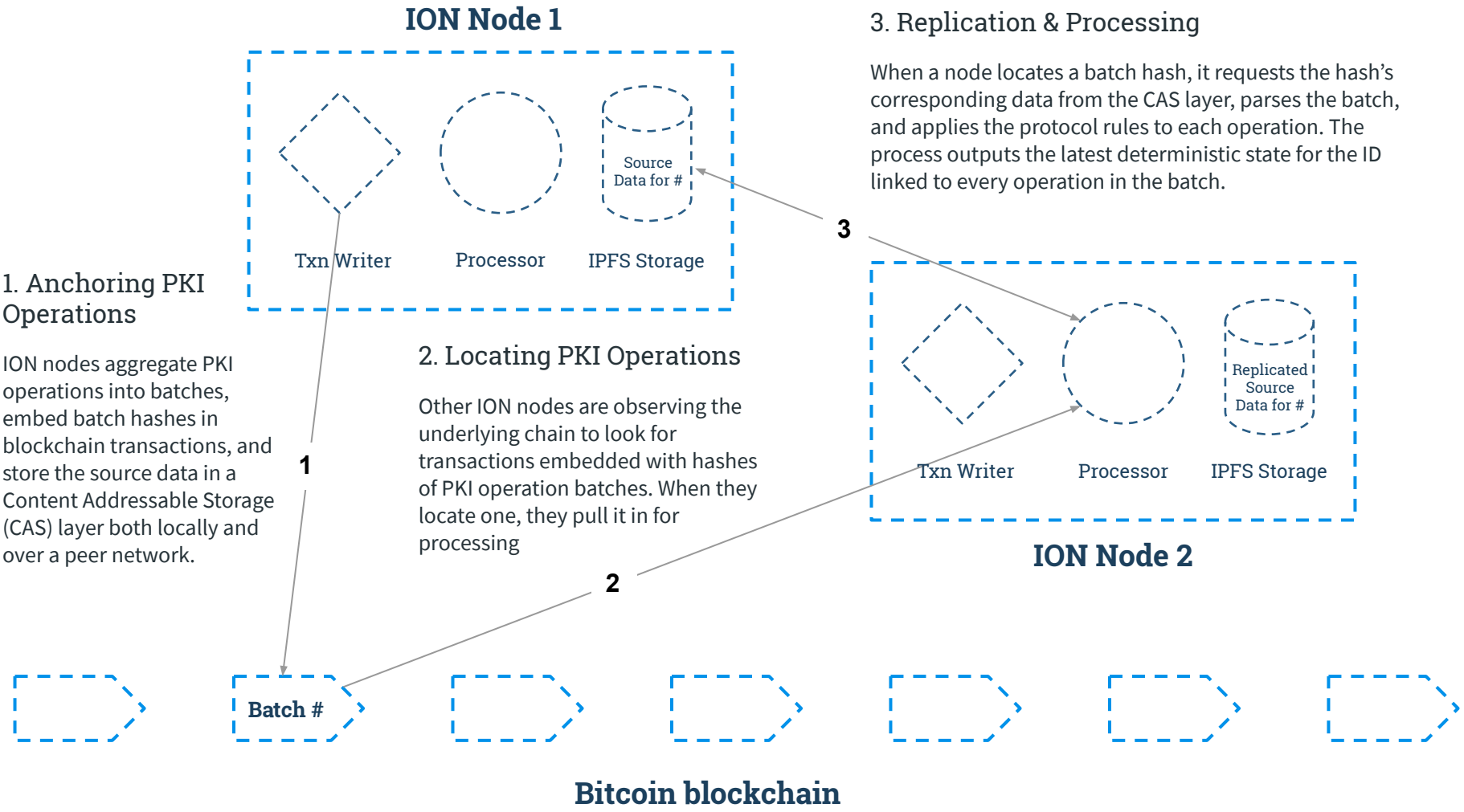
No conflicting states are allowed

The protocol eliminates conflicting PKI states via a strict, deterministic rule set that each node applies individually.

IDs are not transferable between entities

Transferring ownership of IDs between untrusting parties, as you would crypto-assets like Bitcoin, is not a supported function.

System Overview



1. Anchoring PKI Operations

ION nodes aggregate PKI operations into batches, embed batch hashes in blockchain transactions, and store the source data in a Content Addressable Storage (CAS) layer both locally and over a peer network.

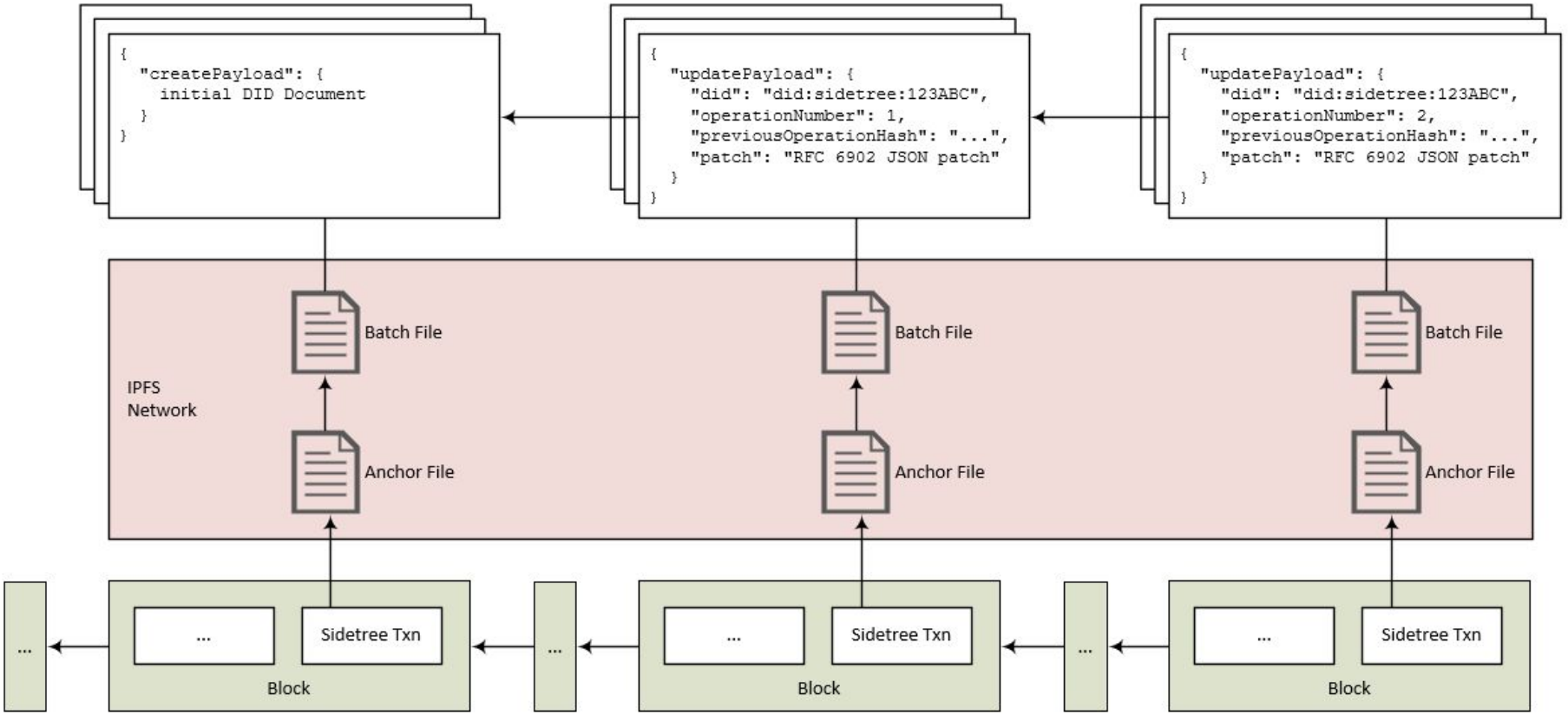
2. Locating PKI Operations

Other ION nodes are observing the underlying chain to look for transactions embedded with hashes of PKI operation batches. When they locate one, they pull it in for processing

3. Replication & Processing

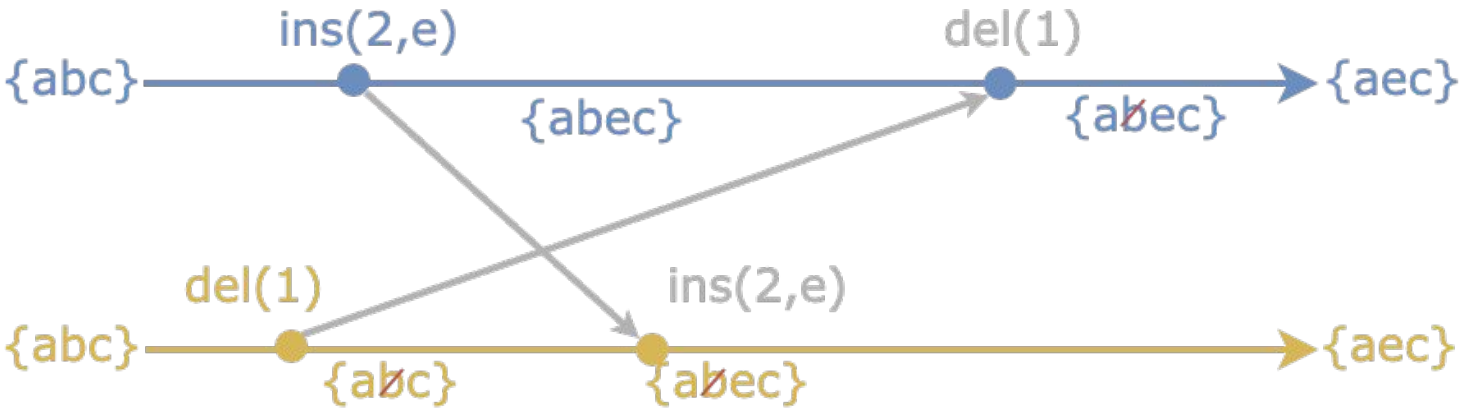
When a node locates a batch hash, it requests the hash's corresponding data from the CAS layer, parses the batch, and applies the protocol rules to each operation. The process outputs the latest deterministic state for the ID linked to every operation in the batch.

Anatomy of an Operation



DID PKI State Convergence

- The Sidetree protocol that underpins ION uses a form of Conflict-Free Resolution Datatype to converge the PKI state of DIDs.
- CRDTs deterministically merge changes to objects without a centralized database, trusted coordinator, etc. Typically, ordering of operations in a CRDT is based on vector clocks (Lamport timestamps).
- Sidetree uses a Delta-based CRDT, but instead of writers subjectively incremented vector clocks, operations are anchored in batches to the blockchain, which acts as a decentralized sequencing oracle that orders operations in a single, deterministic, linear history.



Traditional Delta-based CRDT converging changes using vector clocks

ION enables key features to enhance our offerings:

Massive Scale

The network can collectively process tens to hundreds of thousands of operations per second, even on consumer-grade machines.

Cost Efficient

Decentralized blockchains provide unique features, but the come at a high monetary/energy cost. ION's batching mechanism reduces per-unit op costs by several orders of magnitude.

Permissionless

Many other blockchain-based systems used for identity purposes rely on central authority schemes to scale their networks. ION is able to meet and exceed requirements while remaining decentralized.

Flexible Nodes

Unlike a blockchain, nodes of the ION network that runs atop the underlying decentralized system do not need to maintain the full history of transactions.

3.

Building the Network

ION is an organic system that requires care to develop, grow, and flourish.

Protocol Development and Network Upgrades

1 . 2 . 3

Major Protocol Evolution

Protocol advancements so large they require separate codebases

Forks & Required Upgrades

Critical updates, forking changes, or security patches that require all nodes to upgrade

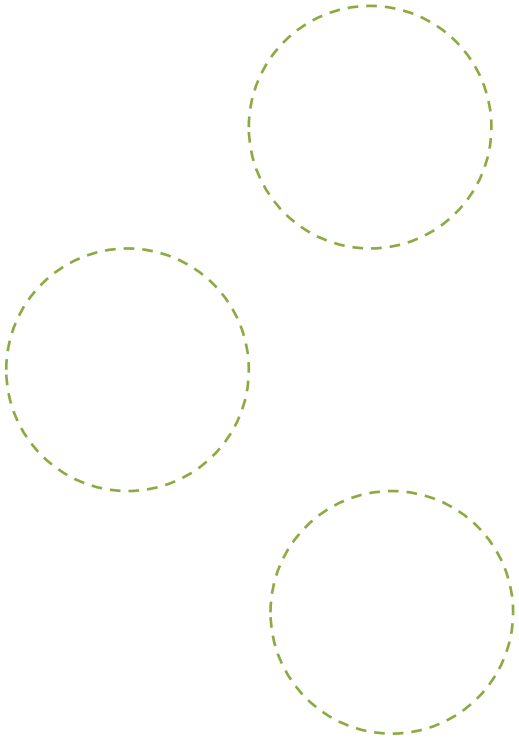
Discretionary Updates

All non-critical change that do not require all nodes to upgrade

Upgrade Process

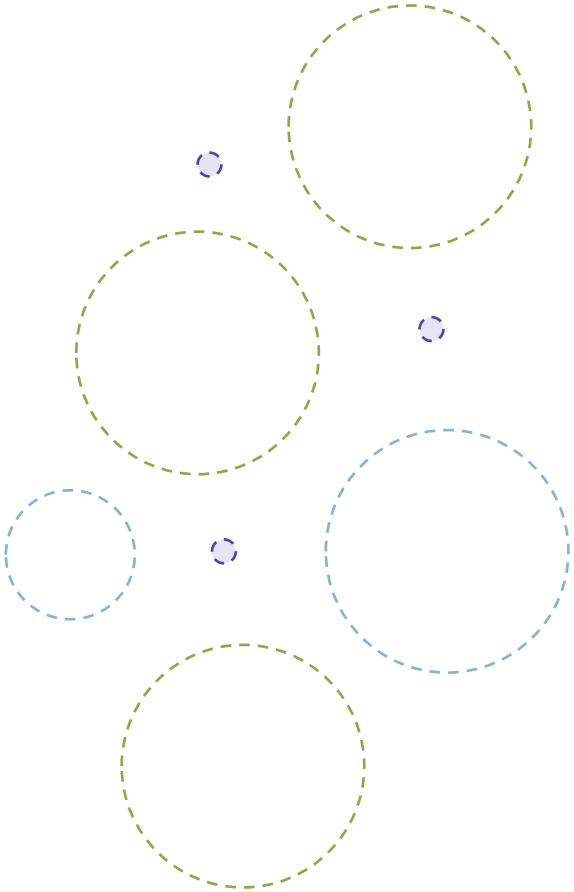
1. Tag release
2. Update install guides
3. Add an entry to the change log
4. Broadcast upgrade to node operators

The path to a robust network - a three stage journey:



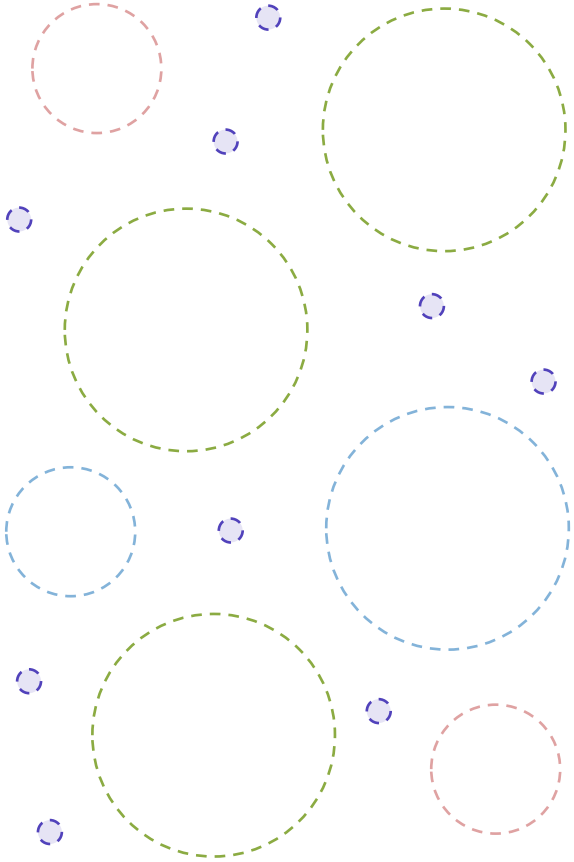
Stage 1

Larger entities run full nodes to jumpstart the network



Stage 2

Entities with product needs and early adopter hobbyists start running full nodes ad hoc



Stage 3

The long tail of developers, users, and organizations run a mix of light and full nodes to suit their needs

How to get involved:

Help shape specifications

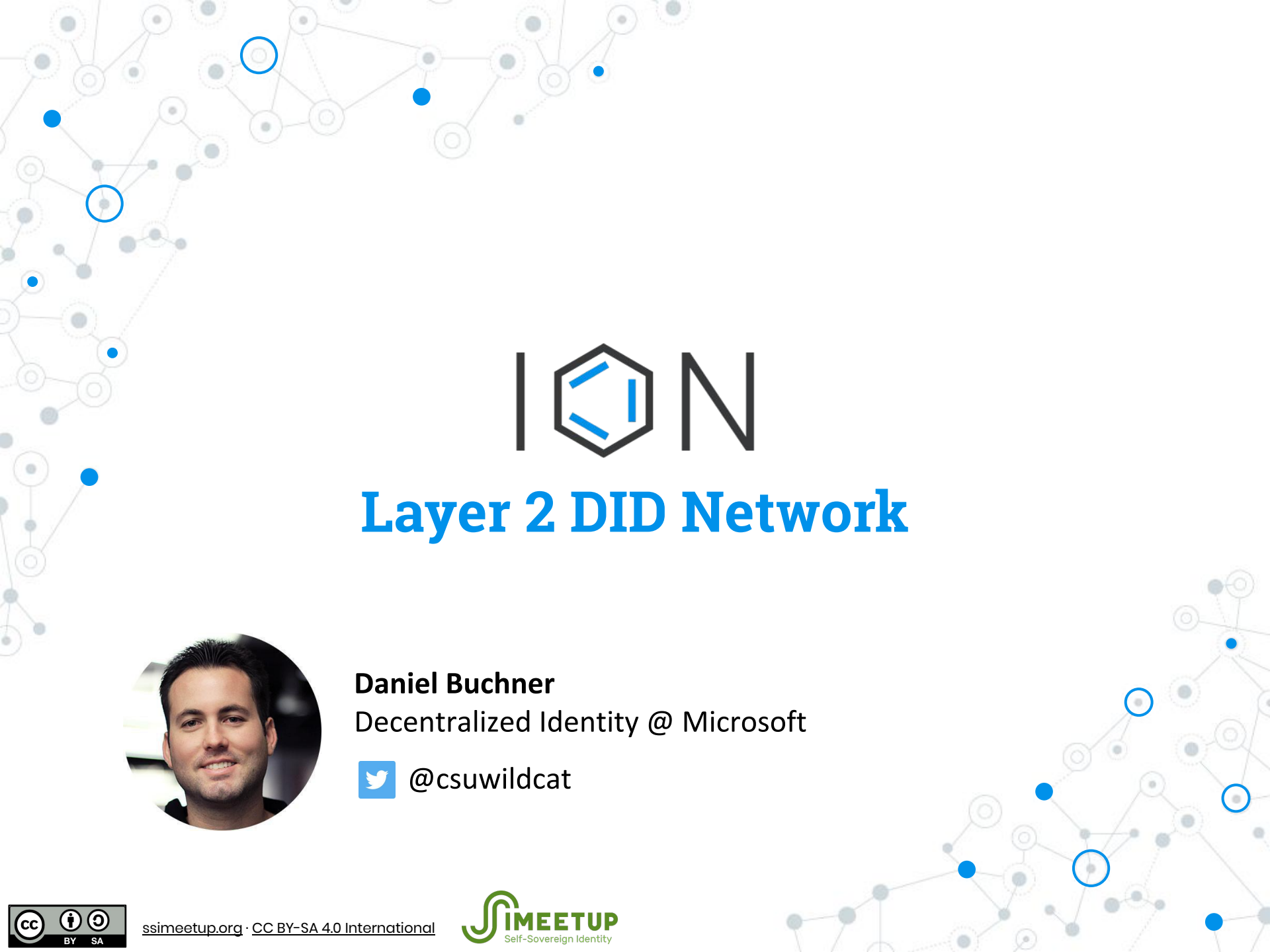
To ensure these systems meet the needs of all the individuals, organizations, and use cases that will rely on them, help shape the Sidetree protocol spec and technical decisions in ION.

Contribute to open source development

Contribute open source code to the DIF Sidetree protocol and ION node code in the DIF repositories on GitHub.

Run a node, participate in the ecosystem

In order to realize the value decentralized identity can deliver, participate in running the foundational components it relies on.



Layer 2 DID Network

Daniel Buchner
Decentralized Identity @ Microsoft

@csuwildcat