Verifiable Credentials in a Decentralizing World

SCALING THE TRUST LAYER OF THE INTERNET

Natalie Smolenski

Head of Business Development, Hyland Innovation

CommunityLIVE

AGENDA

- Bitcoin ION Network
- Verifiable Credentials
- Demo

CommunityLIVE

BITCOIN ION NETWORK

"Decentralized digital identity (DDID) is not just a technology buzzword: It promises a complete restructuring of the currently centralized physical and digital identity ecosystem into a decentralized and democratized architecture.
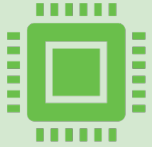
- Forrester

Prepare For Decentralized Digital Identity: Security SWOT, 2020

CommunityLIVE

ION = IDENTITY OVERLAY NETWORK

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

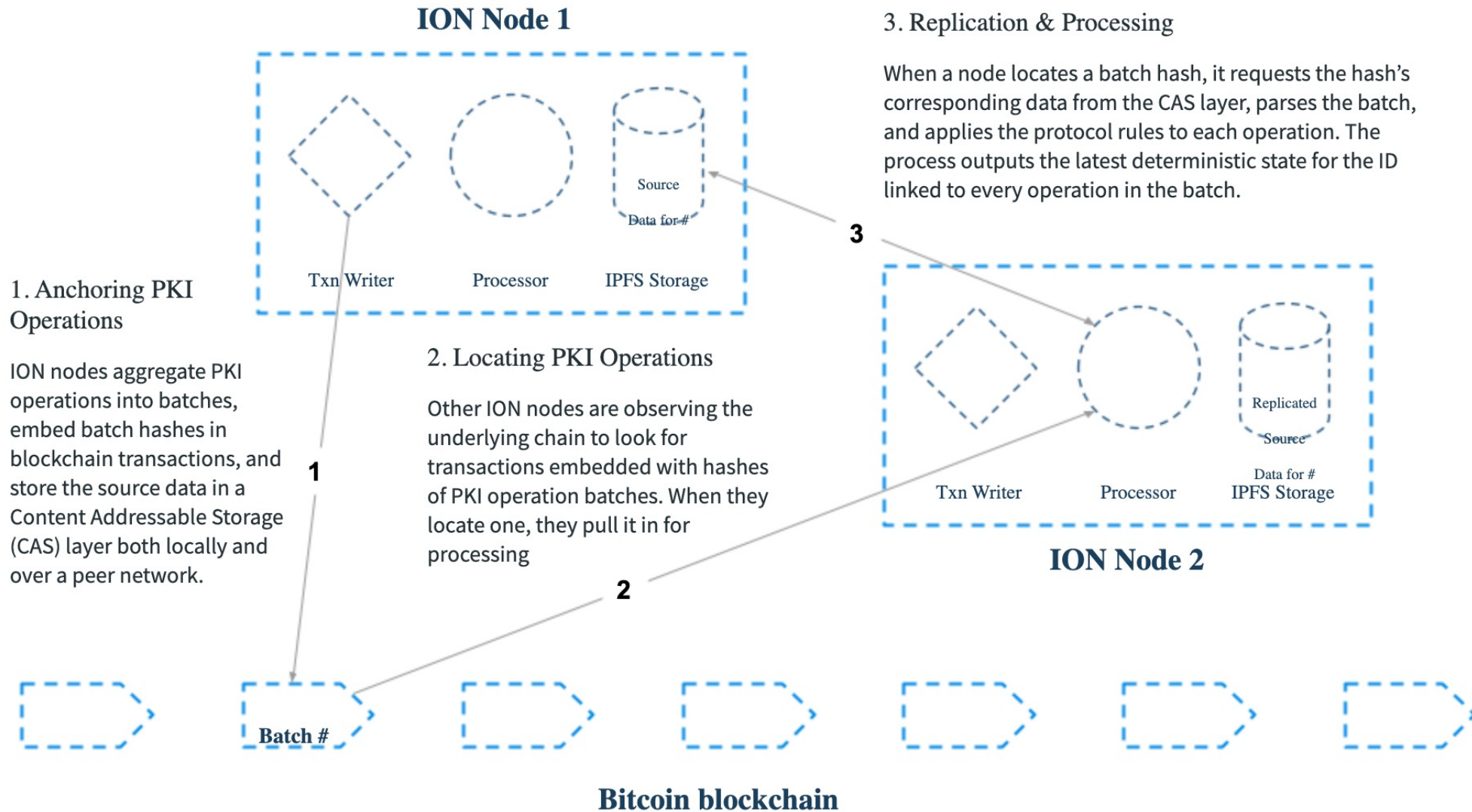Enables scale: tens of thousands of DID/PKI operations per second.

No additional consensus schemes, validator lists, or special protocol tokens.

Layer 2

Layer 1

**ION Node 1**

Txn Writer   Processor   IPFS Storage

Source
Data for #

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.

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

Replicated
Source
Data for #
Txn Writer   Processor   IPFS Storage

ION Node 2

Batch #

**Bitcoin blockchain**

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.
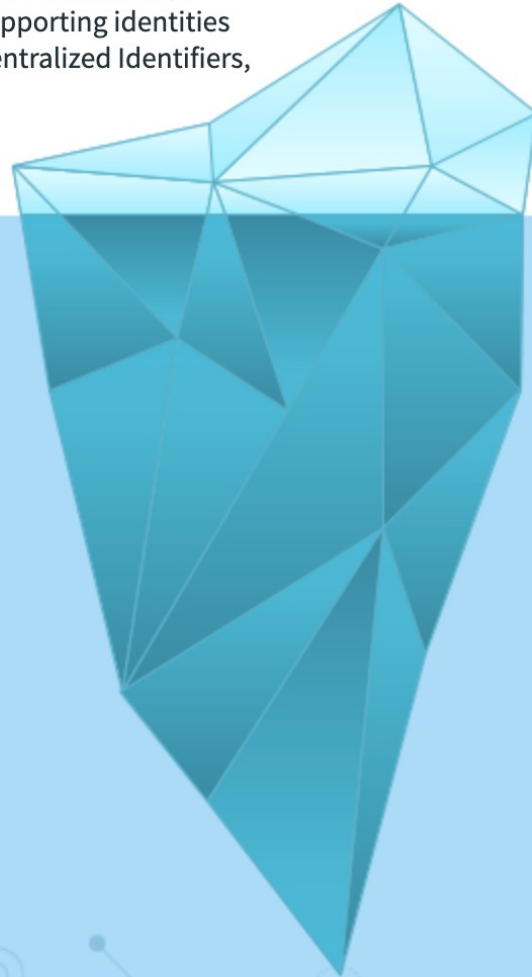
Identity of All Things.

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.
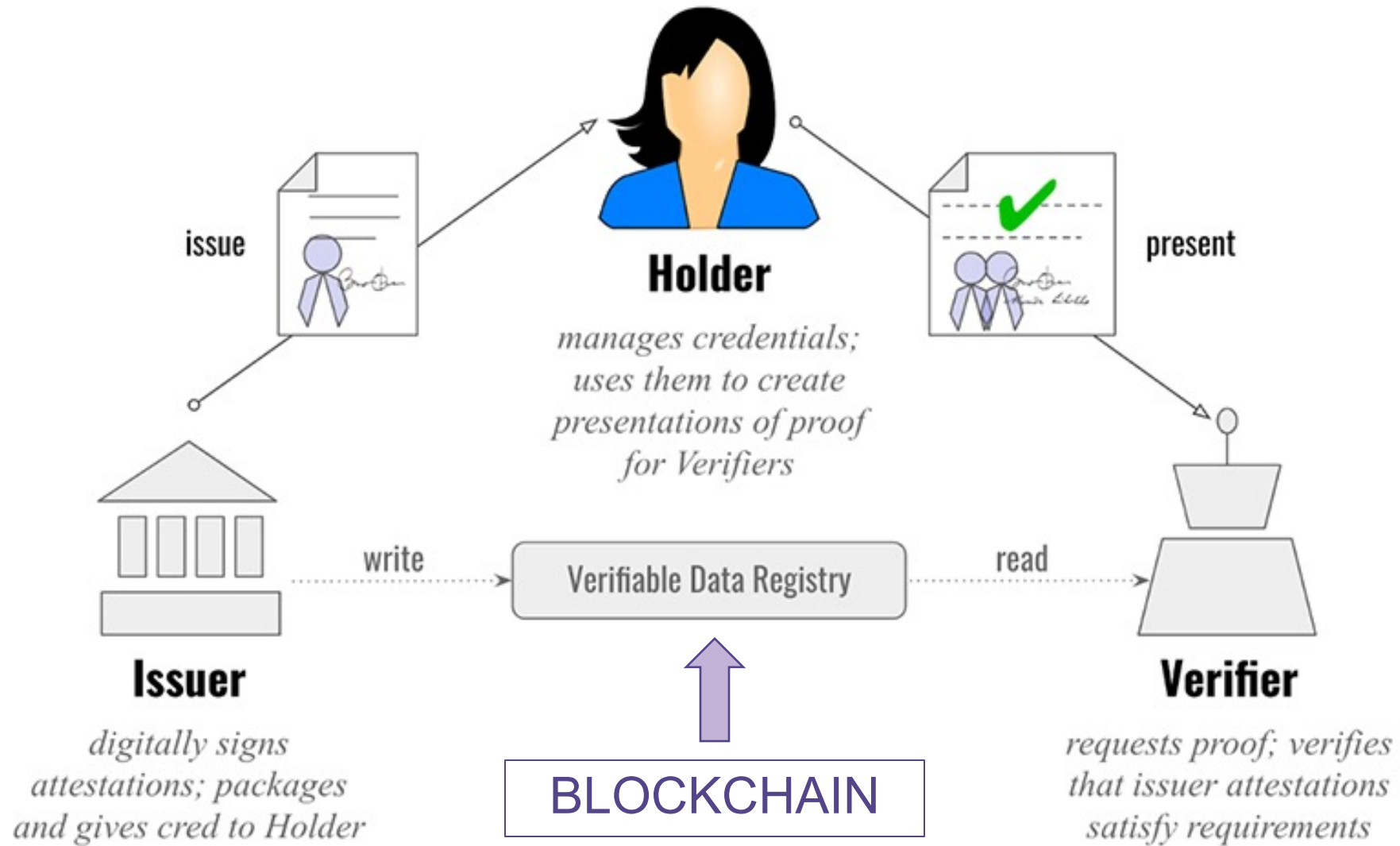
IDENTITY YOU OWN AND TAKE ANYWHERE
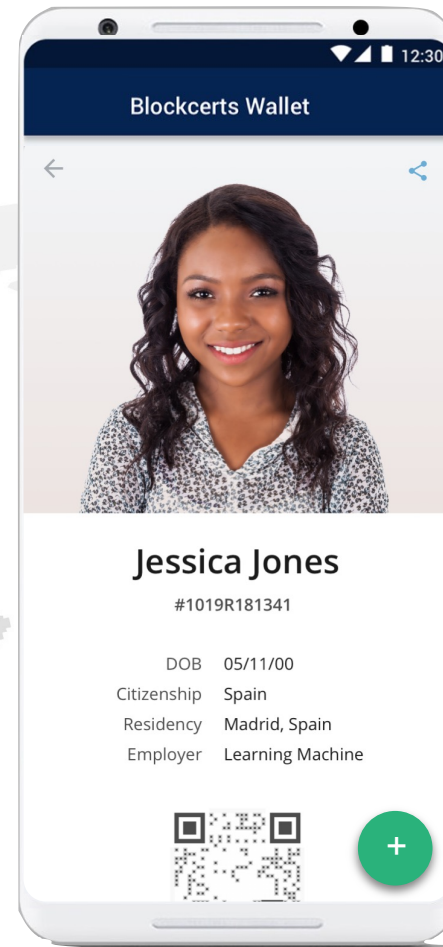
VERIFIABLE CREDENTIALS

VALIDATING CLAIMS ON THE WEB

- A Verifiable Credential is a tamper evident, digital credential with authorship that can be cryptographically verified.

- Verifiable Credentials is a technical standard for expressing credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable.

Holder

manages credentials; uses them to create presentations of proof for Verifiers

issue

present

Issuer

digitally signs attestations; packages and gives cred to Holder

write

Verifiable Data Registry

read

BLOCKCHAIN

Verifier

requests proof; verifies that issuer attestations satisfy requirements

ADVANTAGES OVER DIGITAL SIGNATURES

DIGITALLY-SIGNED PDFS

File Format	PDF – Fixed layout. Optimized for human readability.	
Data Flexibility	Open	✓
Recipient Ownership	No – Recipients do not control cryptographic keys	
Tamper Evidence	Yes	✓
Time Stamping	Yes	✓
Integrated Data/Display	Yes	✓
Shareable	Yes	✓
Revokable	Yes, by Certificate Authority only	✓
Expireable	Yes, by Certificate Authority only	✓
Vendor-Indepedent Verification	No	
Legal Enforcement	Yes	✓

W3C VERIFIABLE CREDENTIALS

File Format	JSON – Human and machine-readable, generates any display	✓
Data Flexibility	Open	✓
Recipient Control	Yes	✓
Tamper Evidence	Yes	✓
Independent Time Stamping	Yes	✓
Integrated Data/Display	Yes – lightweight envelope open to any schema	✓
Shareable	Yes	✓
Revokable	Yes	✓
Expireable	Yes	✓
Vendor-Indepedent Verification	Yes	✓
Legal Enforcement	Yes	✓

DEMO

QUESTIONS?

THANK YOU

Name: Natalie Smolenski
Email: natalie.smolenski@hyland.com
Phone: (972) 358-5542
Twitter: @NSmolenski
www.hyland.com