

# Verifiable Credentials in a Decentralizing World

SCALING THE TRUST LAYER OF THE INTERNET

Natalie Smolenski

Head of Business Development, Hyland Innovation

CommunityL/VE

## **AGENDA**

- Bitcoin ION Network
- Verifiable Credentials
- Demo





## 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

Community L/VE

### 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.

### **HOW DOES IT WORK?**

**Operations** 

## 3 ayer

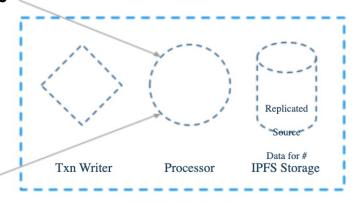
# ayer

#### **ION Node 1** Source Txn Writer **IPFS Storage** Processor 1. Anchoring PKI 2. Locating PKI Operations ION nodes aggregate PKI operations into batches, Other ION nodes are observing the embed batch hashes in underlying chain to look for blockchain transactions, and transactions embedded with hashes store the source data in a of PKI operation batches. When they Content Addressable Storage locate one, they pull it in for (CAS) layer both locally and processing over a peer network.

Batch #

#### 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.



**ION Node 2** 



#### Bitcoin blockchain

## **HUMAN IDENTITY IS JUST THE BEGINNING**

#### **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.

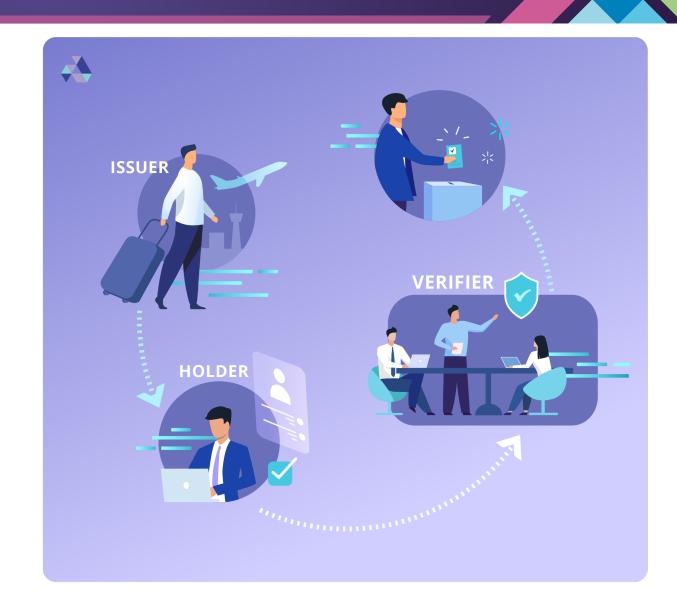
## **IDENTITY YOU OWN AND TAKE ANYWHERE**



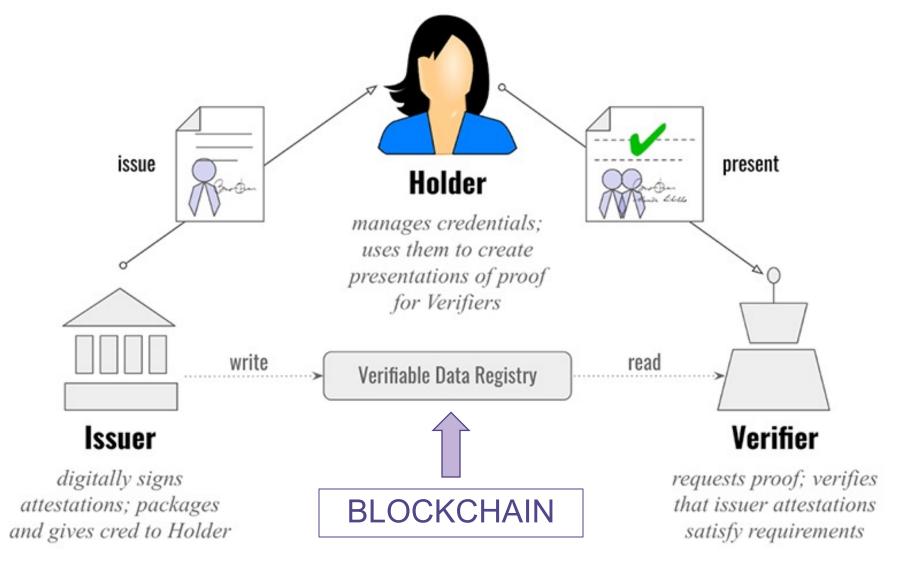


## VALIDATING CLAIMS ON THE WEB

- 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 machineverifiable.



### **ROLE OF BLOCKCHAIN**



## ADVANTAGES OVER DIGITAL SIGNATURES

#### **DIGITALLY-SIGNED PDFS**

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

#### **W3C VERIFIABLE CREDENTIALS**

File Format	JSON - Human and machine-readable, generates any display	~
Data Flexibility	Open	<b>✓</b>
Recipient Control	Yes	<b>✓</b>
Tamper Evidence	Yes	<b>✓</b>
Independent Time Stamping	Yes	<b>✓</b>
Integrated Data/Display	Yes - lightweight envelope open to any schema	<b>✓</b>
Shareable	Yes	<b>✓</b>
Revokable	Yes	<b>✓</b>
Expireable	Yes	<b>✓</b>
Vendor-Indepedent Verification	Yes	<b>✓</b>
Legal Enforcement	Yes	1

## DEMO



QUESTIONS?

## THANK YOU

Name: Natalie Smolenski

Email: natalie.smolenski@hyland.com

Phone: (972) 358-5542

Twitter: @NSmolenski

www.hyland.com