Internet Identity Workshop

Highlights of Internet Identity Workshop (IIW) #28

Drummond Reed
Chief Trust Officer Evernym
@DrummondReed

The latest and greatest developments in SSI straight from the Internet Identity Workshop (April 30-May 2, Mt. View, CA)

SIMEETUP SSIMeetup.org
Self-Sovereign Identity

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

Who Am I?

Years

- 20 years in Internet Identity
- 14 years (all 28 instances) of Internet Identity Workshop
- Many Internet Identity standards
  - W3C
  - OASIS
  - OpenID Foundation
  - Open Identity Exchange

SIMEETUP
Self-Sovereign Identity

Who Am I?

Hats

1. Chief Trust Officer, Evernym
2. Trustee, Sovrin Foundation
3. Chair, Sovrin Governance Framework Working Group
4. Co-Chair, OASIS XDI TC
5. Principle Investigator, U.S DHS DID and DKMS Projects
6. Co-Editor, W3C DID Specification

Internet Identity Workshop—Some Background

- First held in Berkeley CA in 2005
- Held every six months since then at the Computer History Museum in Mountain View,
- Hosted by Kaliya Young (@IdentityWoman), Phil Windley (@windley), and Doc Searls (@dsearls)
- Complete history available at http://www.internetidentityworkshop.com/

Internet Identity Workshop—Some Background

- ~230 attendees Day 1; ~150 Day 2, ~100 Day 3.
- The format is entirely open space: https://en.wikipedia.org/wiki/Open_Space_Technology
- The agenda is self-organized by the attendees each morning—5 hour-long slots across 12 meeting rooms
- Lots of informal discussion and hallway meetings
- All-conference dinners Tuesday & Wednesday evenings

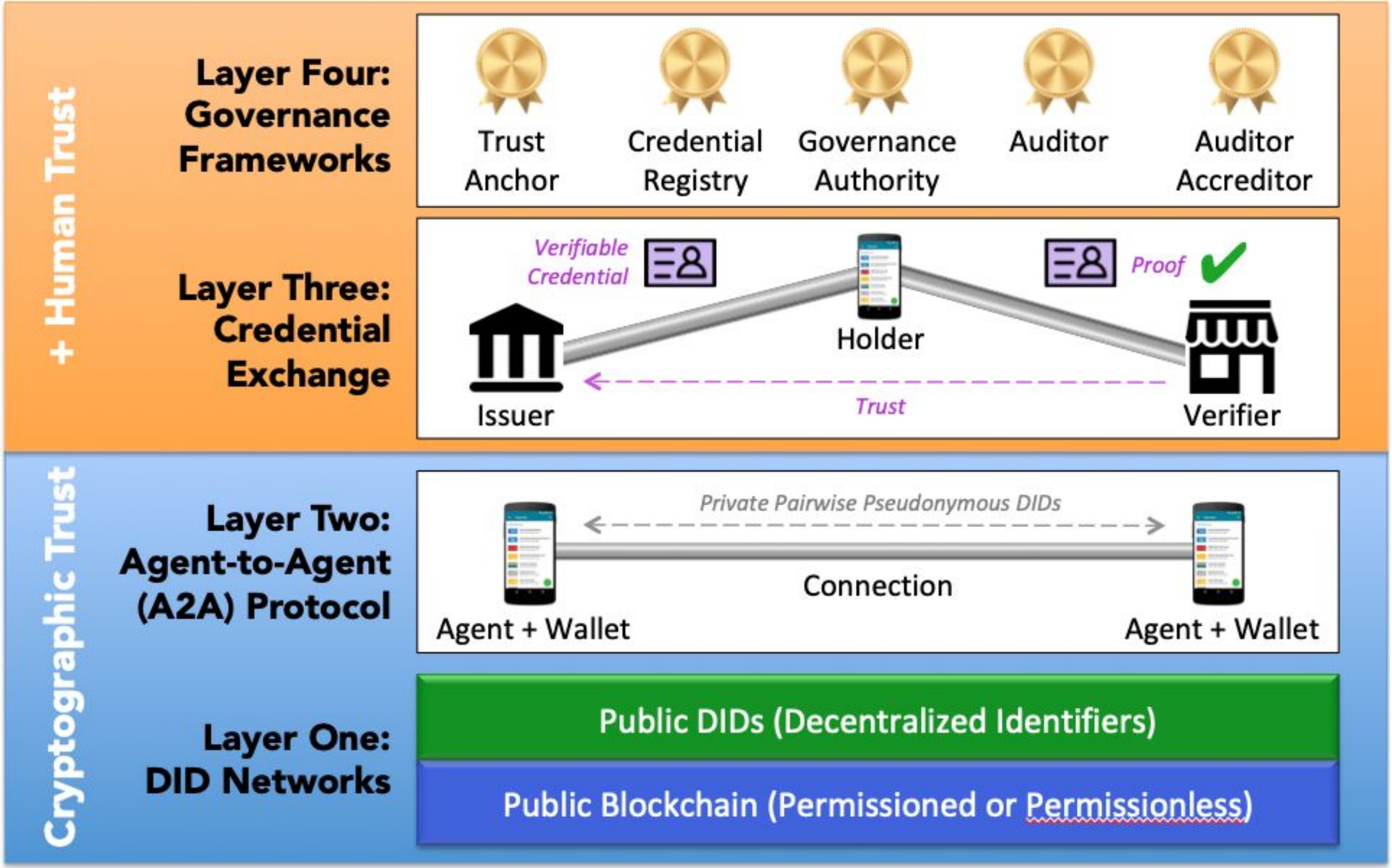
Caveats about these Highlights

- I am just one attendee
- I could only attend one out of each dozen sessions (and I missed several due to other meetings)
- I self-selected sessions on the topics I am most interested/involved in
- Other attendees might have an entirely different set of highlights

#1: DIDs were Everywhere

DIDs have become the lingua franca of SSI

- DIDs (Decentralized Identifiers) are now taken as a given in all decentralized identity and SSI projects
- They provide the cryptographic roots-of-trust for issuers, holders, and verifiers of verifiable credentials
- They can support all modern blockchains, distributed ledgers, and decentralized networks
- Demos included Bitcoin, Ethereum, Sovrin, Ockam, ION, and Element methods (the latter two based on Sidetree)



+ Human Trust

Layer Four: Governance Frameworks

Trust Anchor

Credential Registry

Governance Authority

Auditor

Auditor Accreditor

Layer Three: Credential Exchange

Verifiable Credential

Holder

Proof ✓

Issuer

Trust

Verifier

Cryptographic Trust

Layer Two: Agent-to-Agent (A2A) Protocol

Private Pairwise Pseudonymous DIDs

Connection

Agent + Wallet

Agent + Wallet

Layer One: DID Networks

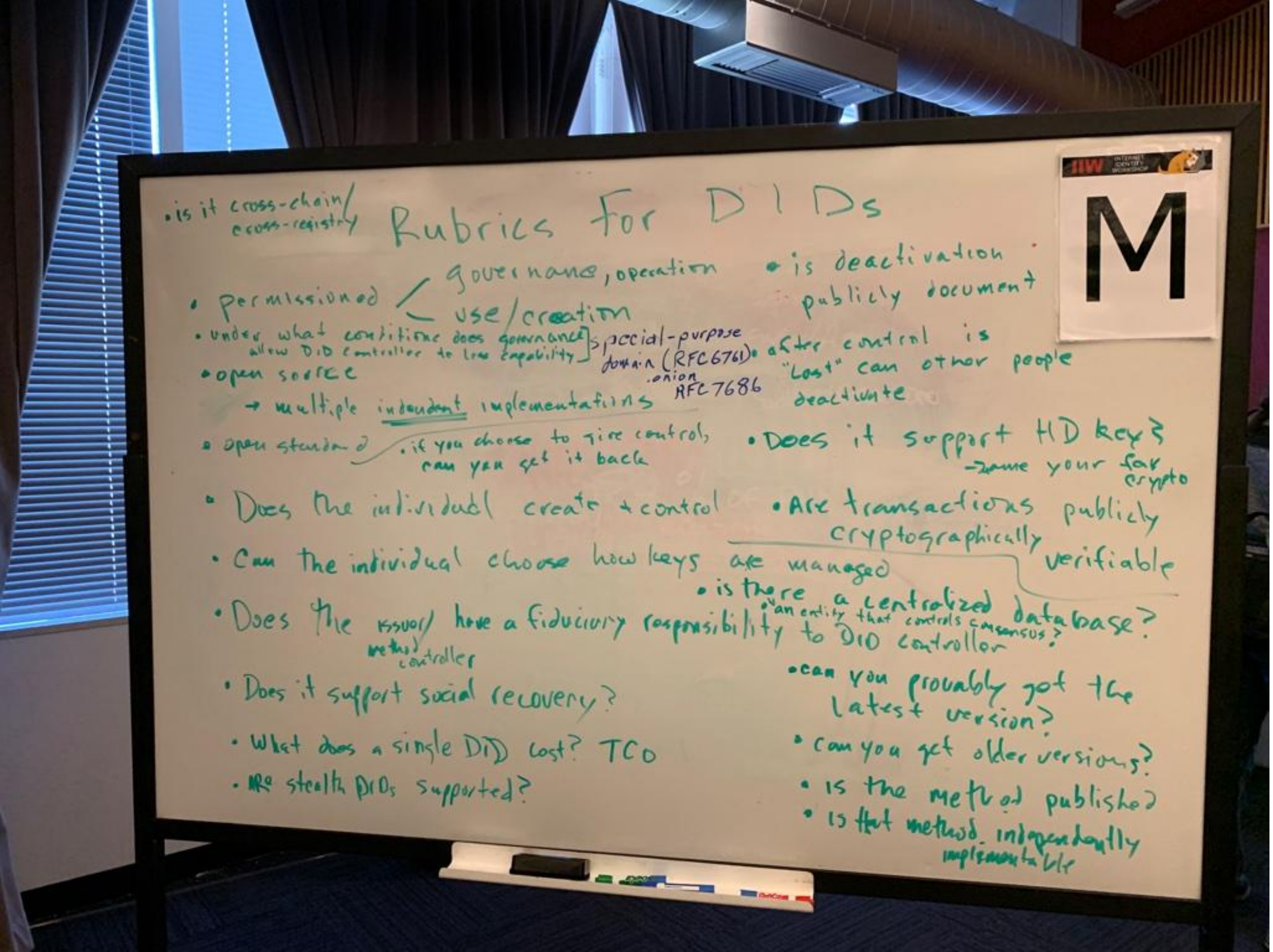
Public DIDs (Decentralized Identifiers)

Public Blockchain (Permissioned or Permissionless)

Decentralization of DIDs has become a hot topic

- The popularity of DIDs is leading to proposals for DID methods that many do not consider decentralized
  - did:web:domain.com
  - did:facebook:
- This is an active topic for the Community Final Draft DID spec and the W3C DID Working Group Charter

Joe Andrieu led a session on DIDs and decentralization--what really makes a system decentralized (and why that is important to SSI)


IIW INTERNET IDENTITY WORKSHOP
M

Rubrics for DIDs

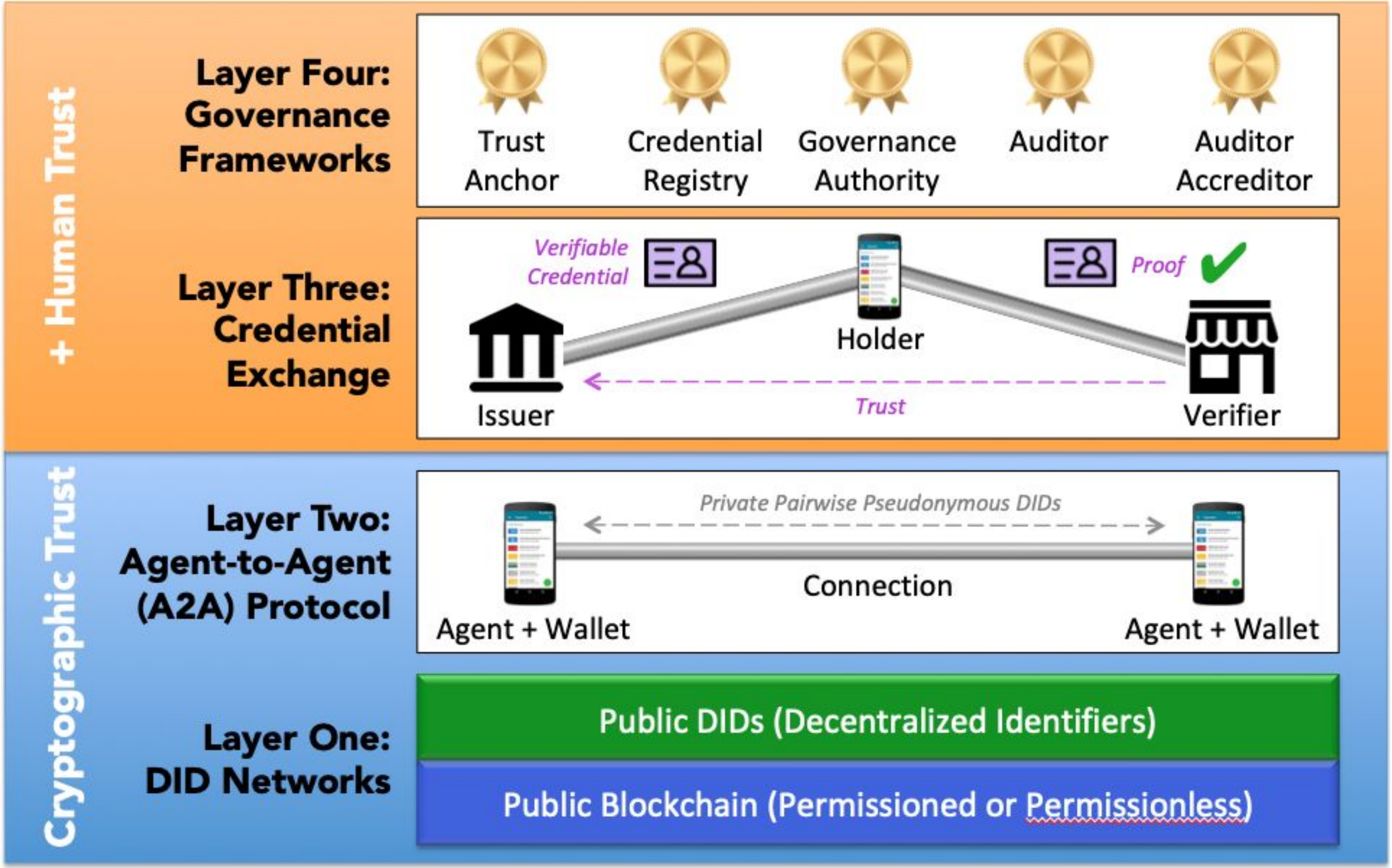
- is it cross-chain/ cross-registry
- permissioned < governance, operation / use/creation
- under what contitions does governance allow DID controller to lose capability] special-purpose domain (RFC6761) .onion RFC7686
- open source
  → multiple indendent implementations
- open standard
  - if you choose to give control, can you get it back
- Does the individual create + control
- Can the individual choose how keys are managed
- Does the issuer/ method controller have a fiduciary responsibility to DID controller
- Does it support social recovery?
- What does a single DID cost? TCO
- Are stealth DIDs supported?

- is deactivation publicly document
- after control is "Lost" can other people deactivate
- Does it support HD keys? →name your fav crypto
- Are transactions publicly cryptographically verifiable
- is there a centralized database?
  - or an entity that controls consensus?
- can you provably get the latest version?
- can you get older versions?
- is the method published
- is that method independently implementable

Joe's second session produced a whiteboard full of "rubrics" for helping to evaluate DID methods

Peer DIDs are going mainstream

- The rationale for off-ledger DID-to-DID connections to use private pairwise pseudonymous DIDs is becoming clear
- The **did:peer:** method has been published in the W3C Credentials Community Group DID Method Registry
  - https://w3c-ccg.github.io/did-method-registry/
- It will be built into the Hyperledger Aries codebase



+ Human Trust

Layer Four: Governance Frameworks

Trust Anchor

Credential Registry

Governance Authority

Auditor

Auditor Accreditor

Layer Three: Credential Exchange

Verifiable Credential

Holder

Proof ✓

Issuer

Trust

Verifier

Cryptographic Trust

Layer Two: Agent-to-Agent (A2A) Protocol

Private Pairwise Pseudonymous DIDs

Connection

Agent + Wallet

Agent + Wallet

Layer One: DID Networks

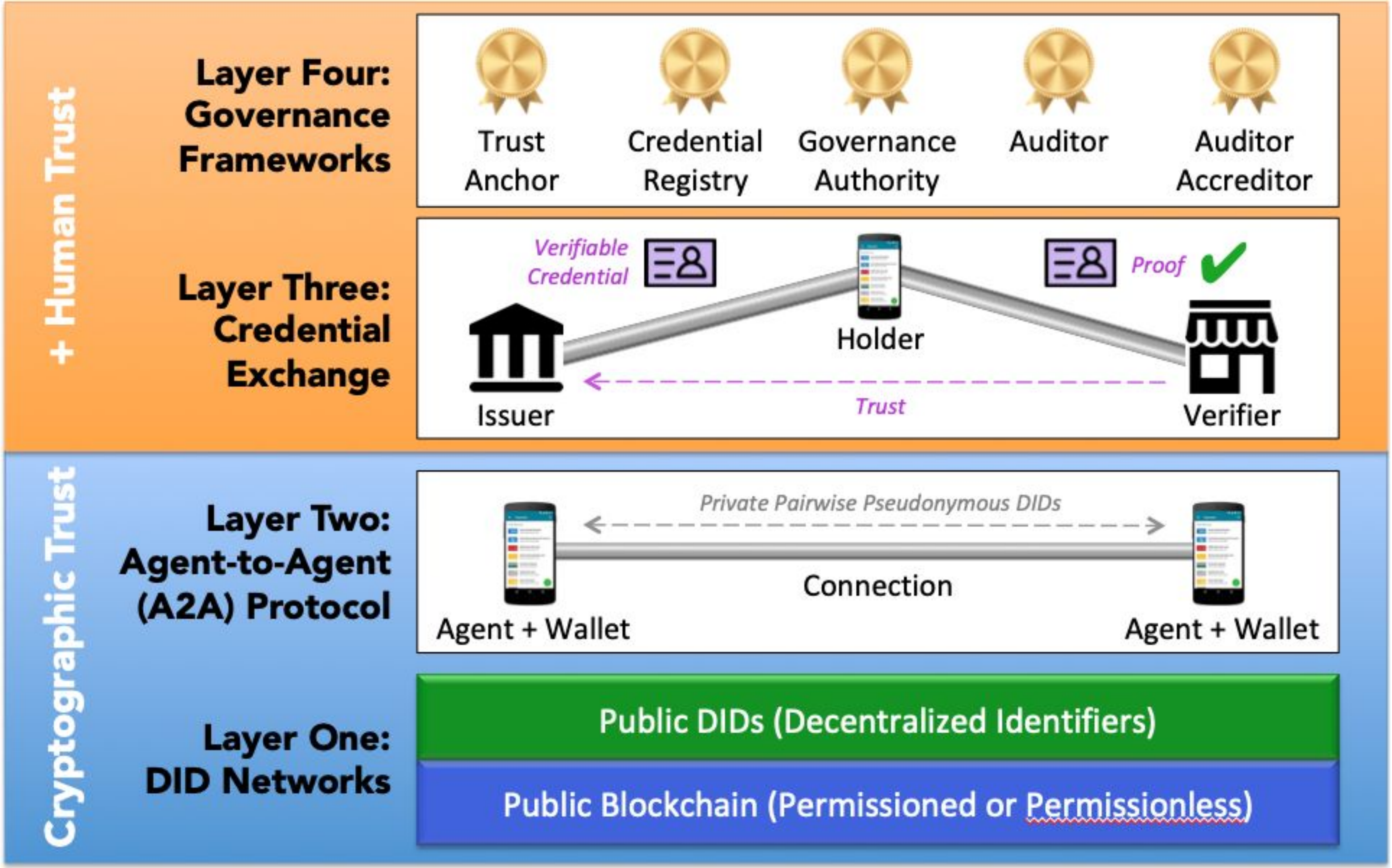
Public DIDs (Decentralized Identifiers)

Public Blockchain (Permissioned or Permissionless)

#2: Agents were everywhere

Layer 2 of the SSI stack is where all the action is

- Six different implementations of Hyperledger Indy agents and wallets were demonstrated
- There was intense interest in converging on a single layer 2 protocol—this will be fundamental to interoperability
- This is also fundamental to widespread adoption of verifiable credentials



+ Human Trust

Layer Four: Governance Frameworks

Trust Anchor

Credential Registry

Governance Authority

Auditor

Auditor Accreditor

Layer Three: Credential Exchange

Verifiable Credential

Holder

Proof ✓

Issuer

Trust

Verifier

Cryptographic Trust

Layer Two: Agent-to-Agent (A2A) Protocol

Private Pairwise Pseudonymous DIDs

Connection

Agent + Wallet

Agent + Wallet

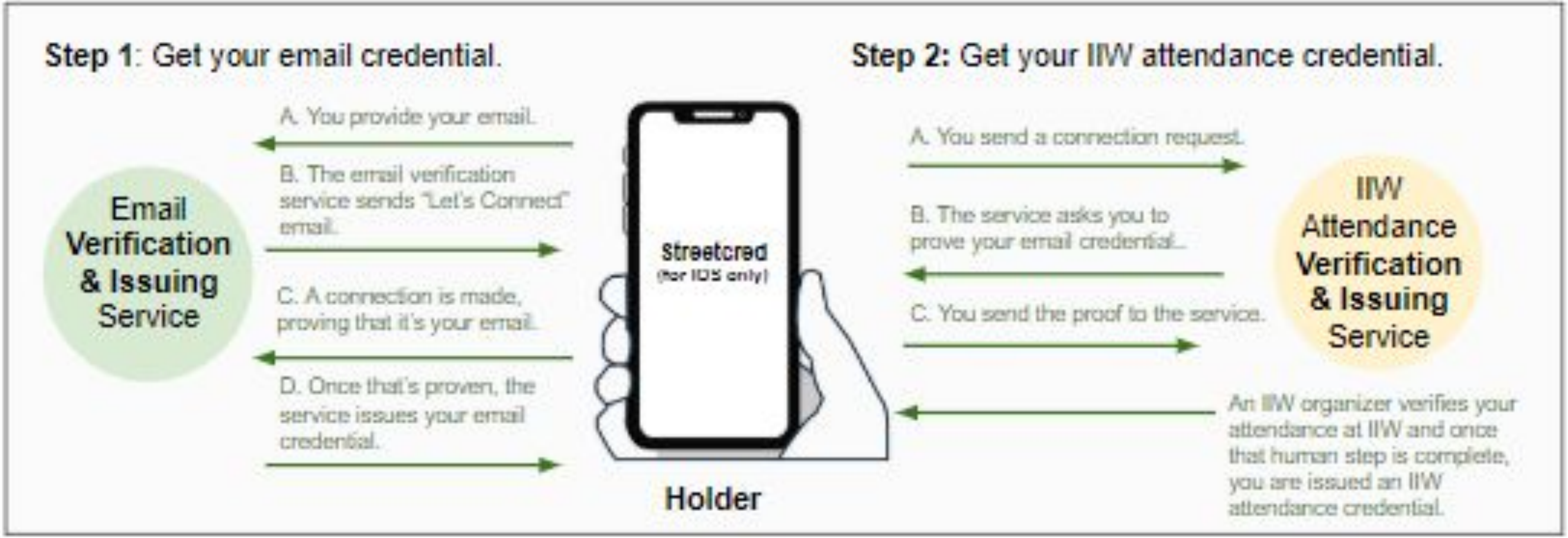
Layer One: DID Networks

Public DIDs (Decentralized Identifiers)

Public Blockchain (Permissioned or Permissionless)

The BC Gov team led a killer agent interop demo

- https://iiw.vonx.io/ to start the demo
- You can use any of 3 different agent/wallet apps
- First you get a verifiable credential of your email address
- Then you get a VC that you were an IIW attendee
- Then you were added to the IIWBook directory
- Then you could create **your own private peer-to-peer connection** with any other IIWBook member



Step 1: Get your email credential.

A. You provide your email.

B. The email verification service sends "Let's Connect" email.

C. A connection is made, proving that it's your email.

D. Once that's proven, the service issues your email credential.

Step 2: Get your IIW attendance credential.

A. You send a connection request.

B. The service asks you to prove your email credential.

C. You send the proof to the service.

An IIW organizer verifies your attendance at IIW and once that human step is complete, you are issued an IIW attendance credential.

Email Verification & Issuing Service
Streetcred
(for IOS only)
Holder
IIW Attendance Verification & Issuing Service

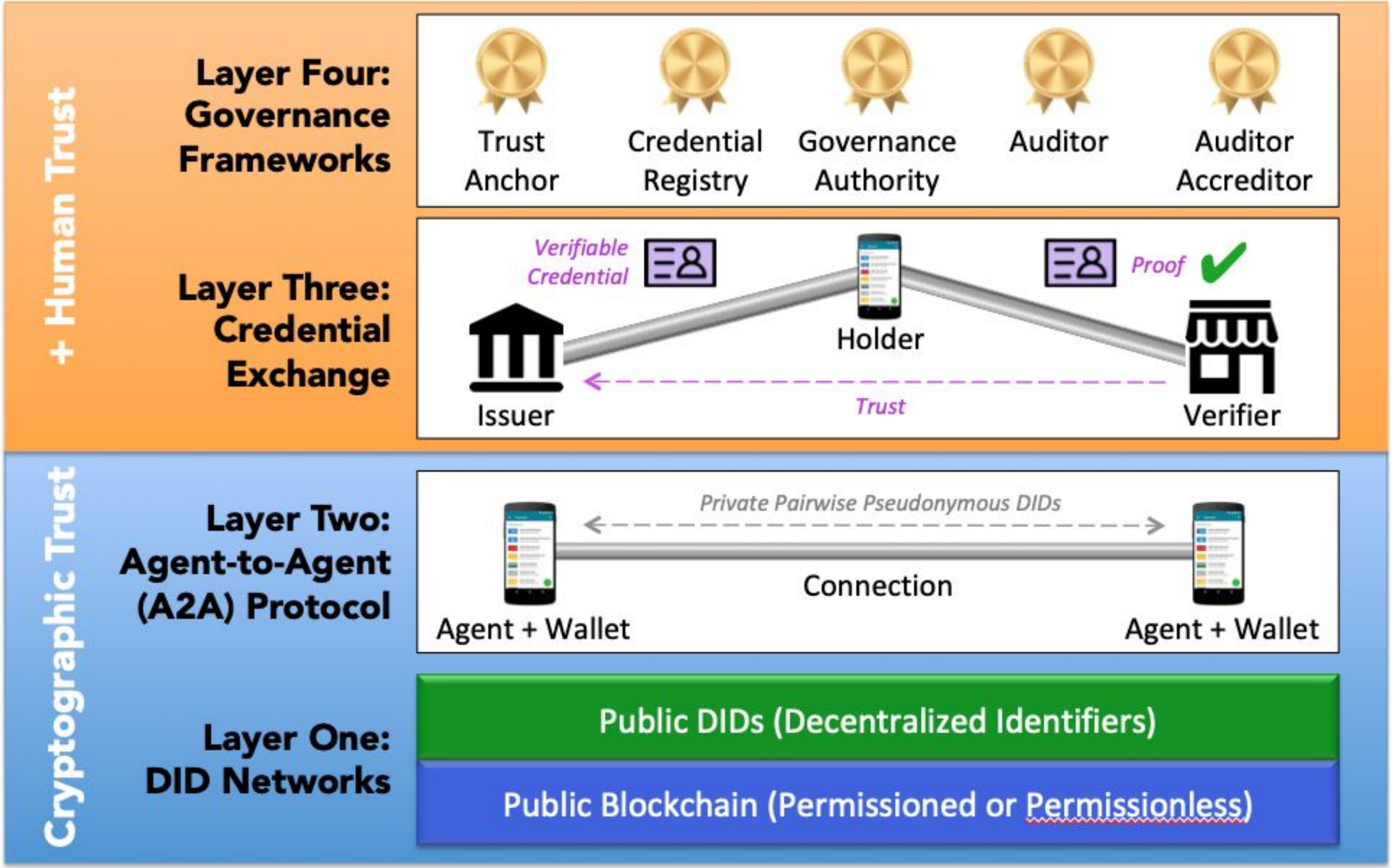
For complete details: https://iiw.vonx.io/

Agents and hubs can be best friends!

- Hubs are the personal data store/replication/sharing project from the Storage & Compute Working Group at the Decentralized Identity Foundation (DIF)
- Indy agent architects and DIF hub architects held multiple sessions to **converge on a unified layer 2 protocol**
- Great progress was made; worldviews are being mapped; optimism that agents & hubs can live in sweet harmony

The Hyperledger Aries project was announced!

- Aries splits off the agent + wallet code that was part of Indy into a new standalone Hyperledger project
- Aries will be completely **ledger-neutral**—it can work with any DID method for any DID network
- The **did:peer:** method will be built-in for universal interop
- Aries will concentrate efforts on a **unified layer 2 protocol**



+ Human Trust

Layer Four: Governance Frameworks

Trust Anchor

Credential Registry

Governance Authority

Auditor

Auditor Accreditor

Layer Three: Credential Exchange

Verifiable Credential

Holder

Proof ✓

Issuer

Trust

Verifier

Cryptographic Trust

Layer Two: Agent-to-Agent (A2A) Protocol

Private Pairwise Pseudonymous DIDs

Connection

Agent + Wallet

Agent + Wallet

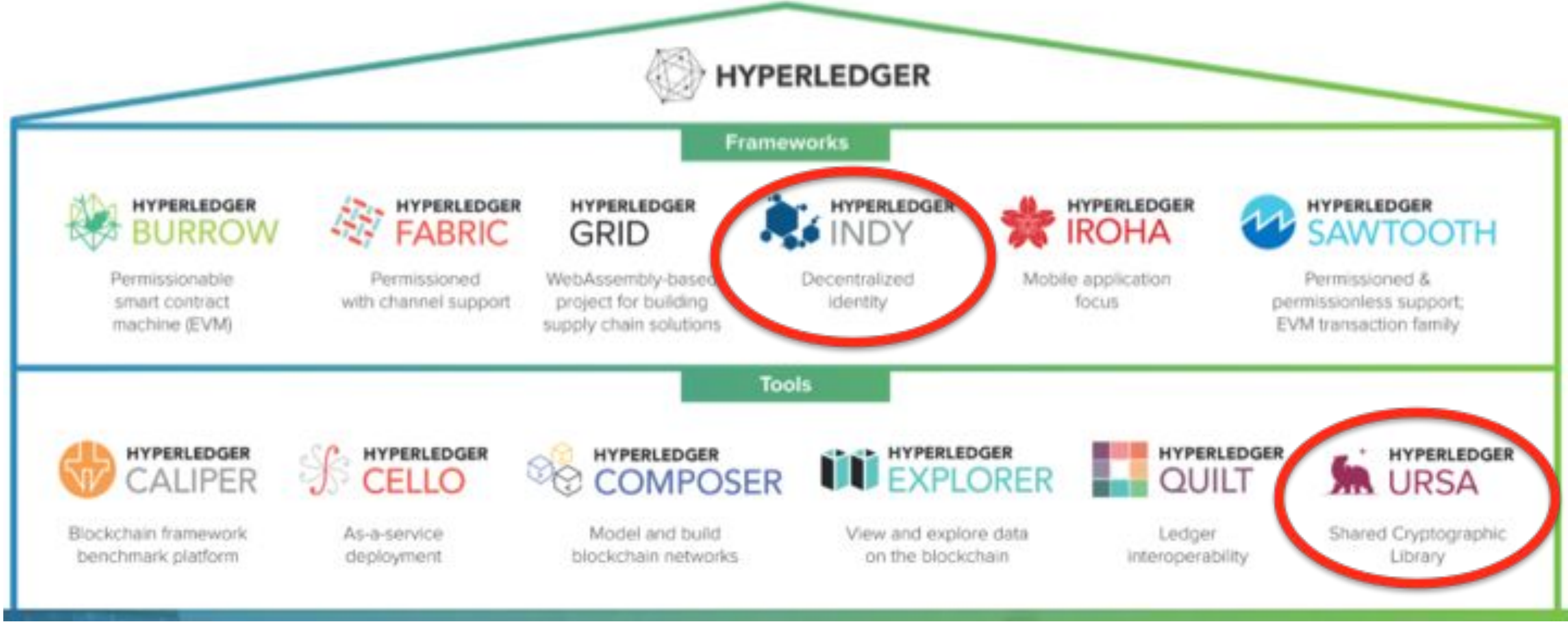
Layer One: DID Networks

Public DIDs (Decentralized Identifiers)

Public Blockchain (Permissioned or Permissionless)

The Hyperledger Greenhouse

Business Blockchain Frameworks & Tools Hosted by Hyperledger



HYPERLEDGER

Frameworks

HYPERLEDGER BURROW
Permissionable smart contract machine (EVM)

HYPERLEDGER FABRIC
Permissioned with channel support

HYPERLEDGER GRID
WebAssembly-based project for building supply chain solutions

HYPERLEDGER INDY
Decentralized identity

HYPERLEDGER IROHA
Mobile application focus

HYPERLEDGER SAWTOOTH
Permissioned & permissionless support; EVM transaction family

Tools

HYPERLEDGER CALIPER
Blockchain framework benchmark platform

HYPERLEDGER CELLO
As-a-service deployment

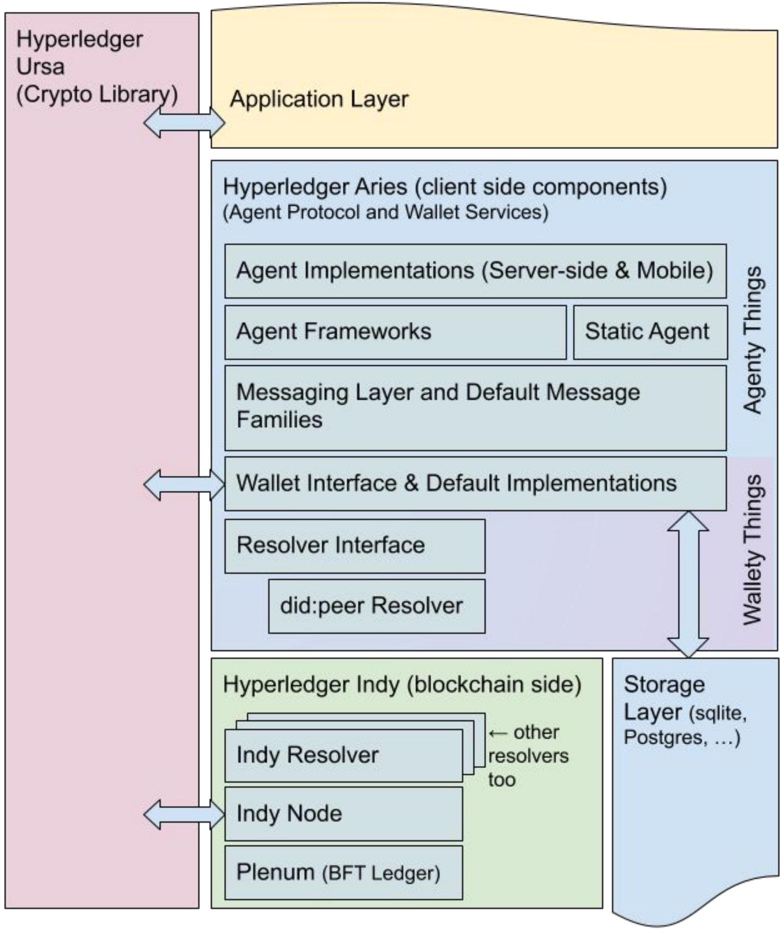
HYPERLEDGER COMPOSER
Model and build blockchain networks

HYPERLEDGER EXPLORER
View and explore data on the blockchain

HYPERLEDGER QUILT
Ledger interoperability

HYPERLEDGER URSA
Shared Cryptographic Library

Hyperledger as a Verifiable Information Exchange Platform



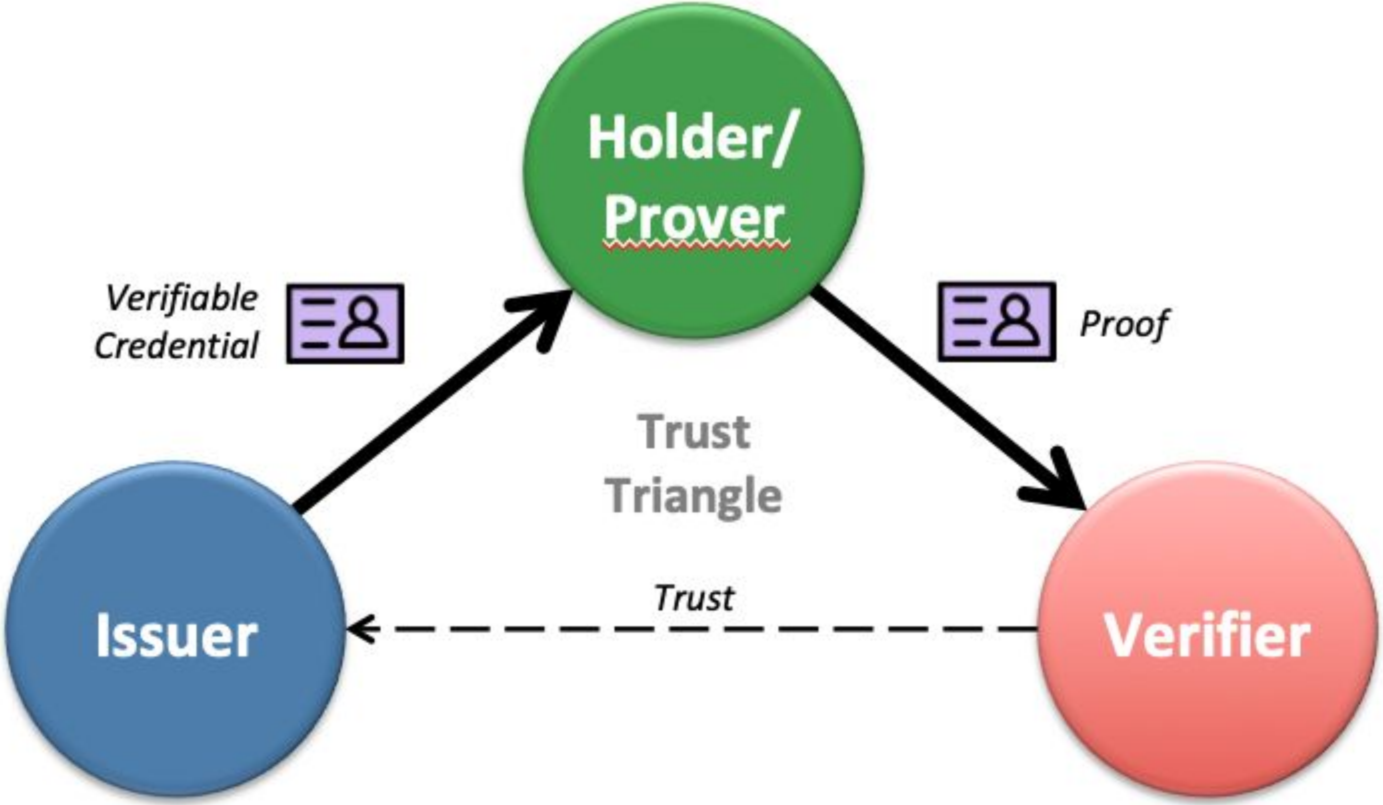
Hyperledger Ursa (Crypto Library)
Application Layer
Hyperledger Aries (client side components)
(Agent Protocol and Wallet Services)
Agent Implementations (Server-side & Mobile)
Agent Frameworks
Static Agent
Messaging Layer and Default Message Families
Agenty Things
Wallet Interface & Default Implementations
Resolver Interface
did:peer Resolver
Wallety Things
Hyperledger Indy (blockchain side)
Indy Resolver
← other resolvers too
Indy Node
Plenum (BFT Ledger)
Storage Layer (sqlite, Postgres, …)

For complete details: https://wiki.hyperledger.org/display/HYP/Hyperledger+Aries+Proposal

#3: Verifiable credentials were everywhere

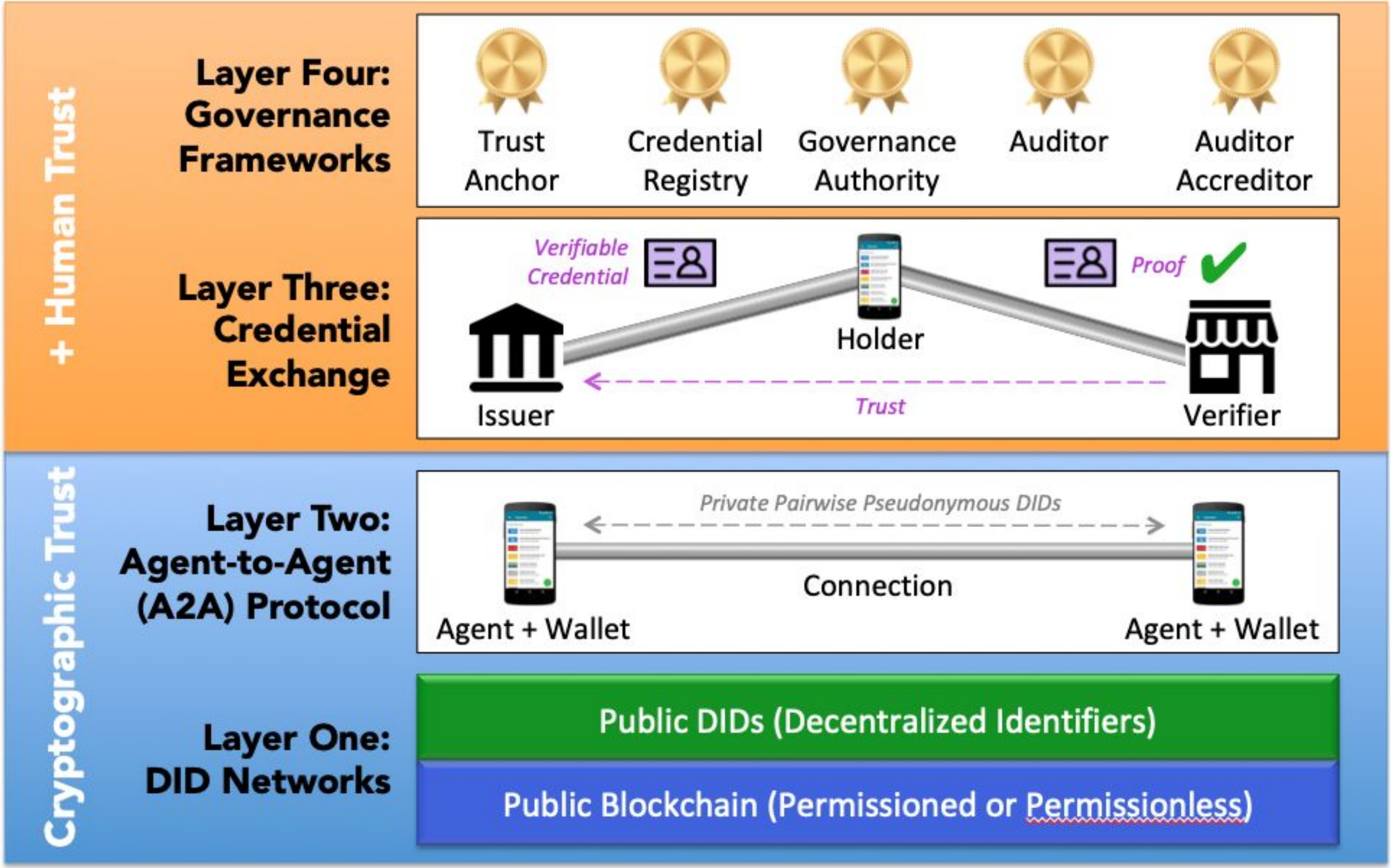
Verifiable creds are the heros of the SSI movie

- The Avengers of trust on the Internet
- They carry all the weight—they are how trust is conveyed from an issuer to a holder to a verifier
- This “trust triangle” is the core pattern for all of SSI


Holder/ Prover
Verifiable Credential
Proof
Trust Triangle
Trust
Issuer
Verifier

VCs are the most advanced standard in SSI

- The W3C Verifiable Claims Working Group has already issued Verifiable Credentials Data Model V1.0 CR (Candidate Recommendation)
- Three major formats will be supported
  - JSON with JWT (JSON Web Token) signatures
  - JSON-LD with Linked Data Signatures
  - JSON-LD with ZKP (Zero Knowledge Proofs—as used by Hyperledger Indy and now Hyperledger Aries)



+ Human Trust

Layer Four: Governance Frameworks

Trust Anchor

Credential Registry

Governance Authority

Auditor

Auditor Accreditor

Layer Three: Credential Exchange

Verifiable Credential

Holder

Proof ✔

Issuer

Trust

Verifier

Cryptographic Trust

Layer Two: Agent-to-Agent (A2A) Protocol

Private Pairwise Pseudonymous DIDs

Connection

Agent + Wallet

Agent + Wallet

Layer One: DID Networks

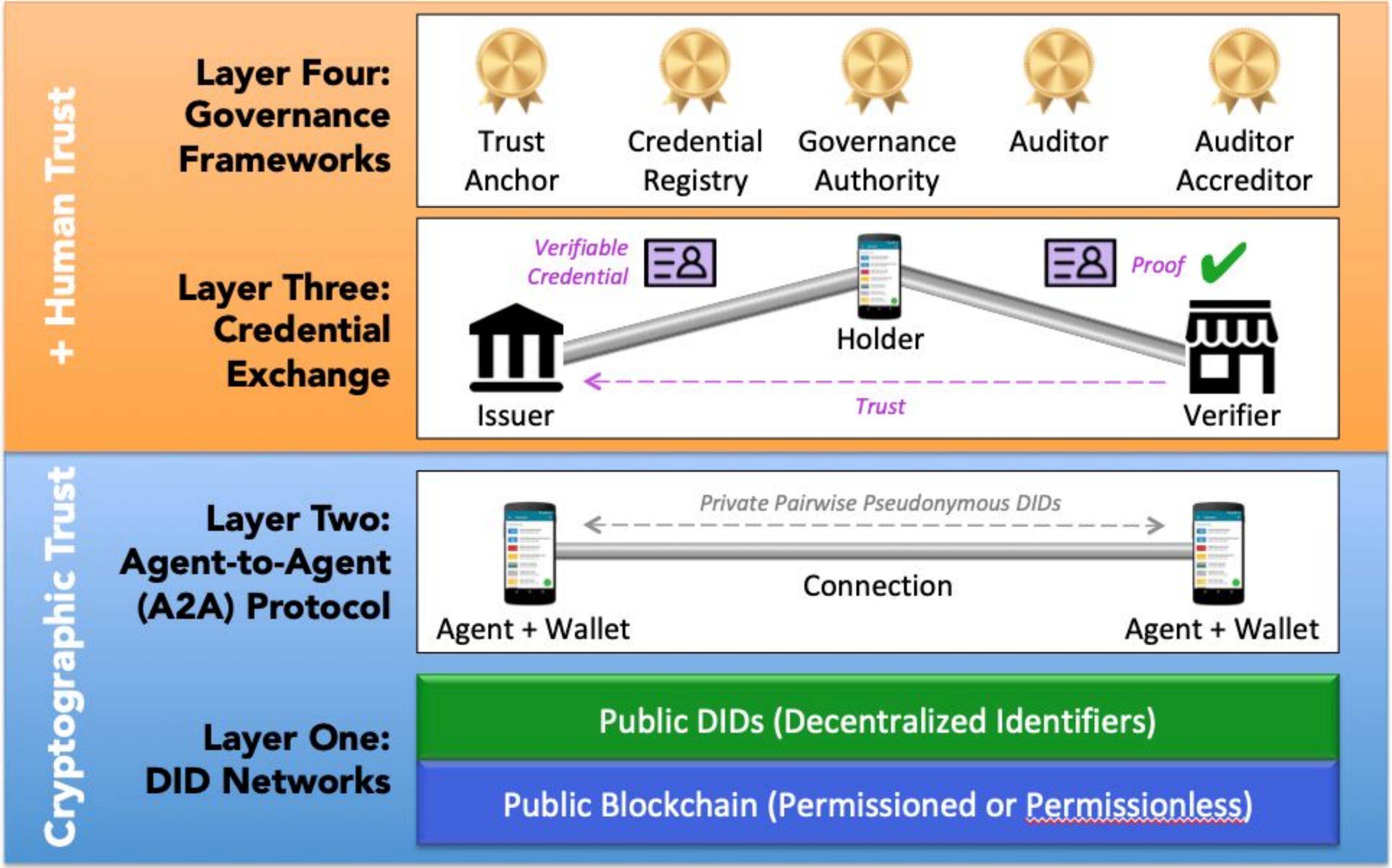
Public DIDs (Decentralized Identifiers)

Public Blockchain (Permissioned or Permissionless)

#4: Governance frameworks were NOT everywhere

The role of governance frameworks is just dawning

- Scott Perry (the only WebTrust auditor attending IIW) and I gave one session on governance frameworks
- We did it as the last session on the last day because attendees needed all the rest of the sessions to have the full context of where governance frameworks fit
- For this session we only needed one graphic: the layer diagram



+ Human Trust

Cryptographic Trust

Layer Four: Governance Frameworks

Trust Anchor

Credential Registry

Governance Authority

Auditor

Auditor Accreditor

Layer Three: Credential Exchange

Verifiable Credential

Holder

Proof ✓

Issuer

Trust

Verifier

Layer Two: Agent-to-Agent (A2A) Protocol

Private Pairwise Pseudonymous DIDs

Connection

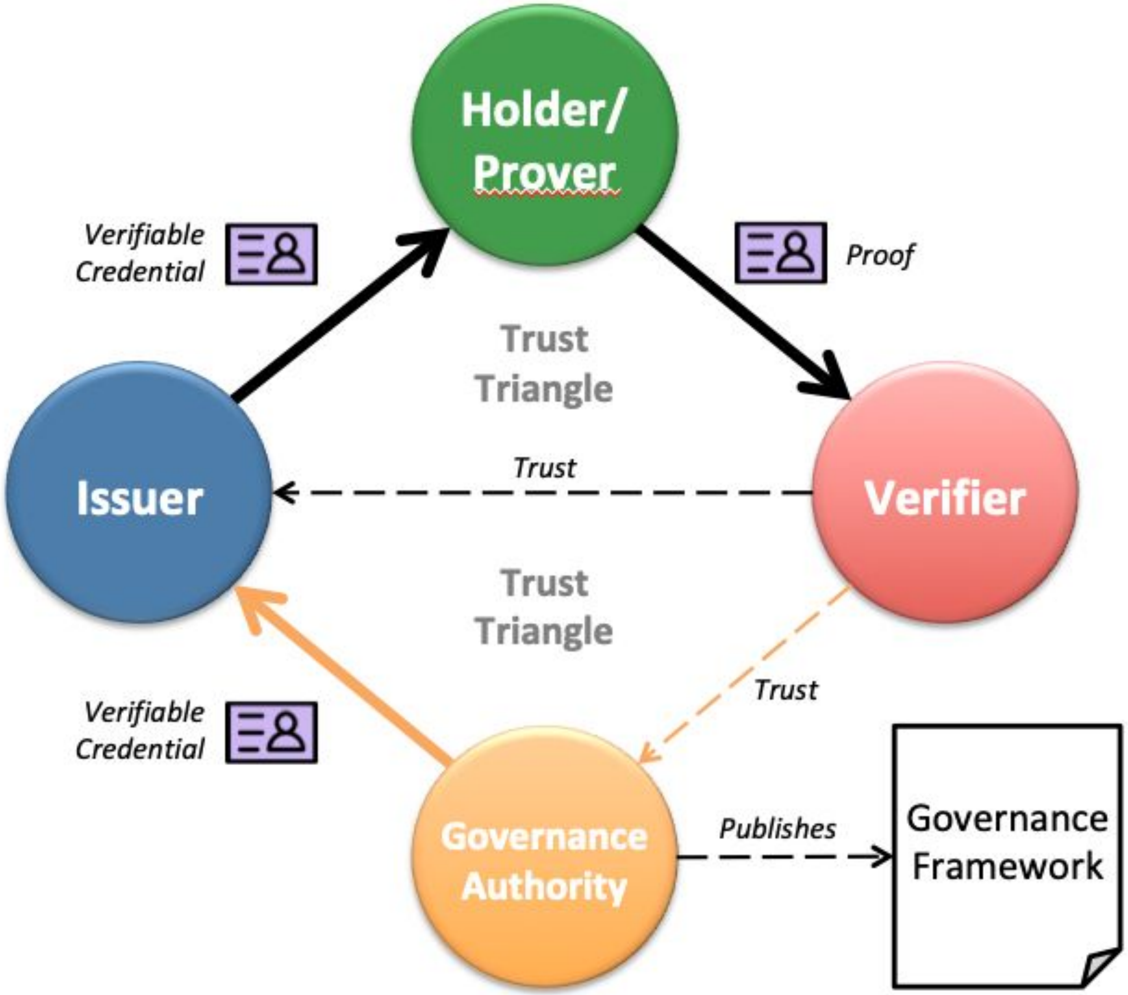
Agent + Wallet

Agent + Wallet

Layer One: DID Networks

Public DIDs (Decentralized Identifiers)

Public Blockchain (Permissioned or Permissionless)

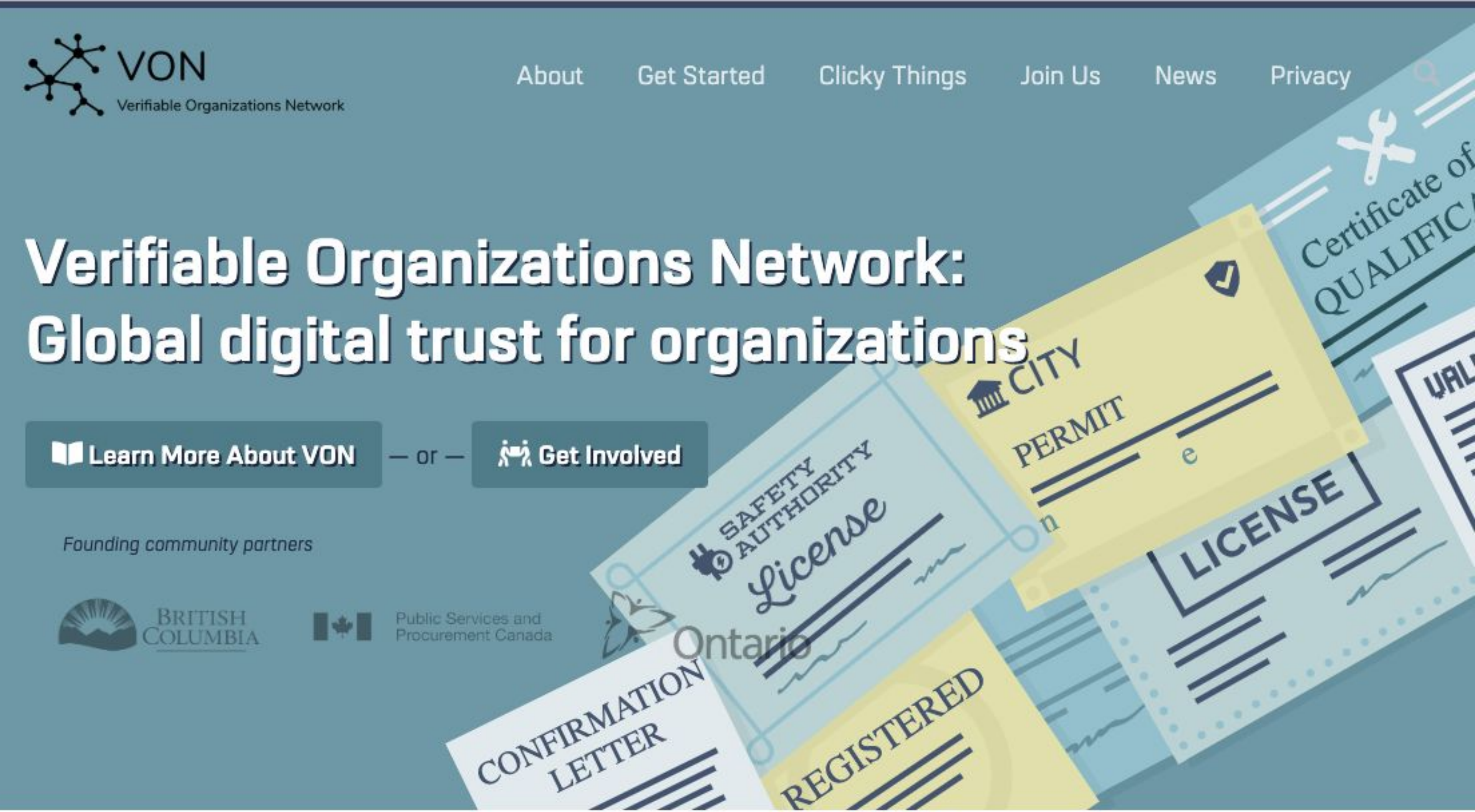

Holder/ Prover
Verifiable Credential
Proof
Trust Triangle
Issuer
Trust
Verifier
Trust Triangle
Trust
Verifiable Credential
Governance Authority
Publishes
Governance Framework

Domain-specific gov. frameworks are coming

- CULedger is working on their governance framework for the MyCUID global digital credential of credit union membership
- Truu is developing a governance framework for their medical doctor’s credentials in the UK
- DignifID is starting work on the DignifID Animal Guardianship Framework for SSI for pets

Credential registries are a major breakthrough

- Verifiable credential architecture enables a new role—a HOLDER that is not the SUBJECT of the credential
- This means any credential that has value in being searchable/discoverable/verifiable can be published to a credential registry
- The canonical example is BC Gov’s Orgbook registry for the Verified Organization Network (VON)—vonx.io



Verifiable Organizations Network: Global digital trust for organizations

This is where lawyers and regulators join the party

- Christopher Savage led a great session called “Occam’s Regulation” that explored how the SSI community could work with regulators
- The goal is “the simplest regulation that can possibly work”
- Example: accepting VCs as legally valid credentials (just like digital signature legislation)

#5: SSI and IoT is becoming a hot topic

SSI was made for people AND things (and orgs!)

- Mrinal Wadhwa of Ockam.io attended (see his great SSI Meetup webinar on DIDs and IoT)
- GS1 also had several people attending
  - GS1 is holding a panel on SSI and IoT at their annual conference in June
- Use cases for people and organizations controlling IoT devices with DIDs and VCs are exploding

#6: The Business of SSI is heating up too

After 14 years, it’s time to show us the money

- Timothy Ruff of Evernym held a session on The Business of SSI—it was very well attended
- The Sovrin Governance Framework Working Group has started a Business of SSI Task Force (http://sovrin.org)
- Read Oskar van Deventer’s blog post on the subject: https://blockchain.tno.nl/blog/self-sovereign-identity-the-good-the-bad-and-the-ugly/

Questions?

Internet Identity Workshop

Highlights of Internet Identity Workshop (IIW) #28

Drummond Reed
Chief Trust Officer Evernym
@DrummondReed

The latest and greatest developments in SSI straight from the Internet Identity Workshop (April 30-May 2, Mt. View, CA)

SIMEETUP SSIMeetup.org
Self-Sovereign Identity