Distributed Ledger Technology (aka Blockchain) Evolution or Revolution

ICANN Technical Experts Group

Internet Society Blockchain Special Interest Group

Wed 1st November 2017

ICANN 60, Abu Dhabi, UAE

pindar.wong@gmail.com

Special Thanks To…

1) ICANN Board and Staff for Arranging this Opportunity
2) ISOC BSIG EC Member Michael Palage - His Thought Leadership
   - https://www.isoc-bsig.org/
3) DID Drummond Reed (Evernym) and Manu Sporny (Digital Bazaar)

ISOC BSIG at #ICANN60

3 Points of Engagement

1) BTC: Blockchain Naming Systems Impact on ICANN: Horizon Opportunities and Risks (Friday 27th Oct)
2) EIT: Blockchain Naming Systems and Decentralized Identifiers (DiDs) (Tuesday 31st Nov)
3) TEG: (Today 1 Nov - 30 goo.gl/dFupZm)

Distributed Ledger Technology (aka Blockchain)

Evolution or Revolution - Discussion Draft

Today's Evolving Context

- Keeping it Loose in Small Pieces
  - The trouble with permissionless Innovation ;)
  - Innovating From the Edge
  - Bitcoin Bad Boy Tech
  - Understanding
    - Change in Assumptions
    - Change in Market Structure
    - *Rate of Innovation and Adaptation*

List of Initial Examples

1. Ethereum Name Service https://ens.domains/
2. BNS 1 : Blockchain Name System (Blockstack)
   a. https://blockstack.org/whitepaper.pdf
3. BNS 2: BLEIF Name Service
   a. Belt and Road Blockchain Consortium (Halal Blockchain)
4. Decentralized Identifiers (DIDs)
   a. https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/topics-and-advance-readings/did-primer.md

Change in Assumptions -> Change in Market Structure

Pre-Internet: Telephone Era

Distance = Cost

Post-Internet

Distance != Cost

Pre-ICANN

Governance = Bilateral Treaties

Post-ICANN

Global Governance = Multi-stakeholder

Pre-Bitcoin

Time = Money

Post-Bitcoin

Time != Money

Data = Money

Pre-Blockchain

Centralized = Secure

Post-Blockchain

Centralized != Secure

Decentralized = Secure

Education, Experimentation and Engagement

Ethereum:

Ethereum Improvement Proposals (EIPs)

DevCon3 (Today - Nov 4, Mexico)

https://ethereumfoundation.org/devcon3/

Bitcoin:

Bitcoin Improvement Proposal (BIPs)

Dev++ @ Scaling Bitcoin

(Tomorrow - Nov 2 - 5, Stanford University)

Modeled off apricot.net

Decentralized IDs - Verifiable Claims

Rebooting The Web of Trust

Primer
https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/topics-and-advance-readings/did-primer.md

Credentials Community Group

https://www.w3.org/community/credentials/

Blockstack

White Paper

https://blockstack.org/whitepaper.pdf

Blockchain governance models

Access \ Validation	Permissionless	Permissioned
Public	Bitcoin, Ethereum, IOTA	Sovrin, IPDB
Private	Hyperledger Sawtooth* * in permissionless mode	Hyperledger (Fabric, Sawtooth, Iroha), R3 Corda, CU Ledger

1) ENS - Ethereum Name System

May 2017 - 8 Week Period

- 180,822 Registrations - 8 weeks
- US50 million raised equiv.
- Equivalent to Total DNS Equiv. Market circa 1997 (pre-ICANN)
- https://medium.com/the-ethereum-name-service/a-beginners-guide-to-buying-an-ens-domain-3ccac2bdc770
- Covered by Leonard Tan (Ethereum Foundation)

2) Decentralized Identifiers (DIDs)

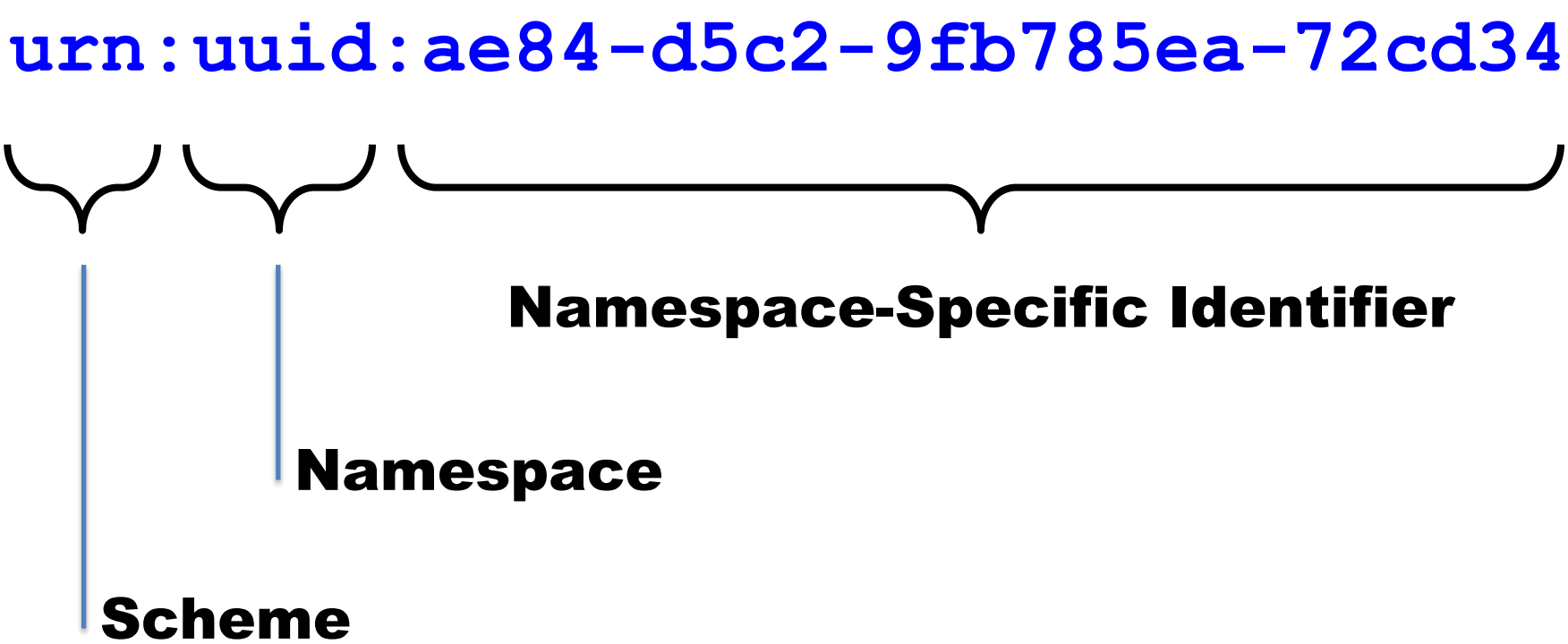
Self-sovereign identity is…

Lifetime portable digital identity for any person, organization, or thing that does not depend on any centralized authority and can never be taken away

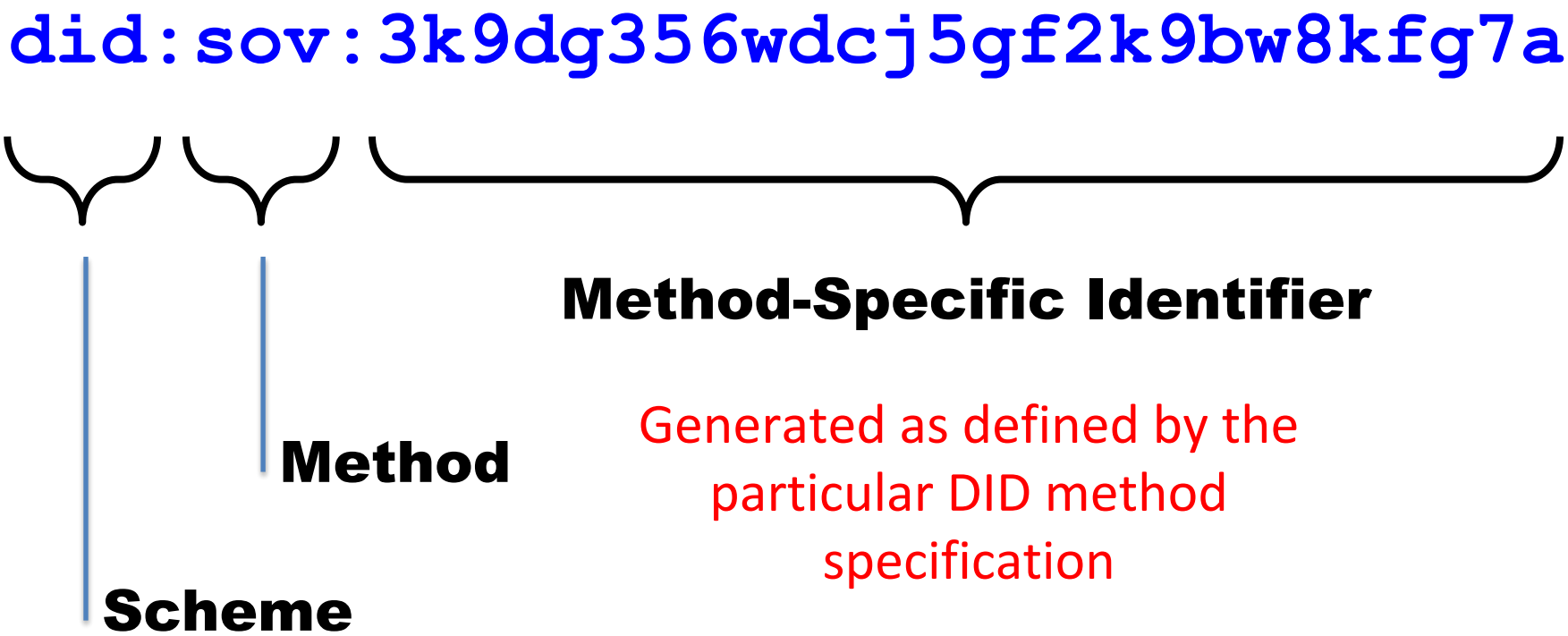
This is only possible with…

Decentralized Identifiers (DIDs):
a new type of globally resolvable, cryptographically-verifiable identifier registered directly on a distributed ledger

URN Syntax (RFC 8141)



DID Syntax



Generated as defined by the particular DID method specification

Initial DID Method Specs: did:doa Prefix?

Method	DID prefix
Sovrin	did:sov:
Bitcoin Reference	did:btcr:
Ethereum uPort	did:uport:
Veres One	did:v1:
IPFS	did:ipid:
IPDB	did:ipdb:
Blockstack	did:bstk:

DID Method References

Primer (Start Here)

- https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/topics-and-advance-readings/did-primer.md

Fluid (Examples)

- https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/topics-and-advance-readings/did-primer.md
- A discussion of the BTCR (Bitcoin Reference) DID method
- A paper about DIDS on Bigchain DB.
- The Veres One DID method spec

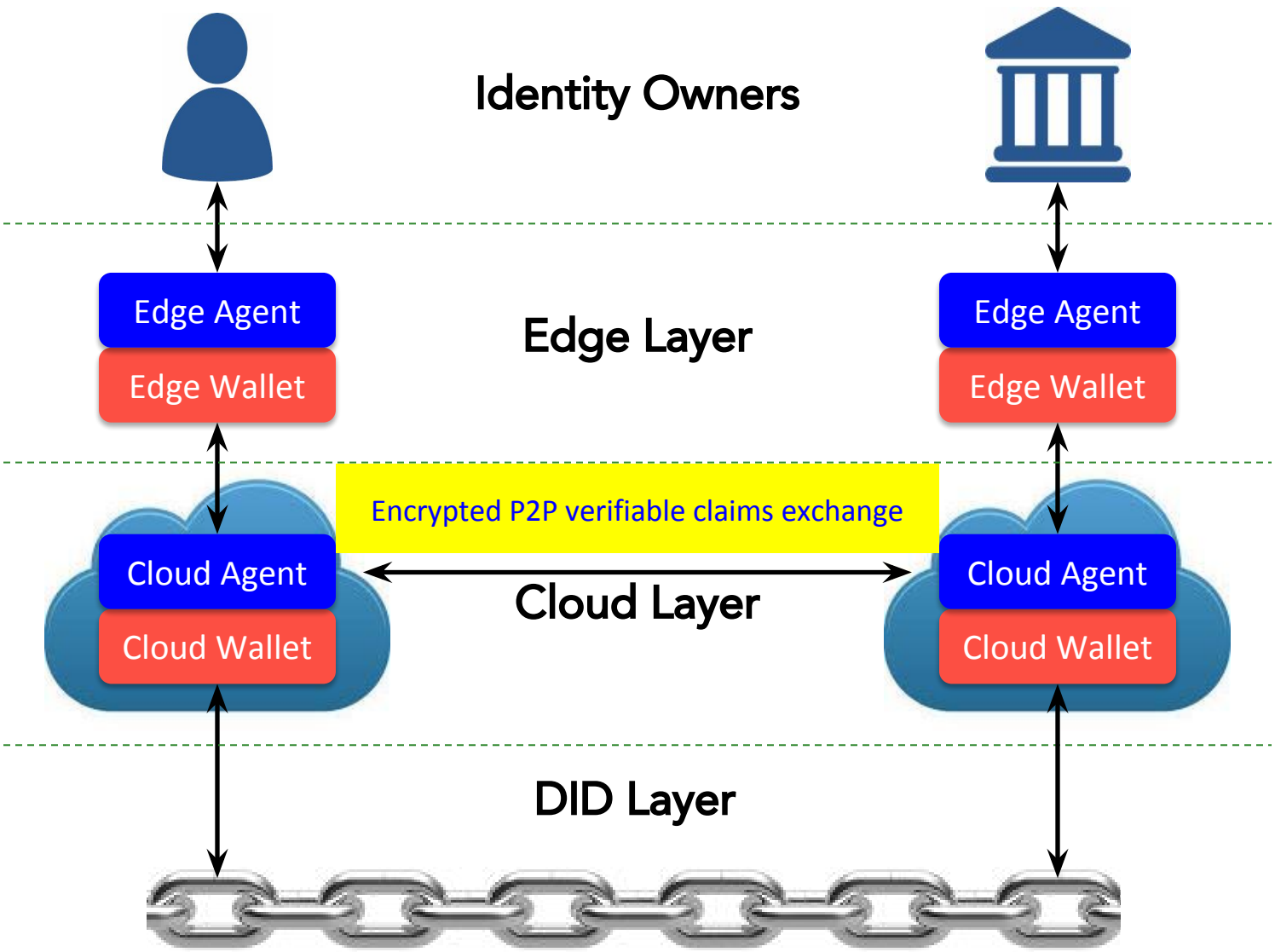
{ “Key”: “Value” }

DID	DID Document
Decentralized Identifier	JSON-LD document describing the entity identified by the DID

The 6 standard elements of a DID doc

1. **DID** (for self-description)
2. **Set of public keys** (for verification)
3. **Set of service endpoints** (for interaction)
4. **Created timestamp** (for audit history)
5. **Updated timestamp** (for audit history)
6. **Signature** (for integrity)

The decentralized identity "stack"

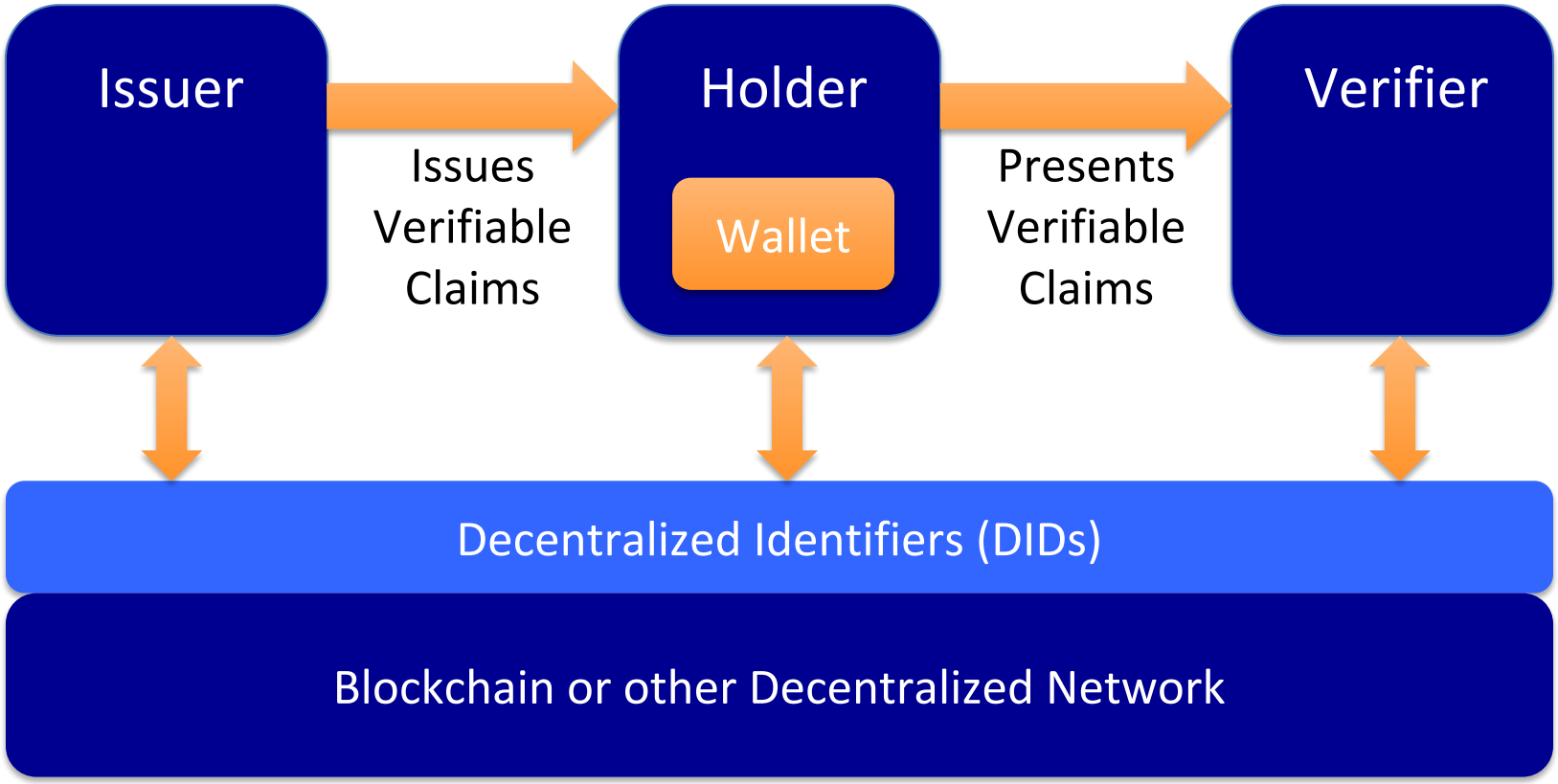


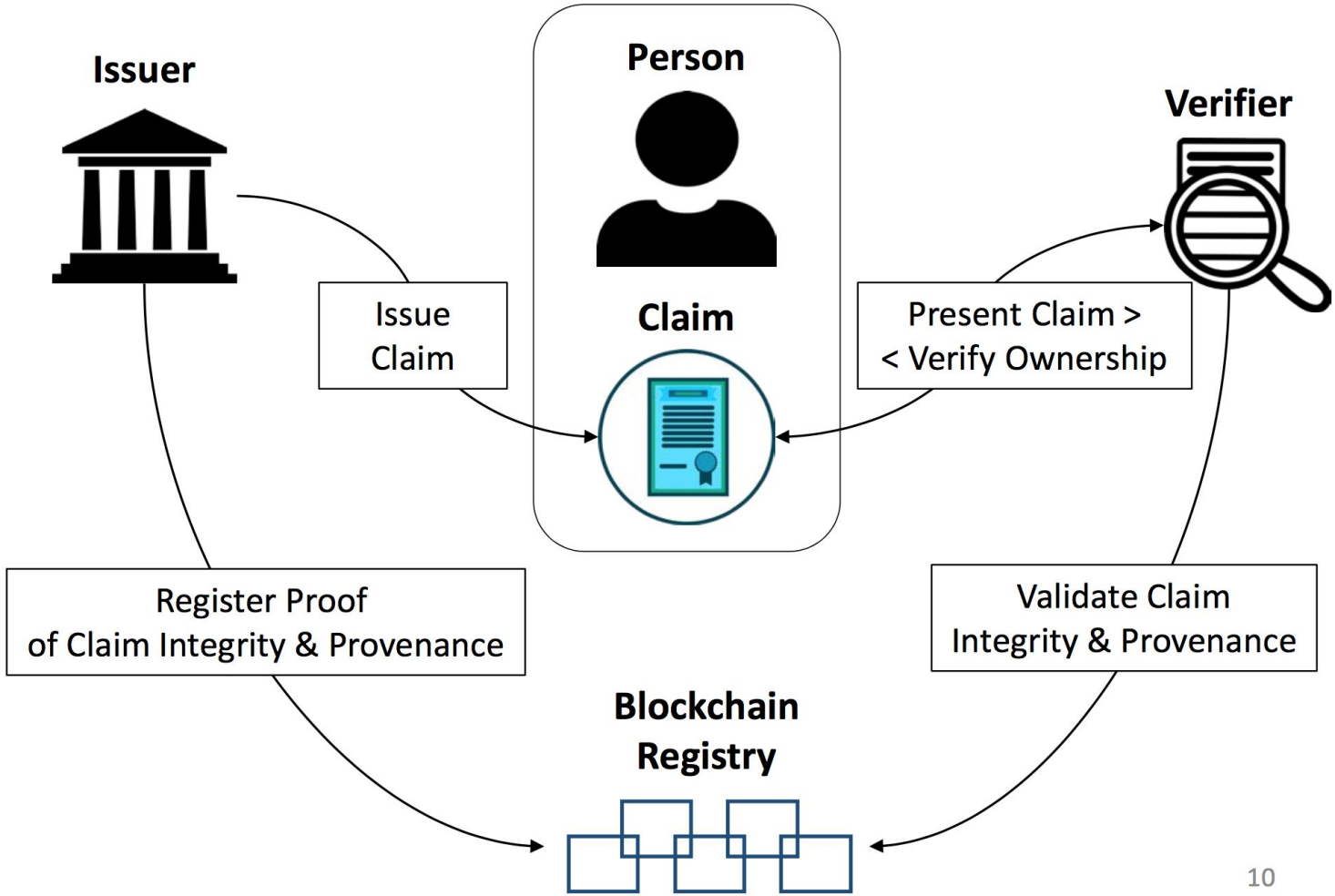
Verifiable claims are…

The new format for interoper-able digital credentials being defined by the W3C Verifiable Claims Working Group

Note: ICANN Technical Liaison Group

W3C Verifiable Claims Ecosystem





10

Homeland Security
Science and Technology

Other Links

- W3C Verifiable Claims Working Group
  - https://www.w3.org/2017/vc/charter.html
- Sovrin White Papers
  - https://sovrin.org/library/
- Sovrin Trust Framework
  - https://sovrin.org/trust-framework/

3) Blockstack
(Blockchain Naming System)

https://blockstack.com/

1. 75,152 Domains Registered (today)
2. Blockstack Technical White Paper
    a. https://blockstack.org/whitepaper.pdf

4) Belt and Road Blockchain Consortium Legal Entity Identifier Foundation Naming System (BNS)

https://docs.google.com/presentation/d/17FLjdWlWPWOiODP4yv36w_3EY9hv7Kamm2rEVuFIL0g/edit?usp=sharing