ICANN Emerging Identifiers Technology: Blockchain Naming Systems and Decentralized Identifiers (DIDs),

Internet Society Blockchain Special Interest Group
Tuesday 31st October 2017
ICANN 60, Abu Dhabi, UAE
pindar.wong@gmail.com
http://tinyurl.com/icann60eit

Special Thanks To…

1) To ICANN Board and Staff for Arranging this Opportunity (1 of 3)

   1) Friday October 27th 15.30pm-4.00pm GST: Blockchain Naming Systems Impact on ICANN

   2) Tue, 31 October, 10:30am - 12pm GST: EMERGING IDENTIFIERS TECHNOLOGY

   3) Wed, 1 November, 5 – 6:30pm GST: JOINT MEETING: BOARD AND TEG (Technical Expert Group)

2) ISOC BSIG EC Member Michael Palage
   - ‘**ICANN & Distributed Ledger Technology (aka Blockchain): Evolution or Revolution?**

3) Drummond Reed (Evernym) and Manu Sporny (Digital Bazaar)

   Slides, Links and Method Examples (fluid)

   NOTE: DID Related Slides and DID Method References (work in progress)

BLEIF (Belt and Road Blockchain Legal Entity Identitier Foundation)

Naming System (BNS) - Sept 12th@Hong Kong Cyberport

Name -> Public Key Mapping

*Chain Peg (which blockchain)
*Chain Mark (c.f. Trademark)

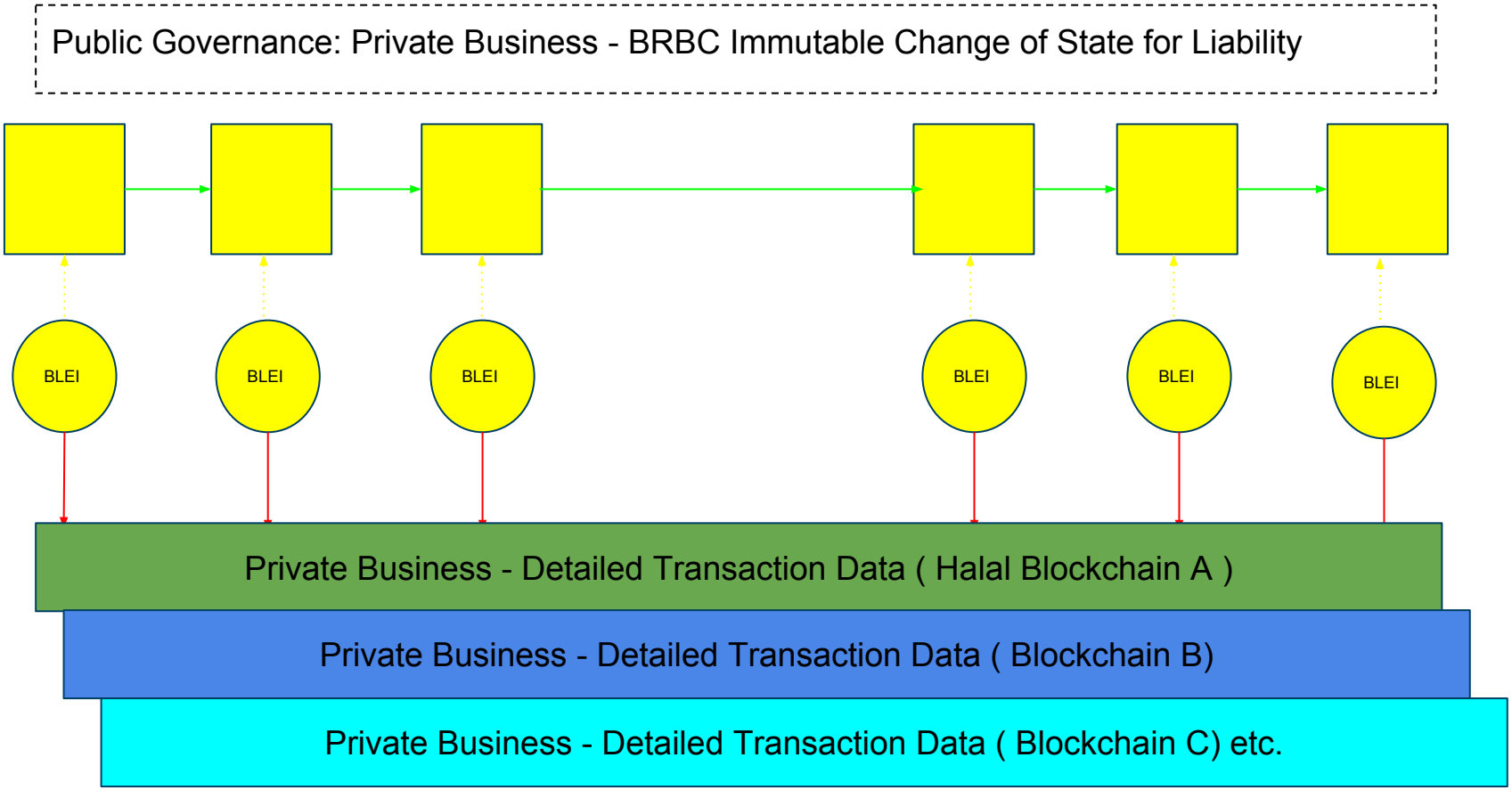
DID Dispute Resolution

Other Foundations:

http://identity.foundation/
https://sovrin.org/

?

Cross-Border Trade Finance and Facilitation Identifiers along the Belt and Road

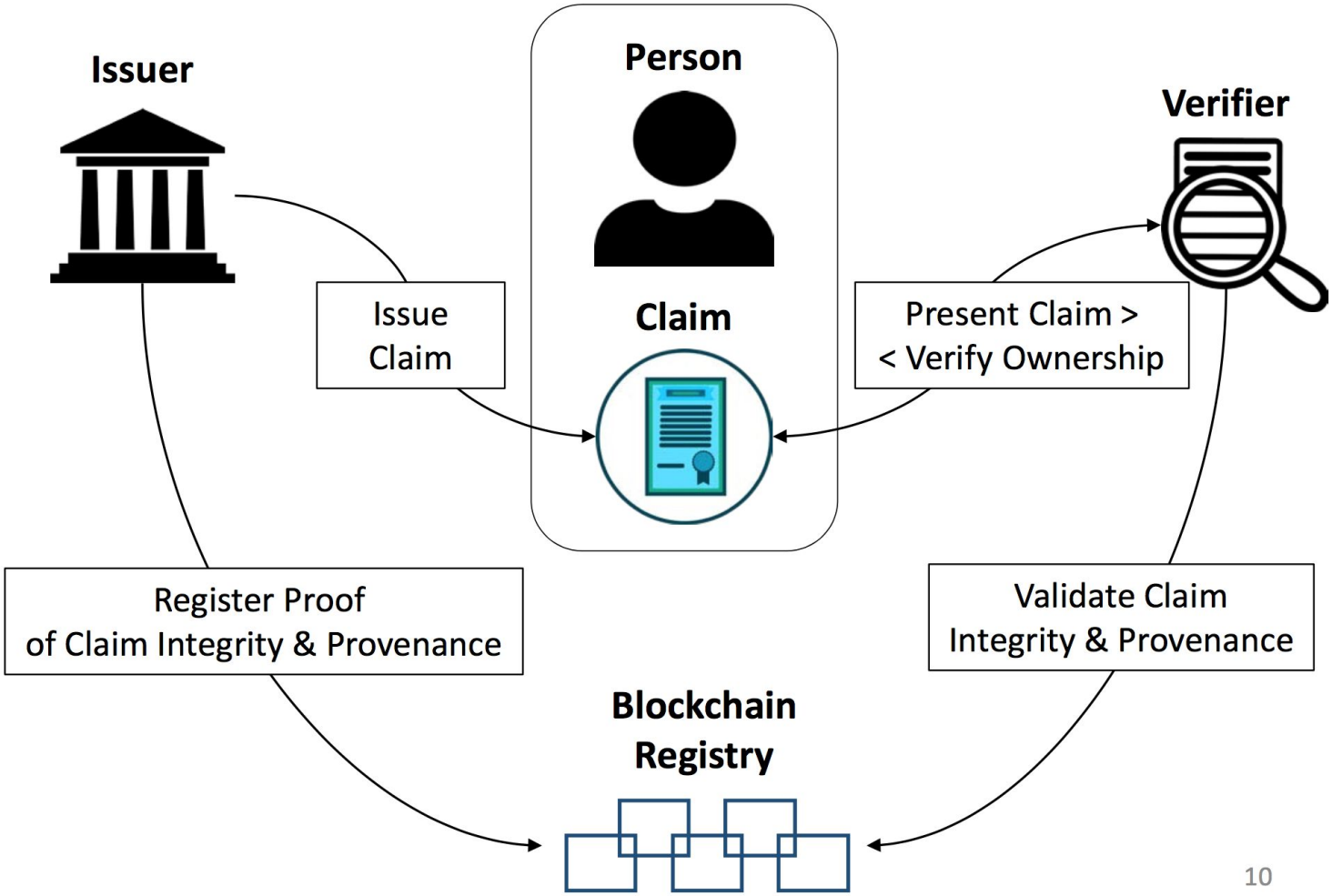


DID Example

`did:example:1234-abcd-56789`

vs.

`https://example.com/people/jdoe`



Homeland Security
Science and Technology

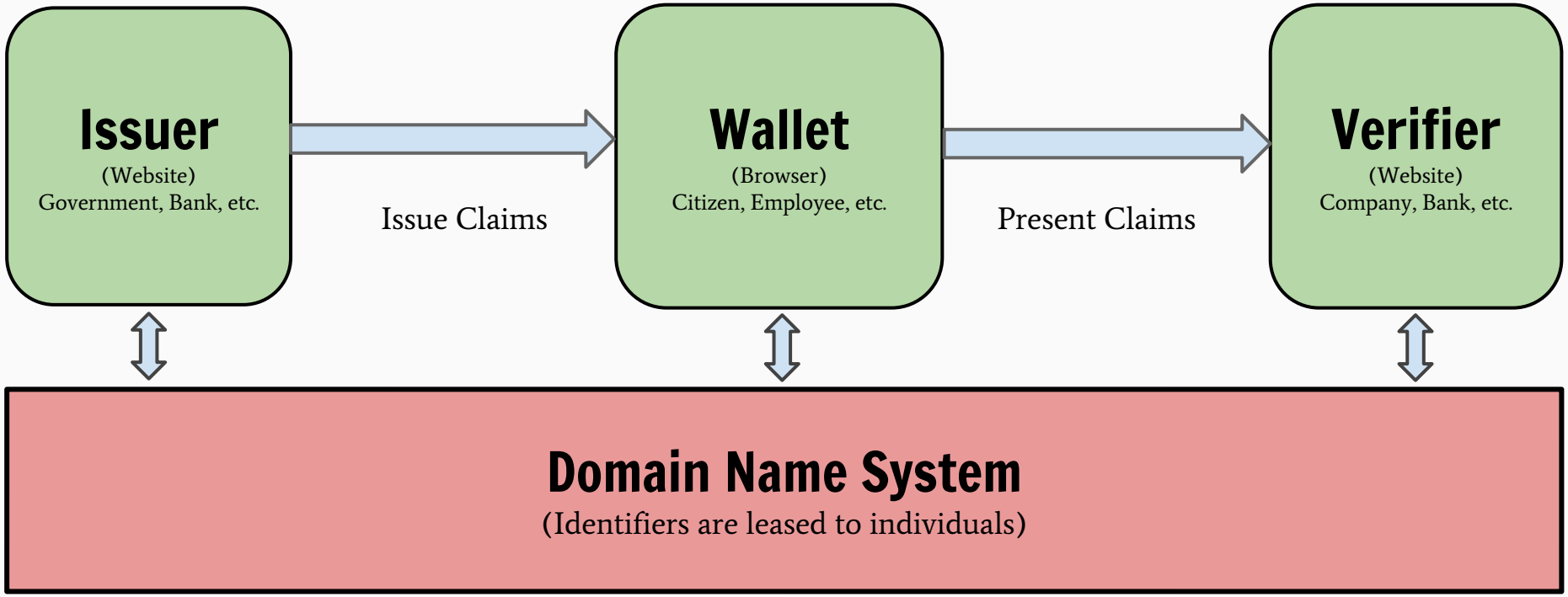
Decentralized Identifiers (DIDs):

a new type of globally resolvable, cryptographically-verifiable identifier registered directly on a blockchain / distributed ledger

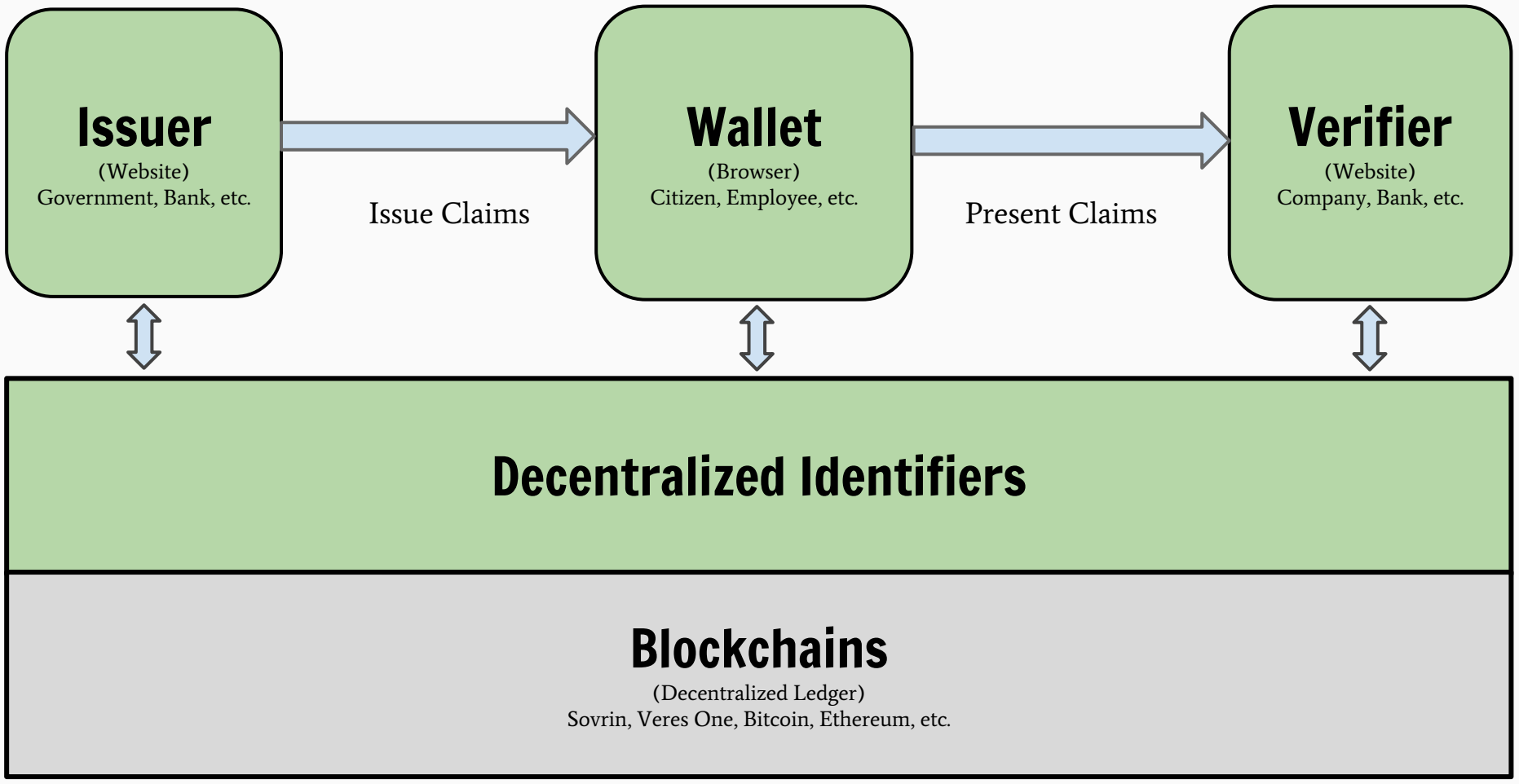
Self-sovereign identity is…

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

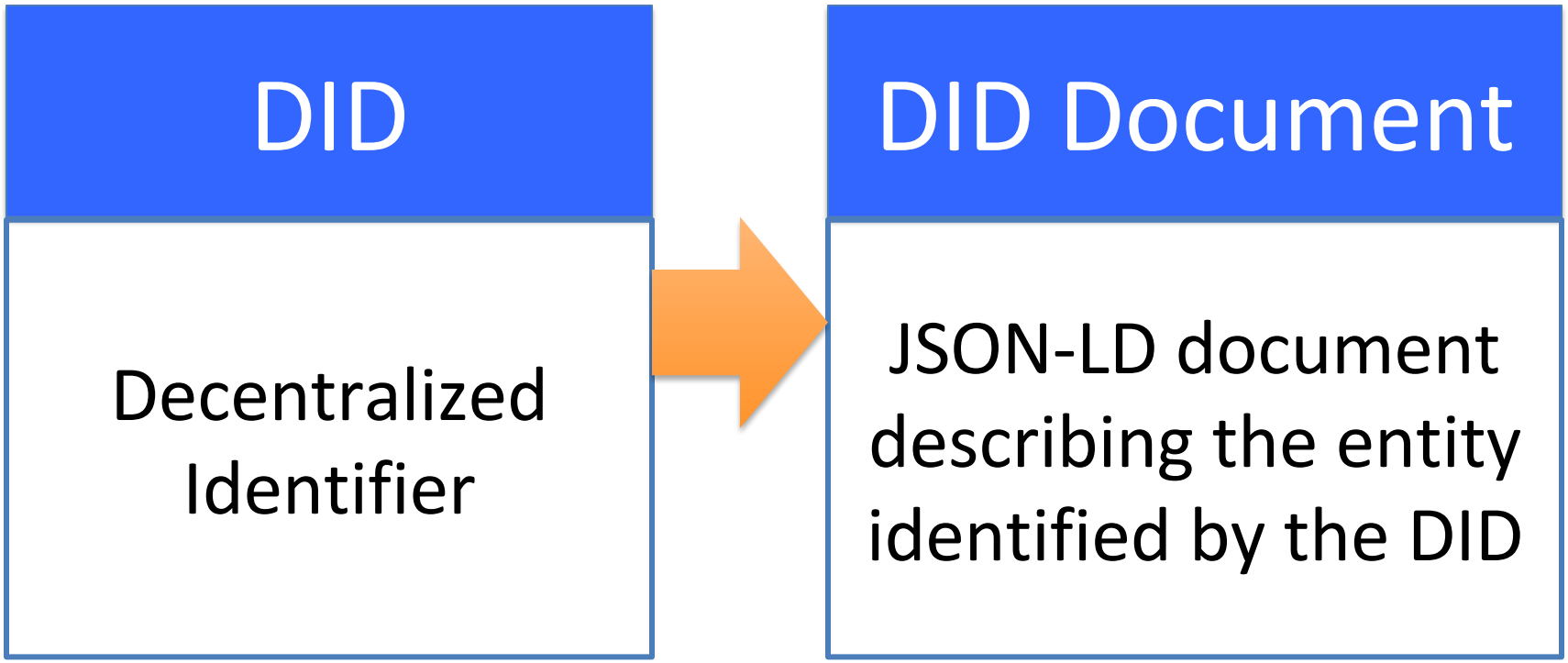
Web Identifiers



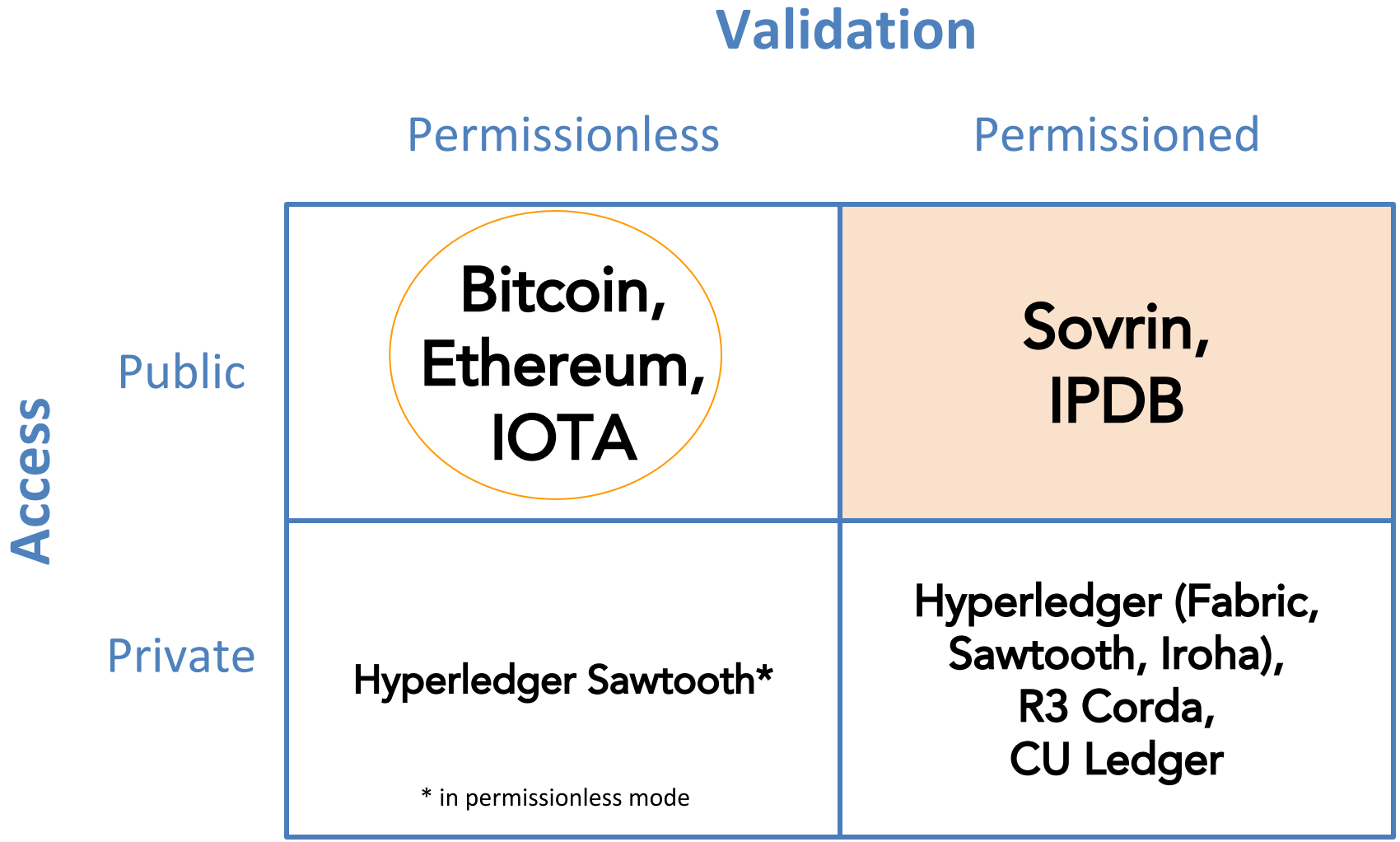
Decentralized Identifiers



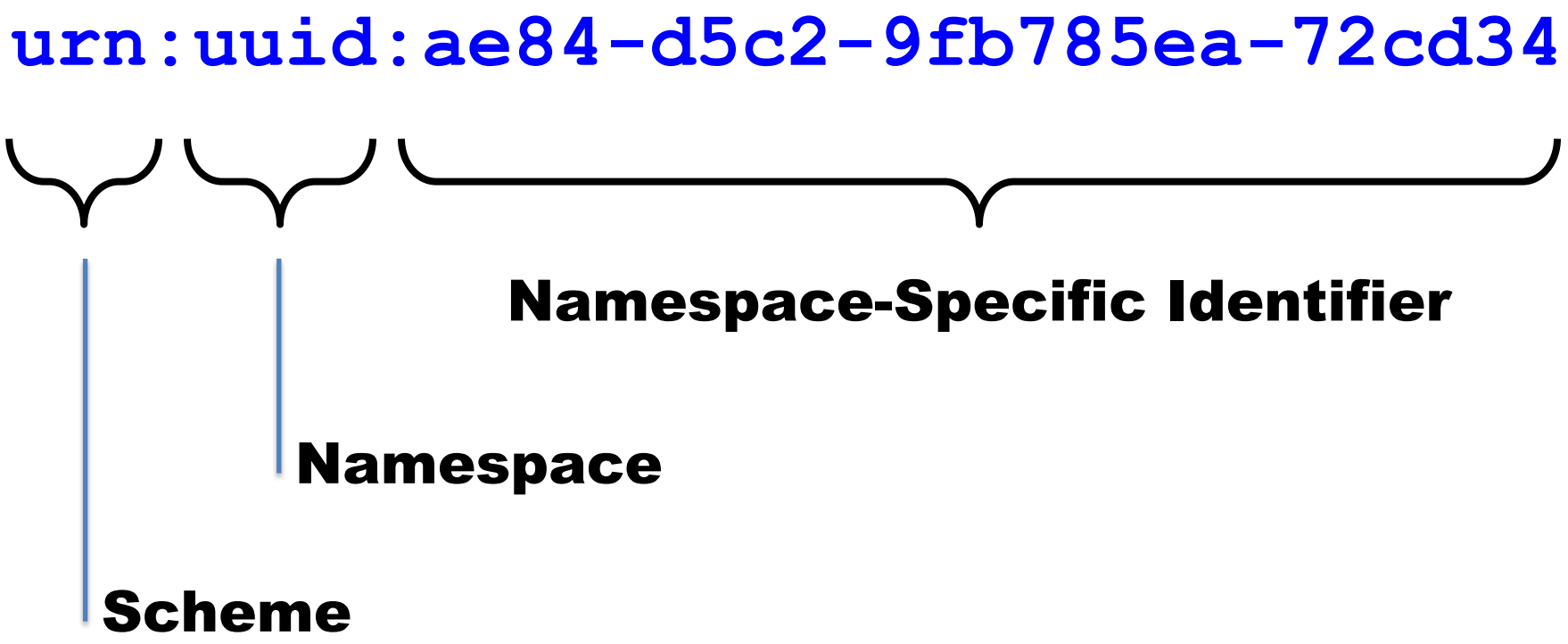
{ “Key”: “Value” }


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

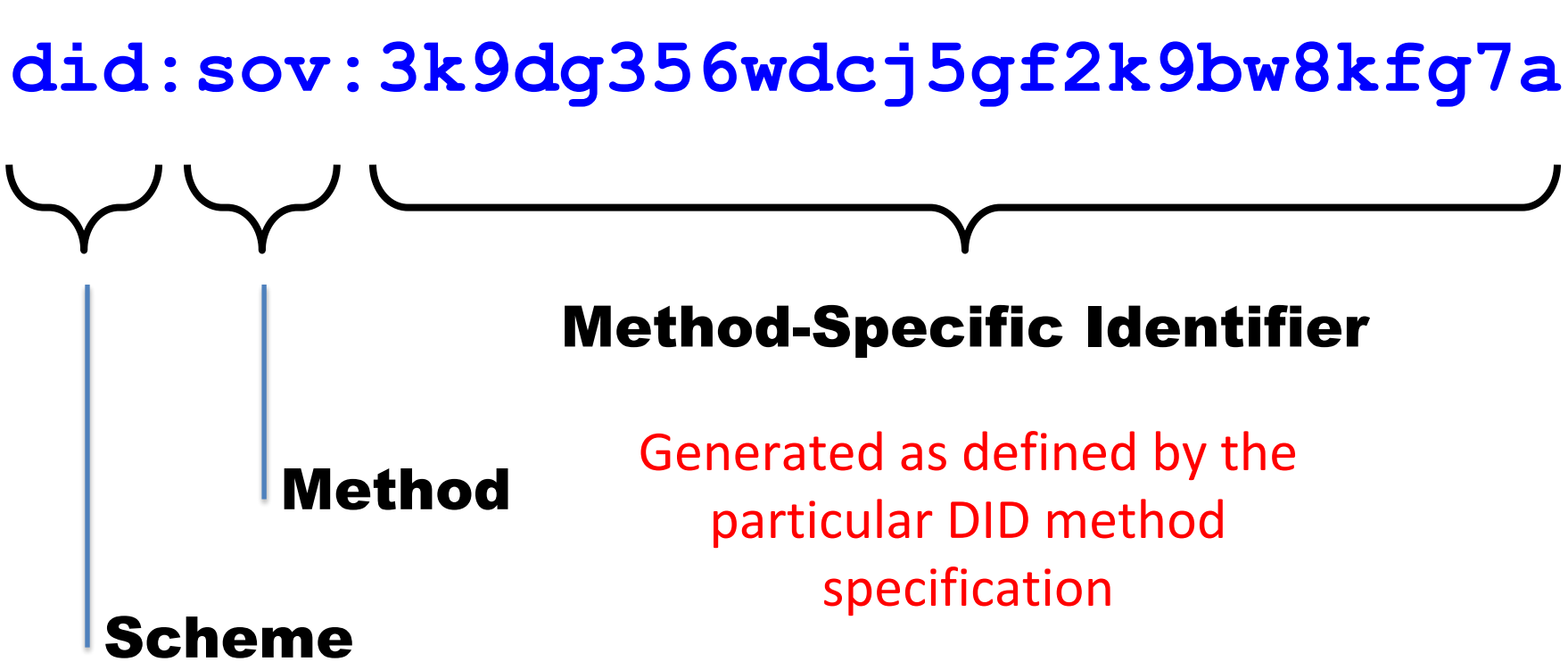
Blockchain governance models



URN Syntax (RFC 8141)



DID Syntax


did:sov:3k9dg356wdcj5gf2k9bw8kfg7a
Method-Specific Identifier
Method
Scheme
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

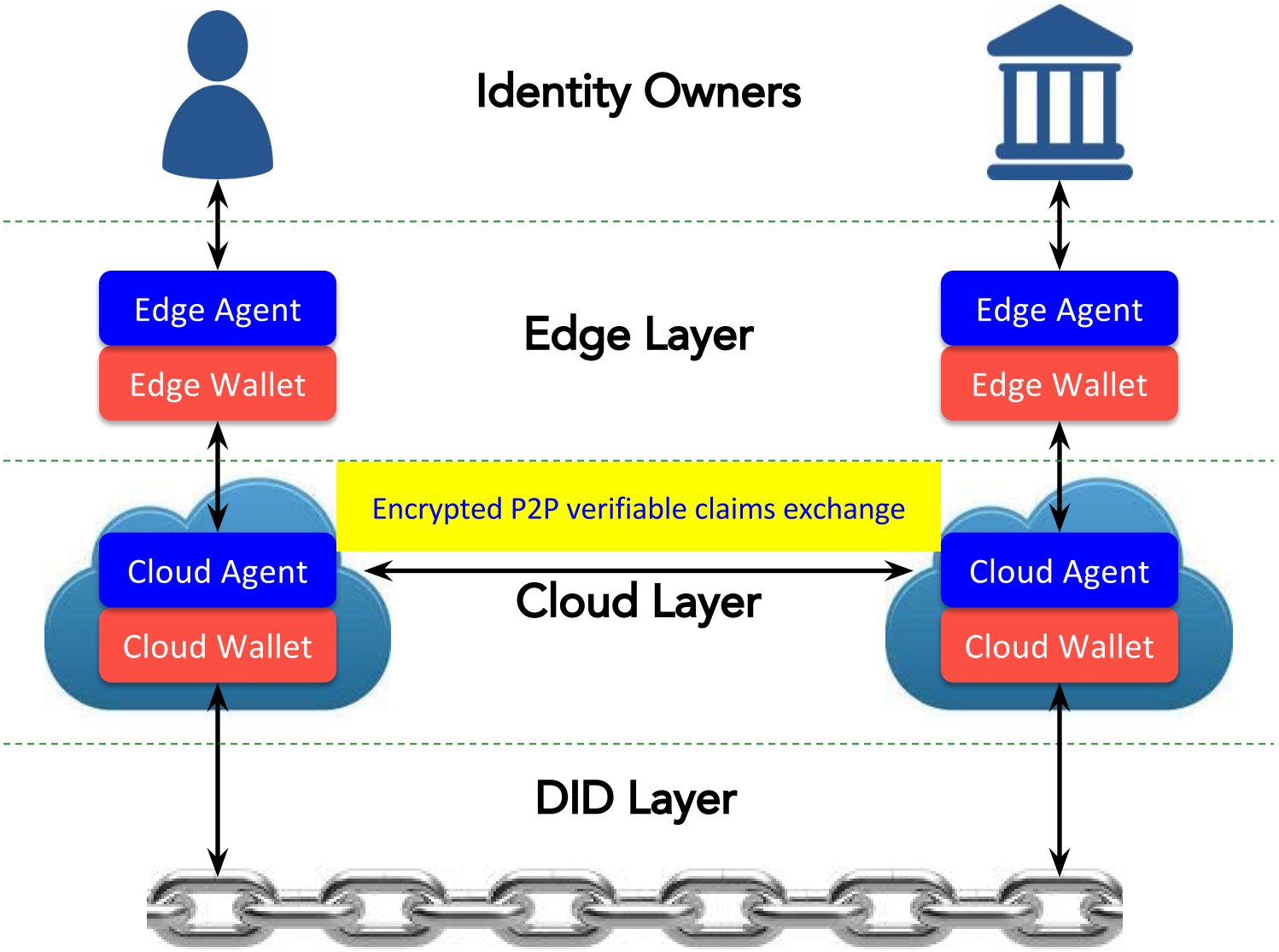
Fluid (Examples)

- 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

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"



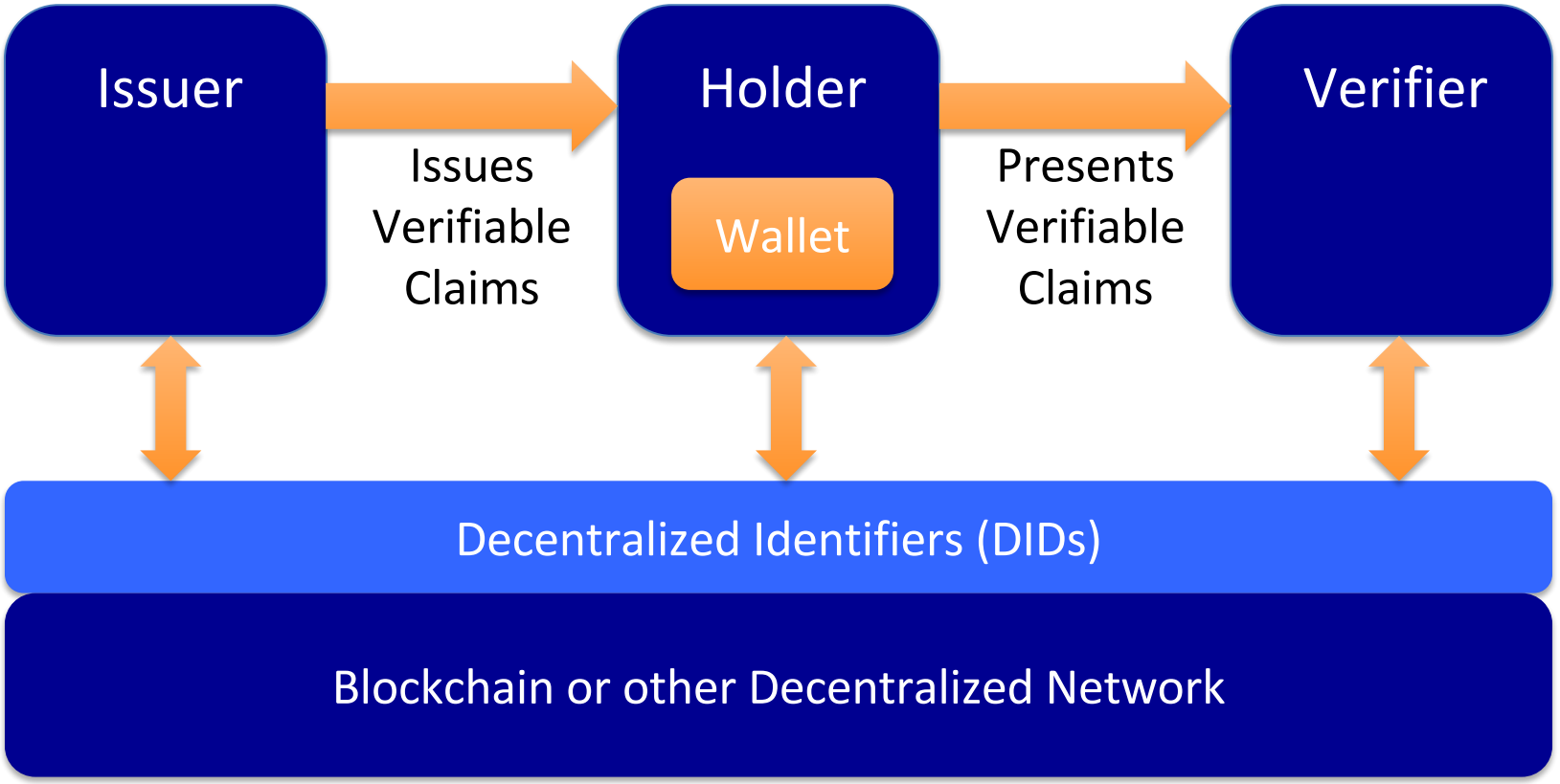
Verifiable claims are…

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

Note: ICANN Technical Liaison Group

W3C TPAC Nov 6-10, USA

W3C Verifiable Claims Ecosystem



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/