DID & VC Architecture Roadmap 2018+

Christopher Allen
Principal Architect & Founder — Blockchain Commons
W3C Credentials CG Chair

Current Efforts at W3C

- Verifiable Claims WG, Verifiable Credentials
  - Anyone can verifiably say anything about anyone.
  - Identity emerges from evaluating multiple sources of information, across multiple interactions
- Decentralized Identifiers (DIDs), draft WG
  - Anyone can publicly manage provable identifiers without administrative interference
  - Move beyond centrally administered IDs
  - Provide for a plurality of authorities

Decentralized Identity Stack

- DIDs – Root Identifiers
  - DID Universal Resolvers — support interoperability between multiple DID methods.
  - DID Methods – Specific approaches using different blockchains
  - DID Documents – Proof of Control & Service References

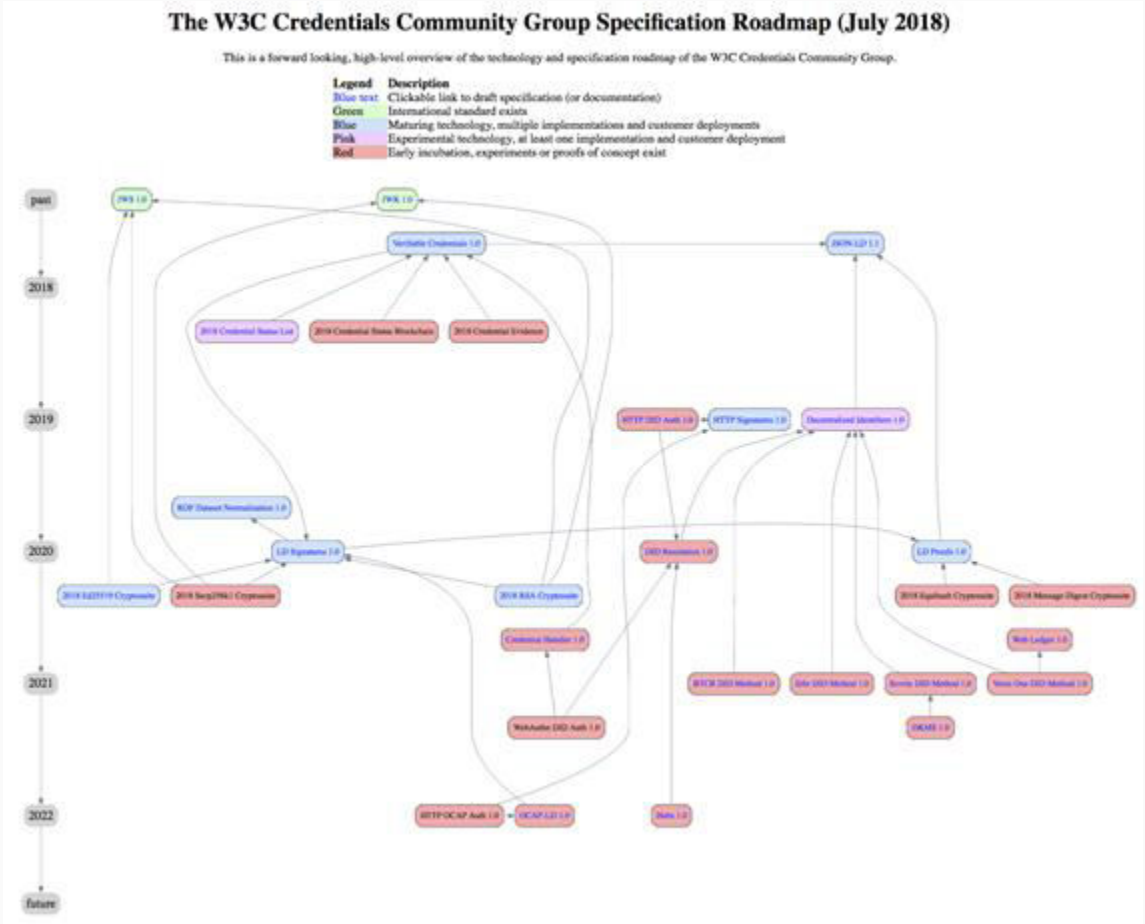
+

Decentralized Identity Stack

- DIDs – Root Identifiers …
- Raw Data – Observed facts & transactions
- Verifiable Credentials – Assertions by knowable authorities
- Profiles / Presentations / Persona – Representations of individuals
- Consent – Records of authorization
- Reasoning – Interpretation & Analysis
- Evaluation – Risk Analysis & Reputation
- Understanding – Internal knowledge representation
- Services – Interactions of value

Potential Technologies for Future Work

- DID-Auth (Authn/Authz)
- OCAP (Authz through Object Capabilities)
- Credential Requests & Exchange
- Data Minimization & Selective Disclosure
- Consent & Consent Receipts
- Storage (Identity Hubs) & Internal Representations
- Analytics & Algorithms for Evaluation
- Cryptographic Proofs
  - Signature, Encryption, Signcryption Suites
  - Time-stamping
  - Zero-knowledge proofs



https://w3c-ccg.github.io/roadmap/diagram.html