Understanding Decentralized Identifiers

Kim Hamilton Duffy
CTO Learning Machine
Co-chair W3C Credentials Community Group
Decentralized Identity Foundation Steering Committee
What is a Decentralized Identifier?

A new type of URL that is:

- globally unique,
- highly available,
- persistent
- cryptographically verifiable, and
- does not require a central admin

![did:btcr:txtest1:8kyt-fzzq-qqqq-ase0-d8](image)
We use DIDs in Verifiable Credentials
DID Implementations (Methods)

Examples:

```
did:v1:nym:BcNkgGmGEpCGSJSMPB4BvWvwVM6YeTR52BSWcZTbzU23
did:btcr:txtest1:8kyt-fzzq-qqqq-ase0-d8
```
DIDs Resolve to DID Documents

```
{
  "@context": "https://w3id.org/veres-one/v1",
  "id": "did:vm:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
  "authentication": [{
    "type": "Ed25519SignatureAuthentication2018",
    "publicKey": [{
      "id": "did:vm:vm:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD#authn-key-1",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:vm:vm:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
      "publicKeyBase58": "DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD"
    }]
  },
  "service": [{
    "type": "ExampleMessagingService2018",
    "serviceEndpoint": "https://example.com/services/messages"
  }],
  ... more DID-specific information here ...
}
```

1. Authentication Mechanisms
2. Public Key Material
3. Service Discovery
DID RESOLUTION

DID: did:btcr:xkyt-fzgq-qq87-xnhn

Universal Resolver

DID Document

DID Method Spec

IPFS
1. DID (for self-description)
2. Public keys (for verification)
3. Auth methods (for authentication)
4. Service endpoints (for interaction)
5. Timestamp (for audit history)
6. Signature (for integrity)
Status

- Incubated at RWOT, IIW
- Currently:
  - Draft report in W3C Credentials Community Group
  - Protocols and prototypes at DIF
  - DID Method Registry
  - DID Auth, DID Resolver
- To Discuss: DID Working Group
DID & VC Architecture Roadmap 2018+

Christopher Allen
Principal Architect & Founder — Blockchain Commons
W3C Credentials CG Chair
Current W3C Standards Track Efforts

- 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 Standards 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
The W3C Credentials Community Group Specification Roadmap (July 2018)

This is a forward-looking, high-level overview of the technology and specification roadmap of the W3C Credentials Community Group.

Legend
Blue text: Clickable link to draft specification (or documentation)
Green: International standard exam
Blue: Marketing technology, multiple implementations and customer deployments
Pink: Experimental technology, at least one implementation and customer deployment
Red: Early incubation, experiments or proofs of concept exist

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