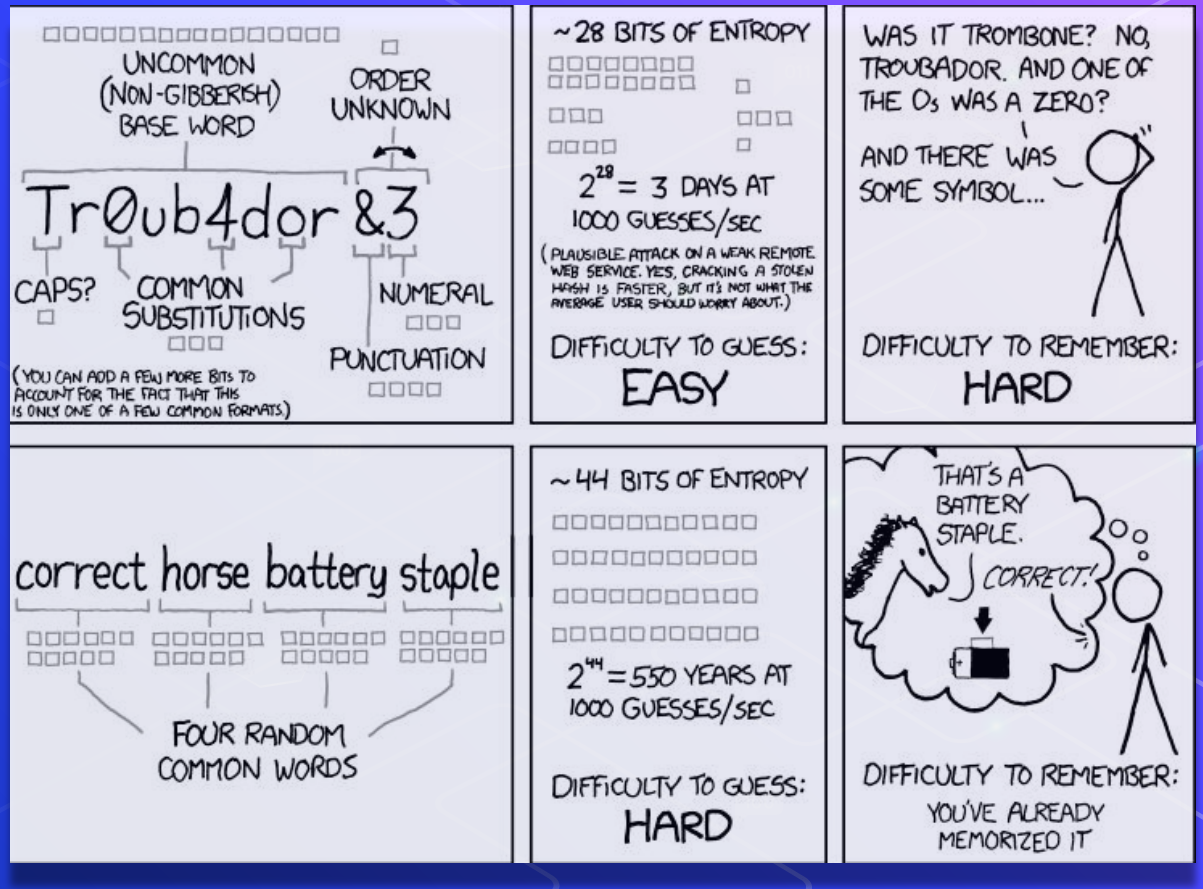
Decentralized Identifiers, Verifiable Credentials

and the next phase of decentralization

Kim Hamilton Duffy
MIT, Digital Credentials Consortium

Typical authentication systems in use today were designed for the pre-mobile-device internet.



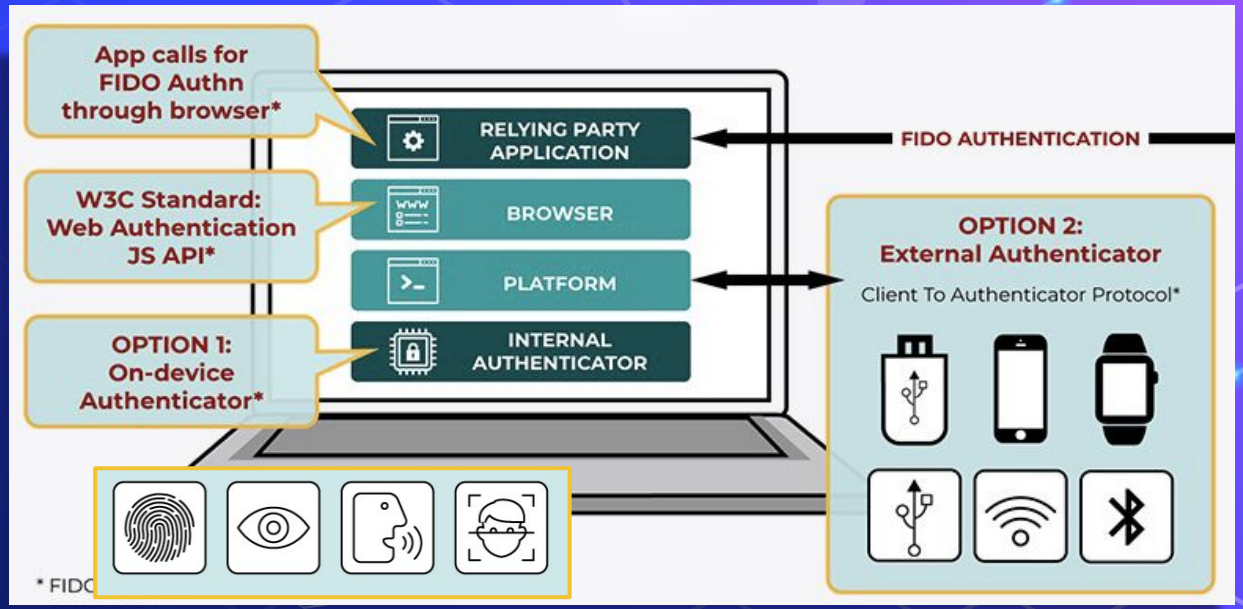
“

The DFS ecosystem requires

standardized,

interoperable,

strong



authentication technologies to reduce risk and protect assets

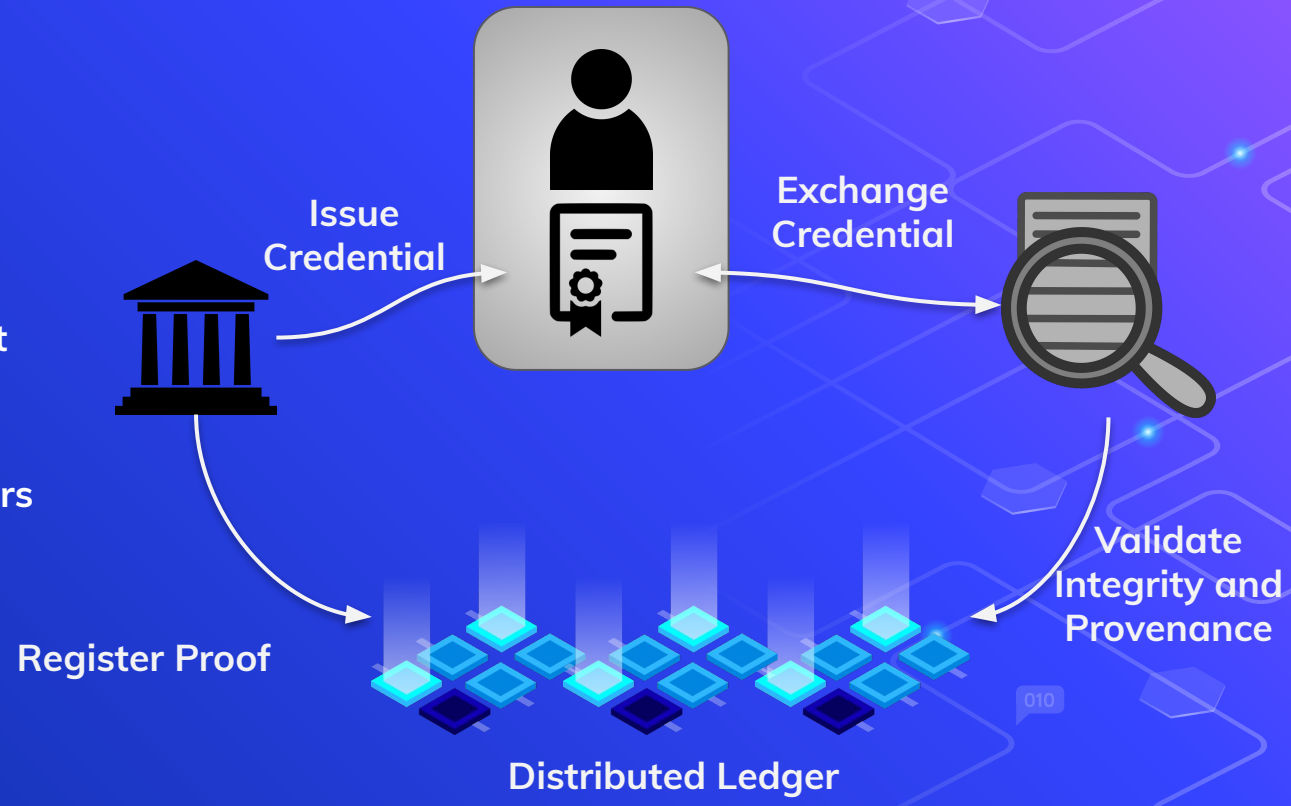
Data Centralization Risks Remain

- Centralized data stores are attractive targets
- Strong incentives for hackers
- Users have to trust data handling policies
- Steady flow of data breaches
  - Equifax: ~143 million US consumers exposed

Enabling decentralized trust

Verifiable Credential

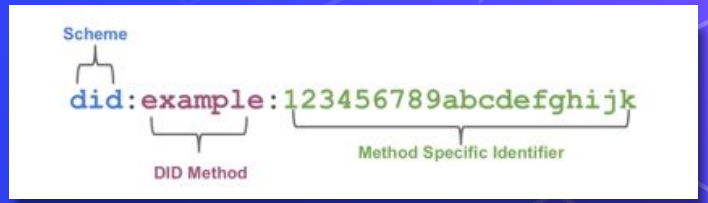
- Claims about a subject
- Metadata
- Strong verification
- Decentralized Identifiers for issuer and subject



Verifiable Credentials and DIDs

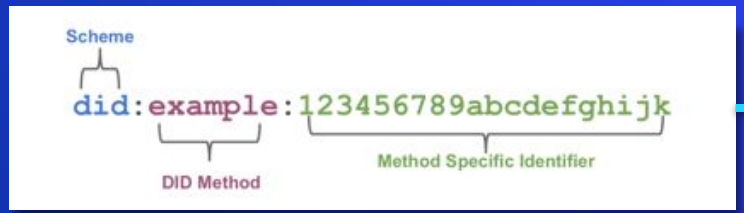
What is a Decentralized Identifier?

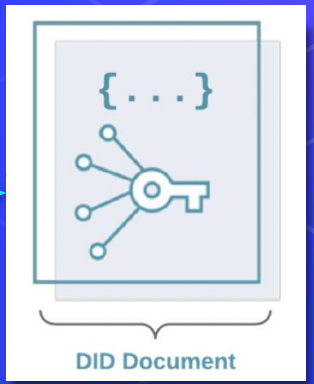
- New type of identifier for verifiable, "self-sovereign" digital identity
- Fully under the control of the DID subject, enabling independence from any specific:
  - centralized registry
  - identity provider
  - certificate authority
- URL enabling trustable interactions with DID subject



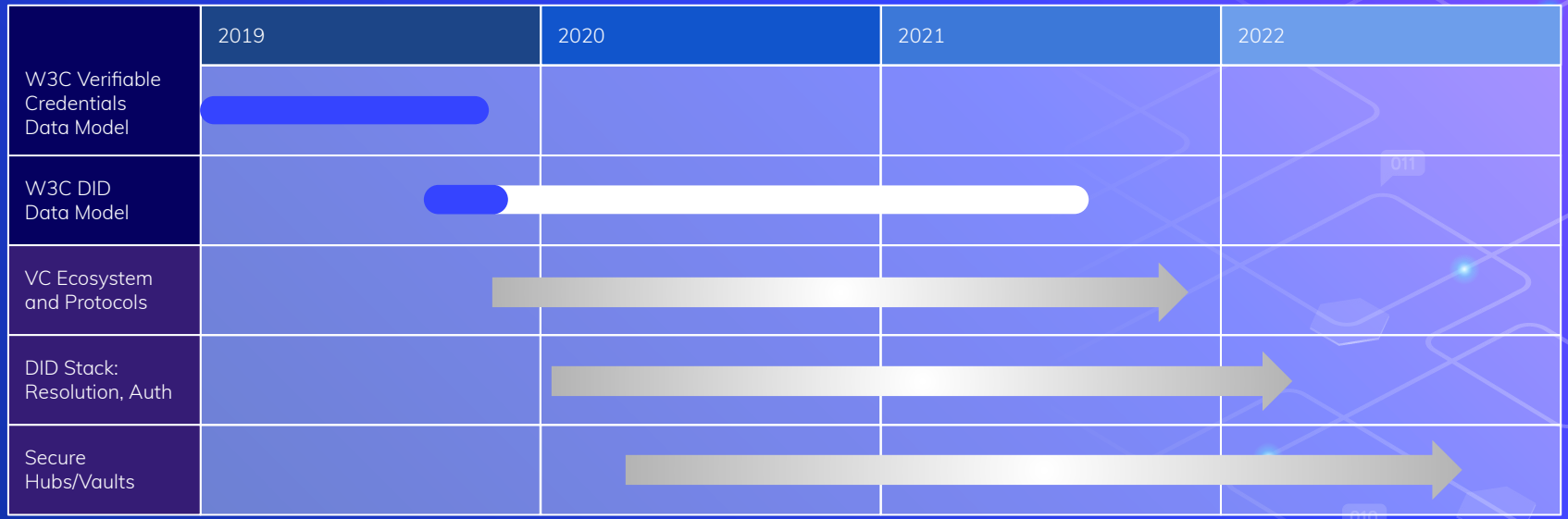
DIDs resolve to DID Documents

- DID Documents contain:
  - Verification methods
  - Service endpoints for interacting with the DID subject
- Examples:
  - Authentication
  - Requesting a digital signature on a document





Standardization Track



Pre-standards pipeline

Thanks!

Any questions?

You can find me at:

@kimdhamilton

kimhd@mit.edu

Design Credits:

- Presentation template by SlidesCarnival
- Photographs by Unsplash