Wyoming Corporate Digital Identity

Demo from the Decentralized Identity Industry

Decentralized Identity Communities: W3C, DIF, Hyperledger

Organizations: Digital Bazaar, Uport, Microsoft, IBM, Evernym, British Columbia, Rabobank, UBS, Accenture, US Homeland Security, & many, many more

Presented by:

Christopher Allen <ChristopherA@LifeWithAlacrity.com> @ChristopherA
Co-chair W3C Credentials Community Group

Christopher Allen | Executive Director | Blockchain Commons

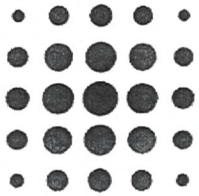
- Co-Author SSL/TLS
- Co-Inventor & Architect of Decentralized Identifiers
- Author Design Principles of Self-Sovereign Identity
- Founder #RebootingWebOfTrust
- Co-Chair W3C Credentials CG
- Former Principal Architect, Blockstream
- Former CTO Certicom
- Former CEO Consensus Development

Email: ChristopherA@LifeWithAlacrity

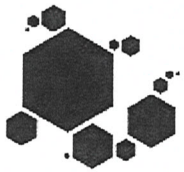
Twitter: @ChristopherA

https://www.linkedin.com/in/ChristopherA/

Standards & Developer Communities



DIF



HYPERLEDGER
INDY

Some Organizations Committed to DID/VCs

IDEO · Microsoft · Gem · BLOCKSTACK · uport · IBM · HYPERLEDGER · civic · accenture · DANUBE · NETKI · RSA · Consent · BIGCHAIN DB · IOTA · mooti · r3. · validatedID · BAYONET · EQUINIX · KYC-CHAIN · BRITISH COLUMBIA · NuID · Meta · DIID · nuggets · TRUSTED KEY · ONTology · LIK·E · VERIDIUMID · pillar · JOLOCOM · enigma · Ledger

WORLD ECONOMIC FORUM

DIF

UBS

MyData

LOCKING THE WEB OPEN
Decentralized Web Summit

Wyoming Law HB-0070-2019

"Not later than **December 31, 2021**, the secretary of state may develop and implement an industry leading filing system through which all required filings, as defined in paragraph (c)(iii) of this section, may be submitted. The secretary of state **shall endeavor to use blockchain technology** and include an application programming interface as components of the filing system, as well as robust security measures and other components determined by the secretary of state to be best practices or which are likely to increase the effective and efficient administration of the laws of this state."

Wyoming Law HB-0070-2019

"…Consult with all interested parties before developing the filing system specified by subsection (a) of this section, including businesses, registered agents, attorneys, law enforcement and other interested persons; **If possible, partner with technology innovators and private companies to develop necessary components of the system**.

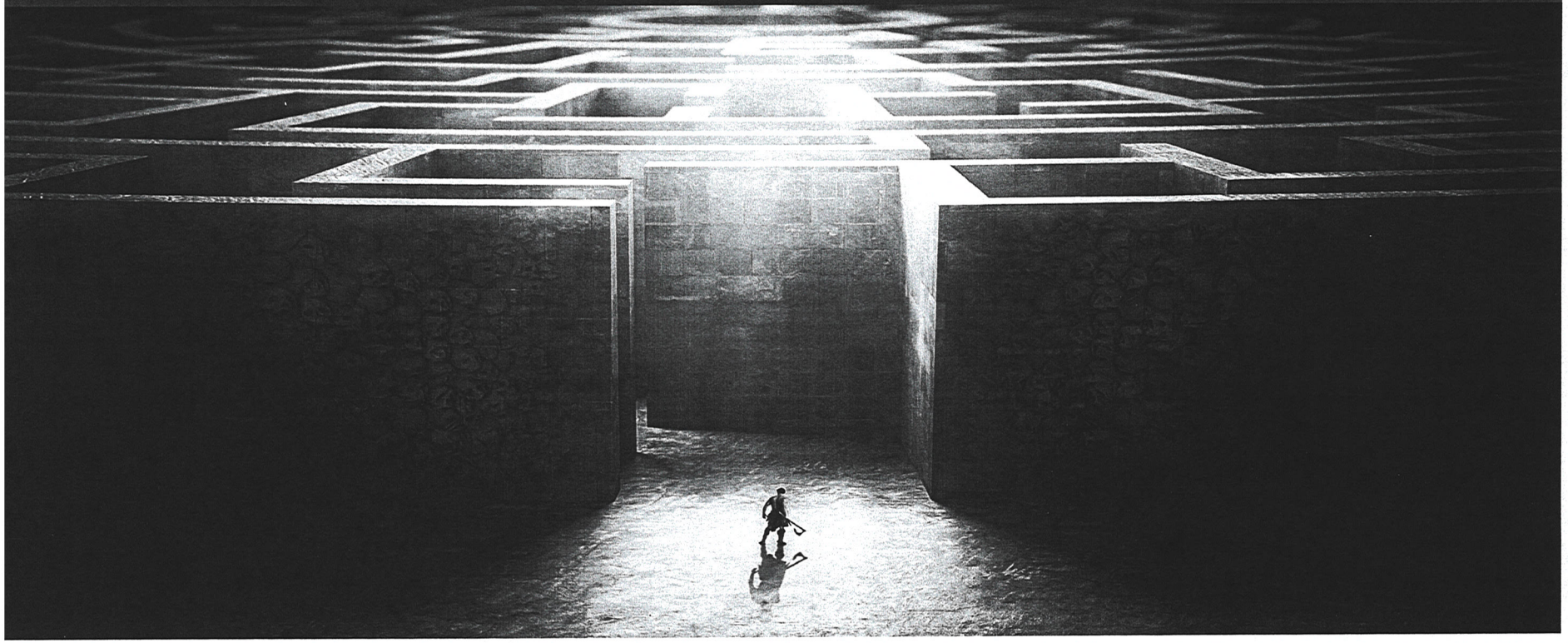
…

(iii) "Required filings" means **all documents, reports, data and other information required by law to be filed with the secretary of state**."

Demo Video

https://www.youtube.com/watch?v=1j_Vi0ePFGg

What are Verified Credentials & Decentralized Identifiers?



Credentials

Credentials are evidence of **authority**, **status**, **rights**, entitlement to **privileges**, or the like, usually written in some formal form.

Credentials

A credential typically consist of:

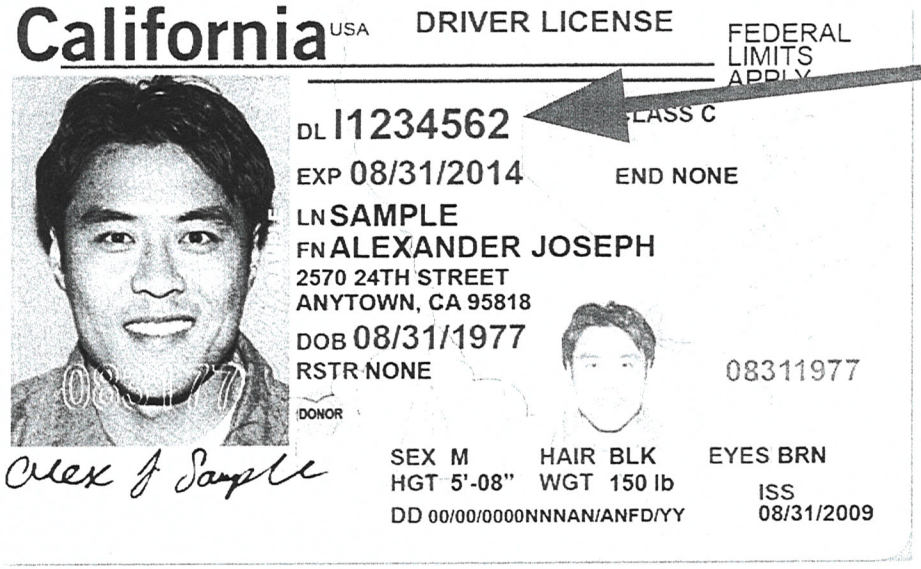
- information related to the **subject** of the credential (e.g., photo, name, and identification number),
- information related to the **issuer** (e.g., city government, national agency, or certification body),
- **evidence** related to how the credential was derived,
- information related to **usage**, such as biometrics or expiration dates

Digital Credential

A **digital credential** can represent all of the same information that a physical credential represents, but adds:

- **Tamper-proof** and therefore more trustworthy
- Holders can generate **presentations** with multiple credentials
- Both credentials and presentations can be rapidly transmitted, making them more **convenient** than their physical counterparts when establishing **trust at a distance**.

The Root of the Digital Credential Problem



- <IDENTIFIER>
  - ~~license: I1234562~~
  - hair: BLK
  - name: ALEXANDER JOSEPH
  - address: 2570 24th STREET ...
  - date of birth: 08/31/1977
  - issued by: California DMV
  - digital signature: MIIB7ZueKqp...

The Identifier Problem

To date, every identifier you use online does not belong to you; it belongs to someone else.

- URLs are **leased** to you by your DNS provider, who leases them from from the gTLD, who leases them from ICANN.
- Phone numbers are **loaned** to you (and often ported away)
- Government-issued identifiers often **misused** commercially
- Management of identifiers is hard, and is being **outsourced**

This results in problems related to **cost**, **data portability**, data **privacy**, and data **security**

What is Missing?

The ability to…

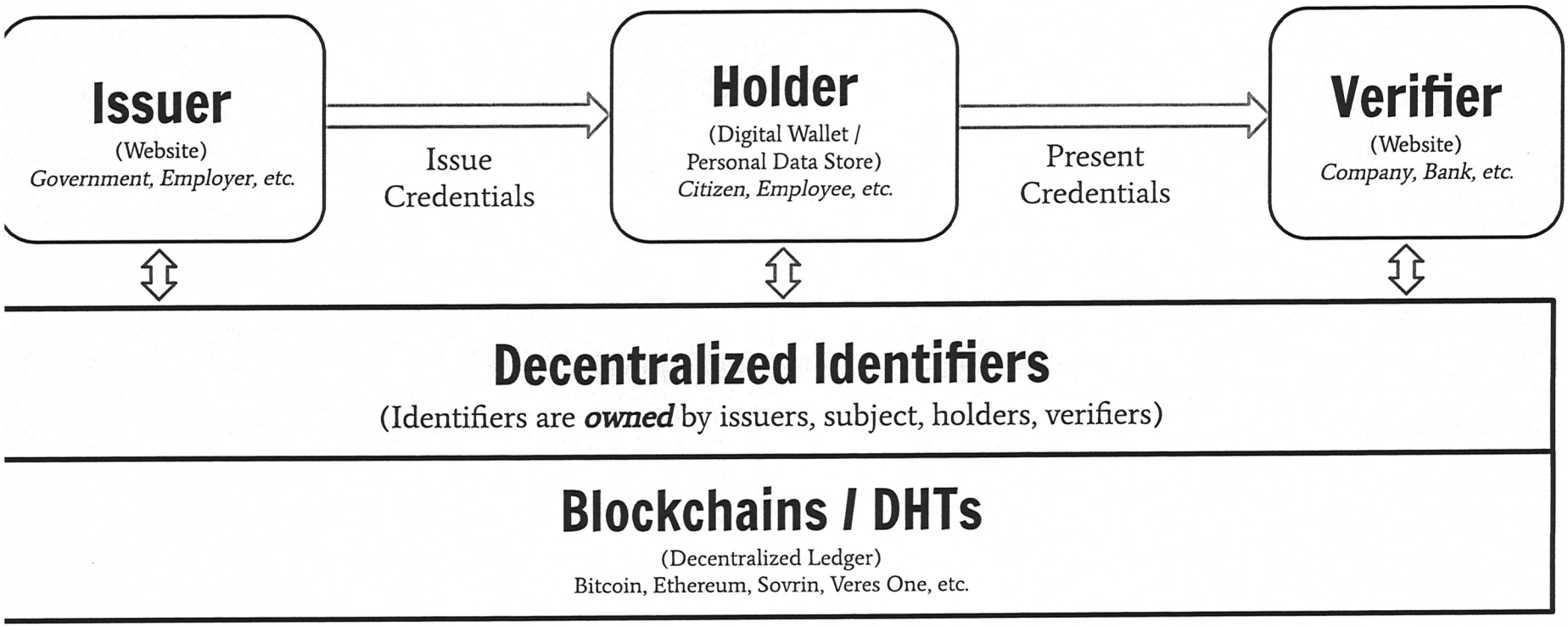
- create **many** identifiers for any **person**, **organization**, or **thing**
- that are **portable**
- do not depend on a **centralized** authority
- are protected by **cryptography**
- and enable **privacy** and **data portability**.

Solution: Decentralized Identifier (DID)

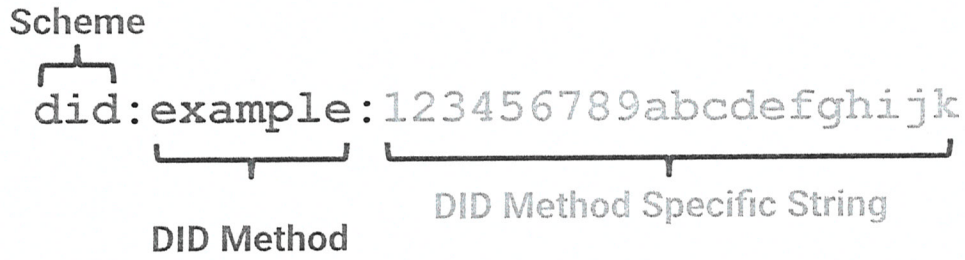
- **A new type of URL that is:**
  - globally unique,
  - highly available,
  - cryptographically verifiable
  - with no central authority.

`did:btcr:xyv2-xzyq-qqm5-tyke`

Decentralized Identifiers



What does a DID look like?



Example:

did:btcr:xyv2-xzyq-qqm5-tyke

Decentralized Identifiers

Also…

- for **individuals**, **organizations**, **things** (phones, IoT).
- registered in blockchain or other **decentralized network** (ledger-agnostic)
- created and managed via **wallet** applications
- resolve to **DID Document** with **public keys** & **service endpoints**
- Other identifier metadata, but **NOT PERSONAL DATA**

Some DID/VC Implementations To Date

Method	DID prefix
Bitcoin Reference	did:btcr:
Blockstack	did:stack:
ERC725	did:erc725:
Ethereum uPort	did:uport:
IPFS	did:ipfs:
IPDB	did:ipdb:
Sovrin	did:sov:
Veres One	did:v1:

more registered at https://w3c-ccg.github.io/did-method-registry/

Increasing International Support

- **British Columbia** — OrgBook & Verifiable Organization Network
  - 534K Business Entities DIDs, 1.4M Verifiable Credentials
- **Canada** — Pan-Canadian Trust Framework
- **Holland** — Self-Sovereign Identity based income proofs for housing
- **Malta** – Ministry Education w/Blockcerts — Education Credentials
- **Sierra Leone** — w/United Nations & Kiva — National Identity System
- **UNHCR** — Digital Identity for Refugees

Increasing US Government Support

- Cross borders
- Improve Supply Chain Management
- Combat Counterfeit Goods

US Department of Homeland Security

To that end, DHS S&T is pursuing two broad courses of action to encourage a more open and inclusive future for blockchain technology:

1. Support development of globally available specifications (precursor to standards) that are open, royalty free, and free to implement to ensure interoperability across systems while ensuring there is no vendor lock-in.
   a. Decentralized Identifiers (DIDs) via World Wide Web Consortium (W3C) Standardization Process
   b. Verifiable Claims Data Model via W3C Standardization Process
   c. Decentralized Key Management System via TBD (Potentially OASIS)
2. Actively work with and support our DHS Component customers, such as CBP, to understand their potential use cases for blockchain and help them achieve their outcomes with the needed R&D expertise and technologies.

Source: DHS Science and Technology Directorate's Testimony before the US House of Representatives, May 8, 2018

Need for Competitive Interoperable Marketplace

- US Department of Homeland Security is championing these principles and technologies
  - Require use of **interoperable standards and specifications** that are **patent free, royalty free and free to implement**
  - Avoid **vendor lock-in** and be **impartial to specific blockchains**, ideally multiple implementations
  - Support **Decentralized Identifiers, Verifiable Credentials**, **Multi-Party Key Management**
- US DHS is supporting the following projects
  - Support free trade agreements through **Certificates of Origin**, for use by US Customs
  - Mitigate Forgery & Counterfeiting of **Official Licenses & Certificates**
  - Citizenship, Immigration & Employment **Authorizations**
- US DHS has funded research and Proofs of Concepts of implementation
  - The technology in this Corporate Identity Demo was partially funded by US DHS

Christopher Allen | Executive Director | Blockchain Commons

- Co-Author SSL/TLS
- Co-Inventor & Architect of Decentralized Identifiers
- Author Design Principles of Self-Sovereign Identity
- Founder #RebootingWebOfTrust
- Co-Chair W3C Credentials CG
- Former Principal Architect, Blockstream
- Former CTO Certicom
- Former CEO Consensus Development

Email: ChristopherA@LifeWithAlacrity

Twitter: @ChristopherA

https://www.linkedin.com/in/ChristopherA/