Decentralized Identity

Ideology & Architecture

Christopher Allen *— Blockchain Commons (a Wyoming LLC!)*
Decentralized Identity & Blockchain Architect
Co-Chair W3C Credentials Community Group

Wyoming Blockchain Task Force
May 6th-7th 2019

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/christopher-v

Basis of Self-Sovereign Identity

Self-Sovereign Identity is based on the principles from our **Bill of Rights**, from the **Enlightenment**, and the **UN Universal Declaration of Human Rights**.

Control of Relationships & Interactions

Self-Sovereign Identity begins with the basic premise that you should **control** your own identity in regards to your **relationships** & **interactions** with other people, organizations and things.

Inherent Dignity

We all have **inherent dignity** independent of our birth place, lineage, or labels, simply because we are **human**.

Digital Identity Today

Identity platforms are administered by **centralized** authorities

- governments
- corporations
- software platform providers:

Each has a **vested interest** in managing people both on & offline because they desire to:

- Enforce a **social contract** (citizenship, employment, trade, services)
- **Lock out** other authorities from changing or profiting from those social contracts.

Limits on Self-Sovereignty

Self-Sovereignty doesn't mean that you are in complete control. But it does define the **borders** within which you can make decisions and outside of which you negotiate with others as **peers**, not as a petitioner.

"Your right to swing your arms ends just where the other man's nose begins."—*Unknown, Yale Book of Quotations*

Security Risks of Centralized Authorities

Data Silos. Huge centralized repositories of personal information are easy **targets** for attackers (Yahoo 3 **Billion**, Equifax 143 Million, many more)

Poor Resilience. Centralization is less resilient to attacks and/or damage

No Recourse. Who is responsible to solve problems? (Aadhaar **deaths**)

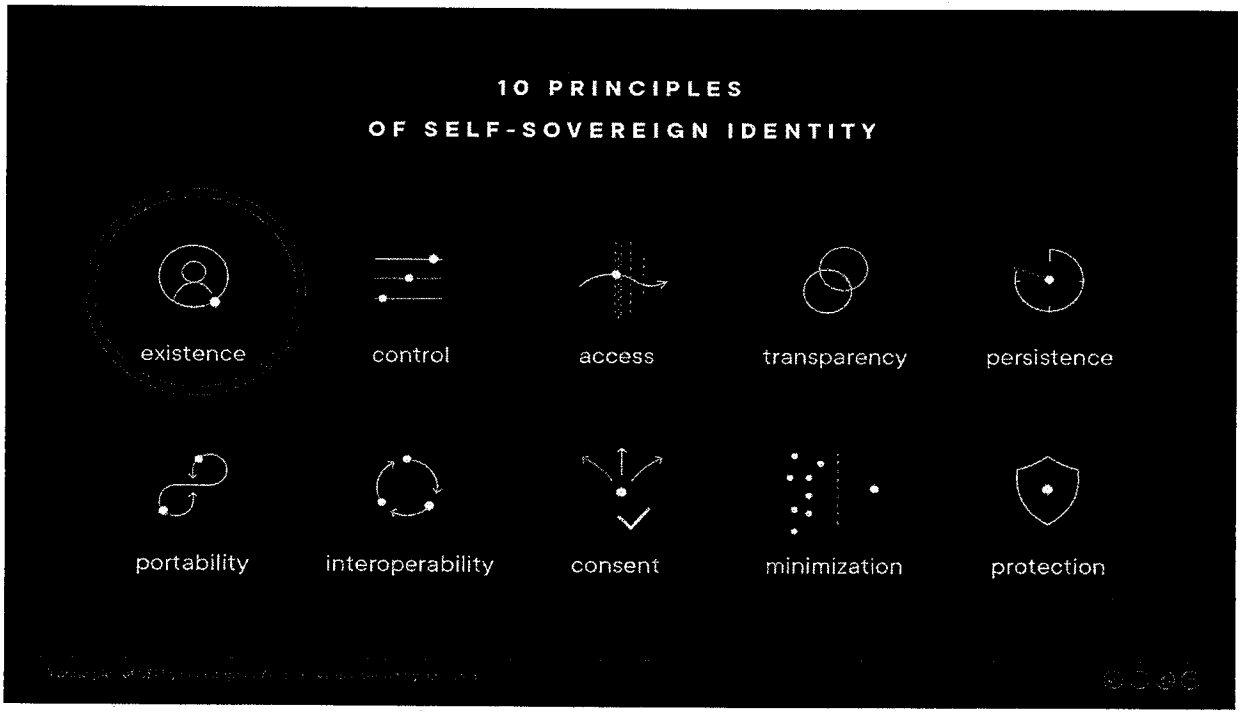
Abuse of Power. Centralized authorities use their dominance and **asymmetric** access to information gives them undeserved advantages

Lack of Transparency. People do not know how information about them is being used.

Hitting Limits: The current architectures have their roots in approaches created 40 years ago, during the days of mainframes & simple nation-state based identity. We are hitting the limits of those architectures.

10 Principles of Self-Sovereign Identity

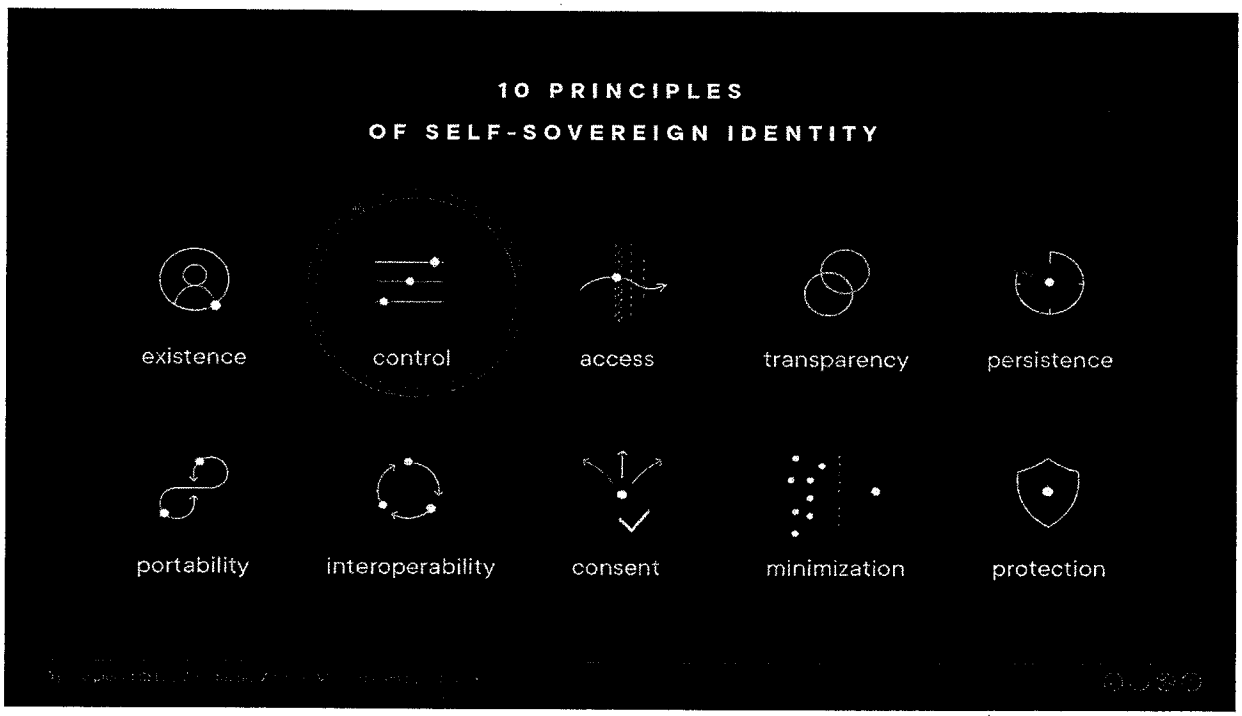
- ***Existence:*** Users have an independent existence — they are never wholly digital
- ***Control:*** Users must control their identities, privacy or celebrity as they prefer
- ***Access:*** Users must have access to their own data — no gatekeepers, nothing hidden
- ***Transparency:*** Systems and algorithms must be open and transparent
- ***Persistence:*** Identities must be long-lived — for as long as the user wishes
- ***Portability:*** Information and services about identity must be transportable by the user
- ***Interoperability:*** Identities should be as widely usable as possible; e.g. cross borders
- ***Consent:*** Users must freely agree to how their identity information will be used
- ***Minimization:*** Disclosure of claims about an identity must be as few as possible
- ***Protection:*** The rights of individual users must be protected against the powerful



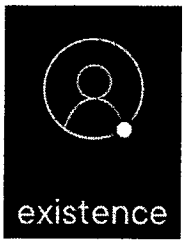
Human Dignity

Human dignity demands that individuals be treated with **respect** no matter which system they interact with, whether **face-to-face** or digitally **online**.

Without that, we become nothing but data in the machine — entries in a ledger to be managed, problems to be solved, digital serfs. **We are not.**



Source of Moral Authority



As our digital representations become more and more how we engage in society, a **free society** demands that we be given a **voice** in deciding how those representations are created and used.

Not because we own that data, but because individual human beings are the ONLY **valid source** for that **moral authority**.

Take Care: Identity is Not Property

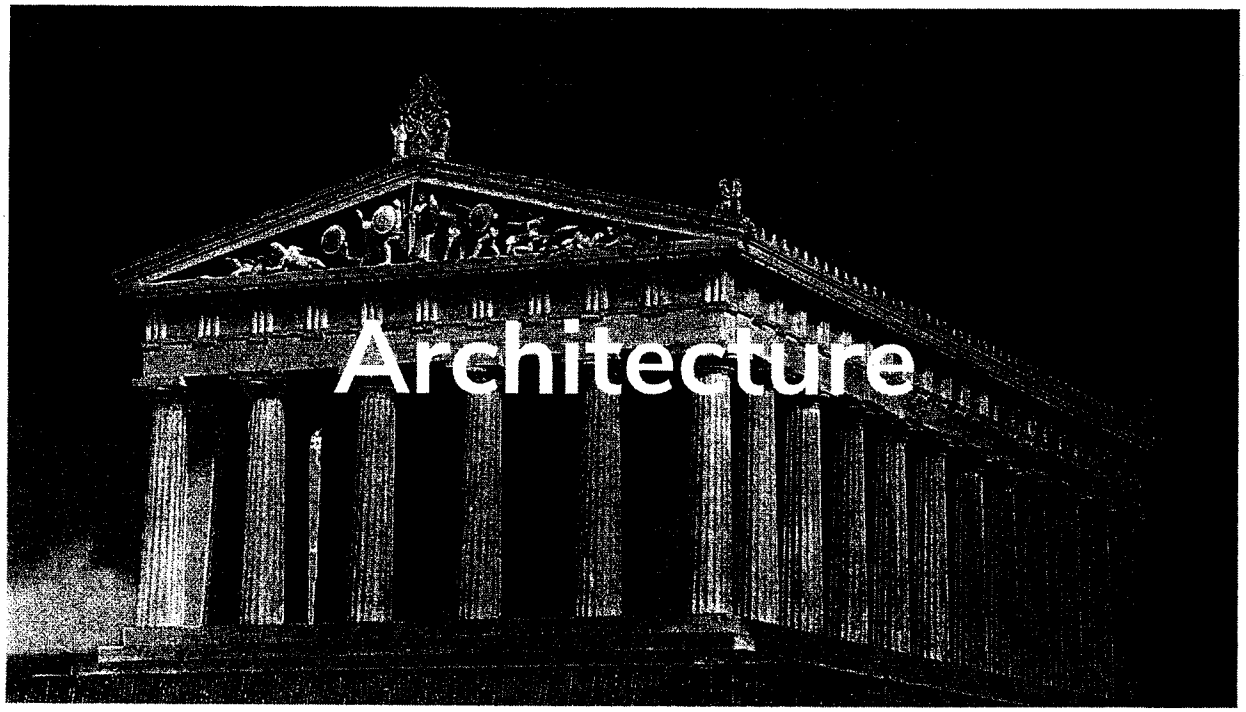
Property rights are extrinsic, alienable in the sense that they can be sold, transferred to another party, or seized by the state. However, **human rights** are **universal**, **indivisible** & **unalienable**. They cannot be divided into sticks in a bundle, and cannot be surrendered, transferred, or sold.

Thus when we speak about digital identity & personal information, we shouldn't use the words "own" or "ownership". Instead we speak of the individual's right to **control** their digital identity as we do our **physical** selves.

Just because something can be seem property-like does not mean that it is—or that it should be—subject to property law.

Balancing Transparence & Privacy

*"We desire to balance need for **fairness** and **accountability** against the need to prevent human rights **abuses** and the right to be able to **freely associate**. When these needs conflict, we err to preserve the **freedom** and **rights** of the individual over the needs of the **group**."* — Christopher Allen



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**.

Many Identities, Many Contexts

Another problem is that you have **many** identities, each with different **contexts**:

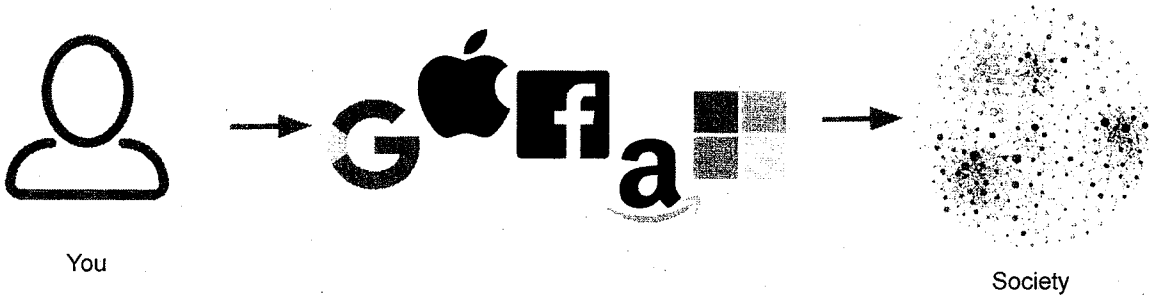
- **Family** (spouse's family, ex's family, blended families)
- **Friends** from different **eras** of your life (high school, college, early or different career)
- Different **communities** (church, culture, ethnic, lifestyle, neighborhood, special interests, hobbies/avocations)
- **Institutions** (employment, school, residency, citizenship)

Too many Contexts

Each of these contexts has an identifier

- **Family** (name, relationship "aunt")
- **Friends** from different **eras** of your life (nickname, relationship "roommate", Instagram account...)
- Different **communities** (usernames, email addresses...)
- **Institutions** (employee ID, SSN, driver's license, passport...)

Intermediaries Wedge In



You

Society

41

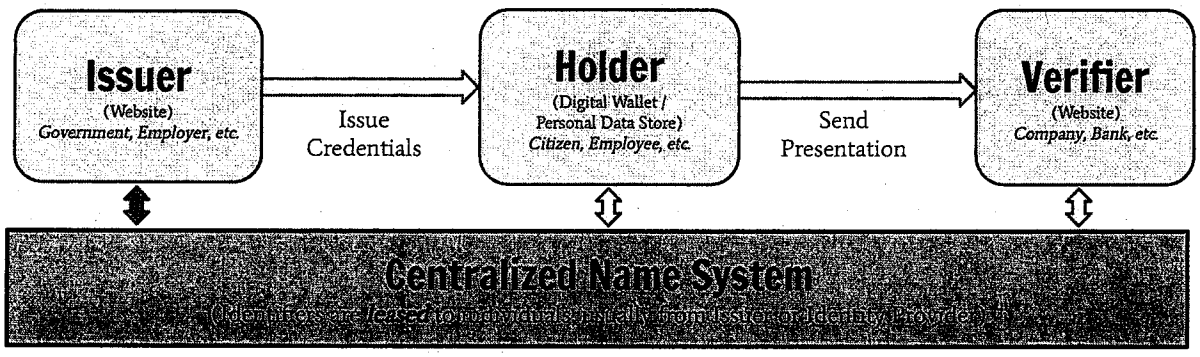
Unmanagable Contexts

You

Society

42

Digital Identifiers Today

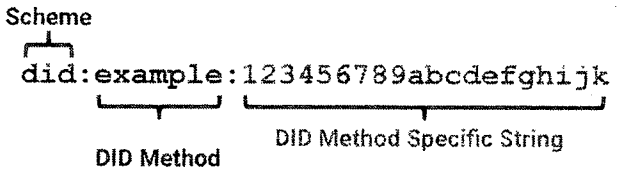


What is Missing?

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**.

What does a DID look like?



Example:

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

Decentralized Identifiers

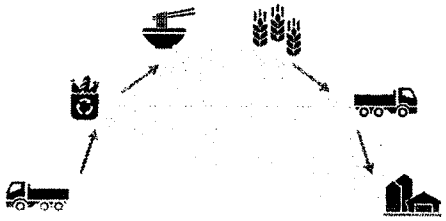
Also...

- 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 Organizations Committed to DID/VCs

Increasing US Government Support

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

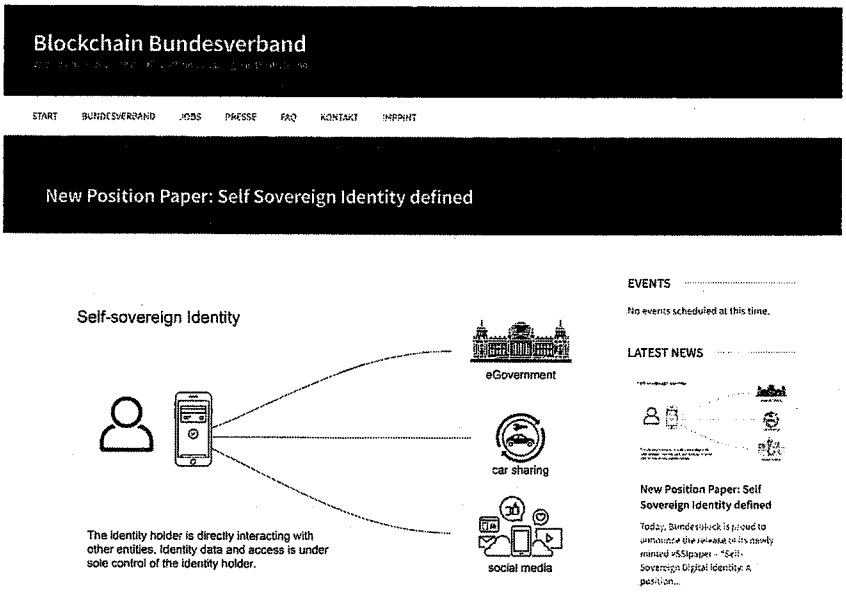


US Department of Homeland Security

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



http://bit.ly/ssipaper_feedback