Distributed ledgers finally brought me a usable digital identity!

Richard Esplin
February 2019
Agenda

- What is self-sovereign identity
- Verifiable credentials
- Hyperledger Indy
- Governance
What is Self Sovereign Identity?
On the Internet, nobody knows you're a dog

"On the Internet, nobody knows you're a dog" is an adage and meme about Internet anonymity which began as a cartoon caption by Peter Steiner and published by *The New Yorker* on July 5, 1993.[1][2] The cartoon features two dogs: one sitting on a chair in front of a computer, speaking the caption to a second dog sitting on the floor listening to the first.[3] As of 2011, the panel was the most reproduced cartoon from *The New Yorker*, and Steiner had earned over US$50,000 from its reprinting.[1][4][5]
Digital Identity

- Sign in with Facebook
- Sign in with Google+
- Sign in with Twitter
- Sign in with LinkedIn
- Sign in with Amazon
AND INTRODUCED TREMENDOUS PROBLEMS
A year-long investigation into Facebook, data, and influencing elections in the digital age

Facebook's week of shame / The Cambridge Analytica fallout

"Politicians can't control the digital giants with rules drawn up for the analogue era" - Andrew Rarnsley

"Did they just use me? Was I naive?" - Brexit whistleblower speaks out
Facebook Could Face Up to $1.63 Billion Fine for Latest Hack Under the GDPR

Facebook’s stunning disclosure of a massive hack on Friday in which attackers gained access tokens to at least 50 million accounts—bypassing security measures and potentially giving them full control of both profiles and linked apps—has already stirred the threat of a $1.63 billion dollar fine in the European Union, according to the Wall Street Journal.
Ten Principles of Self-Sovereign Identity

1. Users must have an independent existence.
2. Users must control their identities.
3. Users must have access to their own data.
4. Systems and algorithms must be transparent.
5. Identities must be long-lived.
6. Information and services about identity must be transportable.
7. Identities should be as widely used as possible.
8. Users must agree to the use of their identity.
9. Disclosure of claims must be minimized.
10. The rights of users must be protected.

Christopher Allen, 2016
Also Known As

User-Centric Identity
User-Controlled Identity
User-Owned Identity
Bring Your Own Identity
Verifiable Credentials
W3C Verifiable Credentials Ecosystem

Issuer
- Signs Credential

Holder
- Issues Credential
- Wallet
- Countersigns Credential

Verifier
- Presents Credential
- Verifies Signatures

Decentralized Identifiers (DIDs)

Public Blockchain or other Decentralized Network
Sovrin Verifiable Credentials Ecosystem

- **Issuer**: Signs Credential
- **Prover**: Issues Credential, Countsigns Credential
- **Verifier**: Presents Credential, Verifies Signatures

- Pairwise Pseudonymous DIDs
- Decentralized Identifiers (DIDs)
- Public Blockchain

- Sovrin
Sovrin Verifiable Credentials Ecosystem

Issuer

Signs Credential

Zero Knowledge Encoding

Prover

Issues Credential

Countersigns Credential

Wallet

Presents Credential

Verifier

Verifies Signatures

Zero Knowledge Proof

Decentralized Identifiers (DIDs)

Public Blockchain

sovrin
Shopping for a tiger
Aaliyah’s International

Save a tiger; make a friend!

Verify our story!

Credential from: Tiger Stewardship Advocates

Claim: tigers distributed by Aaliyah’s International are captive bred and not suitable for reintroduction to the wild.

Inspection Date: December 8, 2018

Inspection Number: 1576295029659
Aaliyah’s International

Credential request: Aaliyah’s International

Would like:
- Proof of age
- Permit for owning an exotic species
- Proof of tiger handler training
- Certification of veterinary availability
Credential from: Utah State University
Claim: Richard Esplin is permitted to possess an exotic species within our city.
Date: January 10, 2019

Credential from: Utah State University
Claim: Richard Esplin completed the following classes
- Computer Science (B)
- Tiger Handling (C)
- Ecology (C)
- Wildlife Management (D)
Date: June 16, 2018

Credential from: Salt Lake City, Utah, United States
Claim: Richard Esplin is permitted to possess an exotic species within our city.
Date: January 10, 2019

Credential from: Utah Division of Motor Vehicles
Claim: Richard Esplin is a customer of our business in good standing.
Date: December 15, 2018

Credential from: Utah Tiger Veterinarians
Claim: Richard Esplin is a customer of our business in good standing.
Date: December 15, 2018

Credential from: Utah Division of Motor Vehicles
Claim: Richard Esplin is licensed to drive
Address, Birthdate, Restrictions …
Issue Date: December 15, 2018

Credential from: Utah Tiger Veterinarians
Claim: Richard Esplin is a customer of our business in good standing.

Credential from: Utah Division of Motor Vehicles
Claim: Richard Esplin is licensed to drive
Address, Birthdate, Restrictions …
Issue Date: December 15, 2018
Your delivery will be done by: **Speedy Delivery Incorporated**

**Credential from:**
**Aaliyah’s International**

**Claim:**
an employee from **Speedy Delivery Incorporated**
may act on our behalf

**Date range:**
January 16, 2019 to January 31, 2019
Credential from: Richard Esplin

Claim: an employee from Speedy Delivery Incorporated may access a porch delivery box in my possession.

Date range: January 16, 2019 to January 31, 2019
Update: delivery service has changed.

Your delivery will be done by: **Advanced Delivery**

January 28, 2019

---

Credential from: **Aaliyah’s International**

Claim:
an employee from **Speedy Delivery Incorporated** may act on our behalf

Date range: 
January 16, 2019 to January 31, 2019

---

Revoked

Credential from: **Aaliyah’s International**

Claim:
an employee from **Advanced Delivery** may act on our behalf

Date range: 
January 16, 2019 to January 31, 2019
Credential from: Richard Esplin

Claim: an employee from Speedy Delivery Incorporated may access a porch delivery box in my possession.

Date range: January 16, 2019 to January 31, 2019

Credential from: Richard Esplin

Claim: an employee from Advanced Delivery may access a porch delivery box in my possession.

Date range: January 16, 2019 to January 31, 2019

Revoked
Credential from: Aaliyah’s International

Claim:
the following employee of Advanced Delivery
is acting as our representative

Name: Julio Valdez

Date range:
January 28, 2019 to January 30, 2019

Credential from: Richard Esplin

Claim:
a porch delivery box in my possession accepted a package

From:
Julio Valdez
an employee of Advanced Delivery
acting as a representative for Aaliyah’s International

Date: January 29, 2019
Credential from: Richard Esplin

Claim: Luciana Black
has access to my front door

Number of times: Unlimited

Date range: January 16, 2019 to January 31, 2019

Credential from: Richard Esplin

Claim: Luciana Black
has access to a porch delivery box in my possession

Number of times: 1

Date range: January 16, 2019 to January 31, 2019
Note:
The author does not advocate household tiger ownership.

No tigers were harmed in the making of this story.
Purpose-Built Public Blockchain

Engineered solely for privacy-enhancing self-sovereign identity

Global public utility that no single entity owns or controls

Open source, open standards, open governance

Fast, efficient—based on Hyperledger Indy
Hyperledger Indy
Hyperledger Indy

Public Permissioned Blockchain

Custom built for Identity

RBFT Consensus
Hyperledger Indy

- Ursa
  - SDK
    - LibIndy
    - LibVCX
    - LibNullPay
    - Wallet
  - Plenum
  - Node
- Wrappers
  - Rust
  - Python
  - NodeJS
  - Java
  - ObjectiveC
- Catalyst
- Agents
  - Issuer Edge
  - Mobile Edge
  - Cloud
  - Thin
  - Static
The problem is correlation

Correlation = Linkability

Attribute based correlation

Identifier-based Correlation

Signature or Hash-based Correlation

Timing Inferences

Including if Multiple Parties Share Information (Collusion)
Ensuring privacy

The prover chooses when to disclose.

The prover selects what should be disclosed.

Don’t share more attributes than necessary.

Don’t share with more precision than necessary.

The verifier and the issue do not communicate.

The prover can present to any verifier.

A proof can hold multiple credentials from multiple issuers.

A credential is anonymously revocable.
More Than Code
All blockchains are governed—whether it is implicit or explicit.
Creating Trust

Moral Pressure
Reputational Pressure
Institutional Pressure
Security Systems

Bruce Schneier, 2012
*Liars and Outliers: Enabling the Trust that Society Needs to Thrive*
The BLT

Business
Legal
Technical
A credit card network relies on a trust framework to establish trust between the parties
The trust in any SSI digital credential will depend on the trust framework under which it is issued.
Every digital credential intended to serve more than one issuer/verifier needs a domain-specific governance framework. It specifies what issuers will issue what credentials under what policies to achieve a community’s trust objectives.

— Drummond Reed
Chief Trust Officer, Evernym
Digital Credential

Governance Framework
Sovrin Governance Framework

Informational

The Sovrin Web of Trust Model
(White paper)

Constitutional

Sovrin Governance Framework Master Document V2
Sovrin Steward Agreement V2 (Legal contract)

Controlled Documents

Legislative

Sovrin Glossary V2

Compliance

Sovrin Trust Assurance Framework V1
A Usable Digital Identity is Self-Sovereign

- Is built with open source and open standards
- Have a decentralized root of authority (blockchain)
- Keeps personal data off the public ledger
- Allows selective disclosure
- Resists correlation
- Exists within a trust framework