evernym

The decentralized identity company

Self-Sovereign Identity

Transforming Customer Experience and Creating Competitive Advantage

Andy Tobin @actobin

October 2019

Gartner
Cool
Vendor
2018

Imagine if...

- you could onboard every new customer with 1 click.
- each of your customers had a secure, direct connection to you.
- you could instantly verify that every customer is genuine.
- your customers never needed a username and password.
- you never had any more fraudulent card payments.
- you could send every customer verifiable digital receipts.

How much competitive advantage would you gain?

evernym

A seismic change is underway.
The way we think about and use digital identity
is transforming,
touching every aspect of digital life.

Enter **"Self-Sovereign Identity"**

or "decentralized identity"
or "blockchain identity"
or "portable digital identity"

evernym

What Is Self-Sovereign Identity?

The ability for people, organisations and things to **hold**, **manage** and **control** their own digital credentials, just like they do with their physical ones….with added **cryptographic superpowers**

We call these **"credentials"**

They answer the question: **"Says who?"**

Paper is the global standard for credentials

evernym

But paper doesn't work **online.**

The digital world has no equivalent for paper credentials

e·ernym

Yet digital identity underpins every online interaction

evernym

Today's digital identity is killing customer experience
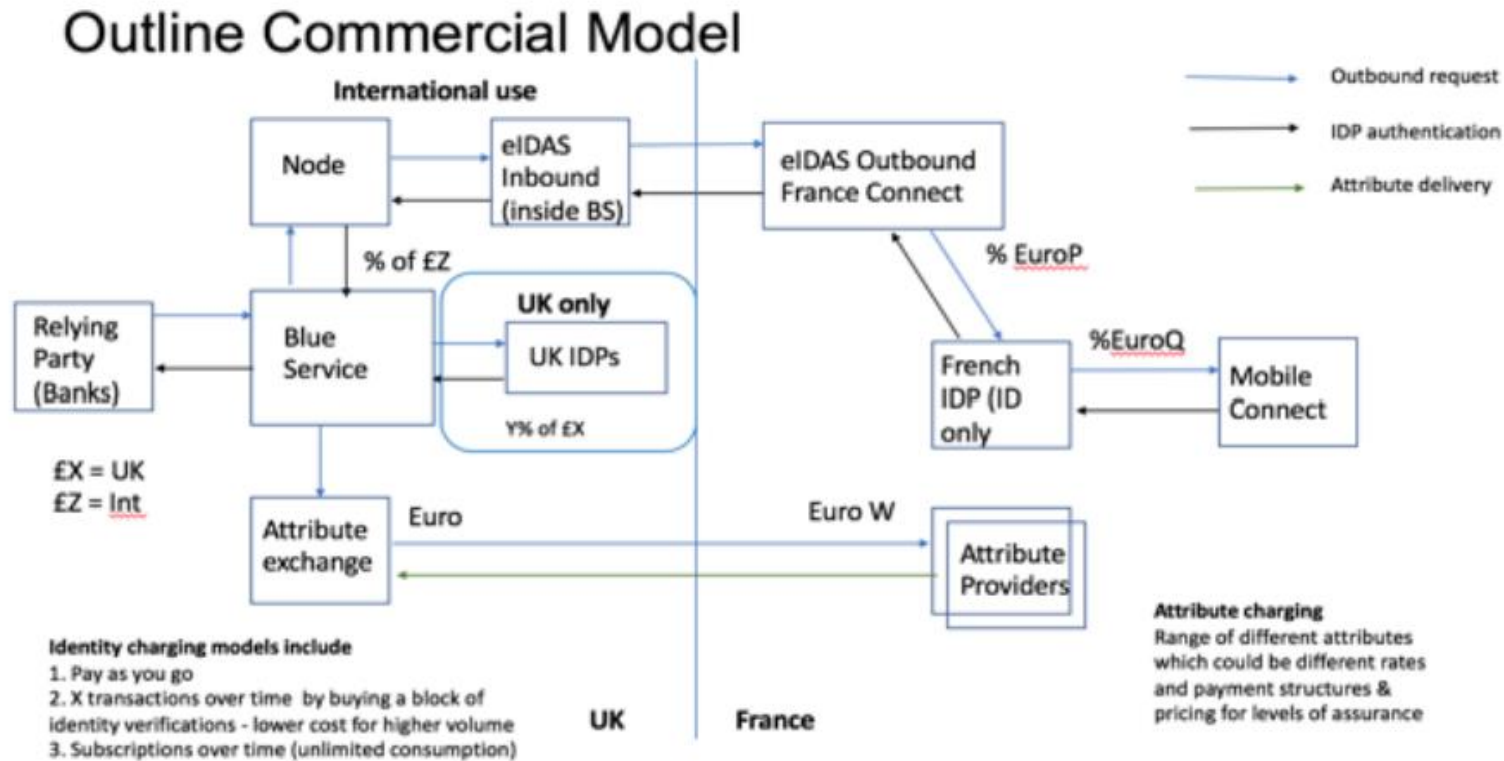
"Institutions will save $1.6 trillion globally"

McKinsey on Digital Identification

evernym

What it looks like today:
using a French digital ID to open a bank account in the UK

Outline Commercial Model

International use

Node — eIDAS Inbound (inside BS) — eIDAS Outbound France Connect

% of £Z

UK only

Relying Party (Banks) — Blue Service — UK IDPs

Y% of £X

% EuroP

%EuroQ

French IDP (ID only) — Mobile Connect

£X = UK
£Z = Int

Attribute exchange — Euro — Euro W — Attribute Providers

Legend:
- Outbound request
- IDP authentication
- Attribute delivery

Identity charging models include
1. Pay as you go
2. X transactions over time by buying a block of identity verifications - lower cost for higher volume
3. Subscriptions over time (unlimited consumption)

UK | France

Attribute charging
Range of different attributes which could be different rates and payment structures & pricing for levels of assurance

OIX UK Europe

This is **easier**

Credential
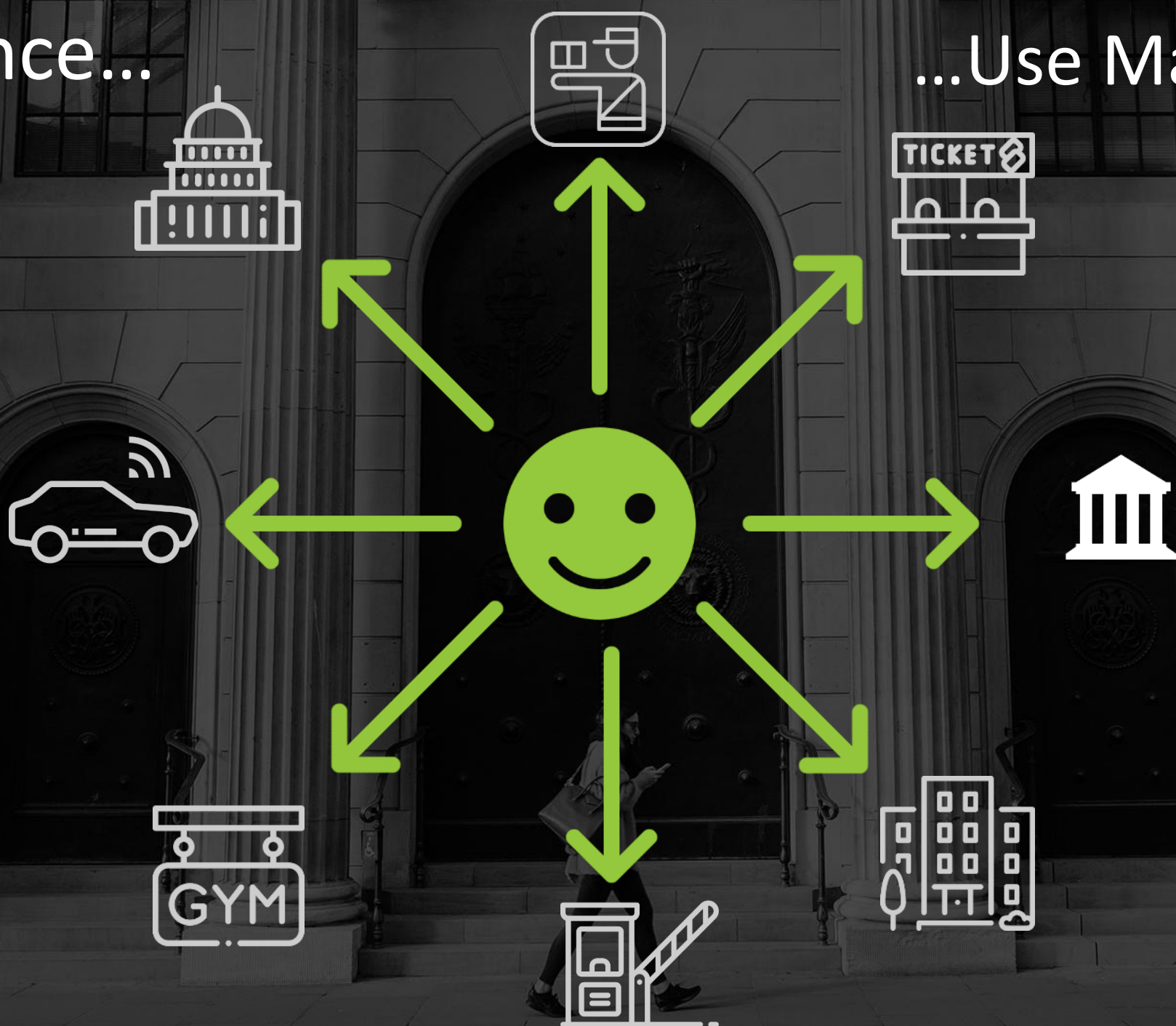Provider (DVLA,
passport office,
utility company,
gym etc etc)

digital
credential

digital
proof

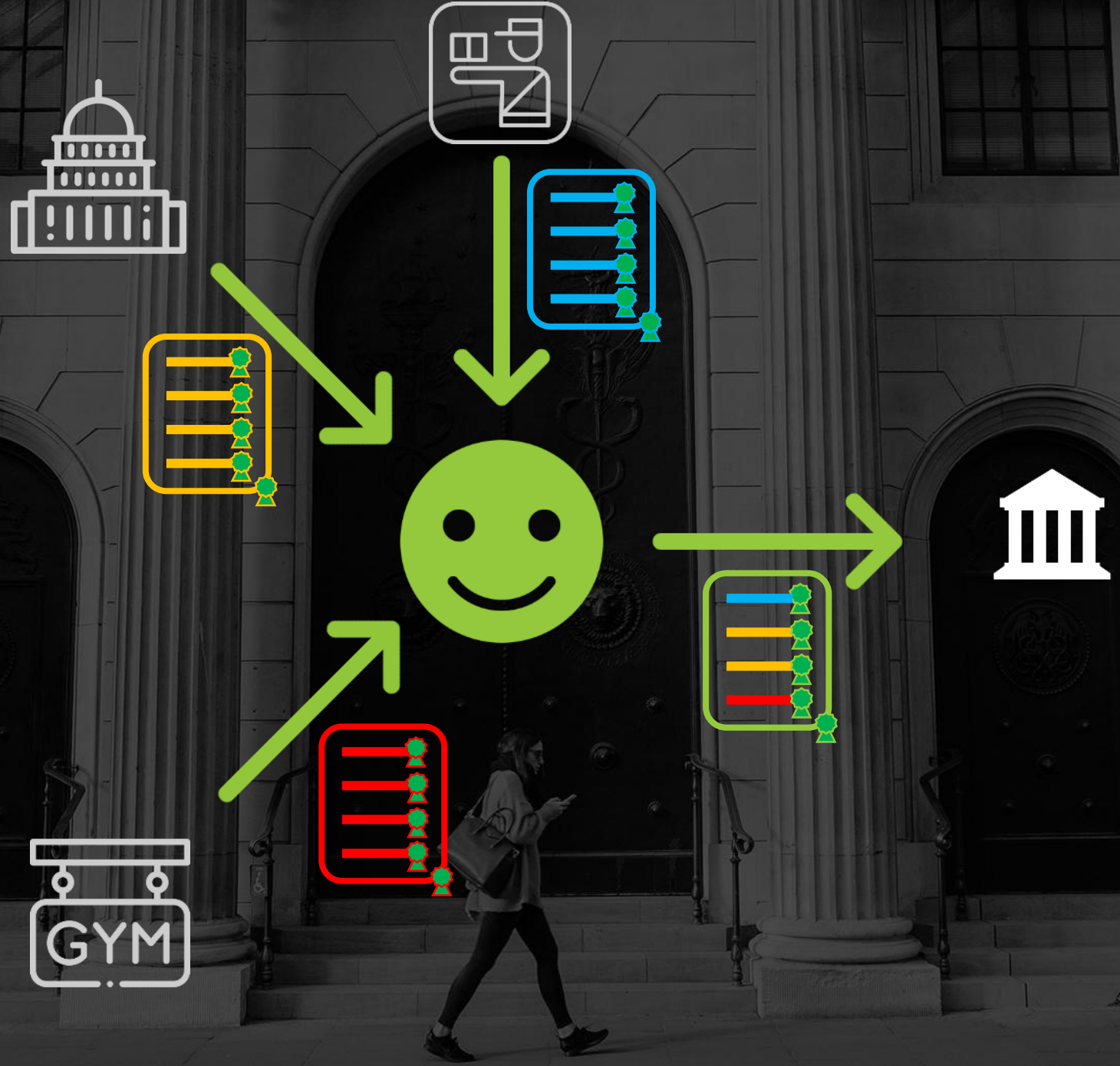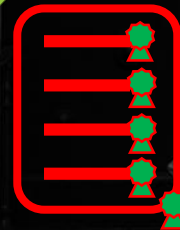Relying Party
(eg bank,
retailer etc etc)

evernym

It is possible to combine attributes from different credentials and present them as a single proof.

You can just present a zero-knowledge proof, without revealing the underlying data.

The Relying Party Can Instantly Check 4 Things
WITHOUT HAVING TO CONTACT THE ISSUER

1. Who issued the credential?
2. Was it only issued to the presenter?
3. Has it been tampered with?
4. Has it been revoked?

digital proof

Relying Party
(eg bank, retailer etc etc)

Thus increasing privacy and reducing correlation risk

evernym

How does the relying party verify data authenticity without contacting the issuer?

They read the issuer's verification keys from a global public distributed ledger.

Writes public verification keys (curve ED25519)

Reads issuer's keys

The Sovrin Ledger

evernym

Every relationship is separate, unique and encrypted.

Connection setup and credential exchange all happens off-ledger, privately, with no intermediaries.

The Sovrin Ledger

evernym

...And they can also give you digital credentials back (they already give you paper or plastic ones)...
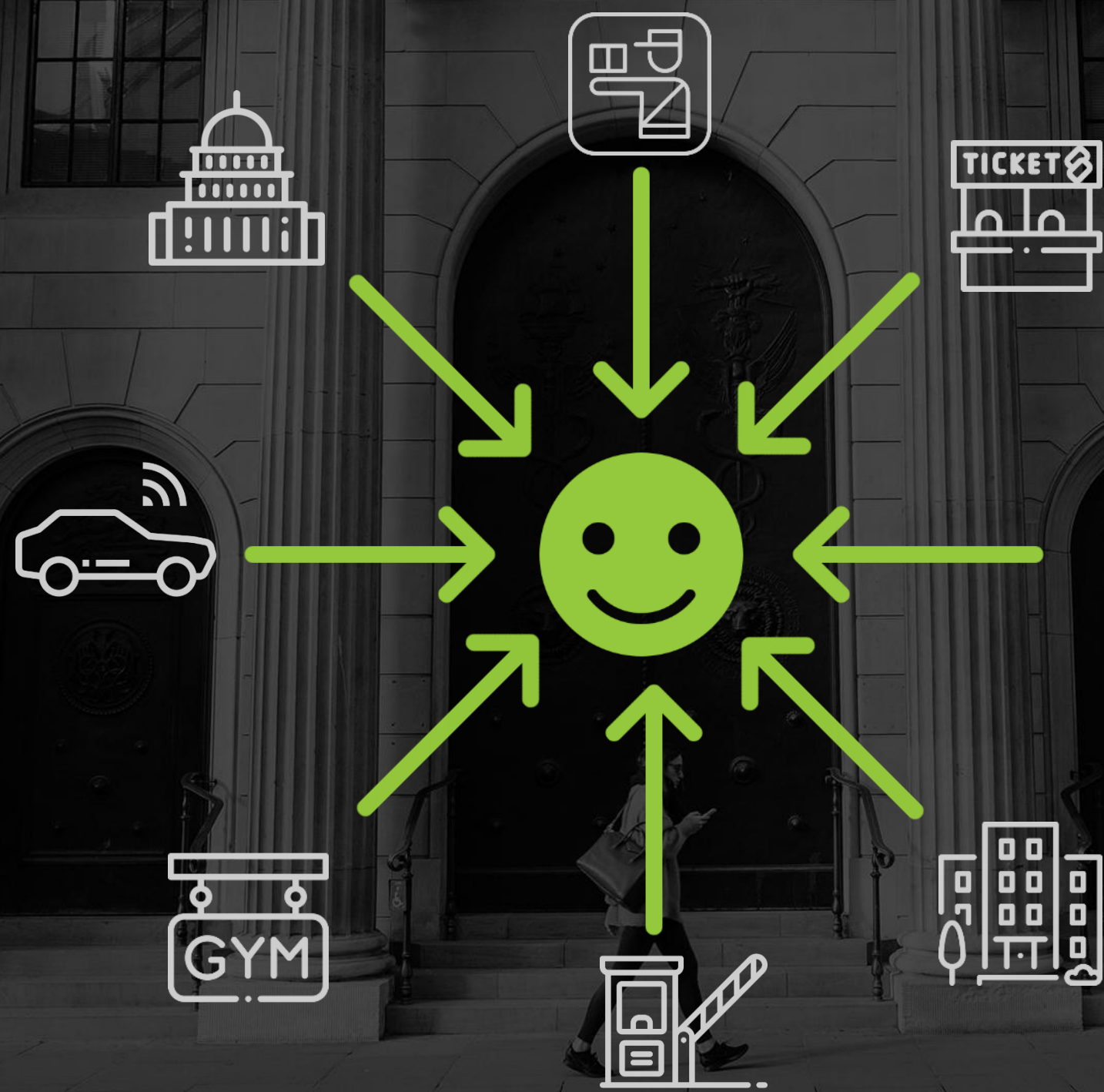
To deliver this vision, we need a new, open, protocol

Like TCP/IP, SMTP, HTML, IEEE 802.11…

This protocol needs to be open, non-proprietary, interoperable, and **usable by everyone**

evernym

Important!

Open Standards, No Vendor Lock-in

…just like the internet

evernym

These are some of the people building it

evernym

established &
donated code

sovrin identity for all

HYPERLEDGER INDY

HYPERLEDGER URSA

HYPERLEDGER ARIES

THE **LINUX FOUNDATION**

Indy, Ursa and Aries are open source, Linux Foundation projects.

"Fuelling innovation at unmatched speed and scale"

Shared crypto-library for advanced cryptographic functions like zero-knowledge proofs.

Protocol for peer to peer connections, wallet, messaging, key management.

Hyperledger as a Verifiable Information Exchange Platform

HYPERLEDGER URSA

HYPERLEDGER ARIES

HYPERLEDGER INDY

Hyperledger Ursa (Crypto Library)

Application Layer

Hyperledger Aries (client side components)
(Agent Protocol and Wallet Services)

Agent Implementations (Server-side & Mobile)

Agent Frameworks | Static Agent

Messaging Layer and Default Message Families

Agenty Things

Wallet Interface & Default Implementations

Resolver Interface

did:peer Resolver

Wallety Things

Hyperledger Indy (blockchain side)

Indy Resolver ← other resolvers too

Indy Node

Plenum (BFT Ledger)

Storage Layer (sqlite, Postgres, …)

2 Important New W3C Standards
DIDs and Verifiable Credentials

W3C®

Decentralized Identifiers (DIDs):
a new type of globally resolvable,
cryptographically-verifiable identifier

`did:sov:3k9dg356wdcj5gf2k9bw8kfg7a`

Method-Specific Identifier (Generated as defined by the particular DID method specification)

Method (here showing the Sovrin ledger)

Scheme

Verifiable Credentials:
The mechanism for encoding, signing,
exchanging and verifying digital credentials.

evernym

Mythbusting 🚫
What Self-Sovereign Identity *isn't*

- It isn't a replacement for civil registers like birth registries, driving license authorities, passport offices.

- It isn't a "rip and replace" for all existing identity schemes. It's enhances them.

And:

- It doesn't work for black lists such as no-fly lists, or PEP & sanctions lists.

- It doesn't mean everyone "self-attests" all the information about themselves removing the need for governments.

evernym

What does this mean for **you and me?**

Simplicity AND Privacy:

- No more usernames or passwords.

- No more registration forms.

- No more spam or phishing.

- Secure private communications by default.

- No more intermediaries watching what I do.

evernym

What does this mean for **organizations?**

Lower friction AND higher security

- Instant customer data verification

- Fast onboarding with great customer experience

- Simplifying regulatory compliance

- Reducing "toxic" data lakes

- A secure, private relationship with each customer

- Interoperability across silos

evernym

Example

One-click secure onboarding and payment for retailers

Problems being addressed:

✓ Shopping cart abandonment

✓ Chargebacks

✓ Fraud

barclaycard

evernym

Example

 Trusted digital identity and single-sign-on for doctors and nurses

Problems being addressed:

✓ Lost clinical hours

✓ £1bn savings through optimising healthcare personnel onboarding

✓ Patient safety

Example

Credit Union customer identification & authentication

Problems being addressed:

✓ Call in, walk in, log in authentication

✓ Single, reusable identity within the credit union industry

✓ Giving customers a digital identity they can use elsewhere

CULedger

e·ernym

Example

Bank "know your customer" regulatory checks

Problems being addressed:

✓ Poor user experience

✓ High onboarding costs

✓ 45 minutes to 45 seconds

ATB Financial™

monese

CURVE

SEEDRS

B-SOCIAL

evernym

Regulatory Engagement Under Way

UK FCA

Financial Conduct Authority

Bank "know your customer" regulatory checks

Evernym is participating in a joint project with Deloitte, Onfido and 6 UK banks within the FCA's Regulatory Sandbox.

The intention is to confirm the viability of digital credentials for new customer onboarding.

Deloitte.

onfido

monese

CURVE

SEEDRS

B-SOCIAL

evernym

Example

Verifiable Organizations Network (VON)

Problems being addressed:

✓ Making it easier to open a business and apply for permits

✓ Streamlining data sharing between agencies

Many projects, many use cases.

For people, organizations, and things.

Same protocol.

This is the shape of things to come

evernym

Imagine if...

- you could onboard every new customer with 1 click.
- each of your customers had a secure, direct connection to you.
- you could instantly verify every customer is genuine.
- your customers never needed a username and password.
- you never had any more fraudulent card payments.
- you could send every customer verifiable digital receipts.

This is all achievable using a single platform using DIDs and verifiable credentials

evernym

Get a head start

Join 50+ organizations that are already taking SSI for a test flight.

evernym.com/early-access

The fastest way to discover and launch self-sovereign identity.

—————

The leading online accelerator program for enterprises, governments, universities, and other organizations looking to benefit from a decentralized identity system.

evernym

Big brands and entrepreneurs are onboard.

Thank you

Andy Tobin @actobin
www.evernym.com

evernym