Distributed ledgers finally brought me a usable digital identity!

Richard Esplin

February 2019

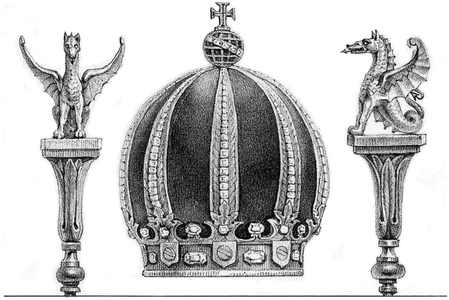
evernym

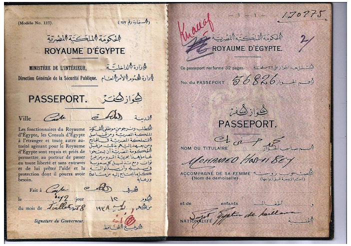
Agenda

- What is self-sovereign identity
- Verifiable credentials
- Hyperledger Indy
- Governance

What is Self Sovereign Identity?

Carriers of Identity





(Modèle No. 117). (استمارة رقم ١١٧)

الحكومة الملكية المصرية

ROYAUME D'ÉGYPTE

MINISTÈRE DE L'INTÉRIEUR, وزارة الداخلية

Direction Générale de la Sécurité Publique. إدارة عموم الأمن العام

PASSEPORT. جواز سفر

Ville Caire القاهرة المدينة

Les fonctionnaires du Royaume d'Égypte, les Consuls d'Égypte à l'étranger et toute autre autorité agissant pour le Royaume d'Égypte sont requis et priés de permettre au porteur de passer en toute liberté et sans entraves et de lui prêter l'aide et la protection dont il pourra avoir besoin.

Fait à Caire القاهرة

le 12 jour ١٢ يوم

du mois de Juillet 1928 ١٩٢٨ من شهر

Signature du Gouverneur. توقيع المحافظ

— 1 — 1 — 120275

الحكومة الملكية المصرية

ROYAUME D'ÉGYPTE. 2/

Ce passeport renferme 32 pages. يشتمل هذا الجواز على ٣٢ صفحة

No. du PASSEPORT 56826 رقم الجواز

جواز سفر

PASSEPORT.

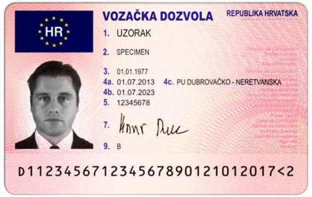
NOM DU TITULAIRE محمد حسني بك اسم صاحب الجواز

Mohamed Hosni Bey

ACCOMPAGNÉ DE SA FEMME (Nom de demoiselle) مصحوب بزوجته (اسم الزوجة قبل زواجها)

et de enfants. أطفال و

NATIONALITÉ Sujet Egyptien de naissance الجنسية

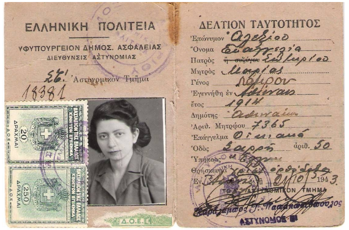


HR

VOZAČKA DOZVOLA REPUBLIKA HRVATSKA

1. UZORAK
2. SPECIMEN
3. 01.01.1977
4a. 01.07.2013 4c. PU DUBROVAČKO - NERETVANSKA
4b. 01.07.2023
5. 12345678
7.
9. B

D11234567123456789012101 2017<2



ΕΛΛΗΝΙΚΗ ΠΟΛΙΤΕΙΑ

ΥΦΥΠΟΥΡΓΕΙΟΝ ΔΗΜΟΣ. ΑΣΦΑΛΕΙΑΣ
ΔΙΕΥΘΥΝΣΙΣ ΑΣΤΥΝΟΜΙΑΣ

26ον Ἀστυνομικὸν Τμῆμα

18381

20 ΔΡΑΧΜΑΙ Δ.Ο.Ε.
250 ΔΡΑΧΜΑΙ Δ.Ο.Ε.
ΒΑΣΙΛΕΙΟΝ ΤΗΣ ΕΛΛΑΔΟΣ ΚΙΝΗΤΟΝ ΕΠΙΣΗΜΑ

Δ.Ο.Ε.

ΔΕΛΤΙΟΝ ΤΑΥΤΟΤΗΤΟΣ

Ἐπώνυμον Αλεξίου
Ὄνομα Ευαγγελία
Πατρὸς ~~ἢ συζύγου~~ Σπυρίδου
Μητρὸς Μαρίας
Γένος Λάμπρου
Ἐγεννήθη ἐν Αθήναις
ἔτος 1914
Δημότης Αθηναίων
Ἀριθ. Μητρῴου 7365
Ἐπάγγελμα Οικιακά
Ὁδὸς Σαρρή ἀριθ. 50
Ὑπήκοος Ελληνις
Θρήσκευμα Χριστ. ορθόδοξος
Ἐν Αθήναις τῇ 21/10 194 3.
ΤΟ 26ον ΑΣΤΥΝΟΜΙΚΟΝ ΤΜΗΜΑ
Χαράλαμπος Γ. Παπαπαναγόπουλος
ΑΣΤΥΝΟΜΟΣ Β'

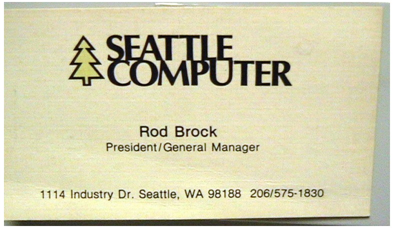
REPÚBLICA PORTUGUESA

UNIVERSIDADE NOVA DE LISBOA

CARTA DE CURSO

GRAU DE LICENCIADO

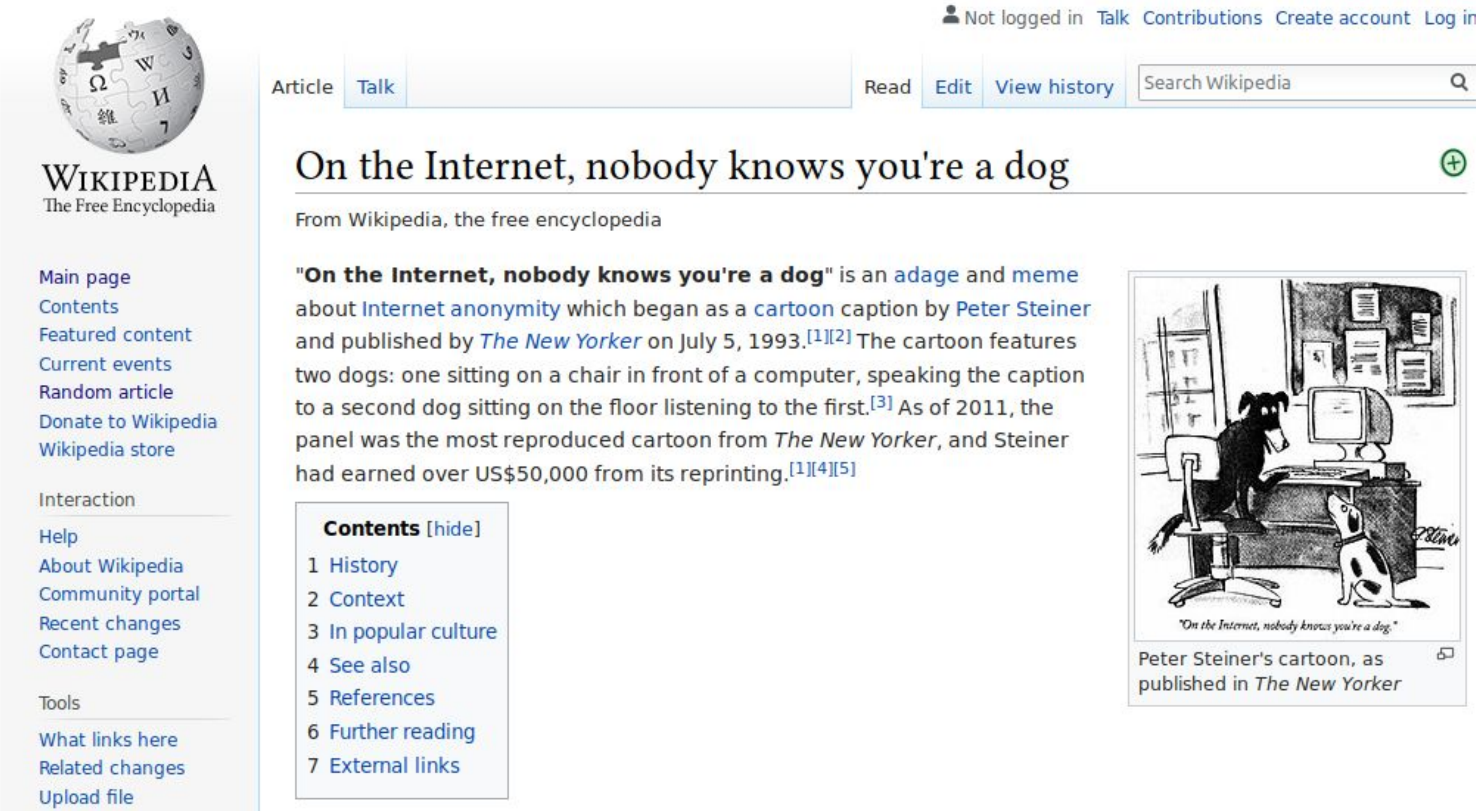
[illegible]



SEATTLE COMPUTER

Rod Brock
President/General Manager

1114 Industry Dr. Seattle, WA 98188 206/575-1830



On the Internet, nobody knows you're a dog

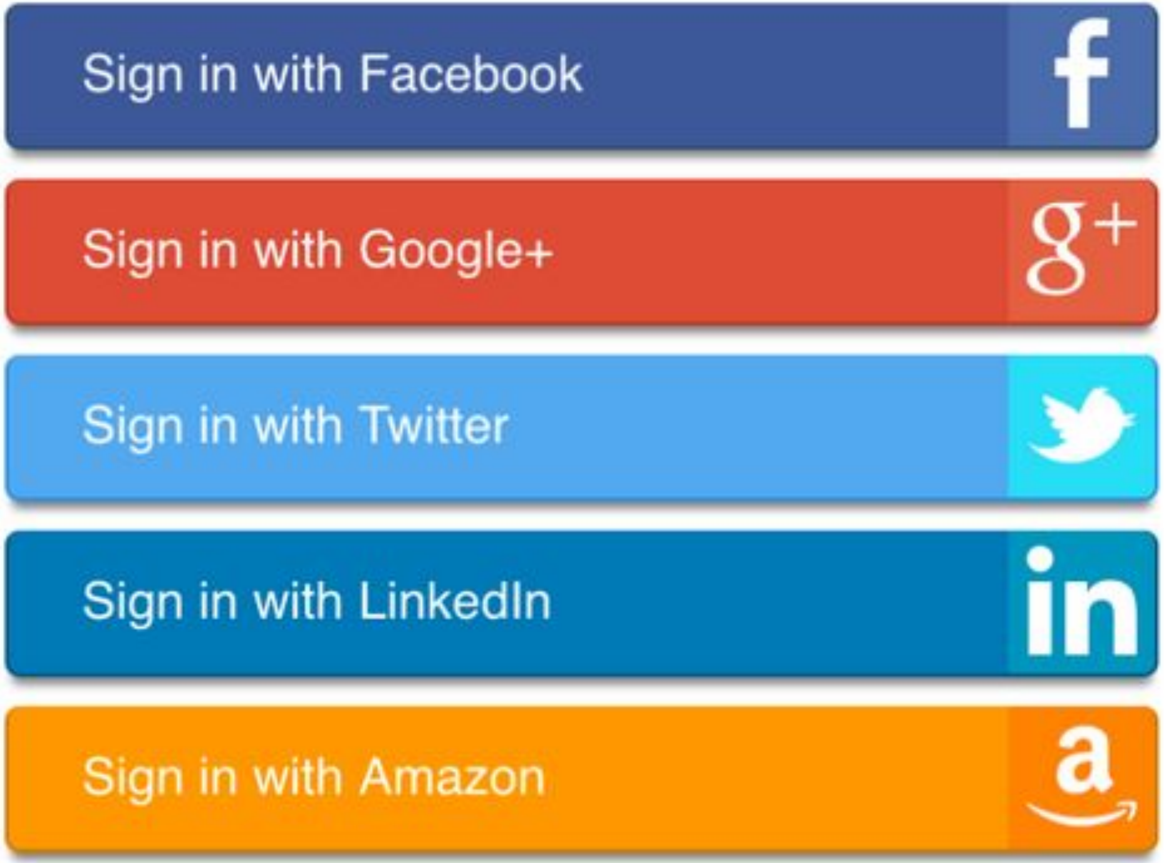
From Wikipedia, the free encyclopedia

"**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]

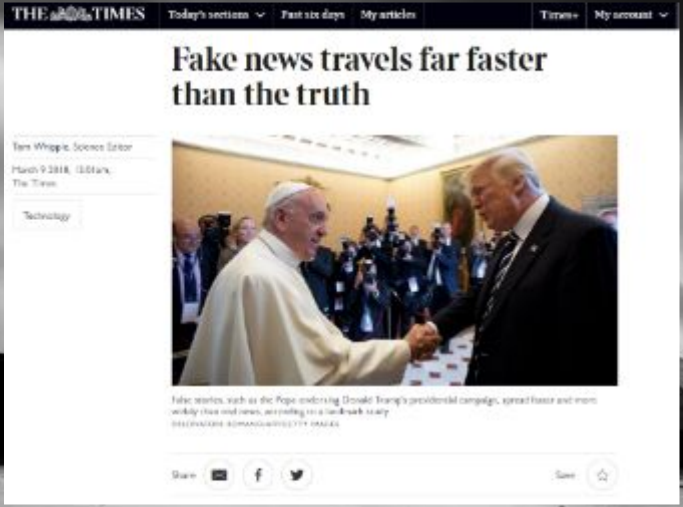
Peter Steiner's cartoon, as published in *The New Yorker*

Contents [hide]

Digital Identity



AND INTRODUCED TREMENDOUS PROBLEMS



Fake news travels far faster than the truth

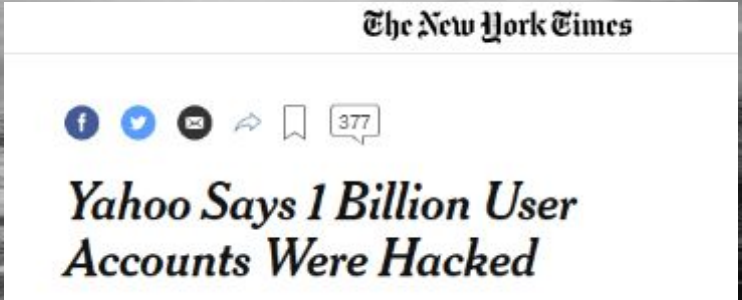
Tom Whipple, Science Editor

March 9 2018, 12:01am,
The Times

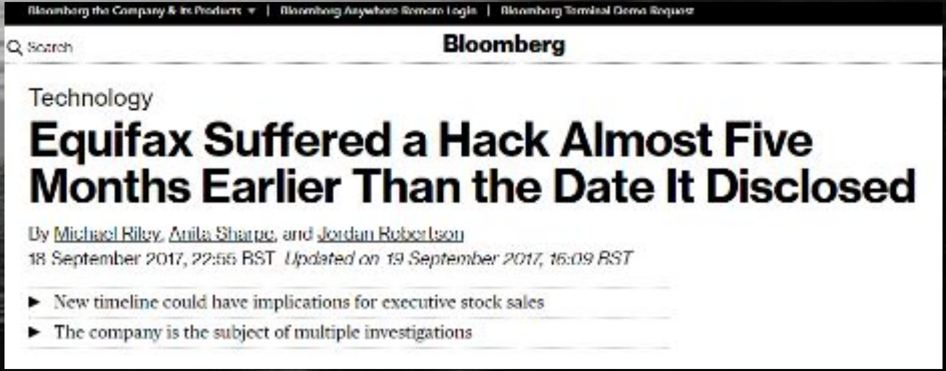
Technology

False stories, such as the Pope endorsing Donald Trump's presidential campaign, spread faster and more widely than real news, according to a landmark study

OSSERVATORE ROMANO/AFP/GETTY IMAGES



Yahoo Says 1 Billion User Accounts Were Hacked


Bloomberg the Company & Its Products ▾ | Bloomberg Anywhere Remote Login | Bloomberg Terminal Demo Request
Search
Bloomberg

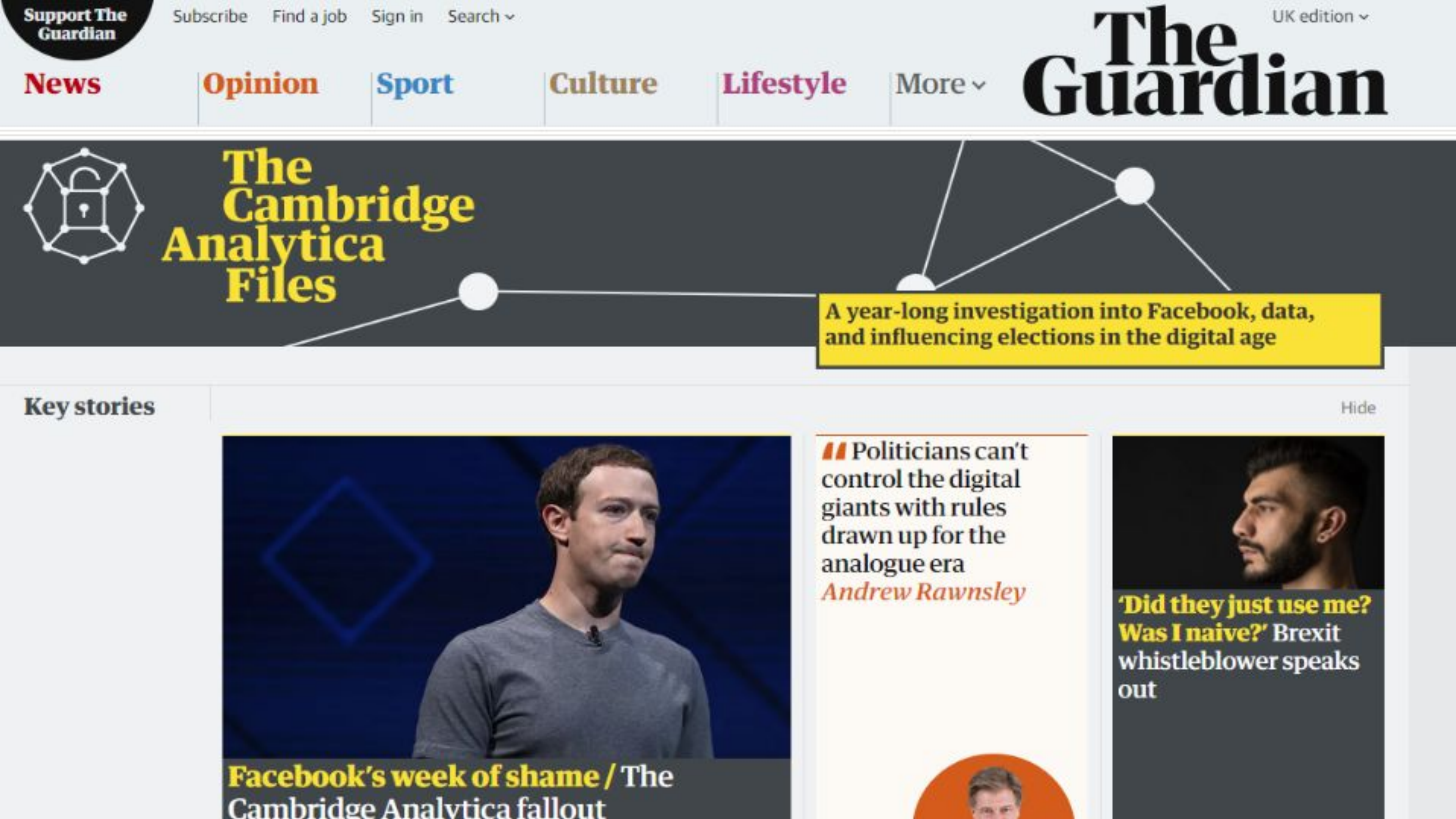
Technology

Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed

By Michael Riley, Anita Sharpe, and Jordan Robertson

18 September 2017, 22:55 BST *Updated on 19 September 2017, 16:09 BST*

- New timeline could have implications for executive stock sales
- The company is the subject of multiple investigations



The Cambridge Analytica Files

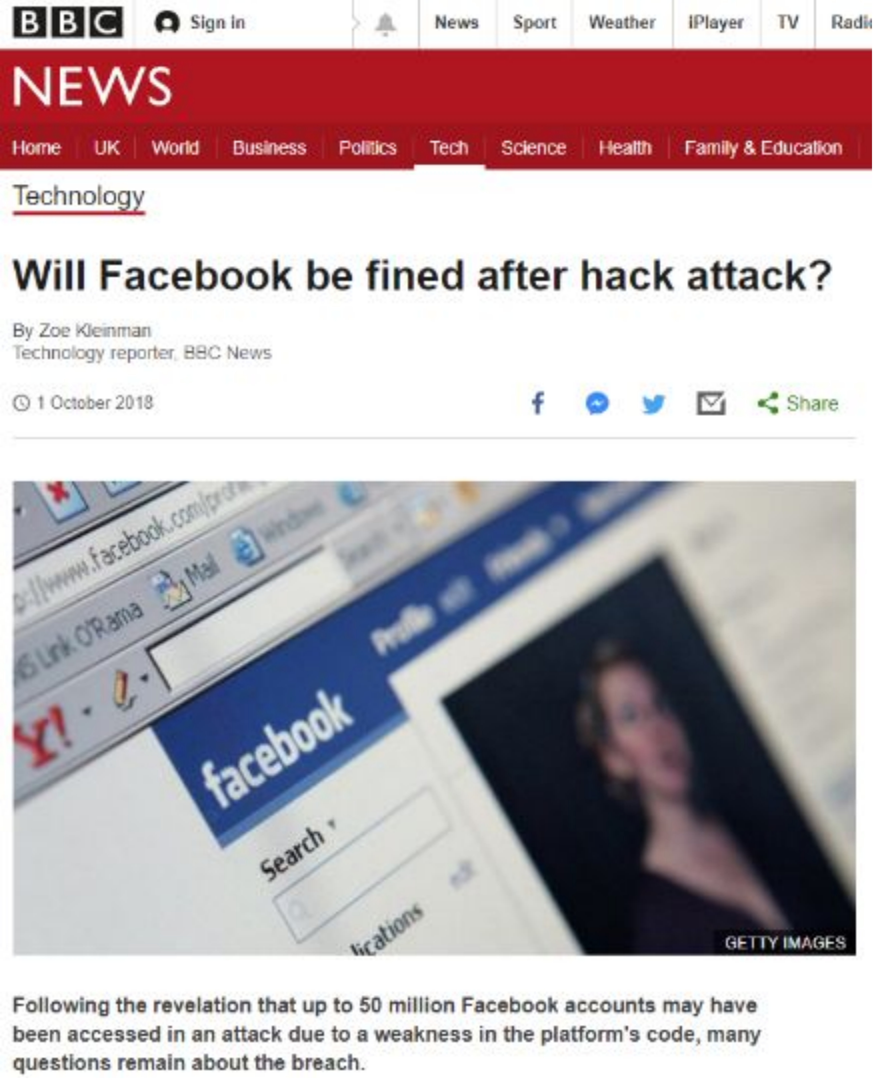
A year-long investigation into Facebook, data, and influencing elections in the digital age

Key stories

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 Rawnsley*

'Did they just use me? Was I naive?' Brexit whistleblower speaks out

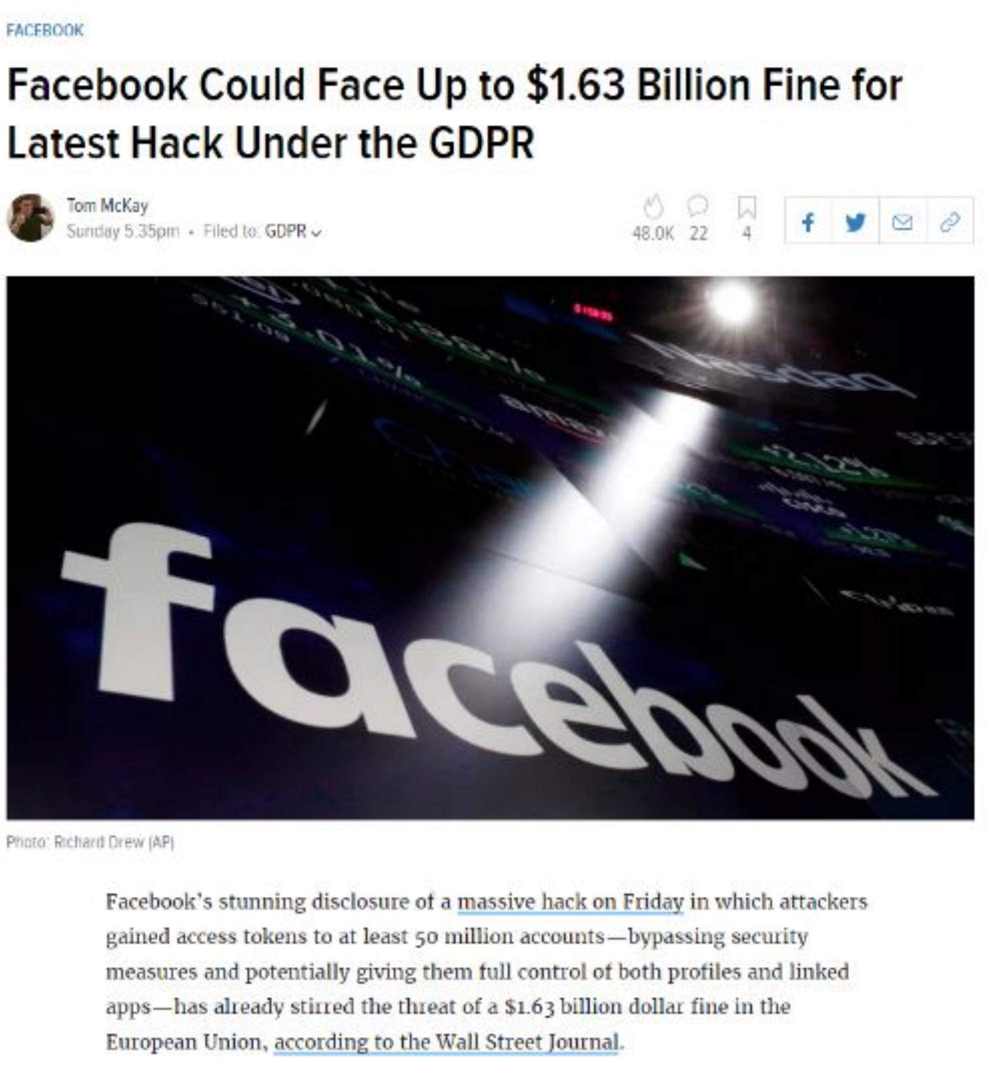


Will Facebook be fined after hack attack?

By Zoe Kleinman
Technology reporter, BBC News

1 October 2018

Following the revelation that up to 50 million Facebook accounts may have been accessed in an attack due to a weakness in the platform's code, many questions remain about the breach.



Facebook Could Face Up to $1.63 Billion Fine for Latest Hack Under the GDPR

Tom McKay
Sunday 5:35pm · Filed to: GDPR

Photo: Richard Drew (AP)

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
http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Also Known As

User-Centric Identity

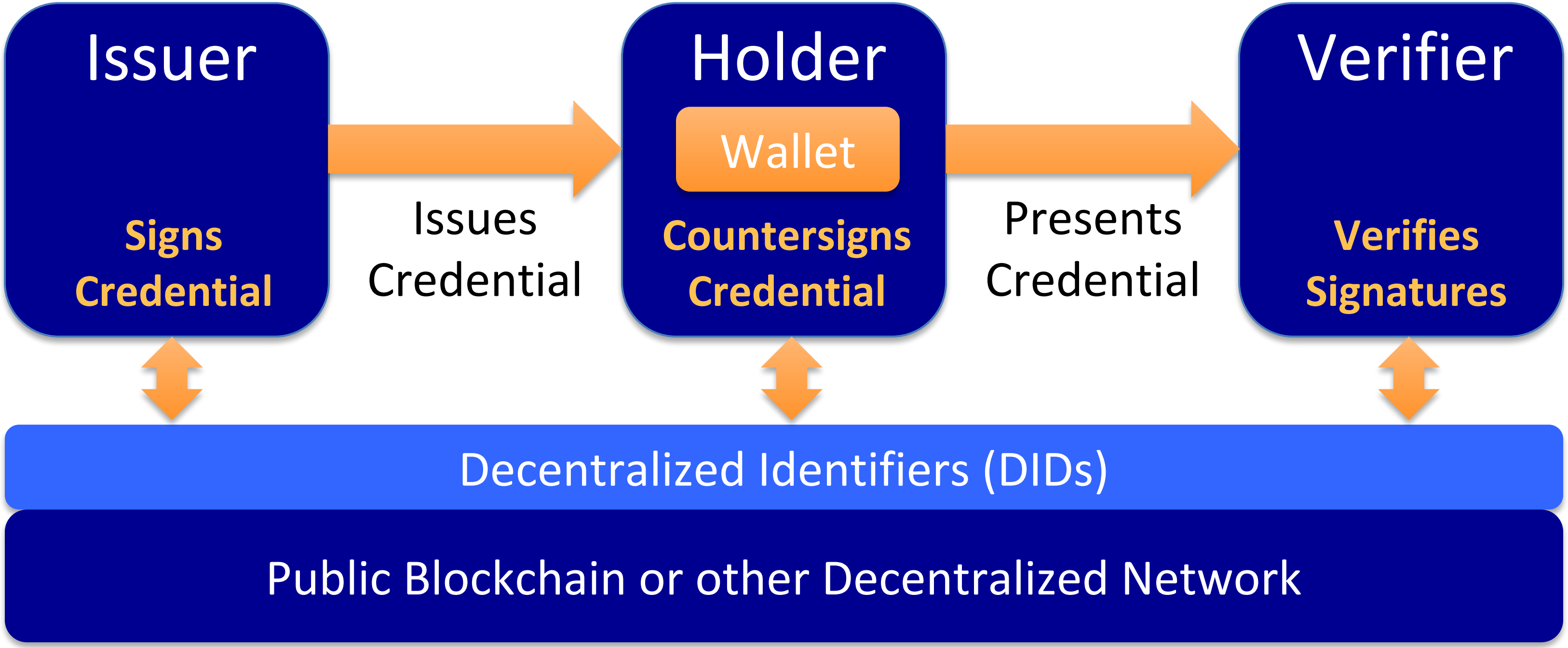
User-Controlled Identity

User-Owned Identity

Bring Your Own Identity

Verifiable Credentials

W3C Verifiable Credentials Ecosystem



Issuer

Signs Credential

Issues Credential

Holder

Wallet

Countersigns Credential

Presents Credential

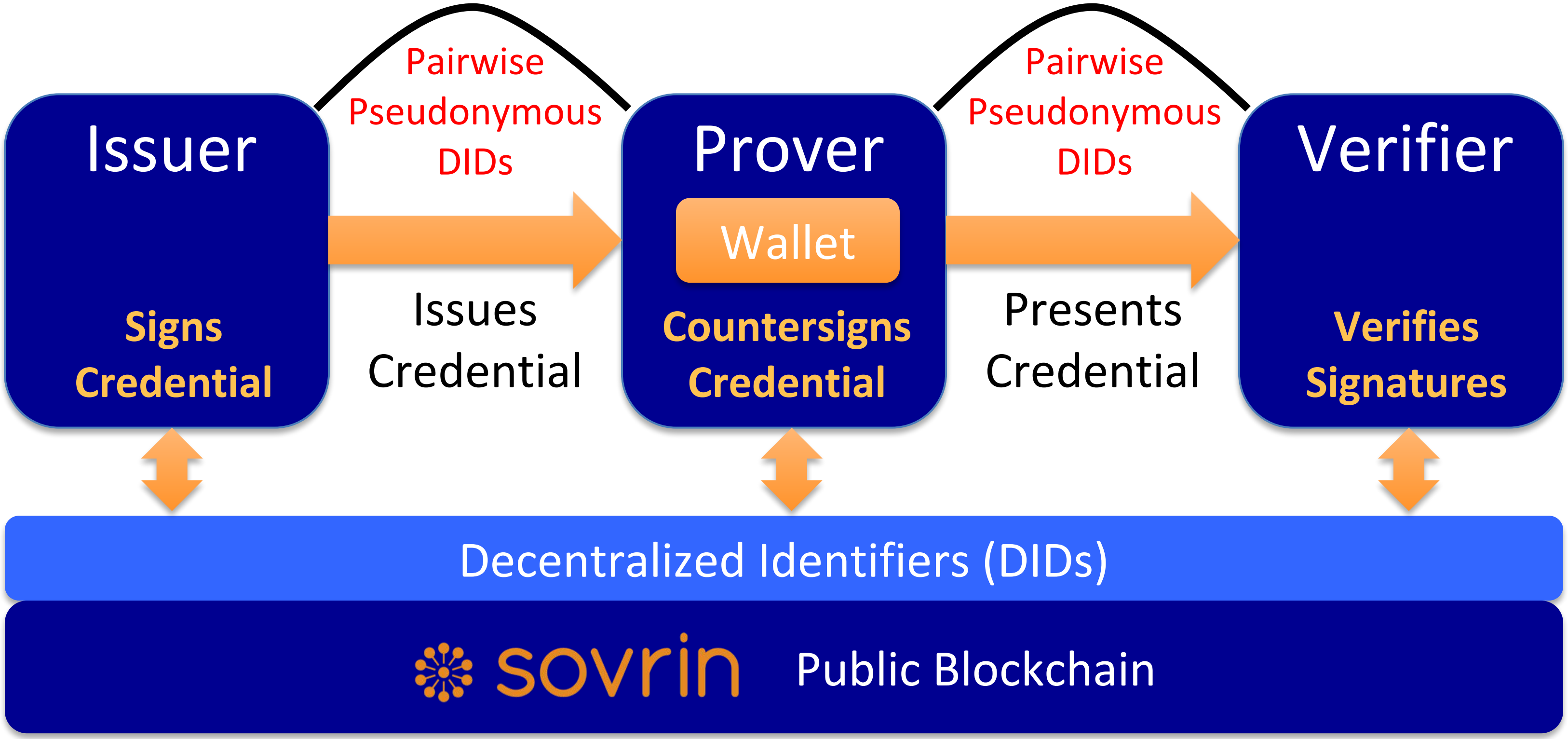
Verifier

Verifies Signatures

Decentralized Identifiers (DIDs)

Public Blockchain or other Decentralized Network

Sovrin Verifiable Credentials Ecosystem



Issuer

Signs Credential

Pairwise Pseudonymous DIDs

Issues Credential

Prover

Wallet

Countersigns Credential

Pairwise Pseudonymous DIDs

Presents Credential

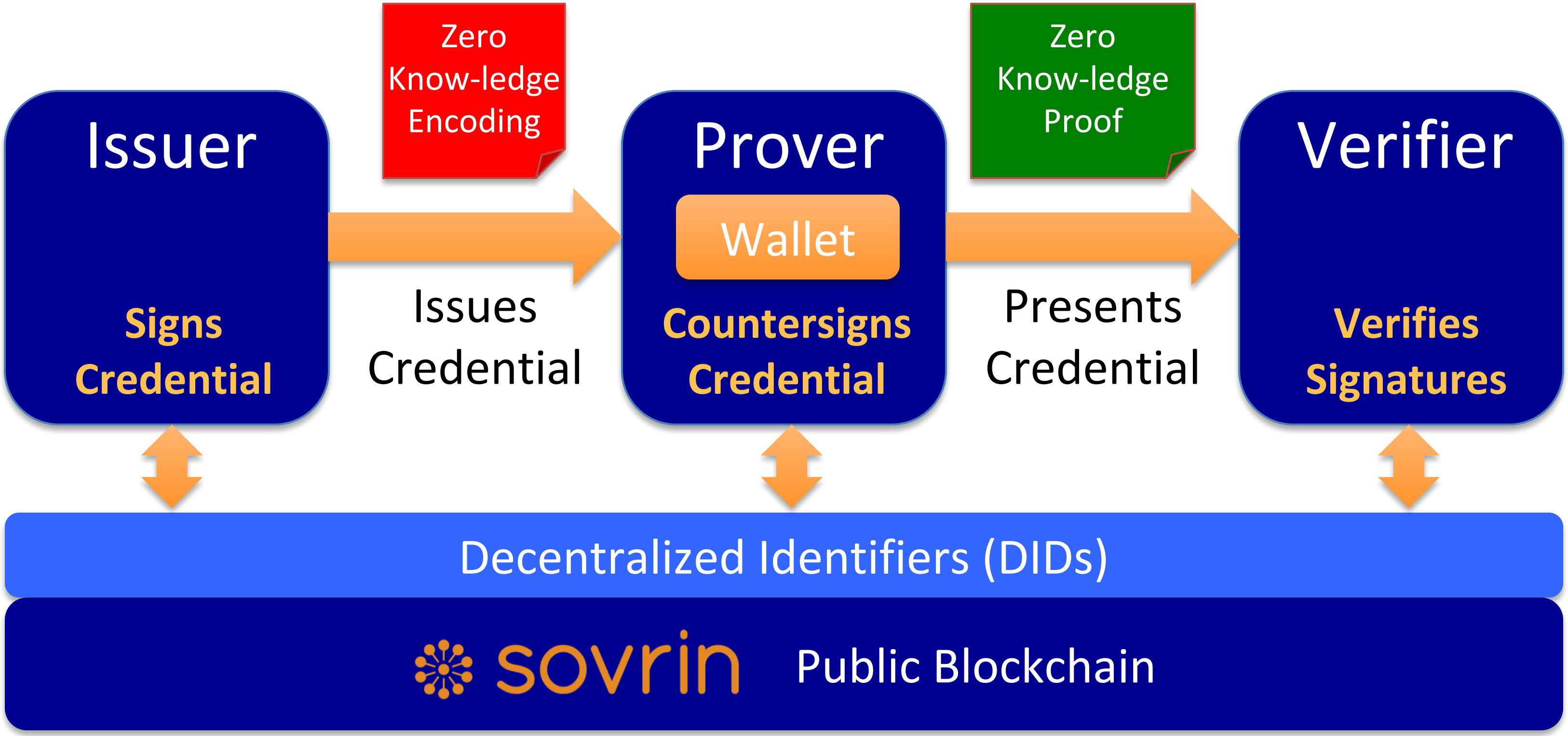
Verifier

Verifies Signatures

Decentralized Identifiers (DIDs)

sovrin Public Blockchain

Sovrin Verifiable Credentials Ecosystem



Zero Know-ledge Encoding

Zero Know-ledge Proof

Issuer

Signs Credential

Issues Credential

Prover

Wallet

Countersigns Credential

Presents Credential

Verifier

Verifies Signatures

Decentralized Identifiers (DIDs)

sovrin Public Blockchain

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

Connect to finalize

Connecting to:

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:
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 Tiger Veterinarians

Claim:
Richard Esplin is a customer of our business in good standing.

Date: December 15, 2018

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:
Utah Division of Motor Vehicles

Claim:
Richard Esplin is licensed to drive

Address, Birthdate, Restrictions …

Issue Date: December 15, 2018

Credential from:
Richard Esplin

Claim:

- Older than 18
  Provided by: Utah Department of Motor Vehicles
- Permit for owning an exotic species
  Provided by:
  Salt Lake City, Utah, United States
- Proof of tiger handler training
  Provided by:
  Utah State University, United States
- Certification of veterinary availability
  Provided by:
  Utah Tiger Veterinarians

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

Revoked

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

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

Revoked

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

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 a porch delivery box in my possession

Number of times:
1

Date range:
January 16, 2019
to
January 31, 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

Note:
The author does not advocate household tiger ownership.

No tigers were harmed in the making of this story.

Purpose-Built Public Blockchain

sovrin

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

HYPERLEDGER INDY

HYPERLEDGER

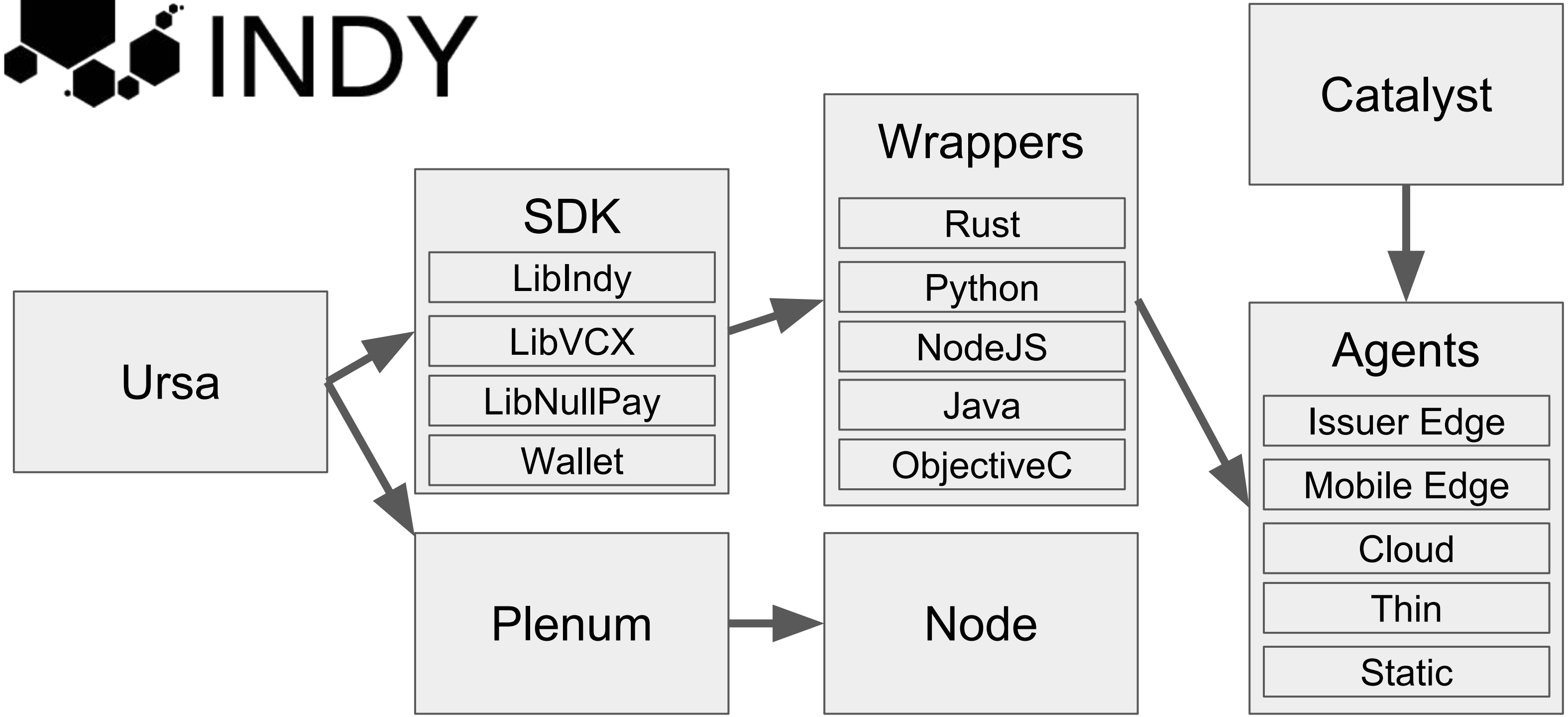
THE LINUX FOUNDATION

Public Permissioned Blockchain

Custom built for Identity

RBFT Consensus

Hyperledger Indy



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

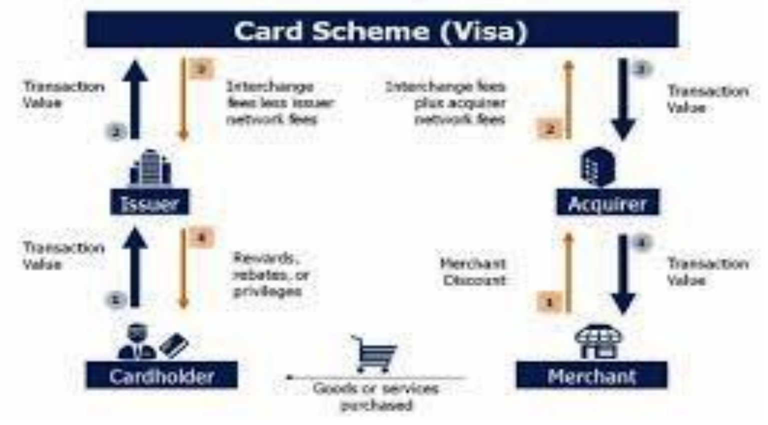
The BLT

Business

Legal

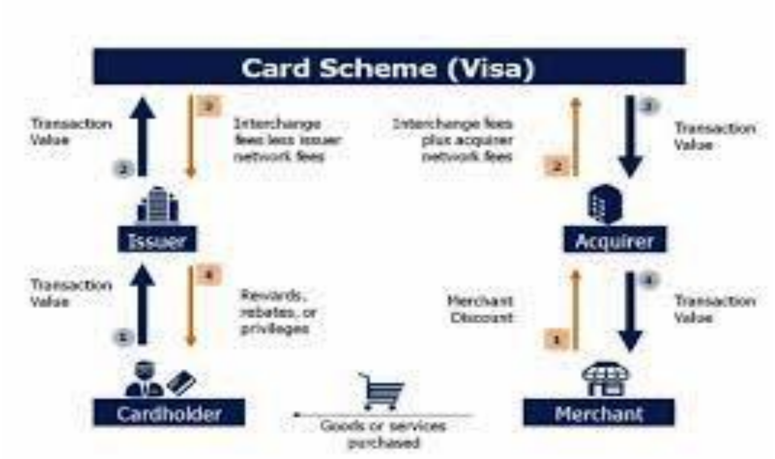
Technical

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

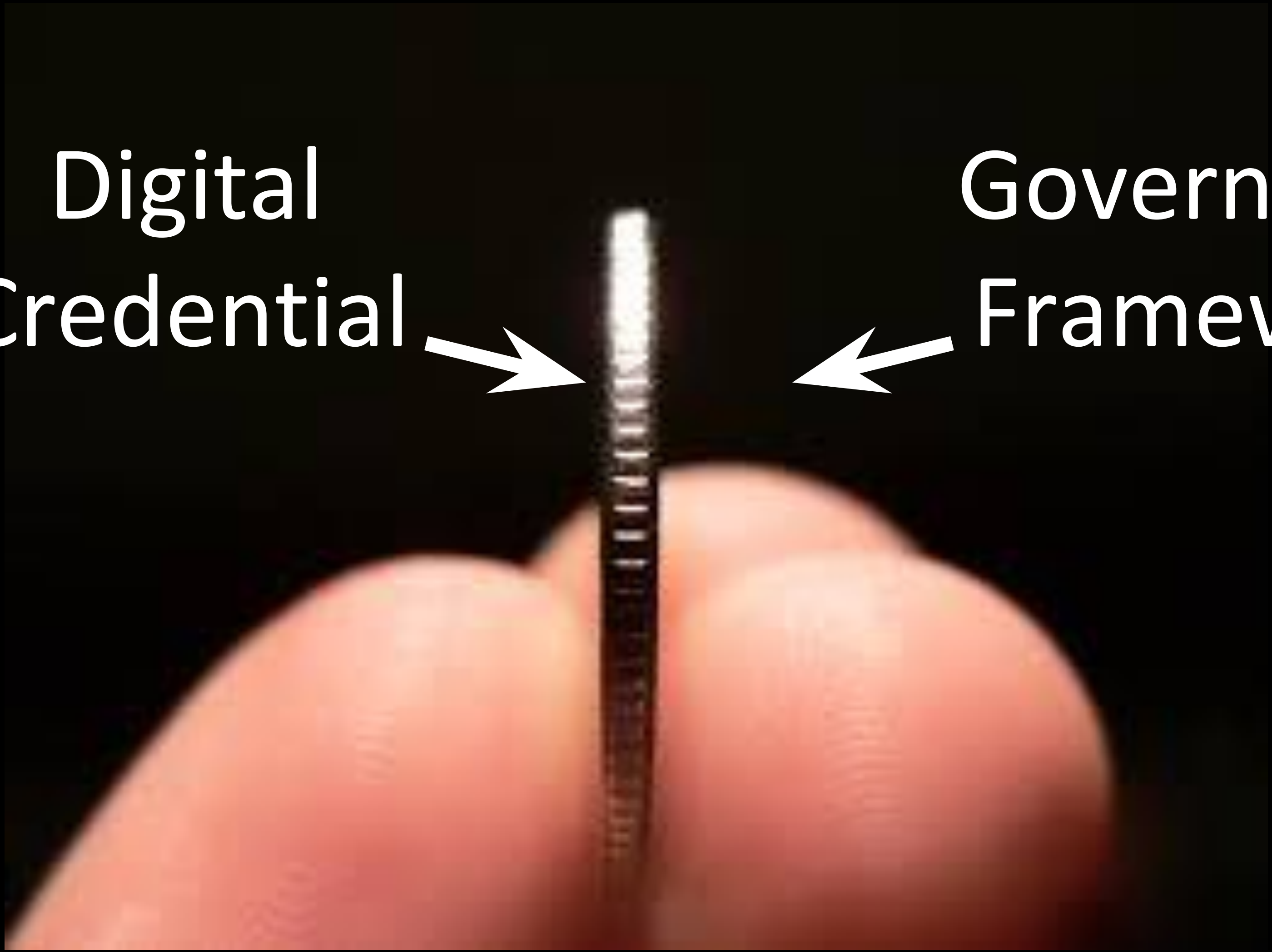
Digital Credential



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.

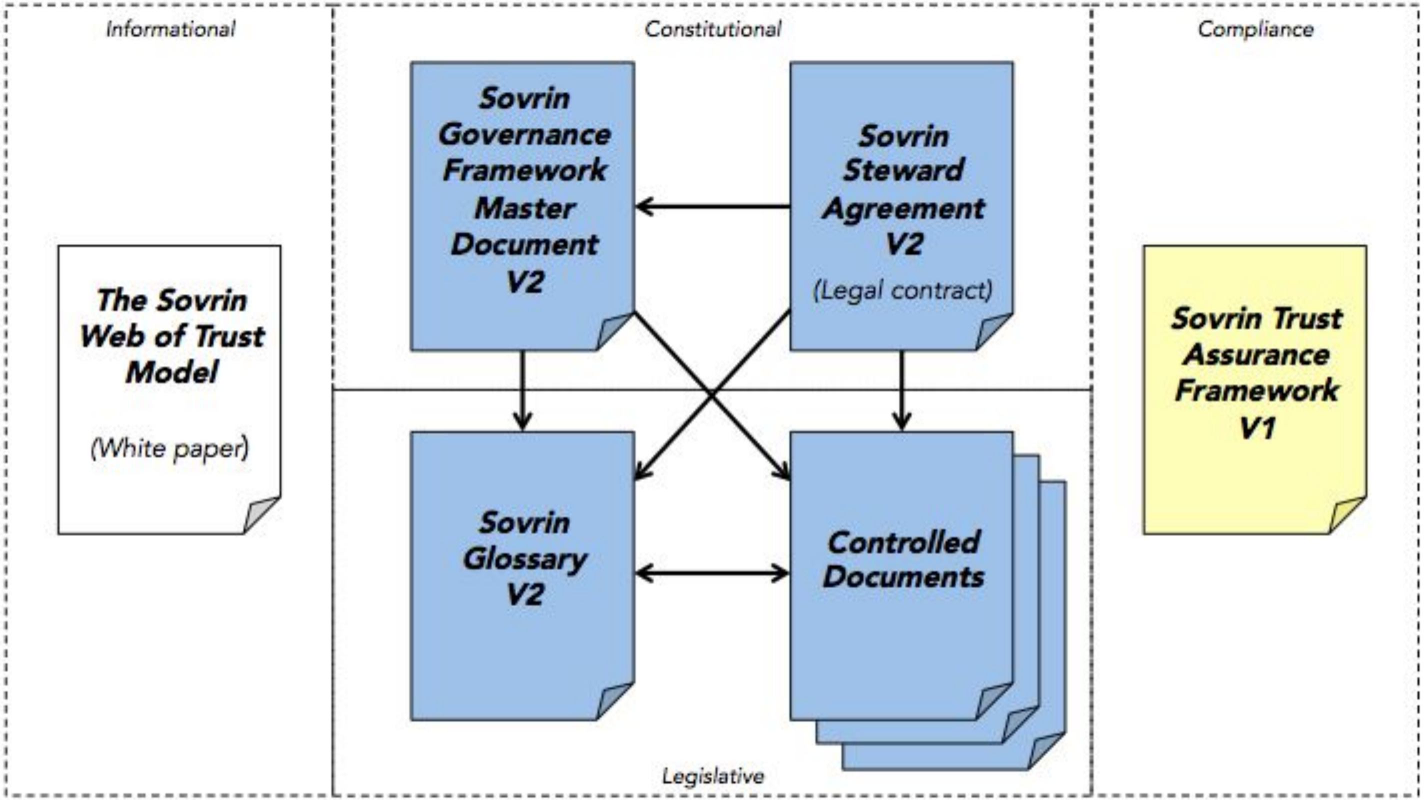
— Drummond Reed
Chief Trust Officer, Evernym



Digital Credential

Governance Framework

Sovrin Governance Framework



Informational
Constitutional
Compliance
The Sovrin Web of Trust Model
(White paper)
Sovrin Governance Framework Master Document V2
Sovrin Steward Agreement V2
(Legal contract)
Sovrin Trust Assurance Framework V1
Sovrin Glossary V2
Controlled Documents
Legislative

sovrin

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