Self Sovereign Identity

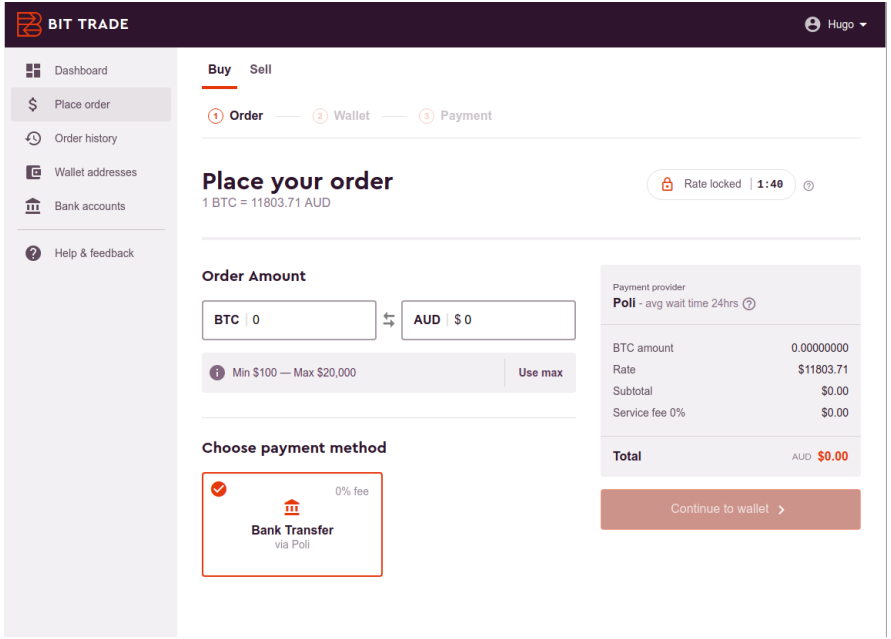
Converging forces, challenges and opportunities

Hugo O'Connor
Co-founder and Blockchain Engineer

BIT TRADE LABS

How I became interested in Identity

- Spot exchange for BTC
- No chargebacks
- Attractive to fraudsters
- Identity is broken



What is Self Sovereign Identity?

Definition: Sovereign

Cambridge English Dictionary: having the highest power or being completely independent

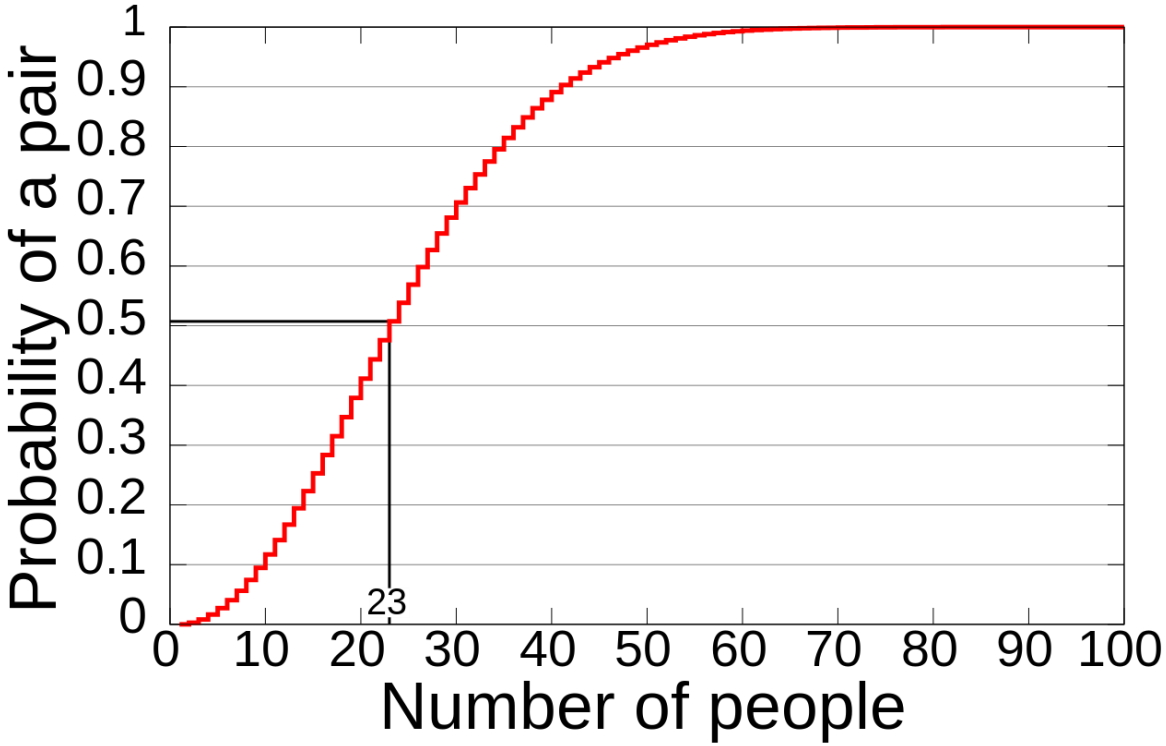
Merriam Webster Dictionary: one that exercises supreme authority within a limited sphere

Definition: Identity

Cambridge English Dictionary: who a person is, or the qualities of a person or group that make them **different** from others

Merriam Webster Dictionary: the **distinguishing** character or personality of an individual

The Birthday Problem



Definition: Self Sovereign Identity

A system for user control of personal information, requiring consent to share subsets of that data with third parties, and a web of signed claims to build trust.

Agenda

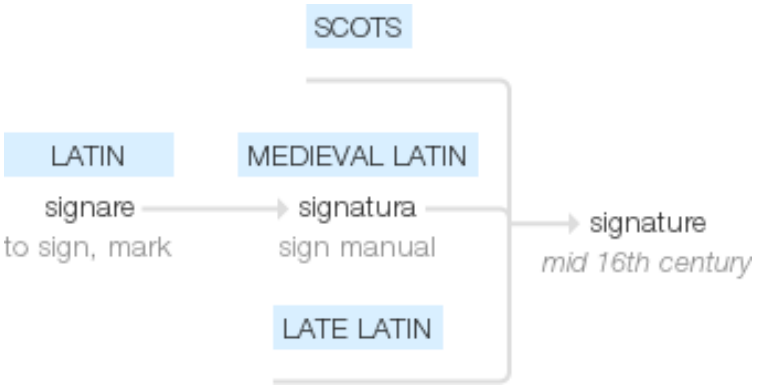
1. Historical Background
2. Evolving Technologies
3. The Human Story
4. Converging Forces:
    a. Human
    b. Business
    c. Legal
    d. Technical
5. Current Trials
6. Proposed Solution
7. Demo
8. Questions

Historical Background

An Ancient Problem

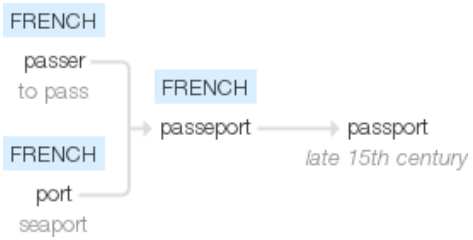
[1] Why Cylinder Seals? Engraved Cylindrical Seal Stones of the Ancient Near East, Fourth to First Millennium B.C. Edith Porada, The Art Bulletin, Vol. 75, No. 4 (Dec., 1993), pp. 563-582

Ancient Infrastructure



[2] Why Do We Sign for Things?, http://www.npr.org/templates/transcript/transcript.php?storyId=345820789

Ancient Infrastructure



[3] A Brief History of the Passport http://www.theguardian.com/travel/2006/nov/17/travelnews

Technologies Evolving

Identity on the Internet

TCP/IP - computers are distinguished by IP addresses

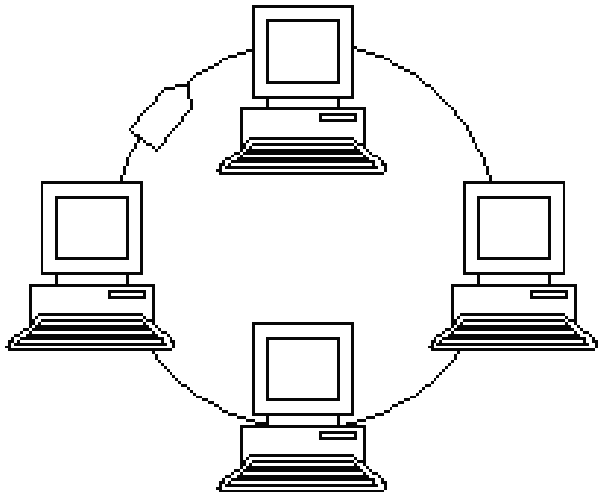
An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

2001:0DB8:AC10:FE01:: Zeroes can be omitted

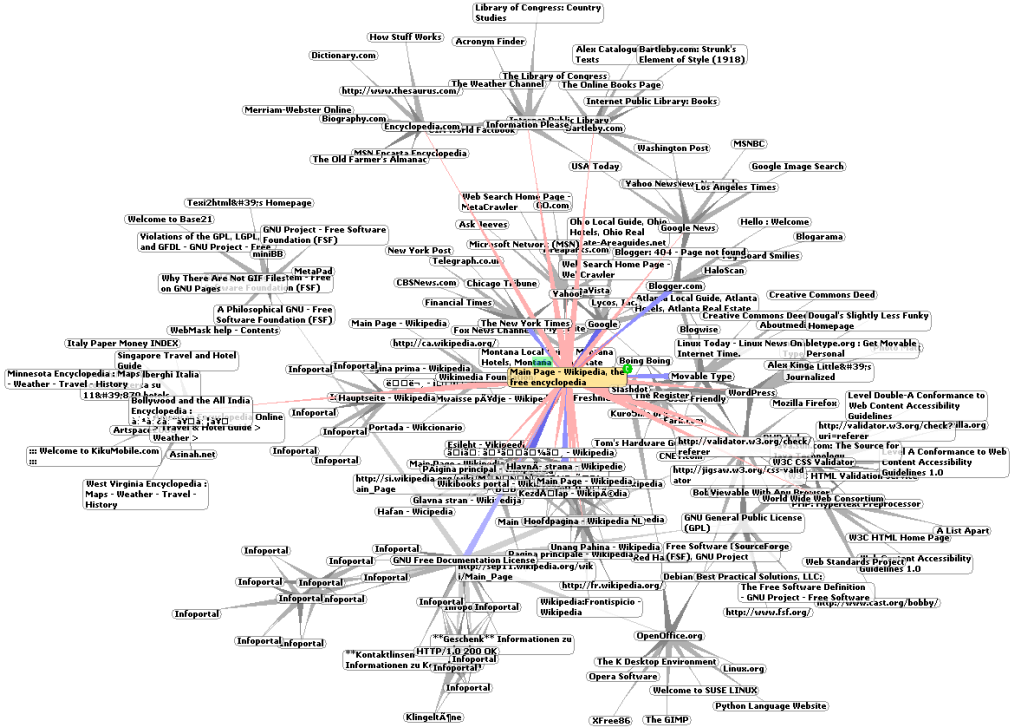
0010000000000001:0000110110111000:1010110000010000:1111111000000001:

0000000000000000:0000000000000000:0000000000000000:0000000000000000



URIs and the World Wide Web

- Resources identified with URIs
- Hyperlinks between documents



Identity on the Internet

MAC addresses - identifiers for devices

The Missing Piece of Internet Infrastructure

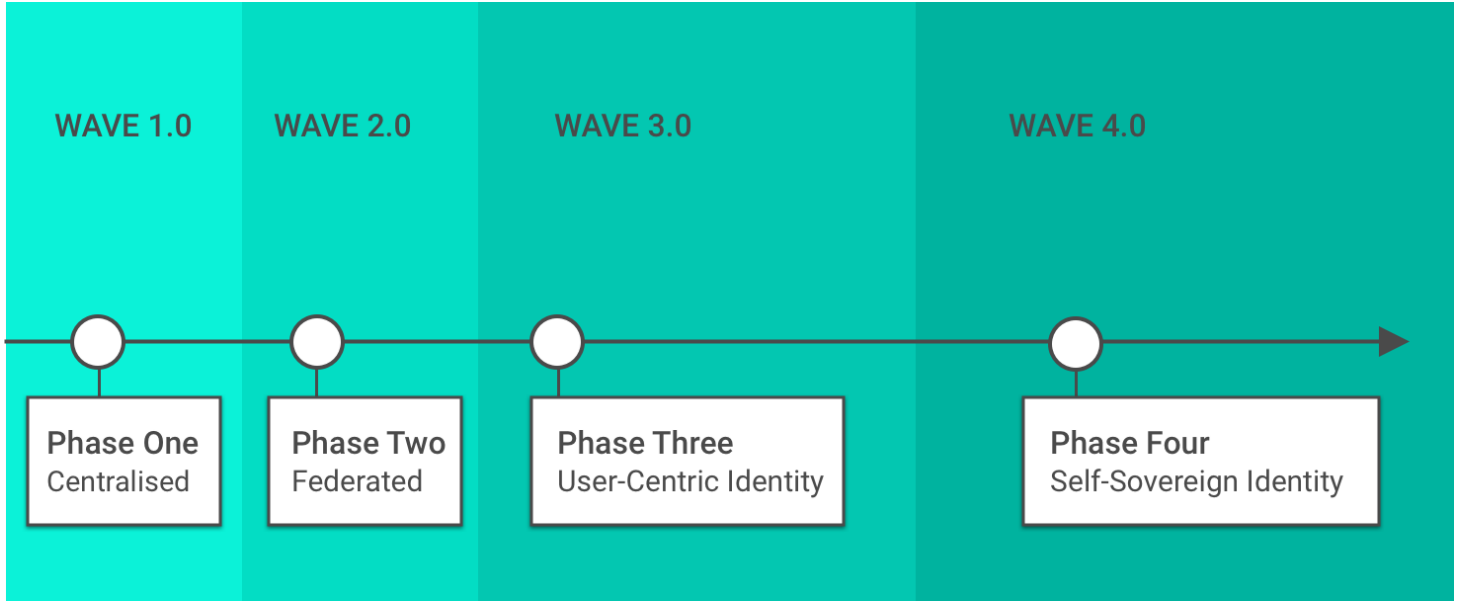
Who is behind the keyboard?

"On the Internet, nobody knows you're a dog."

Image from *The New Yorker* cartoon by Peter Steiner, 1993.

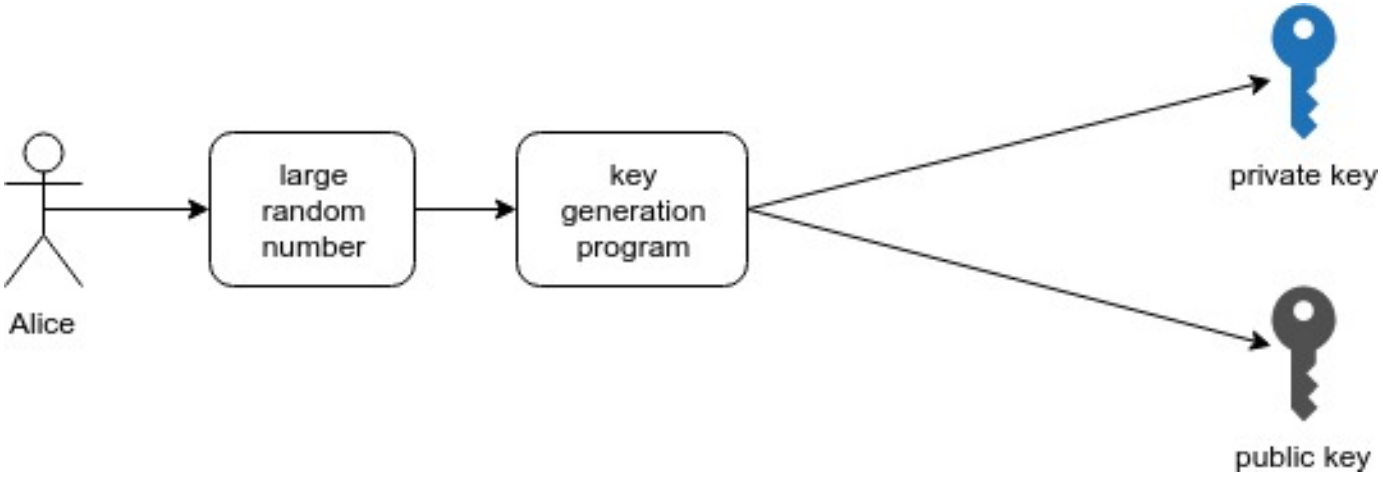
Path to Self Sovereign Identity

Evolution of identity in the past 30 years



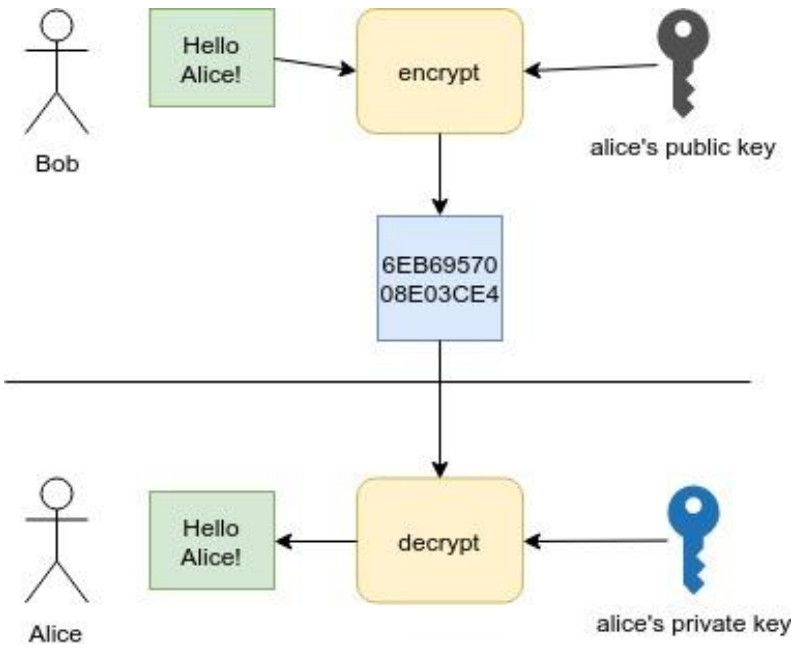
Asymmetric Cryptography - A Primer

- Key generated.
- Public key shared openly.
- Private key kept secret.



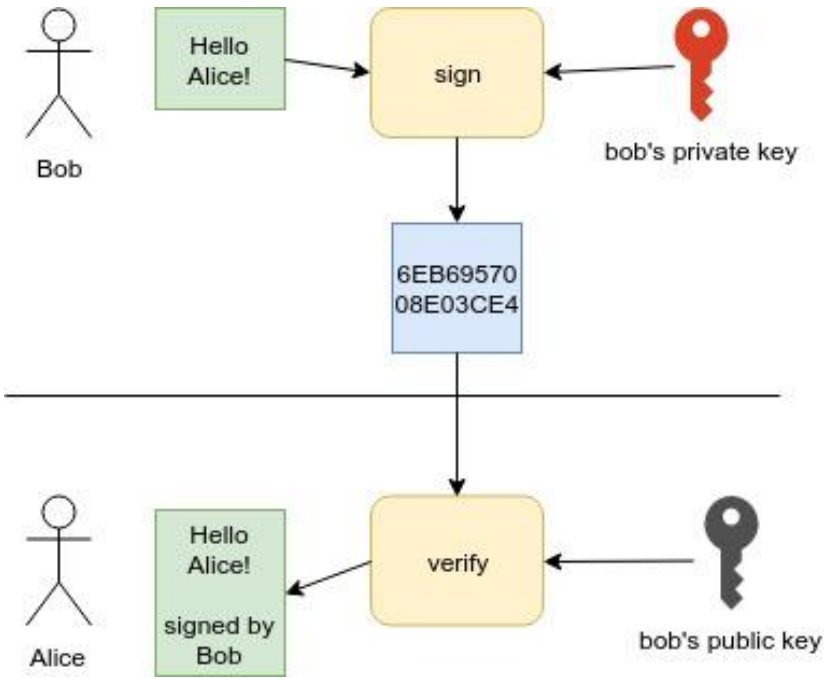
Asymmetric Cryptography - A Primer

- Bob encrypts to Alice's pub key
- Alice decrypts with her priv key



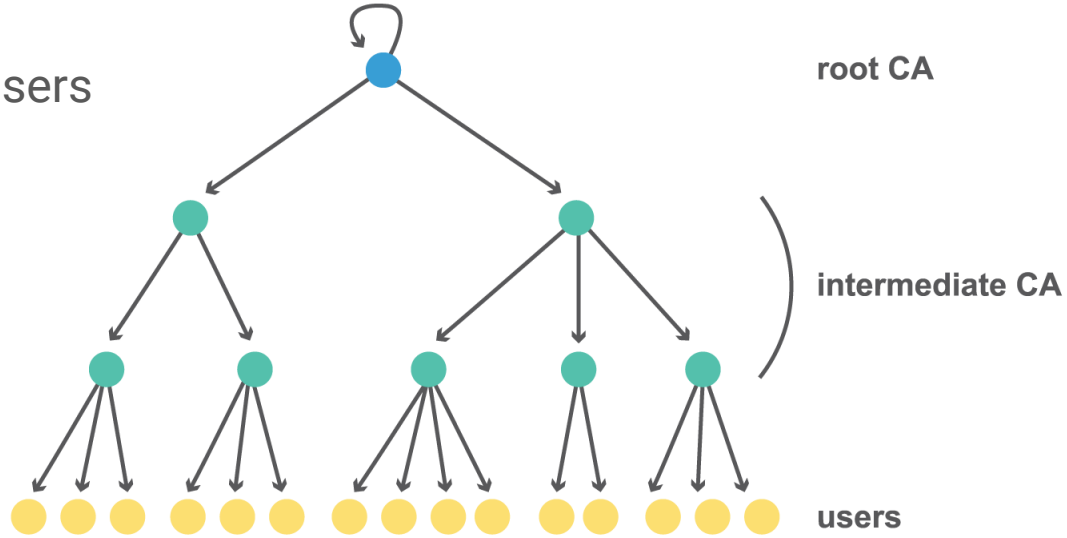
Asymmetric Cryptography - A Primer

- Bob signs message with his priv key
- Alice verifies with Bob's pub key



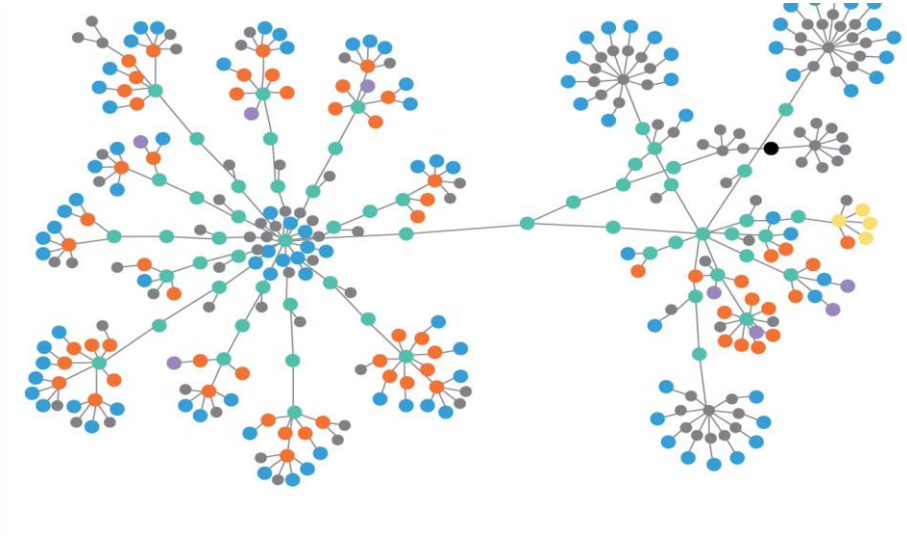
X509

- One direction
- CAs vulnerable
- Users cannot identify other users



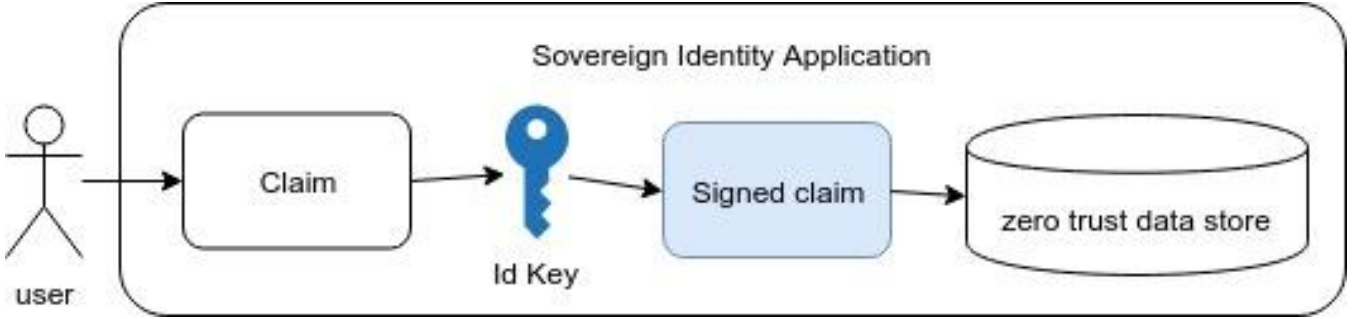
PGPs Web-of-Trust

- directed graph of trust relationships
- each edge represents a key signing event
- each node represents a PGP identity



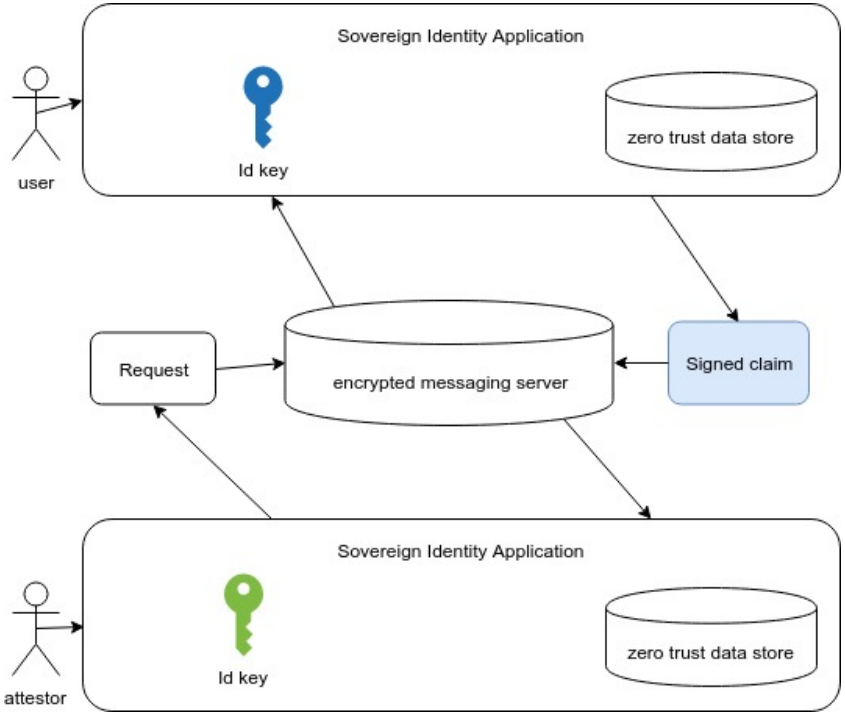
How It Works

- User makes a claim about themselves
- User signs claim with their ID key
- Signed claim is stored in a zero knowledge data store



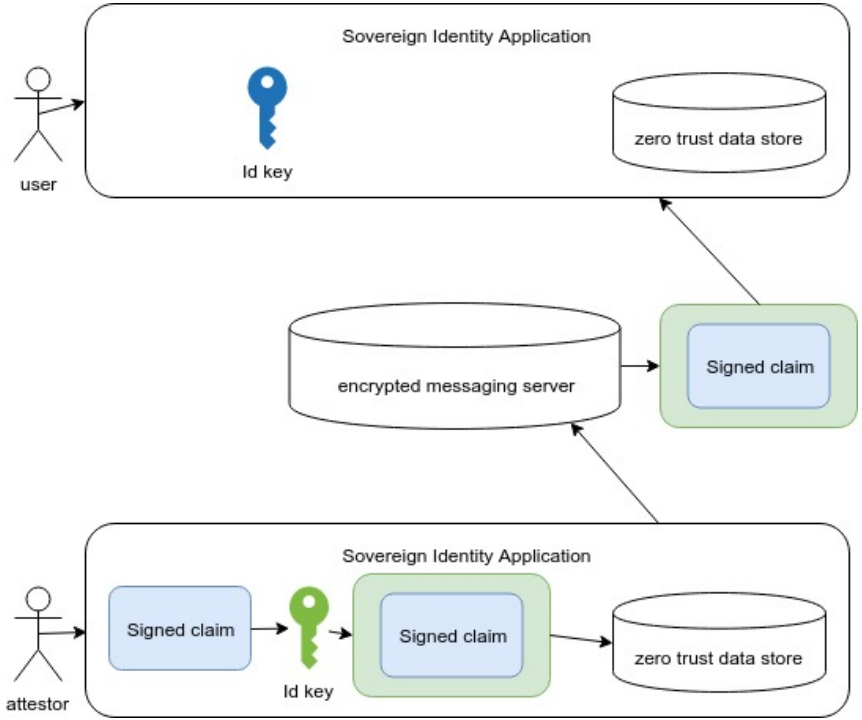
How It Works

- Attestor request certain claim
- Attestor receives and reviews



How It Works

- Attestor signs claim
- Stores a copy and sends to user



The Windhover Principles

- Self-Sovereign Identity & Control of Personal Data.
- Transparent Enforcement and Effective Lite Governance.
- Ensuring Trust and Privacy.
  Open Source Collaboration.

ID3
idcubed.org

The Windhover Principles for Digital Identity, Trust and Data https://idcubed.org/home_page_feature/windhover-principles-digital-identity-trust-data/

Christopher Allen's Principles of Sovereign ID

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

Existence. *Users must have an independent existence*

Control. *Users must control their identities*

Access. *Users must have access to their own data*

Transparency. *Systems and algorithms must be transparent*

Persistence. *Identities must be long-lived*

Portability. *Information and services about identity must be transportable*

Interoperability. *Identities should be as widely usable as possible*

Consent. *Users must agree to the use of their identity*

Minimalization. *Disclosure of claims must be minimized*

Protection. *The rights of users must be protected*

Components of Self Sovereign Identity

Recoverable Public/ Private Key pairs to sign data

Decentralised identifiers - DNS for identities

Zero knowledge data store of personal information

End-to-End Encrypted Communications between IDs

Human Story

Karen, 25, urban professional, Sydney

- Recent Masters Degree graduate
- First year of work, developing skills and competencies
- Applying for a personal loan

Pain Point - Manual Duplicated Processes

- Must upload photos and documents to relying party
- Fill out the same form at multiple banks
- Relying party must check documents against 3rd party verification services
- Cannot easily prove employment history

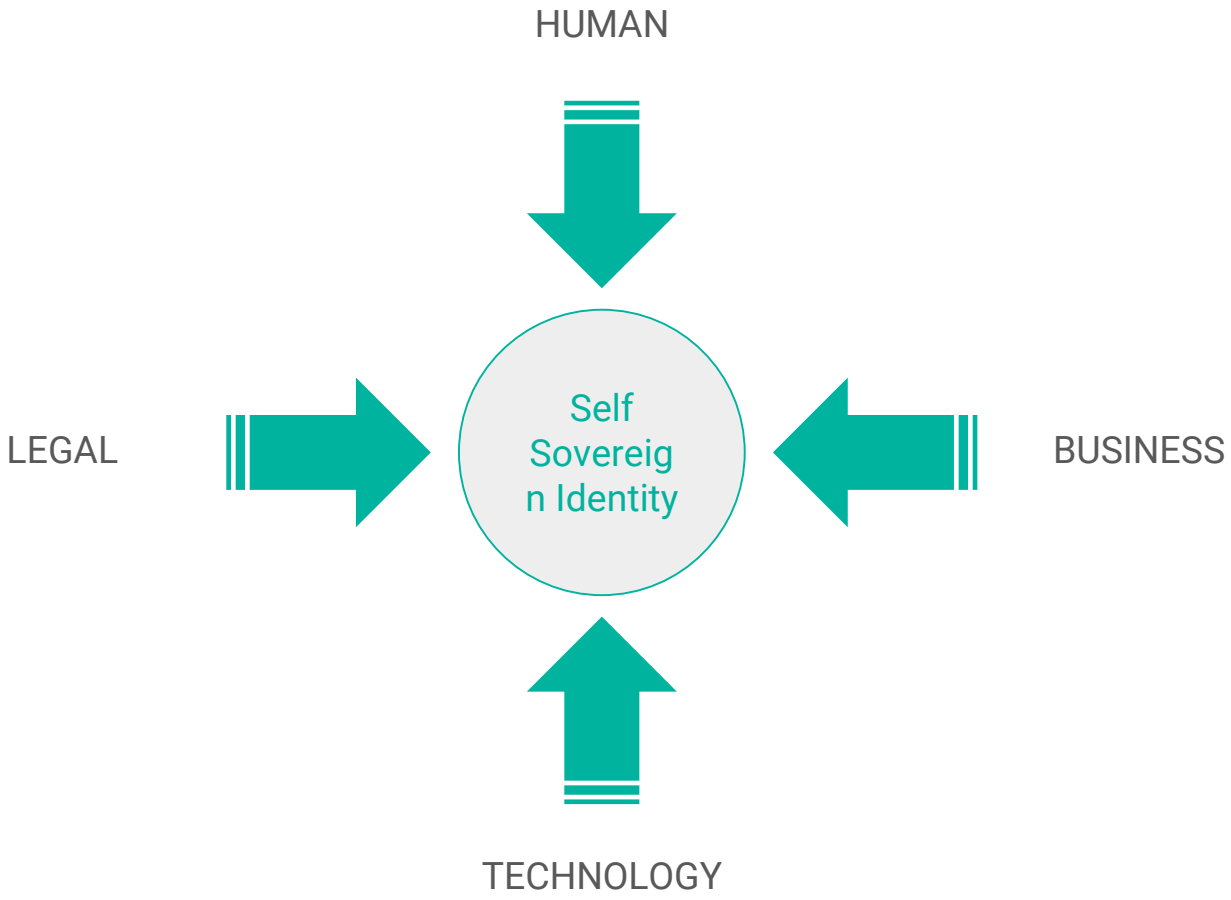
Amena, 27, Syrian refugee in Suruc, Turkey

- Recently fled Kobane after ISIS attacked.
- Only possessions are the clothes on her back.
- No identity documentation.
- Seeking refugee status in Turkey, to establish a new bank account, and seek work.

Pain Point - No Documents to Verify

- Turkish government has no starting point for proving Amena's identity
- Banks cannot verify Amena's identity or her credit worthiness
- Employers cannot verify Amena's work history

Converging forces


HUMAN
LEGAL
Self
Sovereig
n Identity
BUSINESS
TECHNOLOGY


Human

Behaviour and Attitudes

Increasing awareness of surveillance and concerns over privacy (snowden effect, facebook and cambridge analytica, data breaches etc)

Expectations of more personalisation from service providers

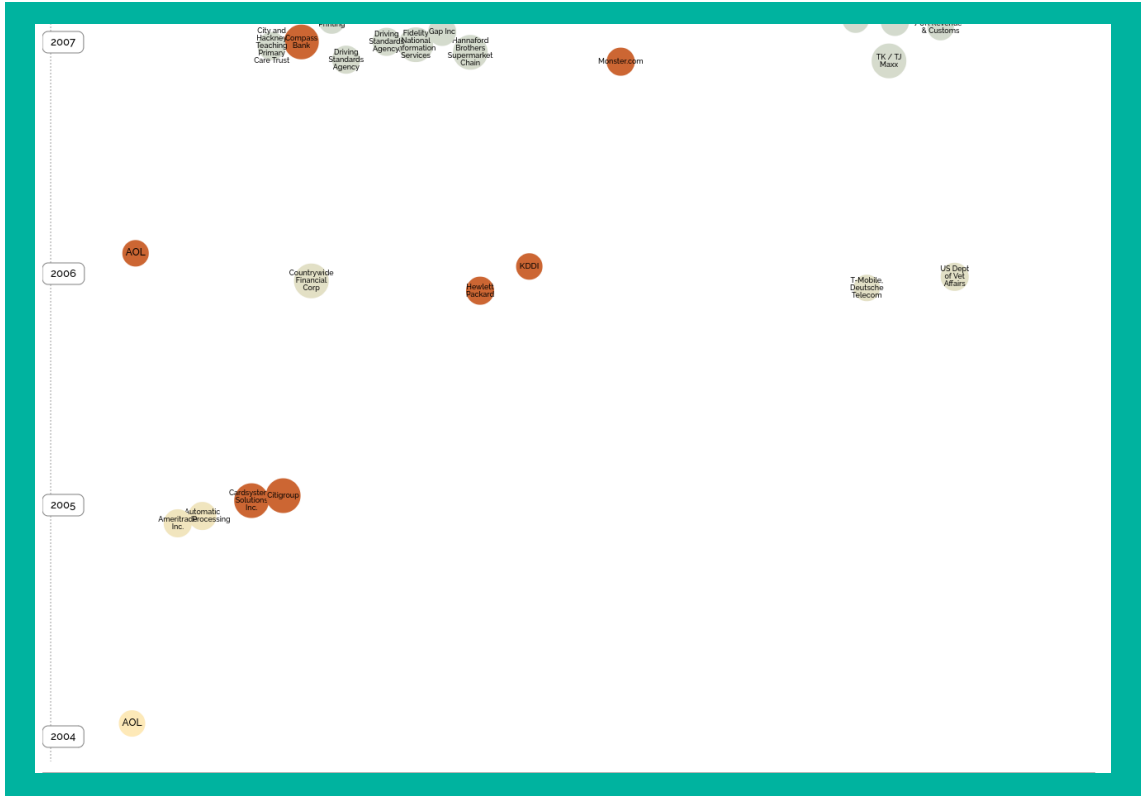
Ad-blockers and online behaviour

Entering of inaccurate data

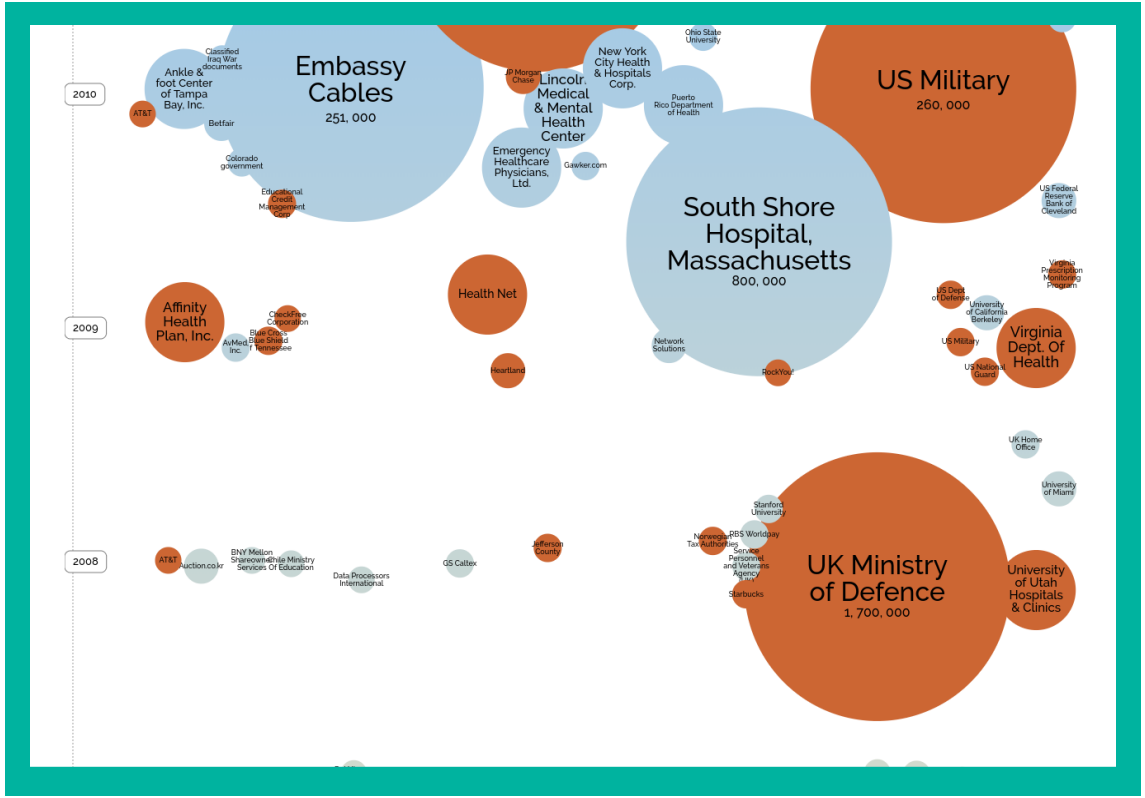
Taking Ownership of Personal Data

- Consumers are increasingly aware of how their personal information is used by companies to advertise products to them.
- Data breaches prove companies cannot be relied upon to secure customer data
- Decentralised technologies offer an alternative paradigm to the issue of ownership.
- Fundamentally, sovereign identity is about giving individuals control over their personal data.

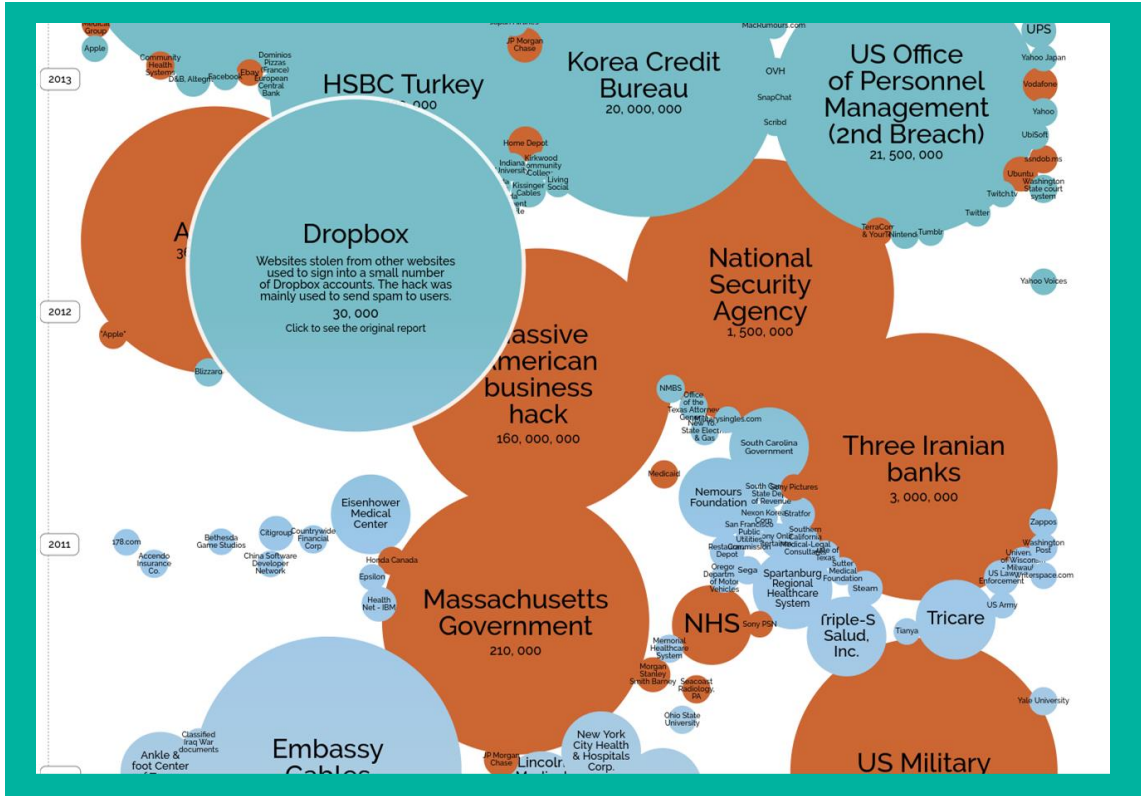
Data Breaches



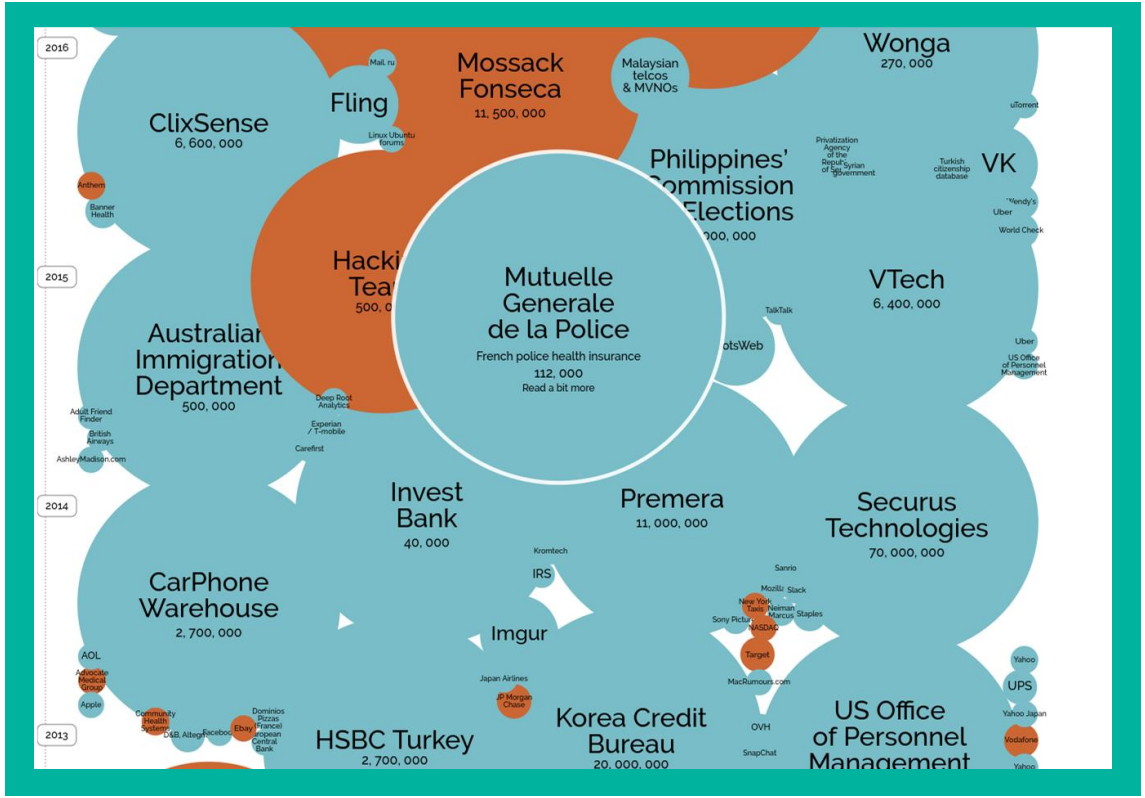
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



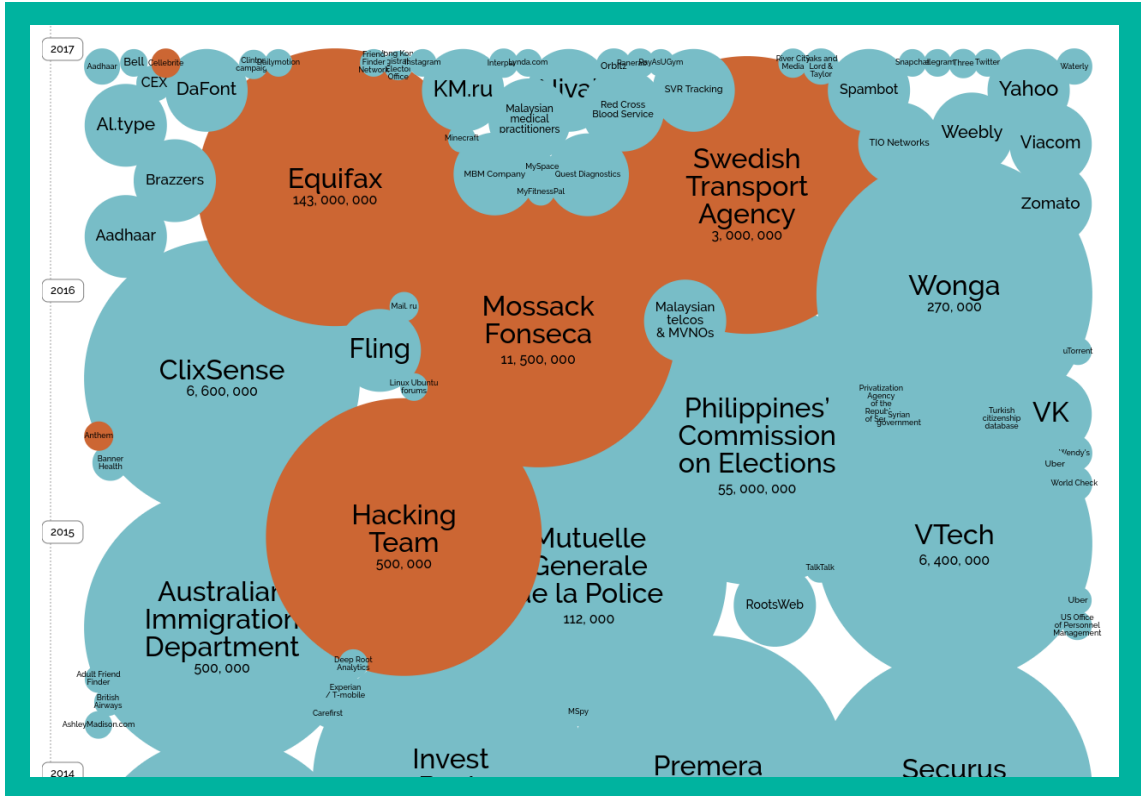
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Example: Equifax Hack

- Hackers stole **145 million** Americans' Social Security numbers, birthdays, driver's license numbers, tax identification numbers, driver's license states and issuance dates, and addresses
- Equifax **stock price dropped 35%** in response

EQUIFAX

Business

Business

Changing business models. "People as the product" no longer viable

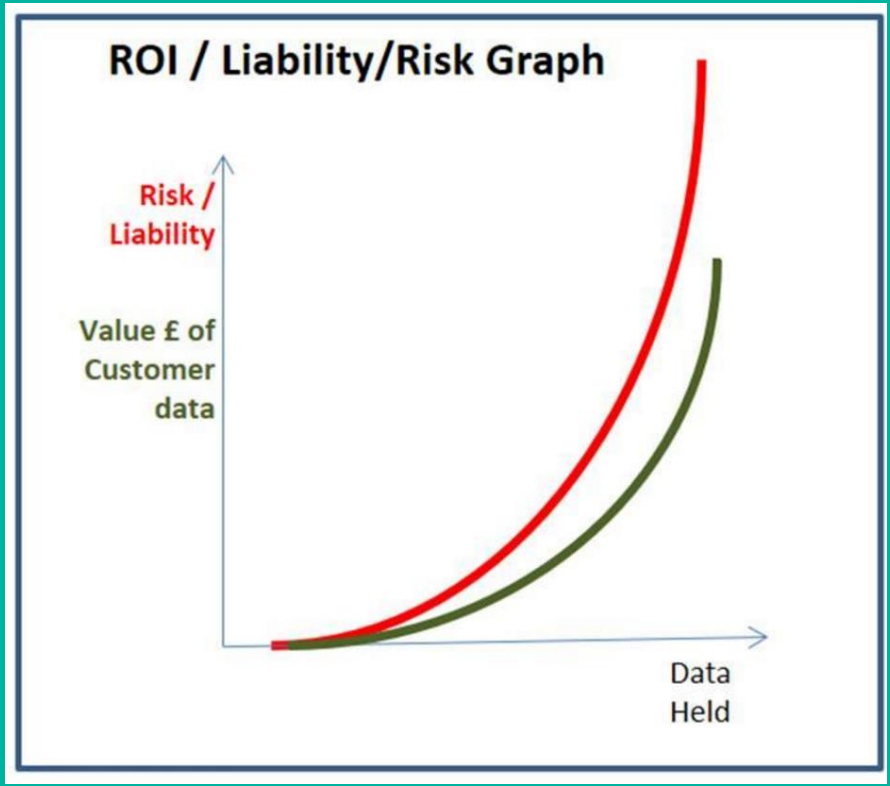
Greater reliance on accurate, up-to-date data

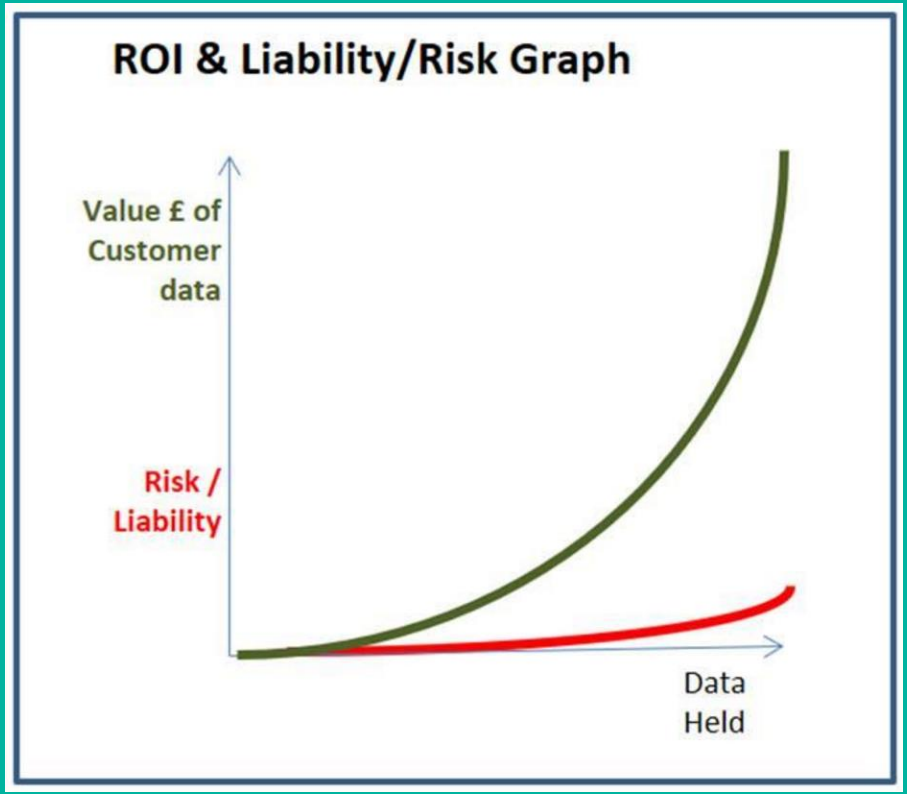
Customer demand for great personalisation

Customer demand for more transparency in data practices

Competitive advantage is crucial as it is easier for customers to switch providers

Data as a toxic asset





https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html


Legal

Legal

Regulations like GDPR and ePrivacy are forcing business to put greater emphasis on privacy, consent requirements, transparency in what data is being used, why it is being used, when it is processed and needed, and for how long access is required.

Breach notifications and reporting requirements

Open Banking initiatives in Europe and Asia Pacific requiring more interoperability and access to peoples financial data through public APIs

Property rights on data and dealing with mine, ours, theirs.

Definition: Personal Data

EU's GDPR: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Australia's Privacy Act: personal information... information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Philippine's Data Privacy Act: *Personal information* refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Financial System Inquiry

"Australia's current approach to identity management results in **significant process duplication**, as individuals apply to, and government and businesses undertake to, verify and re-verify identities at multiple points… Anti-money laundering (AML) projects have resulted in an estimated **$725 million in expenditure**… In 2011, Australians lost an estimated **$1.4 billion through personal fraud** incidents."

http://fsi.gov.au/publications/final-report/chapter-3/digital-identity/#P112_26057

Identity and Human Rights

UN Sustainable Development Goal 16.9: “to provide legal identity for all, including birth registration by the year 2030".

World Bank’s Identification for Development Global Dataset - 15 percent of the global population or **1.1 billion people** lack an official ID.

Without an ID we have no access to financial services, or a social safety net, we cannot own property, we are unaccounted for and our needs are not met.

Technology

Technology

Increasing **adoption** and understanding of blockchain technologies and decentralised and distributed networks

DPKI - people being able to control their own keys.

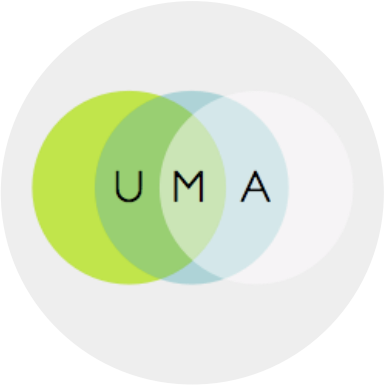
BIP39 - Mnemonic generation. Seed phrases making it easier to deal with than a random string of letters and numbers.

There is now a **commercial imperative** to solve these problems that didn't exist previously

Zero-knowledge storage and **lower barriers to use** and adoption

Oauth, OpenID, User Managed Access

Examples of technologies for User Centric Identity



Enabling Technologies

Examples of technologies for Self-Sovereign Identity

Zero Knowledge Proofs

Zero Knowledge Storage

Distributed Ledger Technologies

Standards and Consortiums

Consortiums and standards emerging for Self-Sovereign Identity

Decentralised Identity Foundation

Word Wide Web Consortium

Working groups and emerging standards

- DIDs - Decentralised Identifiers
- Verifiable Claims

Current Trials

World Food Programme - Building Blocks

- Blockchain trial for cash transfers to deliver aid
- 100,000 Syrian refugees receive transfers via a blockchain based system to purchase goods at participating shops.
- Biometric authentication through iris scans at point of purchase

http://innovation.wfp.org/project/building-blocks

Project FiveARM - Crisis Journalism Reporting Tool

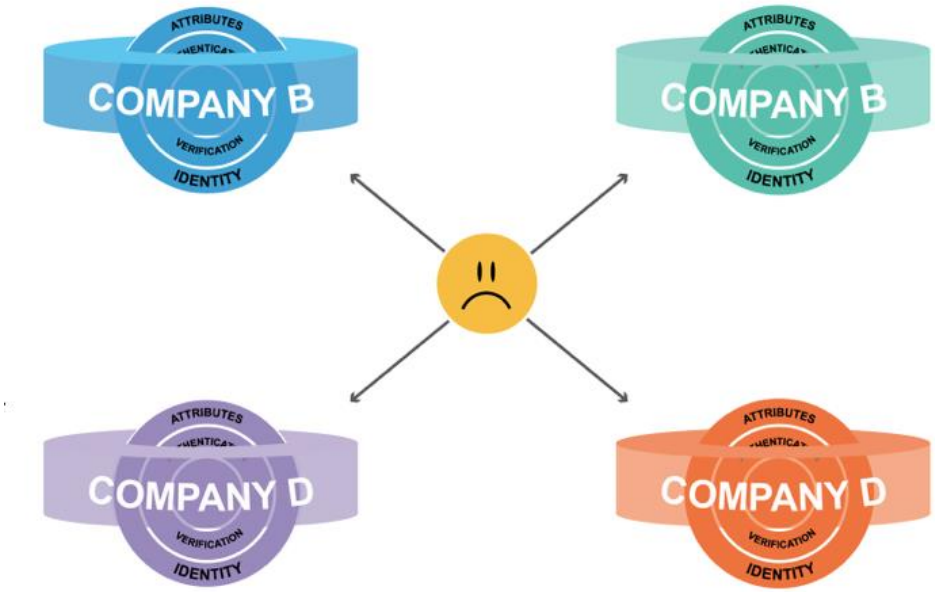
- Challenge: persistent identity for sources without compromising their security.

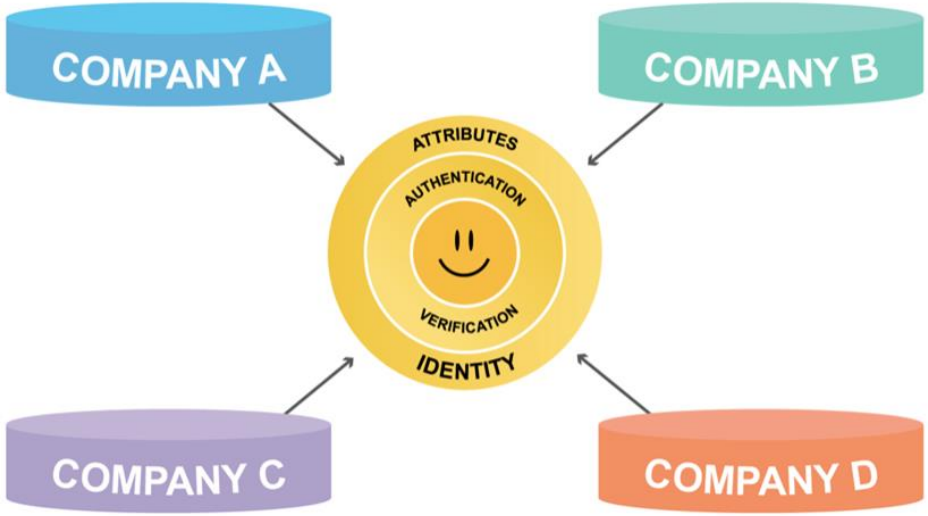
https://fivearm.isafemojo.press/

Where We Go?

The Current Model:

- Information duplicity: sensitive information sent to multiple parties.
- Liability of storage for each party.
- Many ‘honeypots’ for hackers to attack.





The Proposed Model:

- Data held in zero knowledge storage.
- Signed ‘attestations’ develop trust over time.
- Canonical source of data.
- Identity remains under the ownership of the individual.
- Mutual value exchange and asset realisation.

What does this enable for individuals?

Control

User permits access to Id

Audit

Access is logged

Security

No walled honeypots

What does this enable for service providers?

Less Liability

Separate transaction data from id

Veracity of Data

Current and latest

Realtime Updates

Instead of ‘one chance to ask’.

Self-Sovereign ID - Karen

- Proving who you are is a simple as logging in using your identity.
- Bank requests a set of attributes
- Karen consents to the request and shares attributes and verified claims.
- Through progressive disclosure, financial services can be personalised to Karen

Self-Sovereign ID - Amena

- Amena’s identity is bootstrapped with verified claims based on 1st and 2nd degree relationships
- Web-of-trust need not rely on government as the source of authority
- Amena can prove work history using verified claims to get a job in a foreign country.

Dual side of the future

These technologies can amplify or diminish our freedoms.

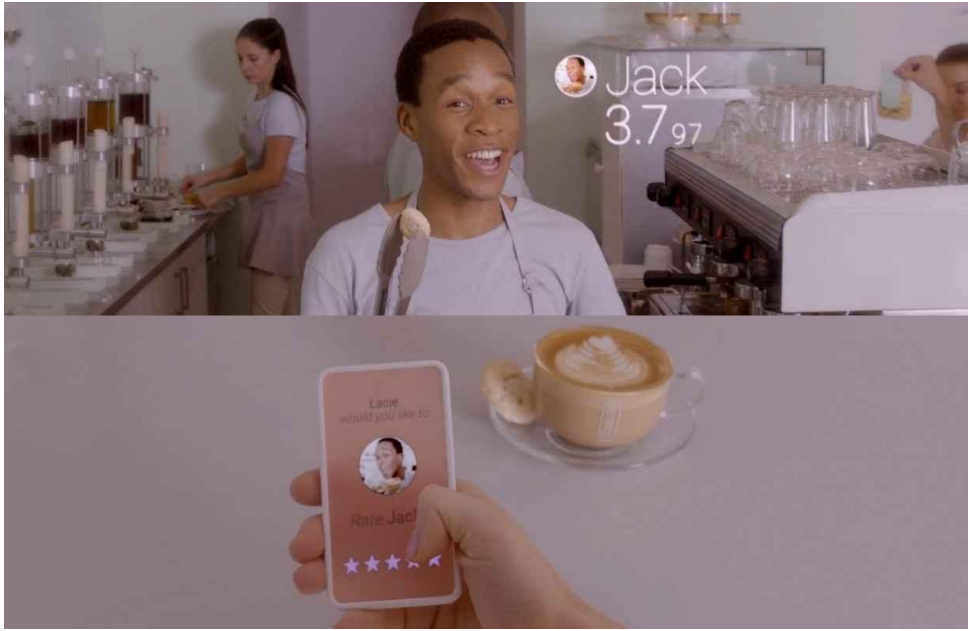
Blackmirror: Eg. Chinas Social Credit Score - Surveillance and authoritarianism

Whitemirror: Eg. Mutual exchange of value - Transparency, trust and democracy

China’s Social Credit System

"Black mirror"

dystopian possibilities



https://newrepublic.com/article/148121/control-14-billion-people

Mutual Value Exchange

"White mirror"

utopian possibilities

Demo

Questions?

BIT TRADE LABS

Explore the future with us
www.bittradelabs.com

Hugo O'Connor
Co-founder and Blockchain Engineer