Blockchain Foundations

Ronald M. Tucker

President + Founder ADCA

PROMOTING BLOCKCHAIN
INNOVATION IN AUSTRALIA

ADCA

About ADCA

ADCA is the industry body that represents Australian businesses participating in the digital economy through blockchain technology.

ADCA aims to encourage the responsible adoption of blockchain technology by industry and governments across Australia as a means to drive innovation in service delivery across all sectors of the economy.

ADCA

About ADCA

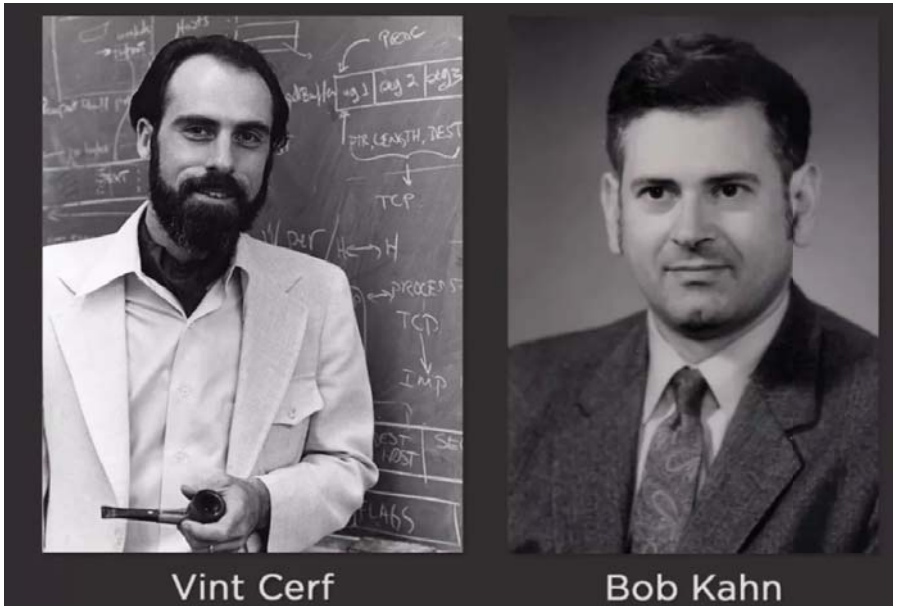
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

ADCA

“Fathers of the Internet”



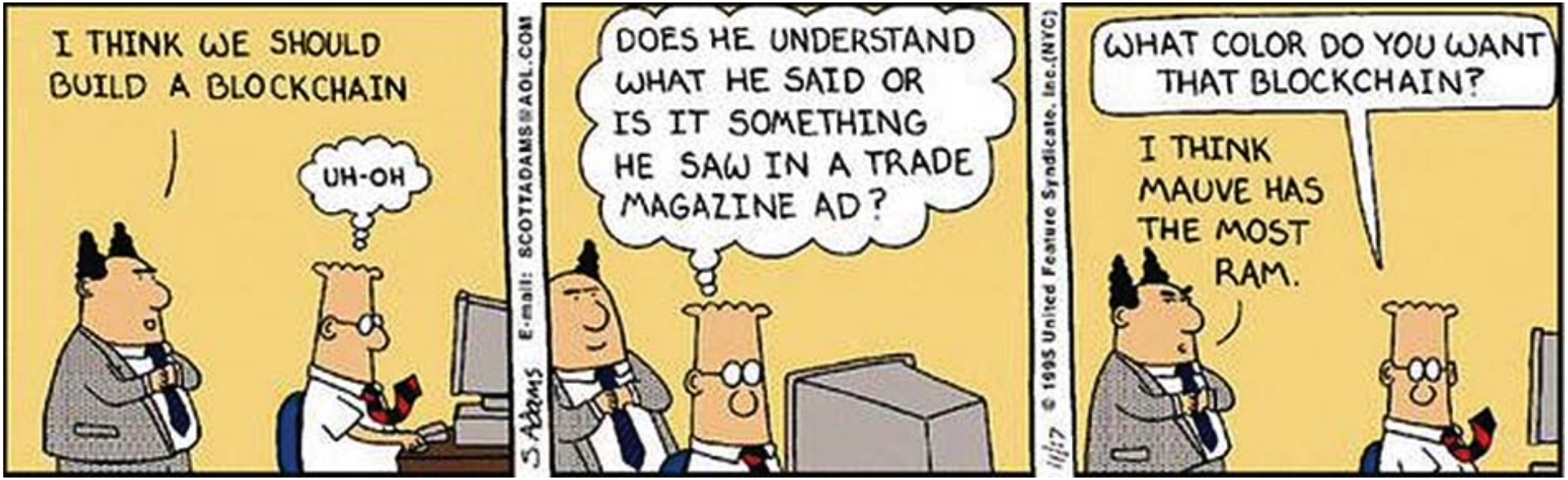
- Co creaters of the TCP/IP protocol
- Cerf is now vice-president of Google while Khan is now chairman CEO and president of the Corporation for National Research Initiatives

ADCA

(The real brains to the operation.)

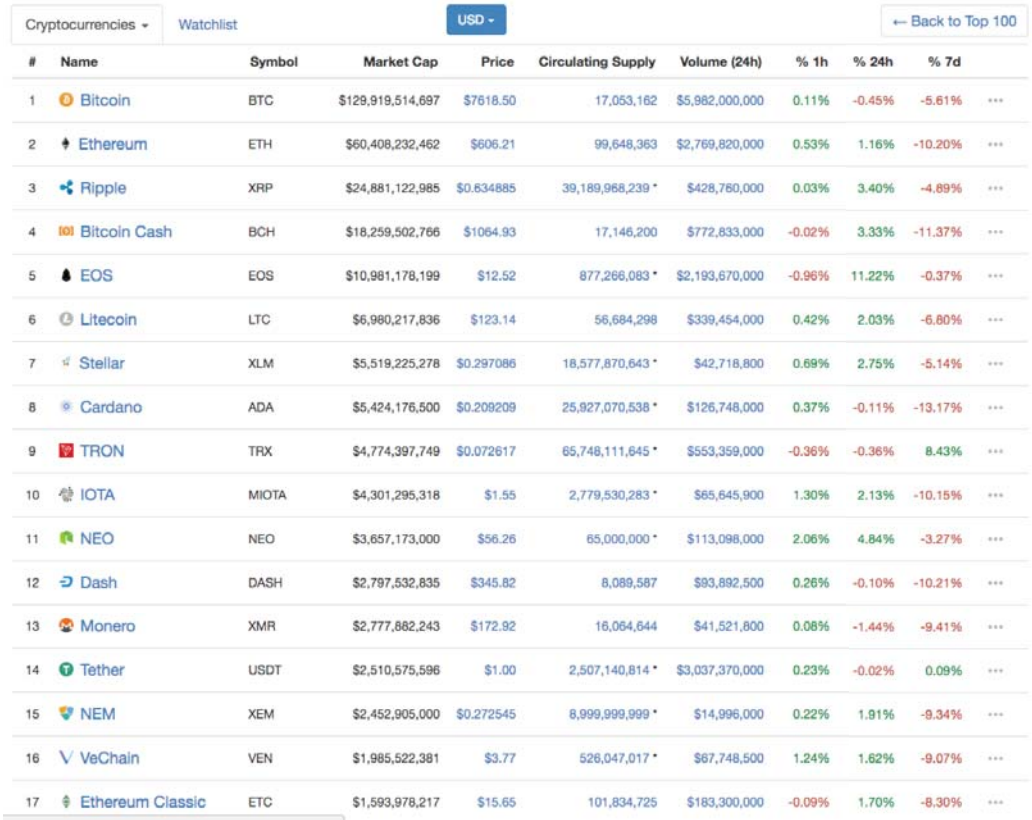
ADCA

Everybody is Talking About Blockchain



ADCA

Blockchain Asset Markets



Cryptocurrencies ▾ Watchlist USD ▾ ← Back to Top 100

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$129,919,514,697	$7618.50	17,053,162	$5,982,000,000	0.11%	-0.45%	-5.61%
2	Ethereum	ETH	$60,408,232,462	$606.21	99,648,363	$2,769,820,000	0.53%	1.16%	-10.20%
3	Ripple	XRP	$24,881,122,985	$0.634885	39,189,968,239 *	$428,760,000	0.03%	3.40%	-4.89%
4	Bitcoin Cash	BCH	$18,259,502,766	$1064.93	17,146,200	$772,833,000	-0.02%	3.33%	-11.37%
5	EOS	EOS	$10,981,178,199	$12.52	877,266,083 *	$2,193,670,000	-0.96%	11.22%	-0.37%
6	Litecoin	LTC	$6,980,217,836	$123.14	56,684,298	$339,454,000	0.42%	2.03%	-6.80%
7	Stellar	XLM	$5,519,225,278	$0.297086	18,577,870,643 *	$42,718,800	0.69%	2.75%	-5.14%
8	Cardano	ADA	$5,424,176,500	$0.209209	25,927,070,538 *	$126,748,000	0.37%	-0.11%	-13.17%
9	TRON	TRX	$4,774,397,749	$0.072617	65,748,111,645 *	$553,359,000	-0.36%	-0.36%	8.43%
10	IOTA	MIOTA	$4,301,295,318	$1.55	2,779,530,283 *	$65,645,900	1.30%	2.13%	-10.15%
11	NEO	NEO	$3,657,173,000	$56.26	65,000,000 *	$113,098,000	2.06%	4.84%	-3.27%
12	Dash	DASH	$2,797,532,835	$345.82	8,089,587	$93,892,500	0.26%	-0.10%	-10.21%
13	Monero	XMR	$2,777,882,243	$172.92	16,064,644	$41,521,800	0.08%	-1.44%	-9.41%
14	Tether	USDT	$2,510,575,596	$1.00	2,507,140,814 *	$3,037,370,000	0.23%	-0.02%	0.09%
15	NEM	XEM	$2,452,905,000	$0.272545	8,999,999,999 *	$14,996,000	0.22%	1.91%	-9.34%
16	VeChain	VEN	$1,985,522,381	$3.77	526,047,017 *	$67,748,500	1.24%	1.62%	-9.07%
17	Ethereum Classic	ETC	$1,593,978,217	$15.65	101,834,725	$183,300,000	-0.09%	1.70%	-8.30%

ADCA

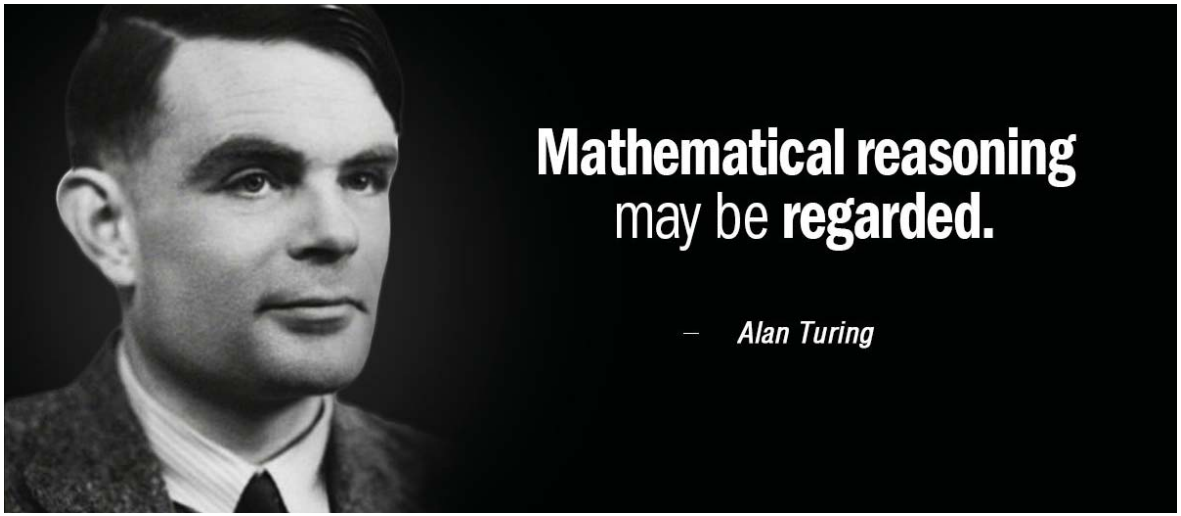
Bitcoin & Blockchain

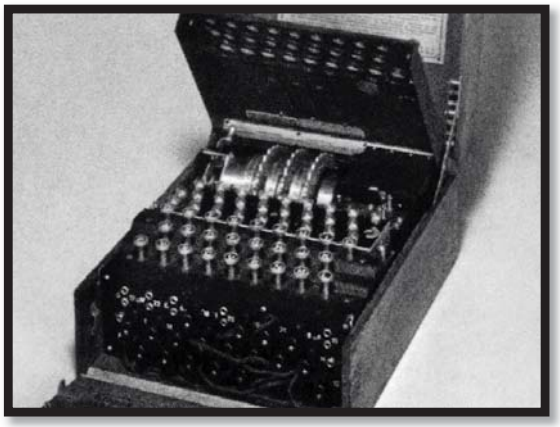
- *"Peer-to-peer electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution"*
- Proposed by Satoshi Nakamoto in May 2008
- Bitcoin "Genesis Block" in January 2009
- Current market value approx. USD 40 Billion

- Underlying technology for Bitcoin
- A distributed database that contains blocks of timestamped transactions linked together in a continuous chain
- Supports consensus methodology and data immutability
- Allows creation and trading of an electronic asset

ADCA

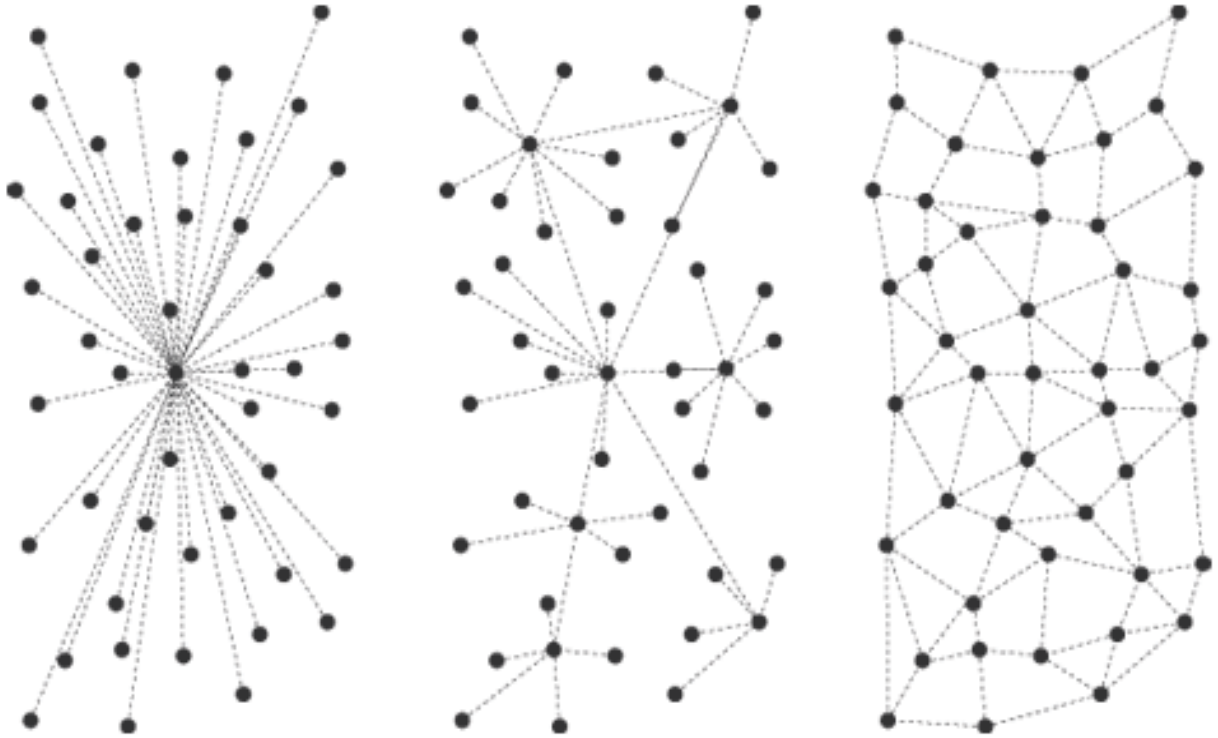
Hashing ('Mining')





ADCA

Distributed Ledger Provides TRANSPARENCY



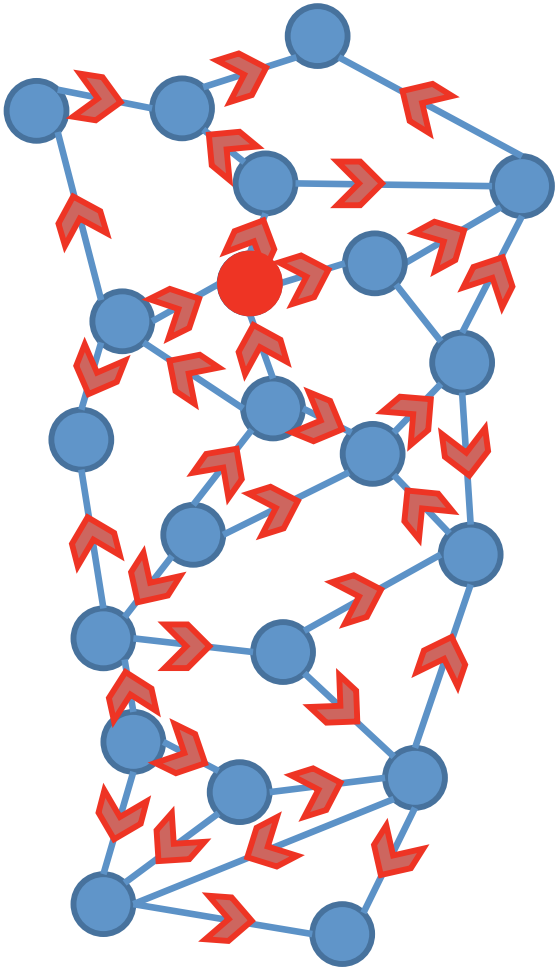
ADCA

Single Source of Truth

I see what you see

ADCA

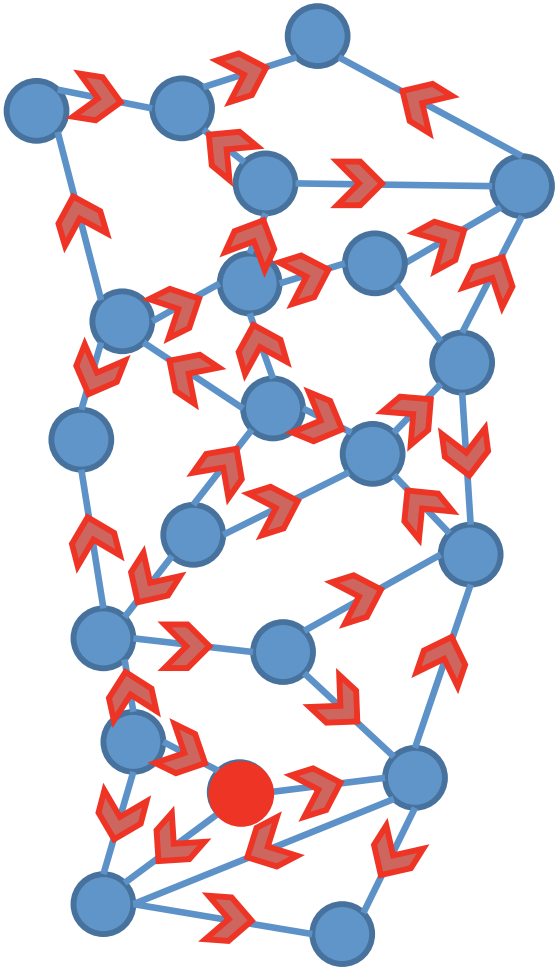
Consensus Protocol establishes ACCURACY

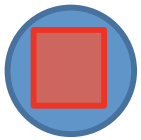


1. A new **transaction** is created on one node
2. The transaction is broadcast to all nodes

ADCA

Consensus Protocol establishes ACCURACY

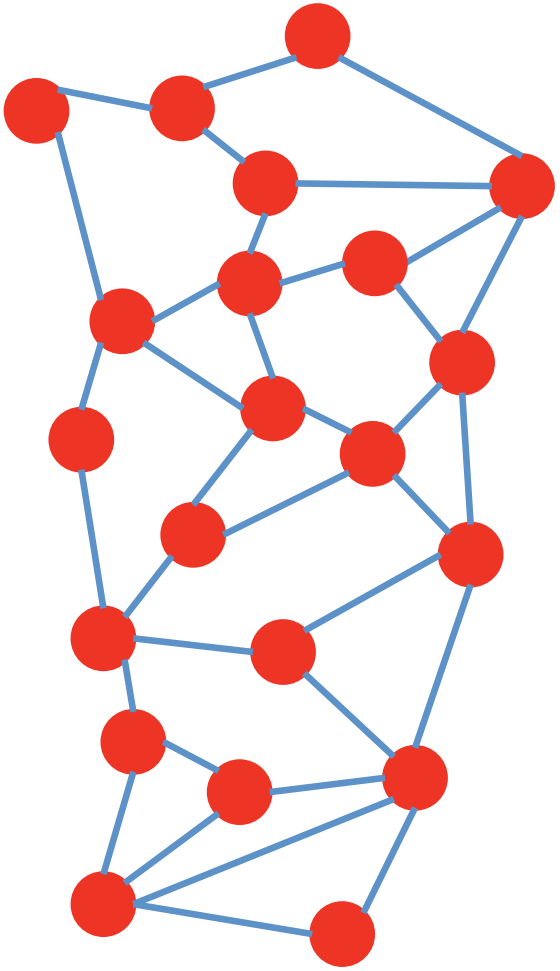




1. A new **transaction** is created on one node
2. The transaction is broadcast to all nodes
3. Each node competes to collect new transactions into a “block”
4. A **random** node ‘wins’
   - and broadcasts the new block to other nodes.

ADCA

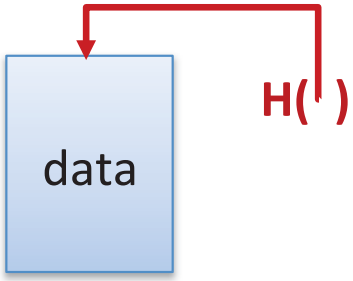
Consensus Protocol establishes ACCURACY



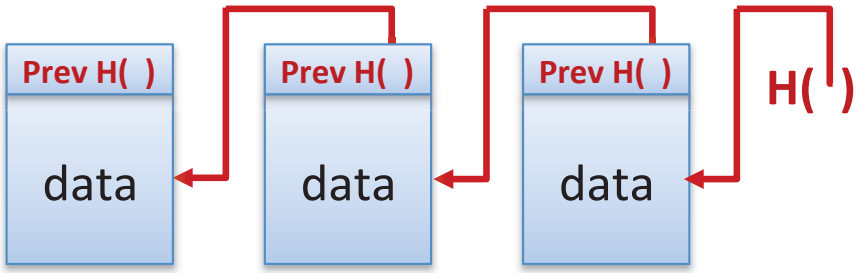
1. A new **transaction** is created on one node
2. The transaction is broadcast to all nodes
3. Each node competes to collect new transactions into a new “block”
4. A **random** node ‘wins’
   - and broadcasts the new block to other nodes.
5. All other nodes add the new block to their blockchain.

ADCA

Blockchain provides IMMUTABILITY



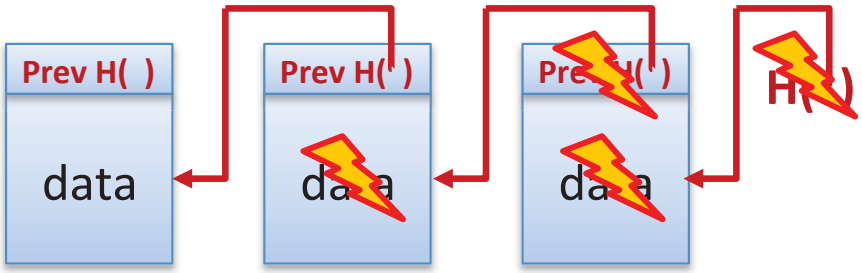
- A hash-pointer is a cryptographic reference to a piece of data
- SHA-256 is a standard compression algorithm
- The hash is **uniquely associated** with the underlying data



- In a Blockchain each new block contains the hash function of the previous block.
- To verify the whole chain – **and every transaction in it** – you only need to be able to confirm the most recent hash

ADCA

Blockchain provides IMMUTABILITY



- If the data is corrupted (accidentally or deliberately) then the next hash and all subsequent blocks fail
- This creates a **tamper-evident ledger**

ADCA

The Elements of TRUST

SECURITY

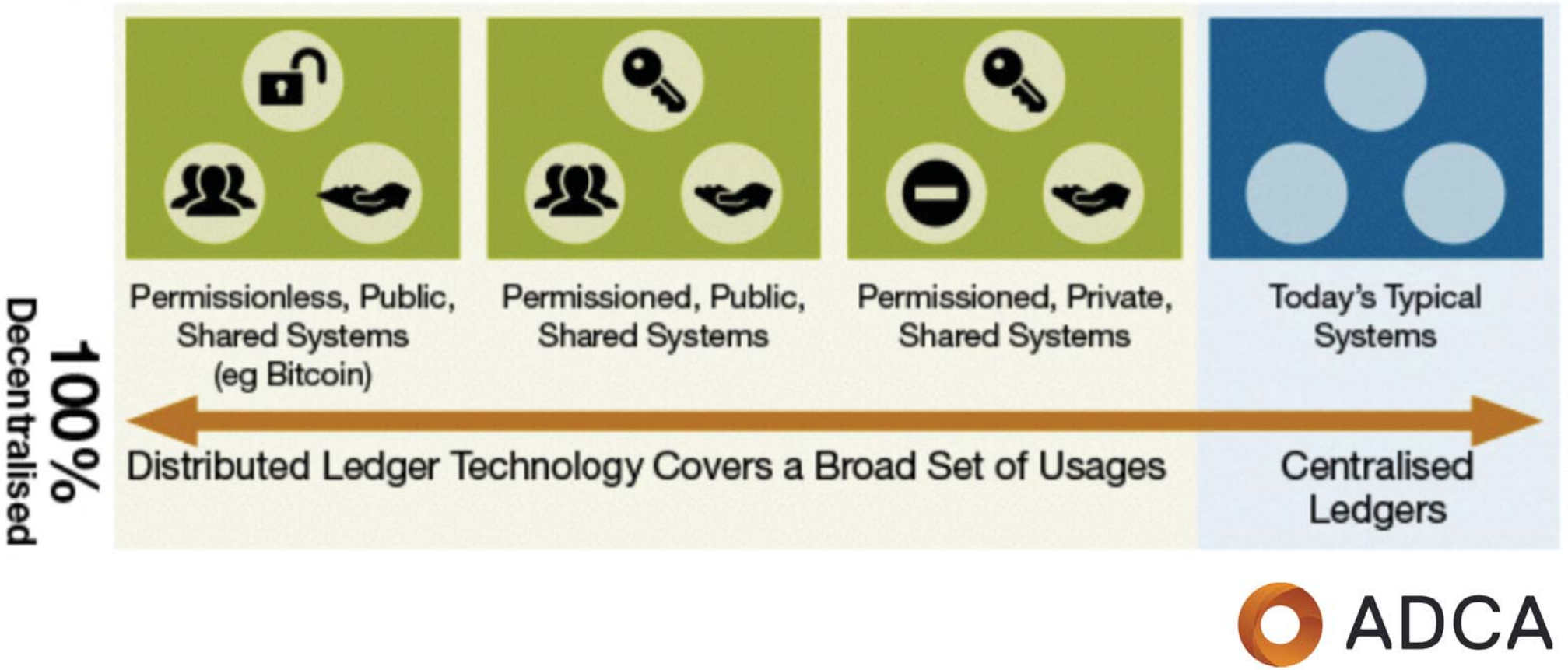
ACCURACY

TRANSPARENCY

IMMUTABILITY

ADCA

Public, Permissioned and Private Blockchains



ADCA

Public, Permissioned and Private Blockchains

Different use cases require different solutions.

Trade offs include:

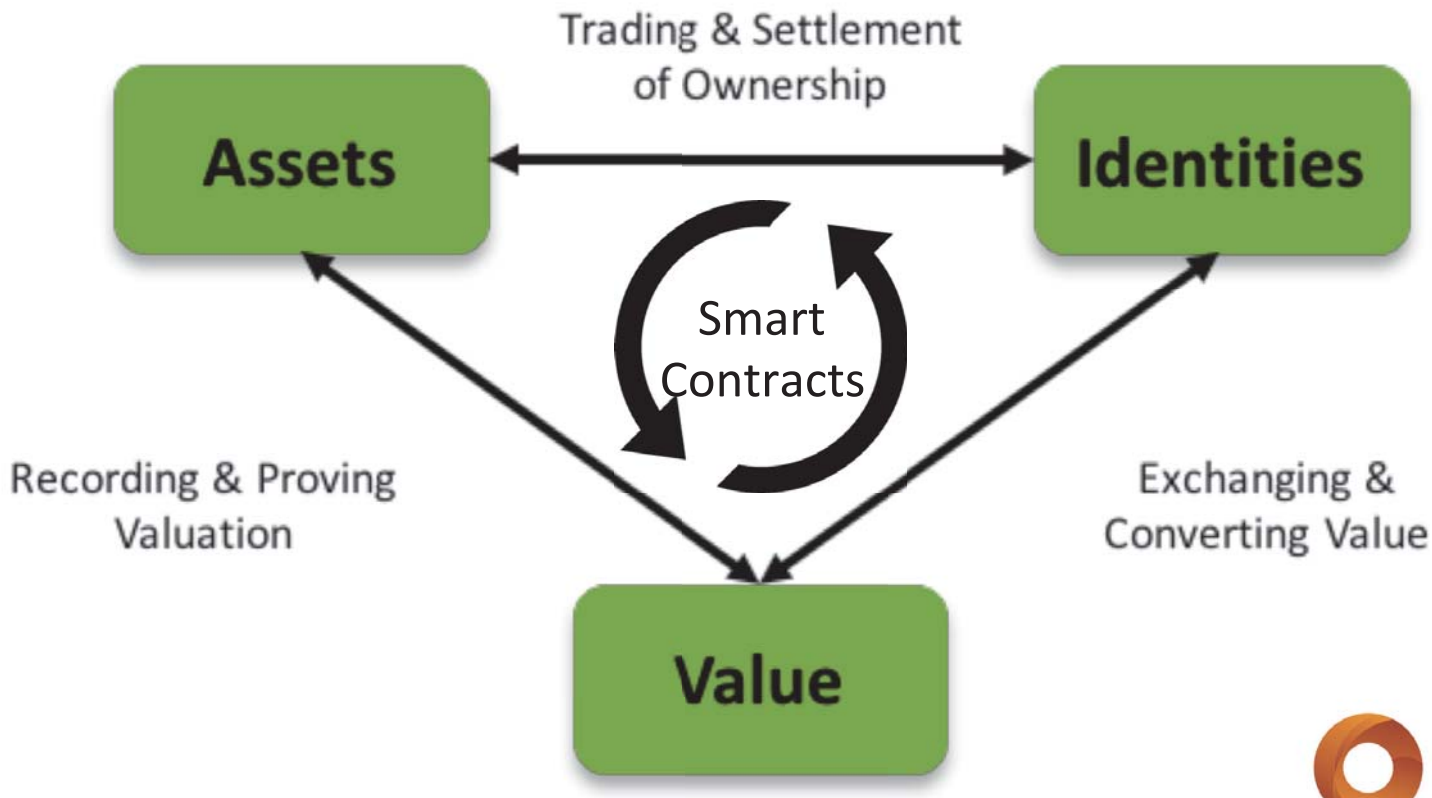
- Security
- Consensus mechanism
- Speed

ADCA

2. Smart Contracts

ADCA

Future Blockchain Ecosystem



ADCA

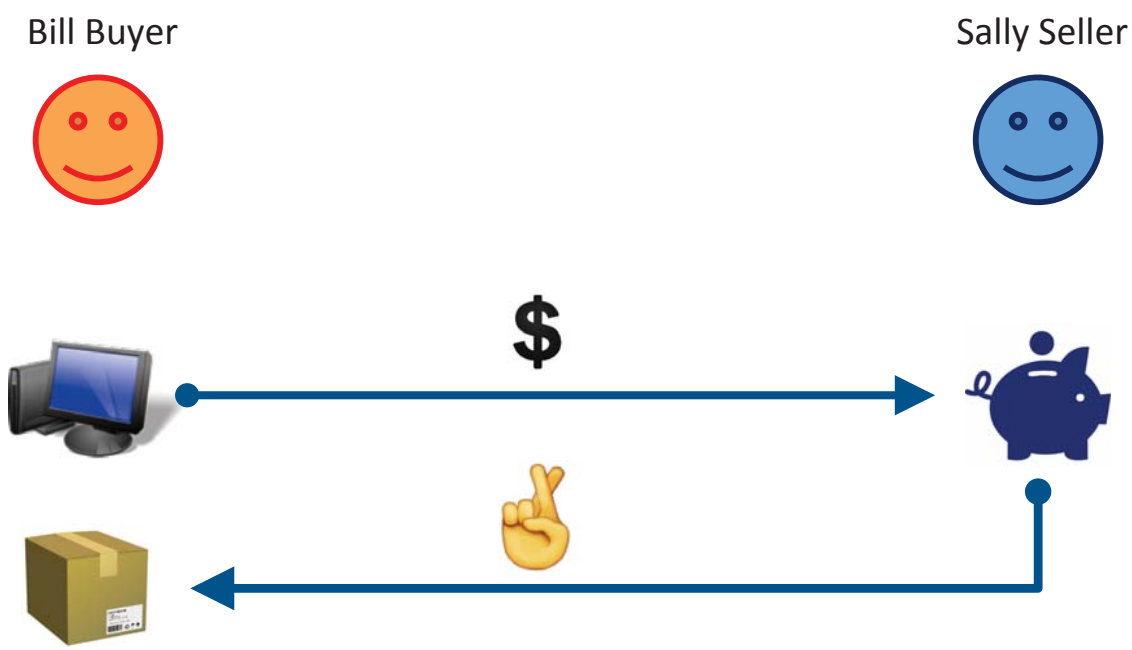
Smart Contracts

Features of a Smart Contract:

- computer programs that emulate (key) contractual clauses
- stored on a blockchain to give all parties confidence that they will operate as intended

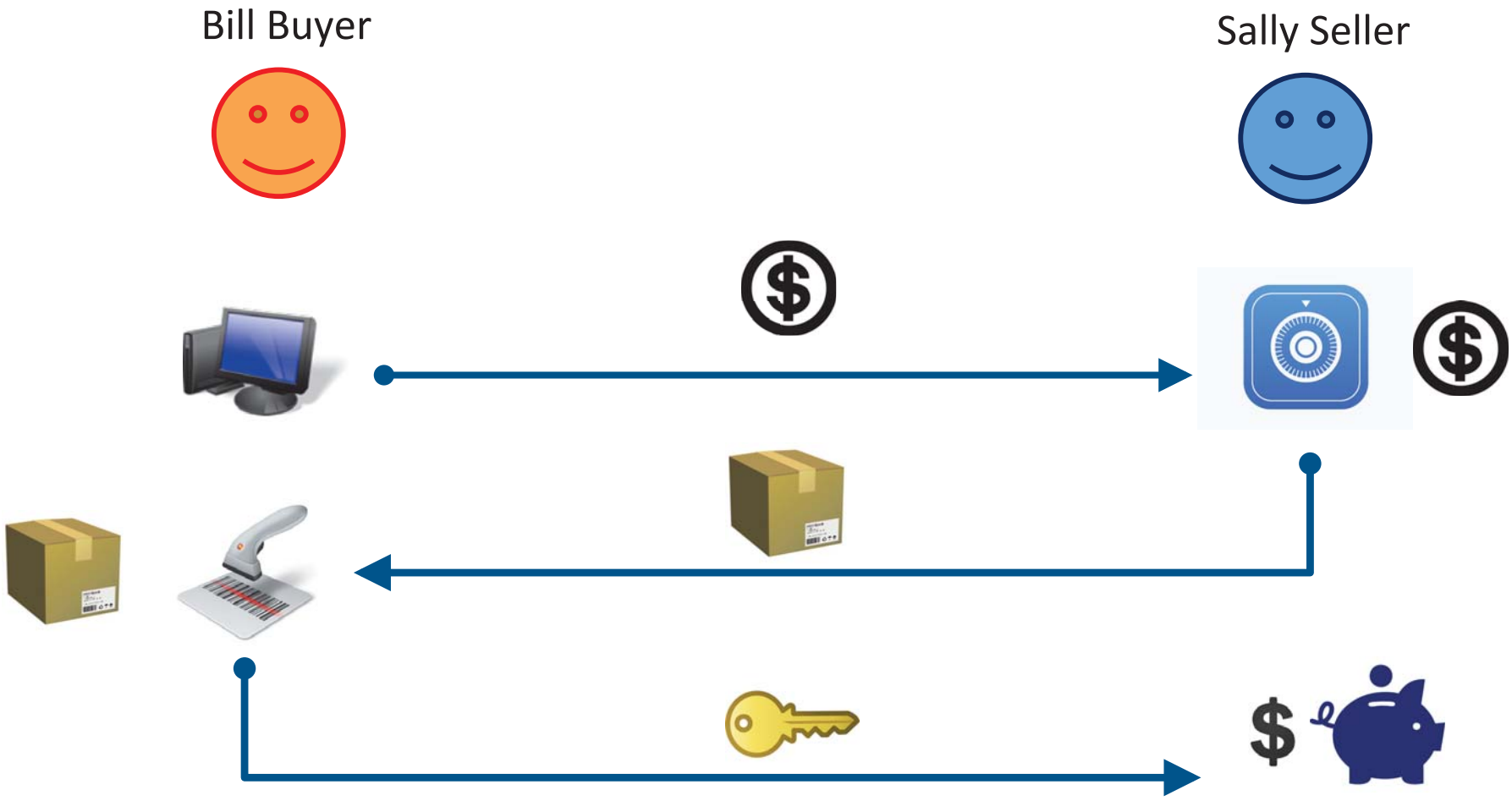
ADCA

Online Escrow Use Case for a Smart Contract



ADCA

Online Escrow Use Case for a Smart Contract

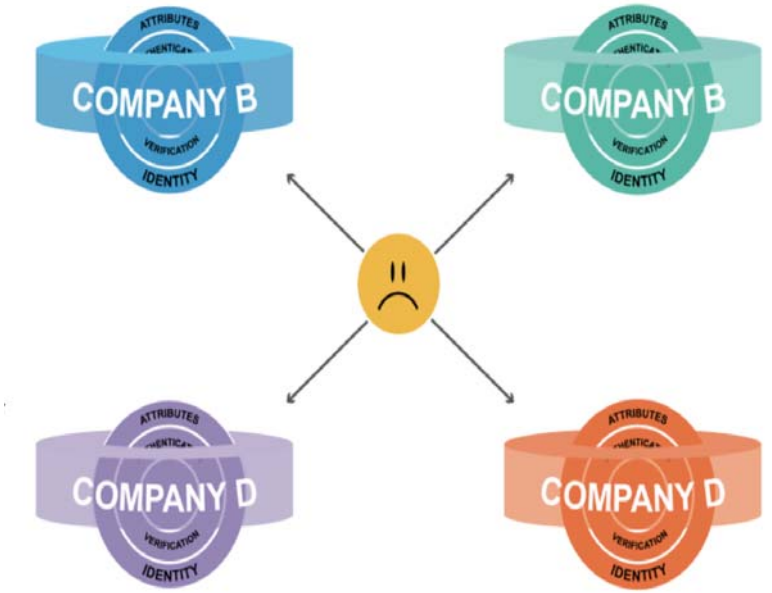


Solving Identity

Identity is a Broken System

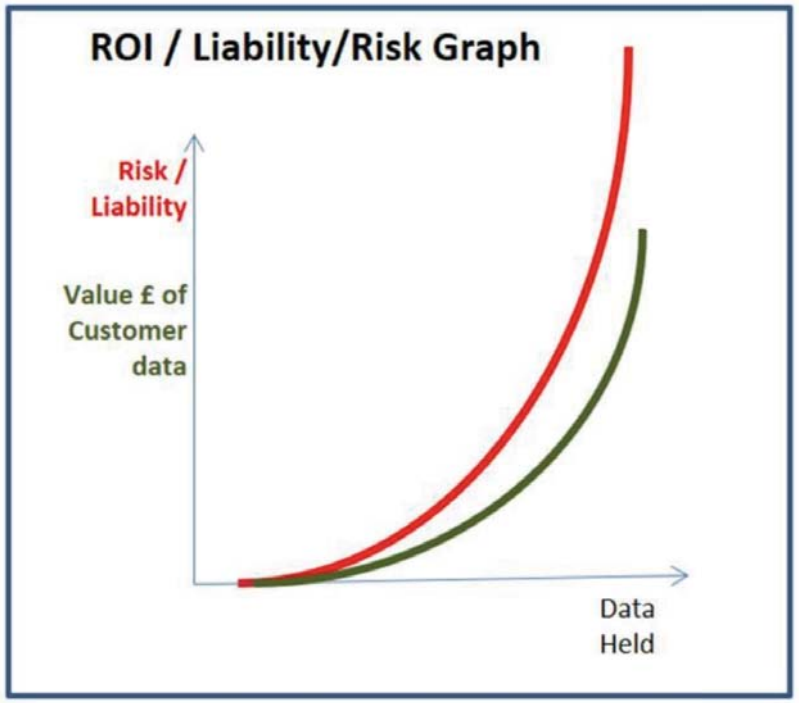
Identity information is currently held by companies about an individual:

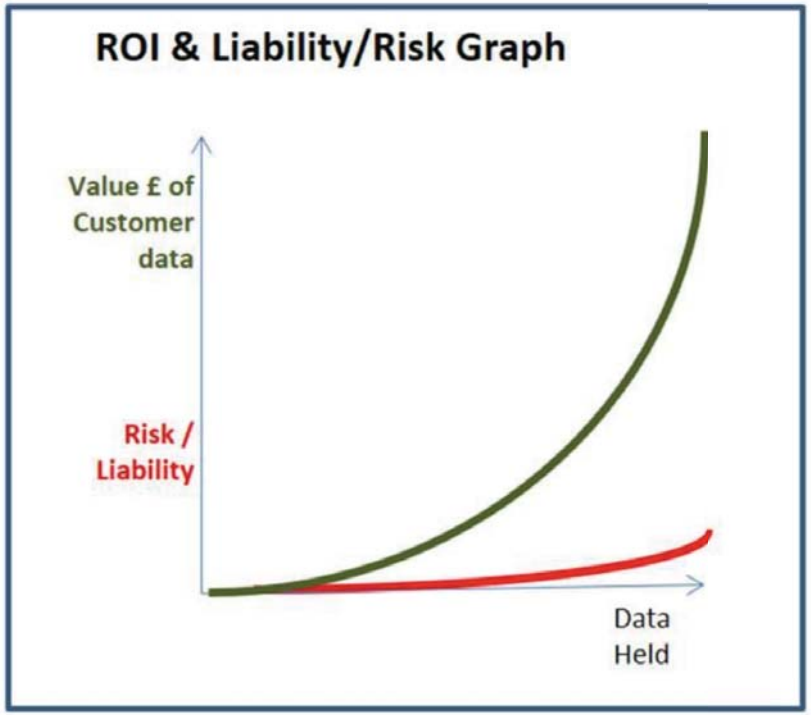
- Duplication
- Sensitive data sent to multiple parties
- Company liable for storage
- Many ‘honeypots’ for hackers to attack



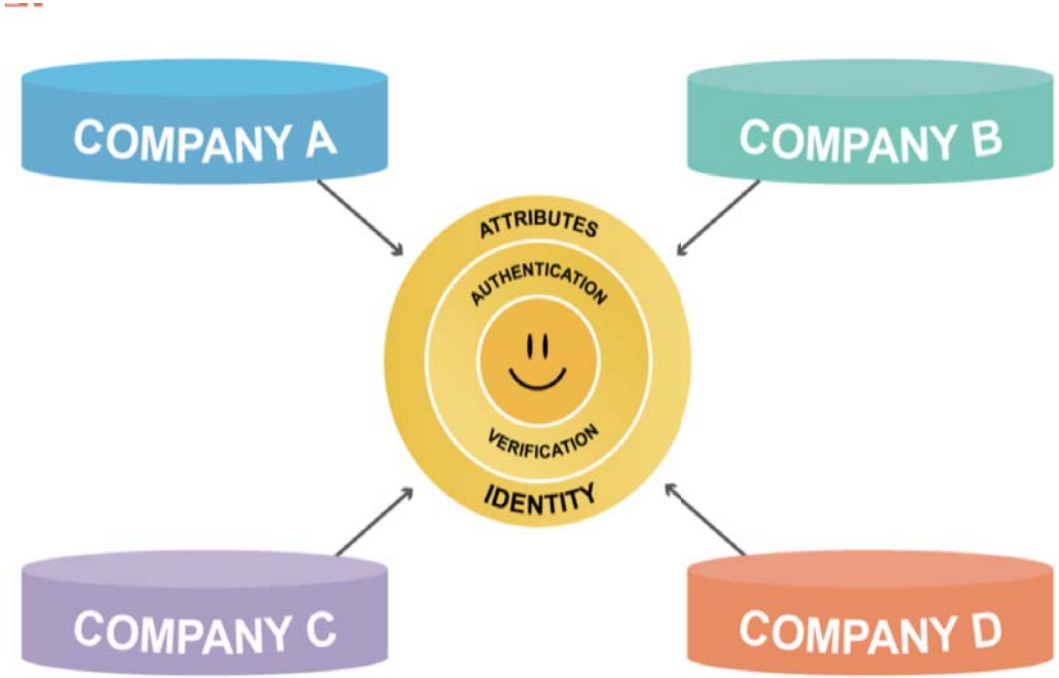
ADCA

Identity is a "Toxic Asset"





Blockchain could enable "Self-Sovereign Identity"



ADCA

Australian Blockchain Innovators

Proof of Event

ADCA

Remittances

ADCA

Energy Markets

ADCA

Agricultural Supply Chain & Finance

ADCA

Water Rights Management

civic ledger

ADCA

Implications

- Valuation of Digital Currency Assets
- Investment "advice"
- Valuation of Tokens
- Token Offerings

ADCA


COINTELEGRAPH


Partners
ADCA


26th New South Wales-Guangdong Joint Economic Meeting


ADCCA
AUSTRALIAN DIGITAL CURRENCY COMMERCE ASSOCIATION
#G20
#Bitcoin
GDCC


Kalgoorlie
Darren Forster 31.2%
Tony Crook 23.9%
Kyran O'Donnell 17.2%
Richard Bolton 12.8%
Mike Lucas 7.2%
Jacqueline Spurling 6.8%
James Erwin 1.0%
vote Flux


GLOBAL
BLOCKCHAIN
FORUM


2017 Australian
Blockchain Mission


singularityNET

ADCA

PROMOTING BLOCKCHAIN INNOVATION IN AUSTRALIA

RONALD M. TUCKER

rtucker@adca.asn.au
WeChat: leo_8100

Self Sovereign Identity

CONVERGING FORCES, CHALLENGES AND OPPORTUNITIES

BARCLAYS

BIT TRADE LABS

What is Self Sovereign Identity?

ADCA

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.

ADCA

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

ADCA

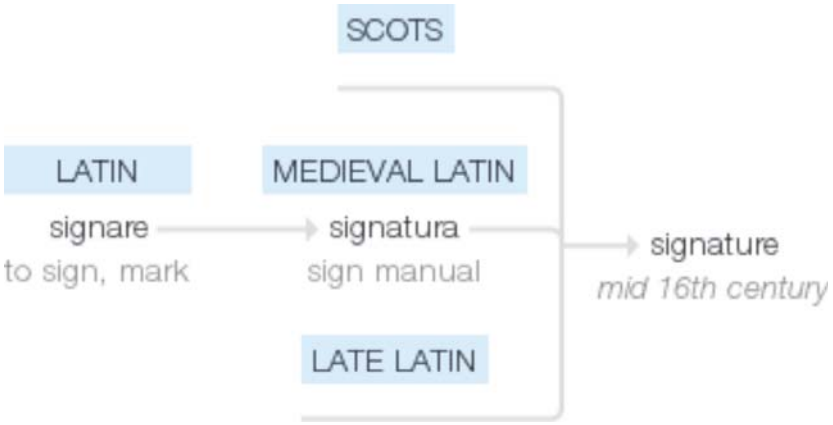
Historical Background

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

ADCA

Ancient Infrastructure



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

ADCA

Ancient Infrastructure

FRENCH
passer
to pass

FRENCH
port
seaport

FRENCH
passeport → passport
late 15th century

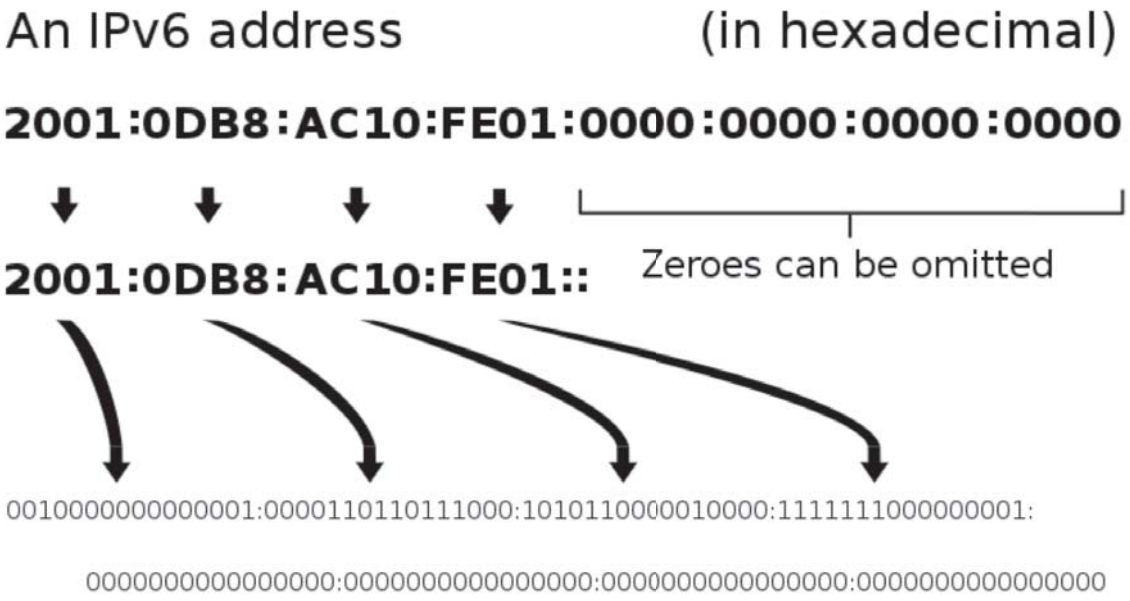
[3] A Brief History of the Passport http://www.theguardian.com/travel/2006/nov/17/travelnews

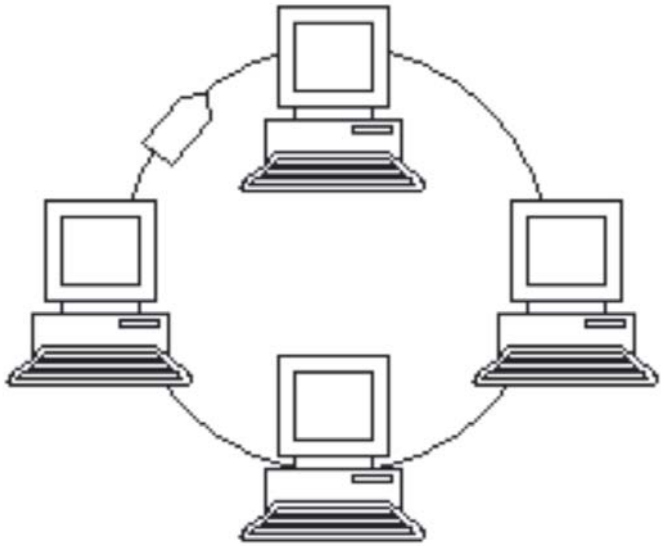
ADCA

Technologies Evolving

Identity on the Internet

TCP/IP - computers are distinguished by IP addresses

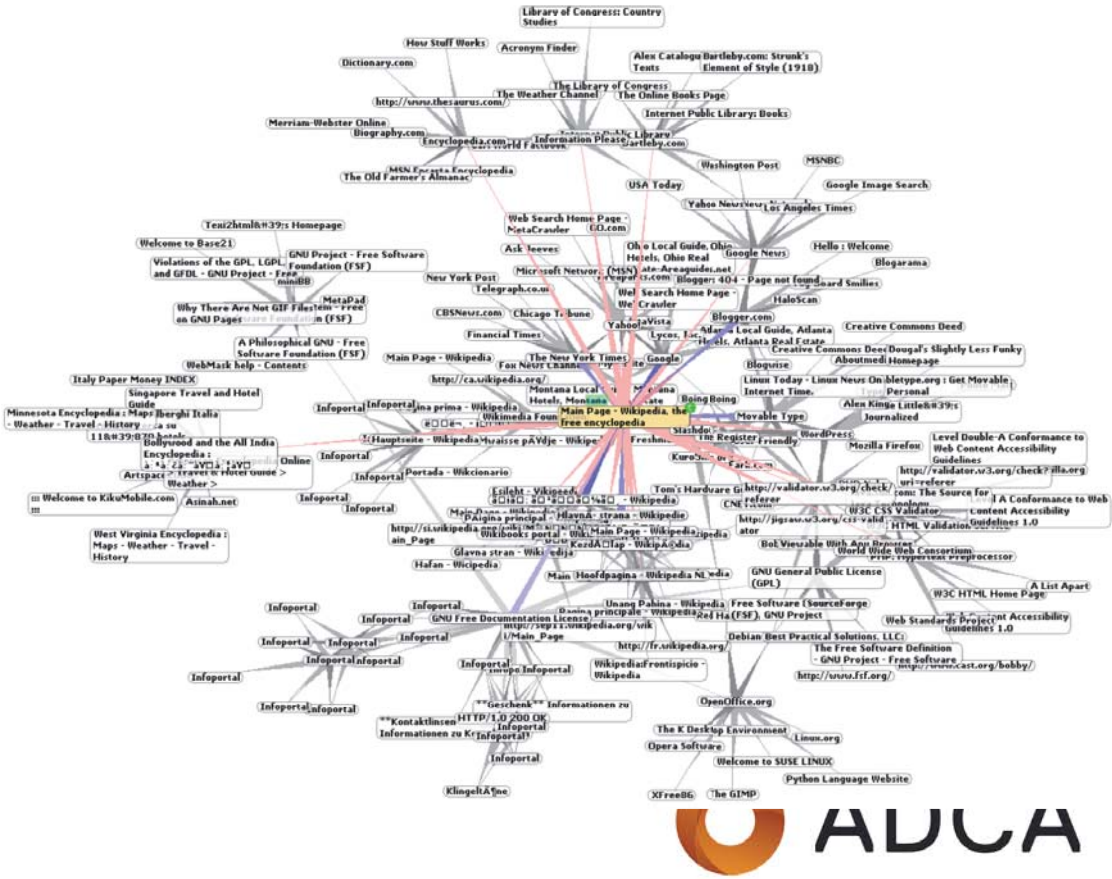




ADCA

URIs and the World Wide Web

- Resources identified with
- Hyperlinks between docu



Identity on the Internet

MAC addresses - identifiers for d

ADCA

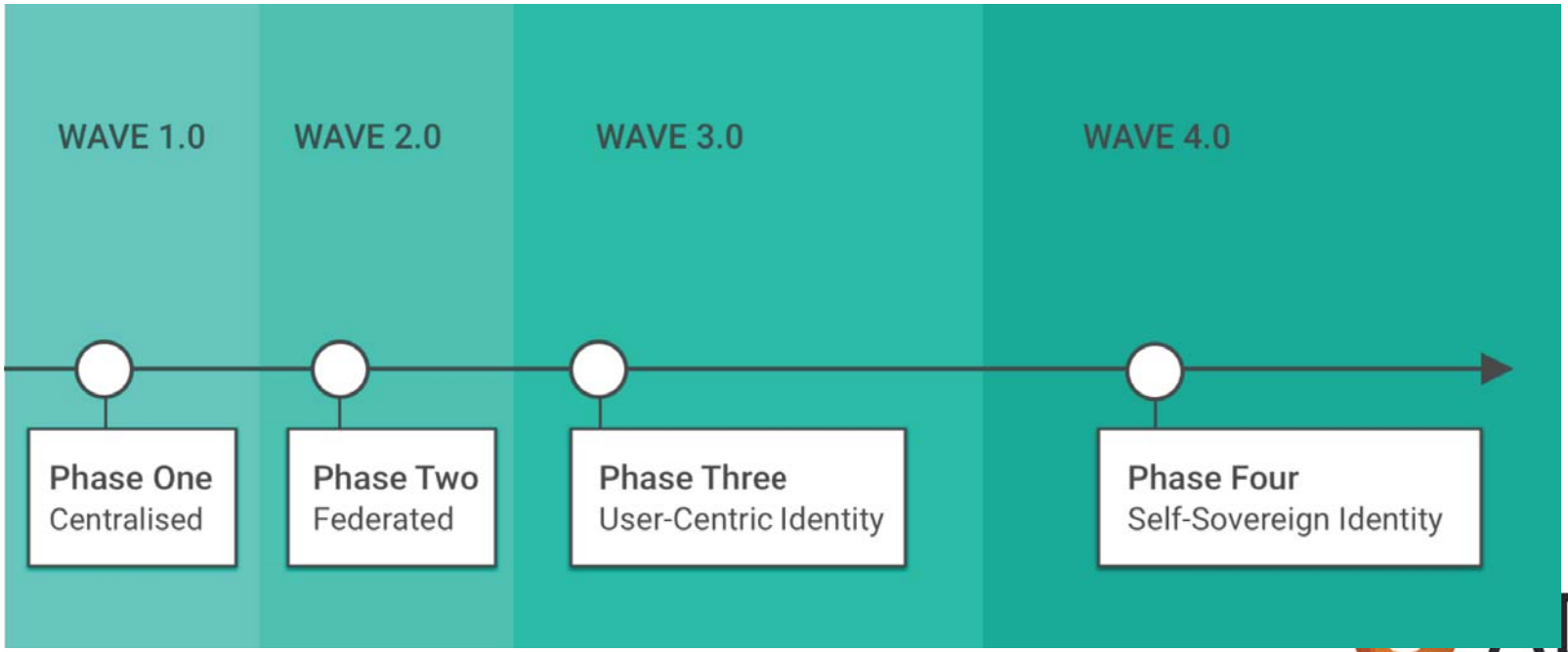
The Missing Piece of Internet Infrastructure

Who is behind the keyboard?

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

Path to Self Sovereign Identity

Evolution of identity in the past 30 years



ADCA

The Windhover Principles

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

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

ADCA

Christopher Allen's Principles of Sovereign ID

http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-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*

ADCA

Human Story

ADCA

Karen, 25, urban professional, Sydney

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

ADCA

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

ADCA

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.

ADCA

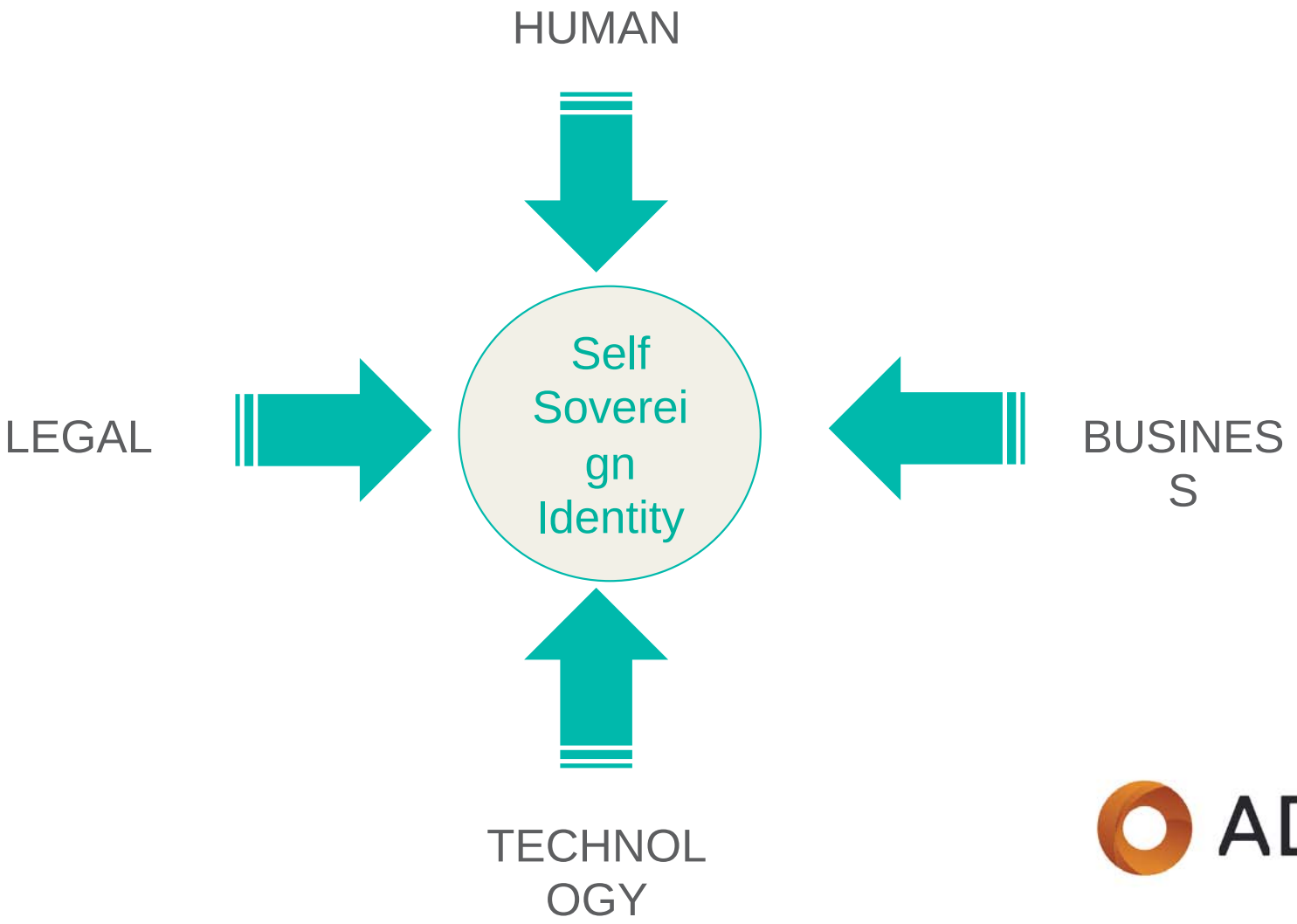
Pain Point - No Documents to Verify

- 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

ADCA

Converging forces

ADCA



ADCA


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

ADCA

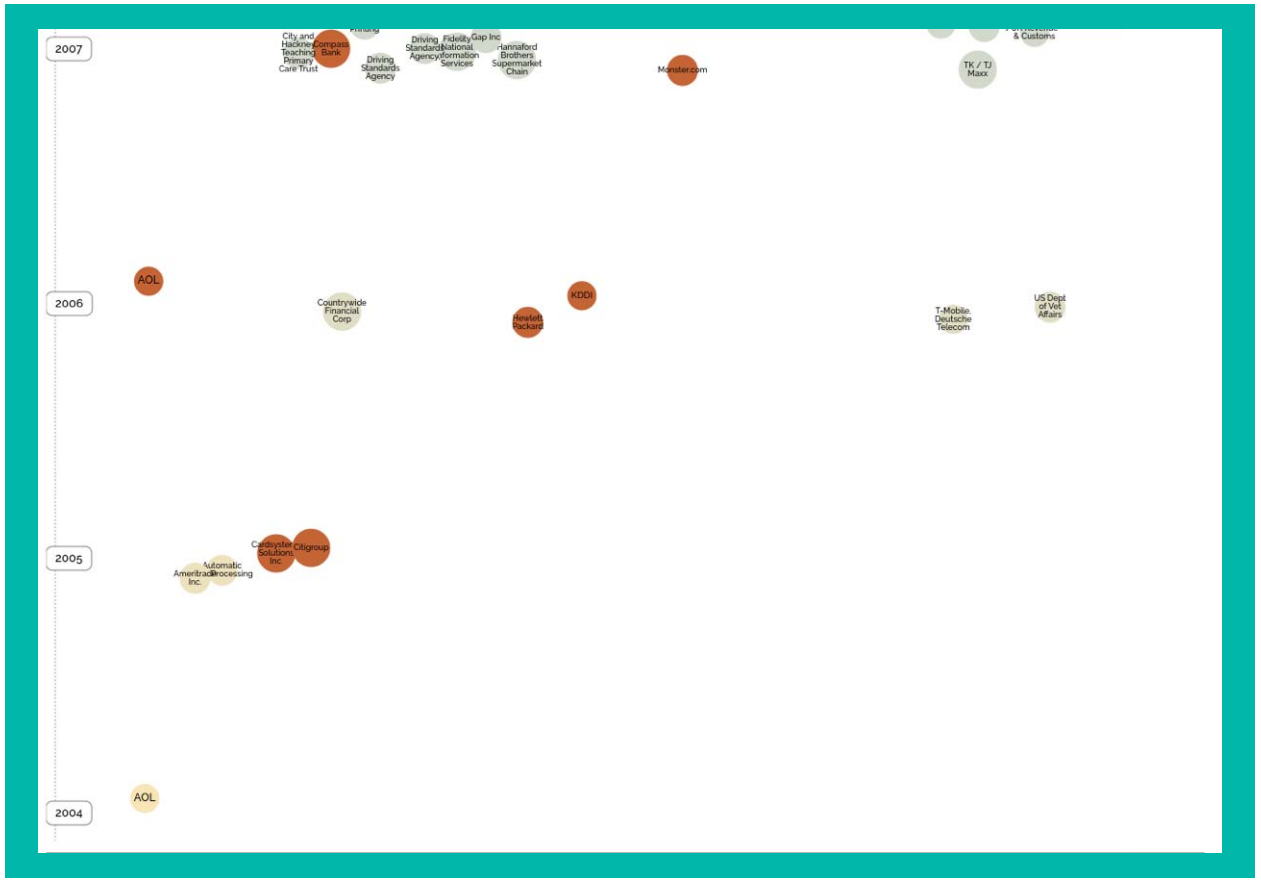
Taking Ownership of Personal Data

- 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.

ADCA

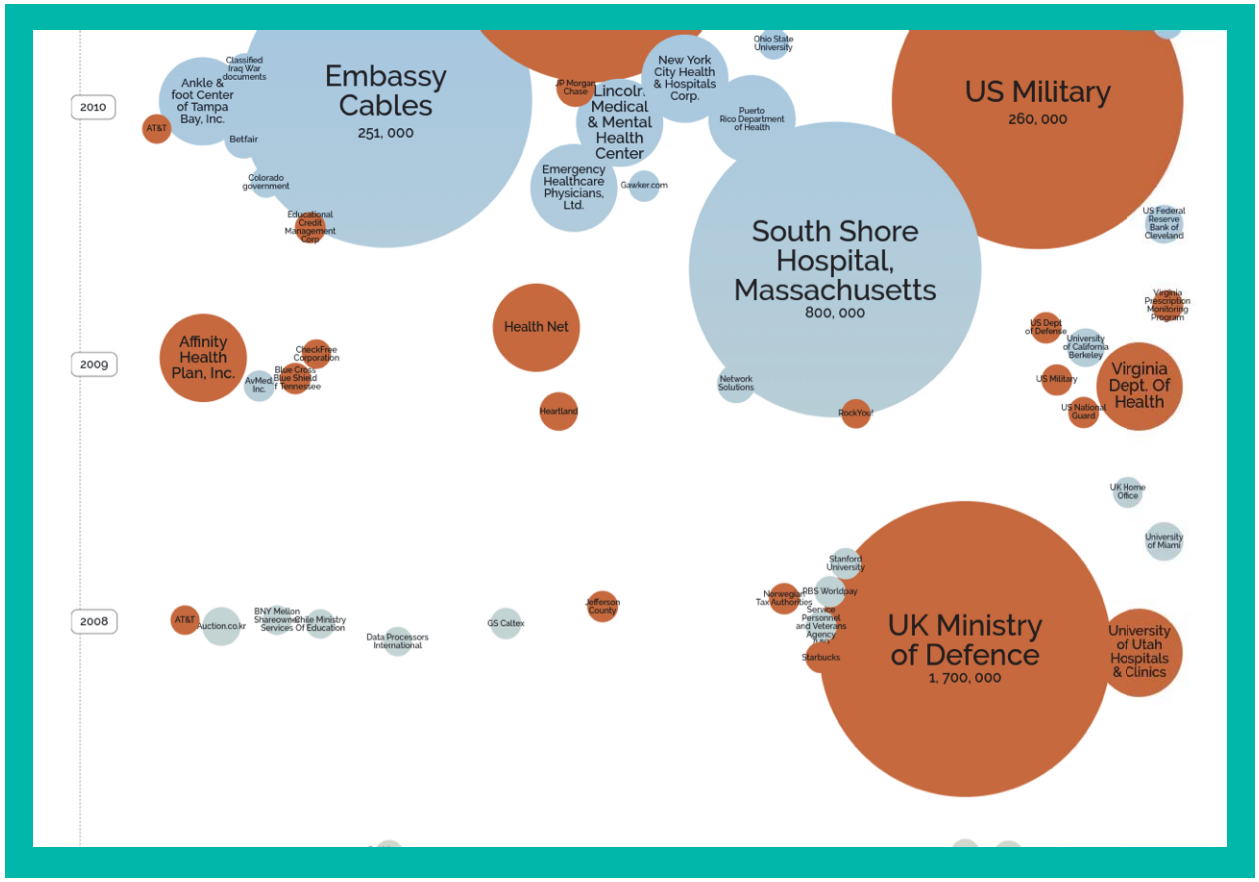
Data Breaches

ADCA



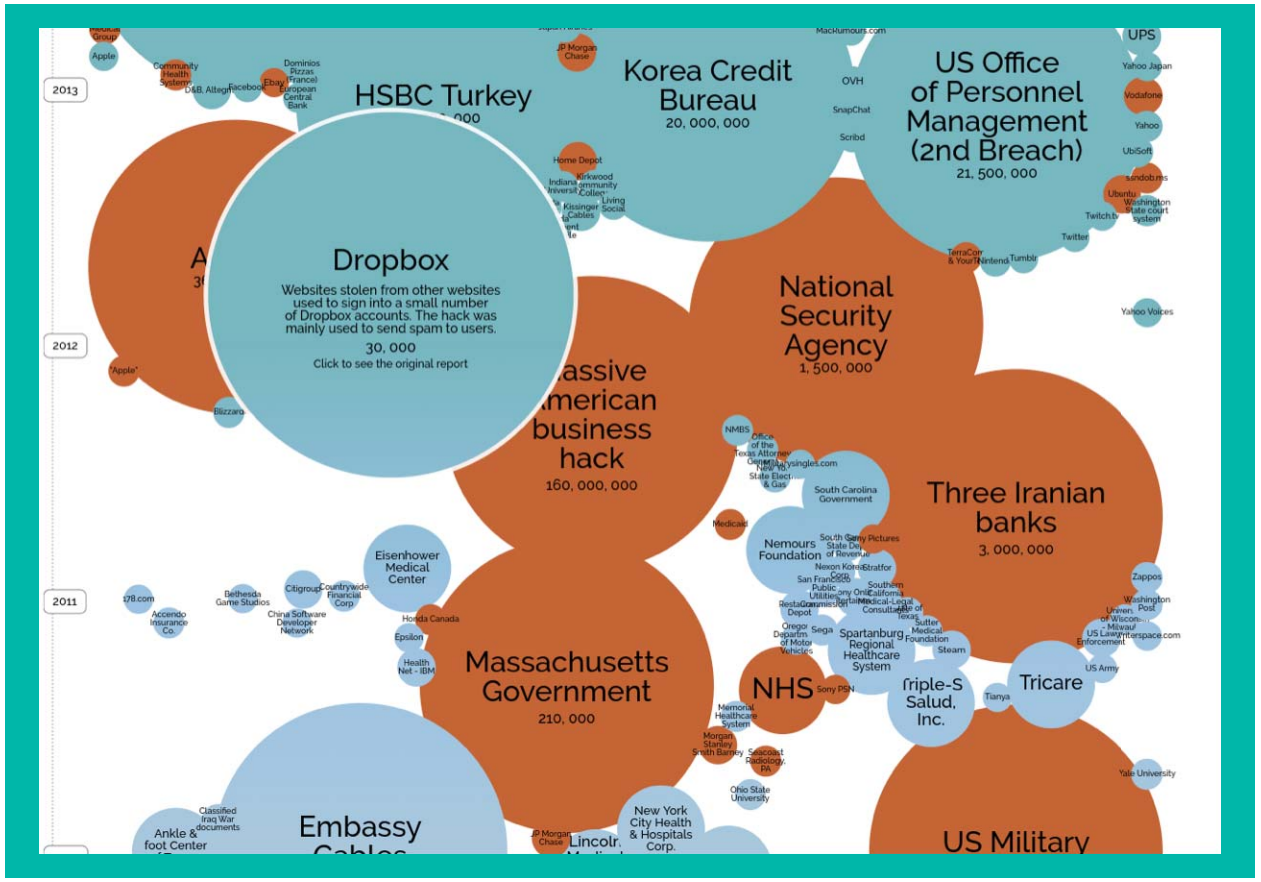
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

ADCA



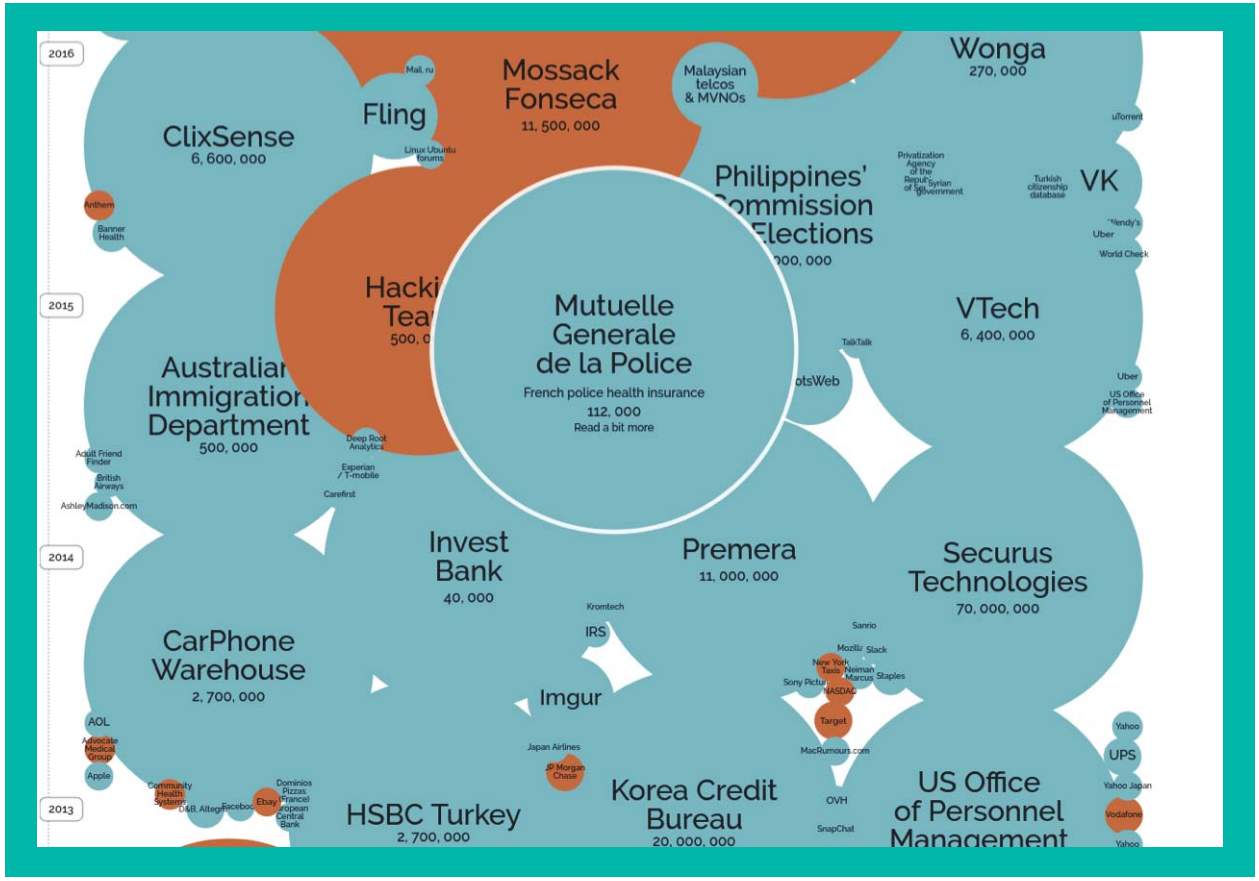
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

ADCA



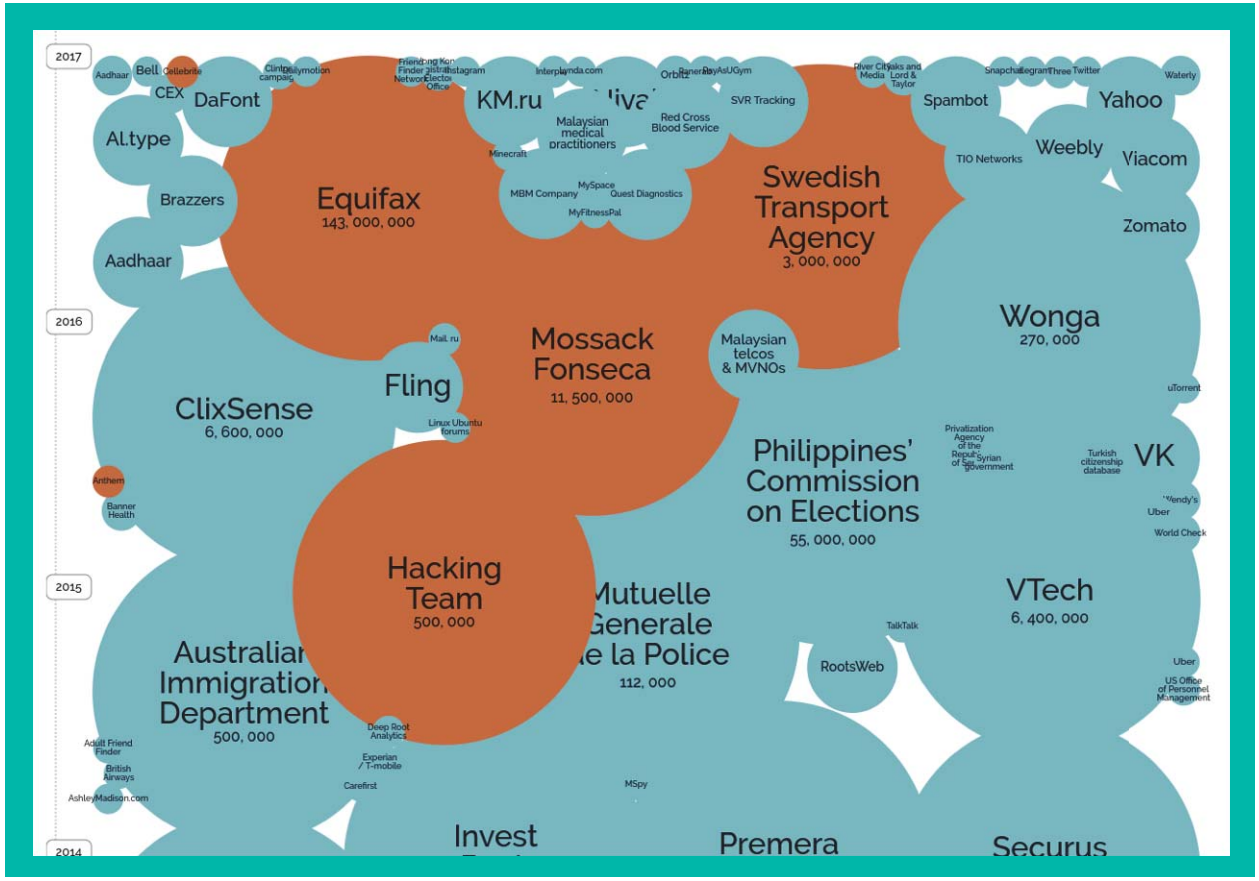
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

ADCA



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

ADCA



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

ADCA

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

ADCA


Business

Business

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

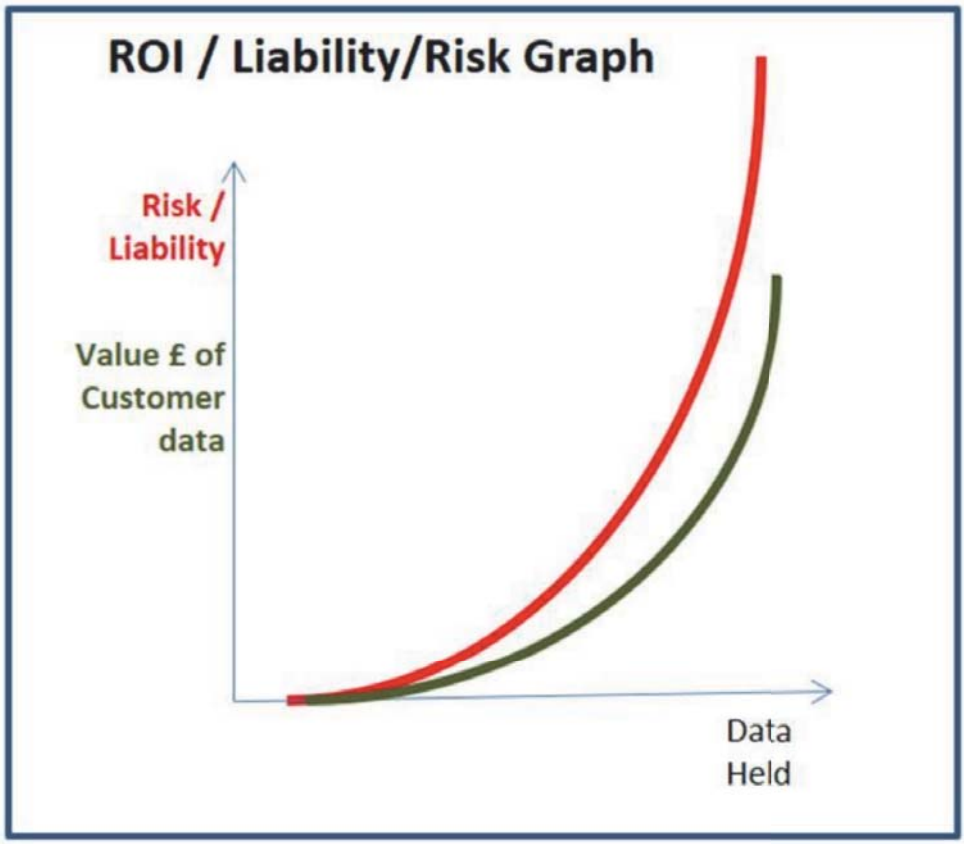
Greater reliance on accurate, up-to-date data

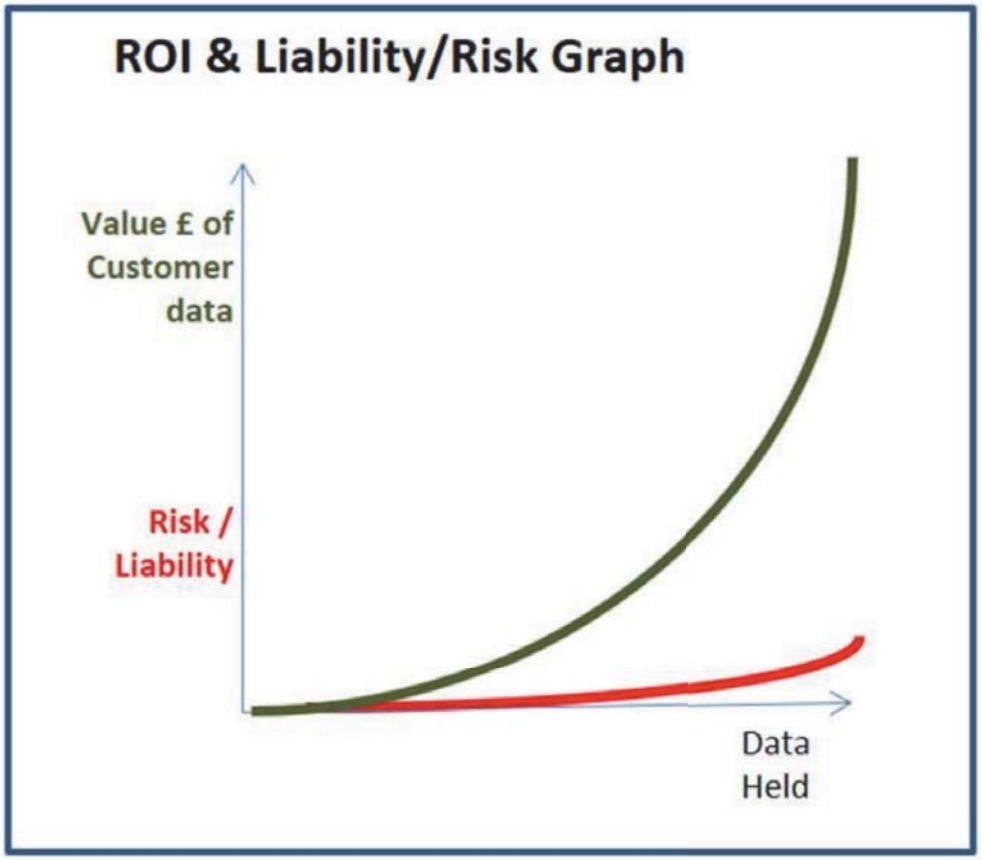
Customer demand for great personalisation

Customer demand for more transparency in data practices

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

ADCA





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

ADCA

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.

ADCA

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

ADCA

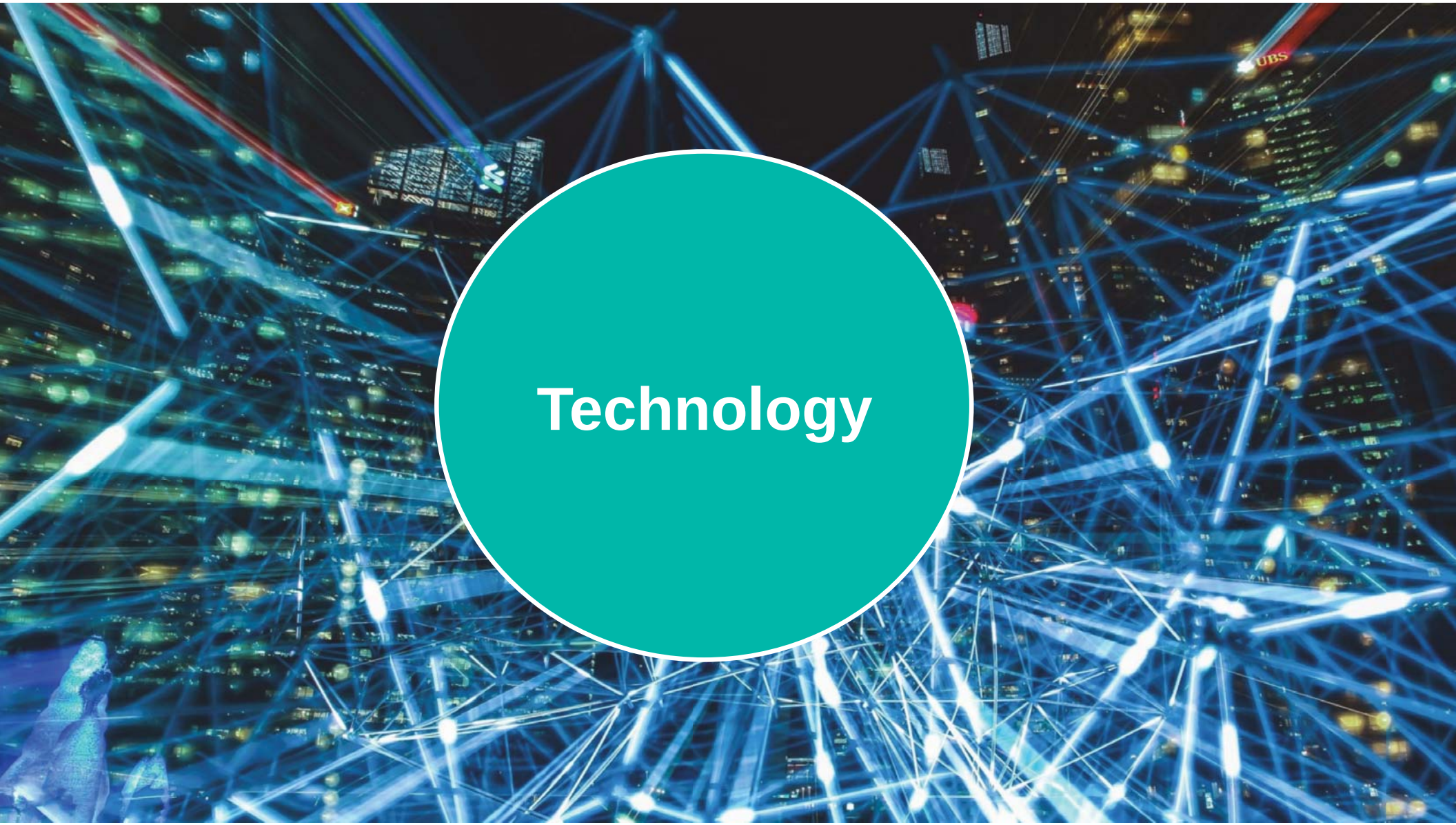
Identity and Human Rights

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.

ADCA



Technology

Technology

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

DPKI - people being able to control their own keys.

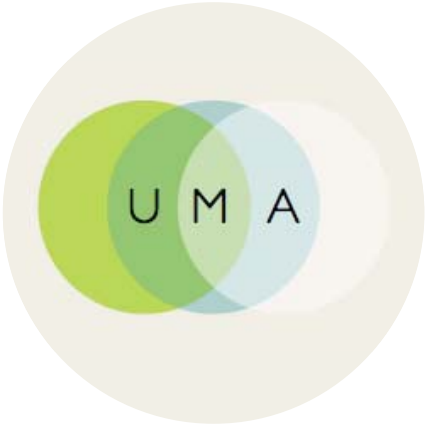
BIP39 - Mnemonic generation. Seed phrases making it easier to deal with than a random string of letters and numbers.

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

ADCA

Oauth, OpenID, User Managed Access



Examples of technologies for User Centric Identity

ADCA

Standards and Consortiums

Consortiums and standards emerging for Self-Sovereign Identity

Decentralised Identity Foundation

W3C

Word Wide Web Consortium

Working groups and emerging standards

- DIDs - Decentralised Identifiers

ADCA

Current Trials

ADCA

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

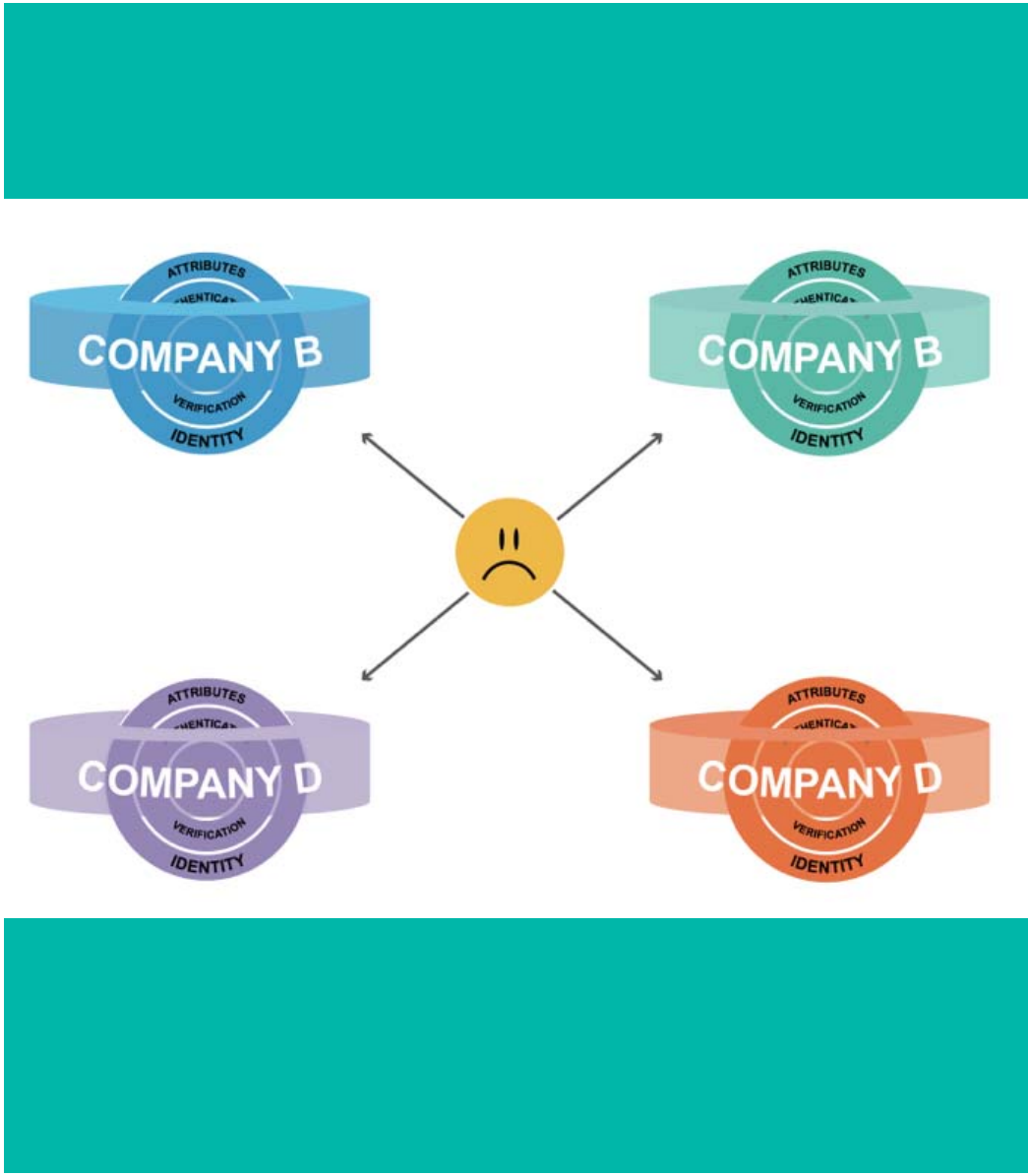
ADCA

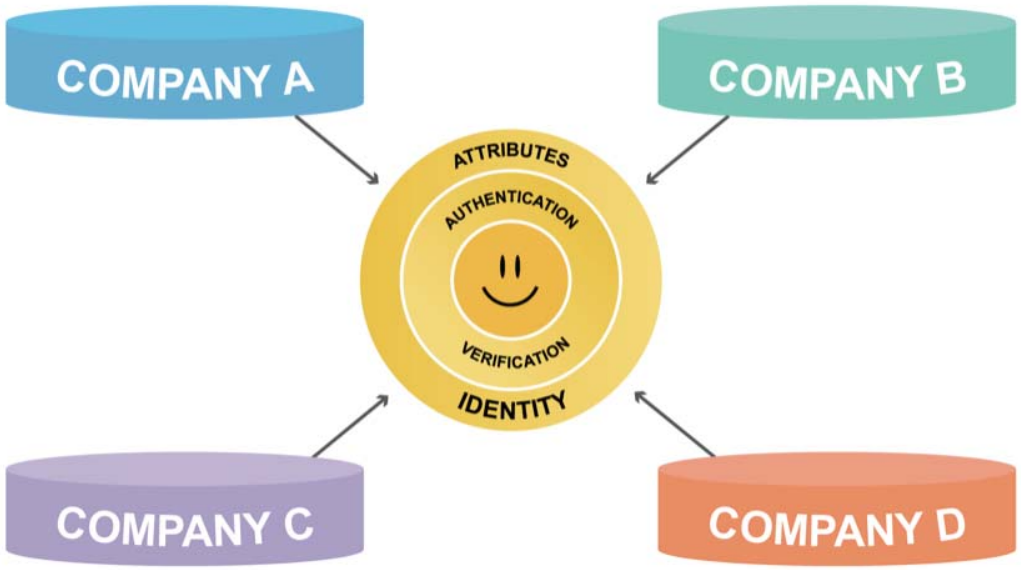
Where Do We Go?

ADCA

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.

ADCA

Control

User permits access to Id

Audit

Access is logged

Security

No walled honeypots

Less Liability

Separate transaction data from id

Veracity of Data

Current and latest

Realtime Updates

Instead of 'one chance to ask'.

ADCA

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

ADCA

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.

Demo

PROMOTING BLOCKCHAIN INNOVATION IN AUSTRALIA

RONALD M. TUCKER

rtucker@adca.asn.au
WeChat: leo_8100