sibos GENEVA
26 - 29 Sep 2016

Education: Blockchain 101 – An introduction to mutual distributed ledgers without the cryptocurrencies

Course agenda

- Establish endeavour: Course objectives
- Assess & appraise:
  - Ledgers
  - Distributed databases
  - Cryptography & hashes
  - Cryptocurrencies
- Lookaheads & likelihoods:
  - Types of MDL
  - Central third parties & natural monopolies
- Options & outcomes: Mutual distributed ledgers in action
- Understanding & undertaking: Applications & ‘use cases’
- Securing & scoring: Possibilities

Mutual distributed ledger timeline

1976 – Diffie-Hellman, Merkle, RSA

1990 – Mondex, Digicash, Flooz

1993 – Encrypted Open Books

1995 – Z/Yen Stacks & Sleeves

1996 – Ricardo payment system

1998 – Wei-Dai b-money, Bitgold

1999 – LOCKSS & CLOCKSS

2000 – Gnutella

2004 – Ripple

2007 – Estonia

2009 – Bitcoin

2012 – Term ‘blockchain’ used

2013 – Silk Road, FBI, Alderney coin

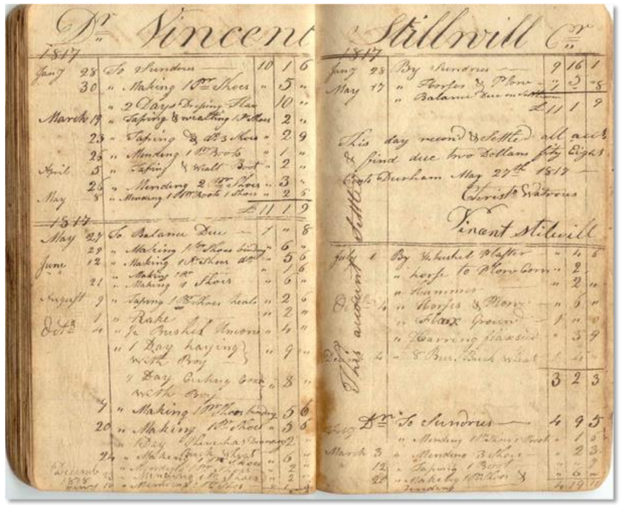
2014 – Regulators – Jersey & Alderney, Isle of Man, FATF, ECB, State of New York

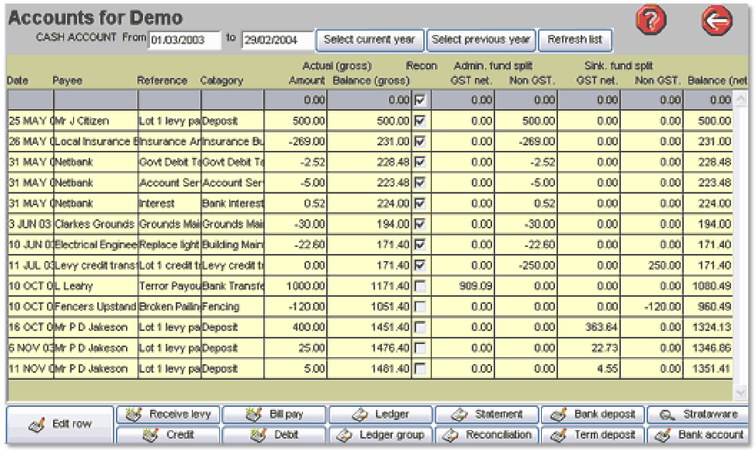
- 2015 – IBM-Samsung, Bank of England research agenda, UK budget for cryptocurrency standards, Barclays, UBS, BNY Mellon, Goldman Sachs, USAA, NASDAQ, Honduras land registry, Channel Islands Standards for MDLs, Fine (sic) Sign of having arrived – Ripple $700,000, Sign of the Tines – Bitcoin forking hell, Economist Special, FT Special

- 2016 – UK government, Blythe Masters DAH, R3, SafeShare Insurance, XLRAS, …

What is a ledger?

“A ledger is a book, file, or other record of financial transactions.”





Source: https://en.wikipedia.org/wiki/Tally_stick]
Source: http://www.rootsweb.ancestry.com/~nygreen2/wpeF7.jpg]
Source: https://en.wikipedia.org/wiki/Ledger]

A ledger of ledgers

- Sumerian cuneiform tablets 4th millennium BC
- Earliest tally sticks record amounts, see Pliny the Elder (AD 23-79)
- Manucci (1299), double entry book keeping documented in Venice by Luca Pacioli in 1484
- Ledgers referred to in England in 16th Century AD, in churches
- 19th century – financial ledgers widespread
- Punch card (Hollerith), paper tape, magnetic tape, disks…

Possibly distributively ledgerable

Area	Possible Applications
Financial instruments, records, models	Currency, private and public equities, certificates of deposit, bonds, derivatives, insurance policies, voting rights associated with financial instruments, commodities, derivatives, trading records, credit data, collateral management, client monies segregation, mortgage or loan records, crowd-funding, P2P lending, microfinance, (micro)charity donations, account portability, airmiles & corporate tokens, etc.
Public records	Land and property titles, vehicle registries, shipping registries, satellite registries, business license, business ownership/incorporation/dissolution records, regulatory records, criminal records, passport, birth/death certificates, voting ID, health and safety inspections, tax returns, building and other types of permits, court records, government/listed companies/civil society, accounts and annual reports, etc.
Private records	Contracts, ID, signature, will, trust, escrow, any other type of classifiable personal data (e.g. physical details, date of birth, taste) etc.
Semi-private/semi-public records	High school/university degrees and professional qualifications, grades, certifications, human resources records, medical records, accounting records, business transaction records, locational data, delivery records, genome and DNA, arbitration, genealogy trees, etc.
Physical keys	Key to home, hotel, office, car, locker, deposit box, mail box, Internet of Things, etc.
Intellectual property	Copyrights, licenses, patents, digital rights management of music, rights management of intellectual property such as patents or trademarks, proof of authenticity or authorship, etc.
Other records	Cultural, historical events, documentary (e.g. video, photos, audio), (big) data (weather, temperatures, traffic), SIM cards, archives, etc.

Evolution of databases

1960s: IBM Develop Hierarchical Databases to store information, taking advantage of new storage capacity, e.g., SABRE, IMS Network Model also developed, but fails to become widely accepted

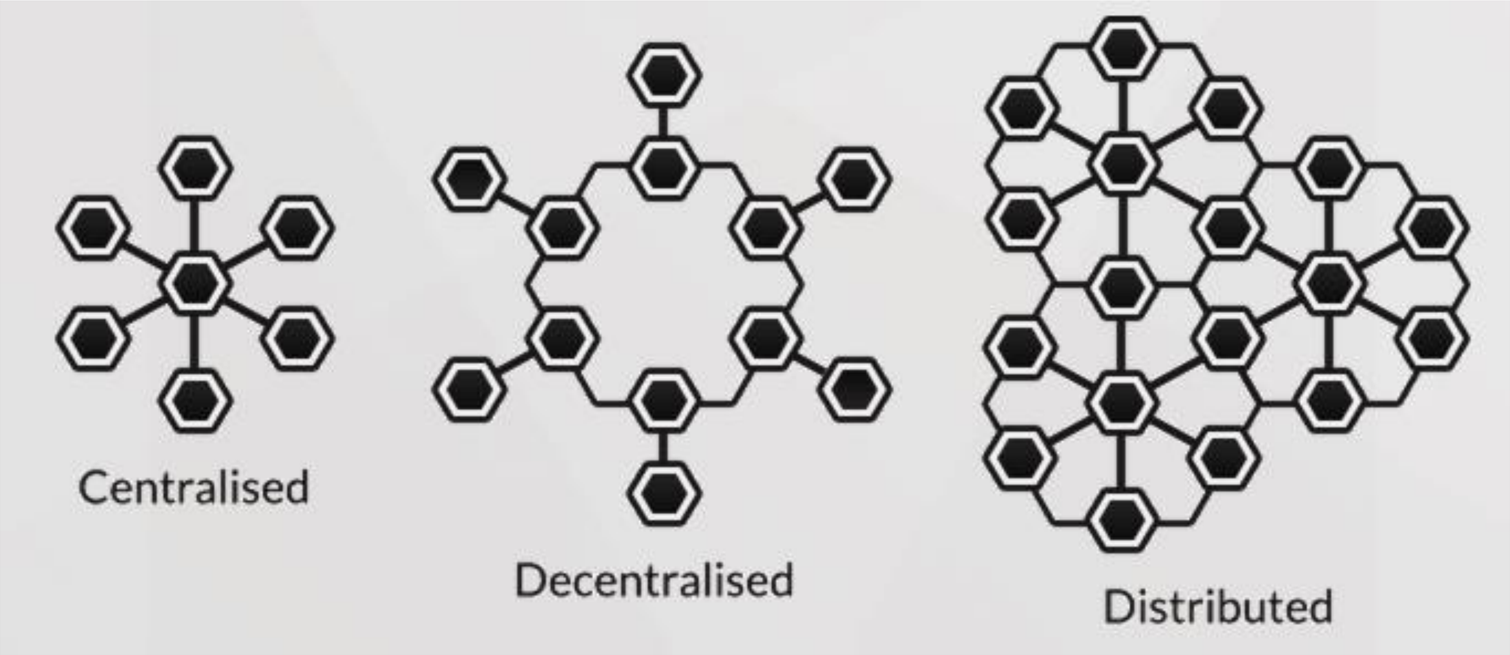
1970s: Codd's Relational Databases proposed, allowing search by content and more flexible relationships, e.g., INGRES, System R

1980s: Increased computing power allows Relational Databases to become dominant, e.g., DB2, PARADOX, RBASE 5000

1990s: Object Oriented Databases followed by Internet Database Connectors allow different types of data to be stored and queried, e.g., Oracle, Access, ODBC

2000s: NoSQL – high performance, highly scalable, denormalized data takes advantage of distributed storage and fast connections, e.g., Cassandra, HBase, Neo4j

Using Peer to Peer (P2P) Networks



napster™

gnutella

Freenet

skype™

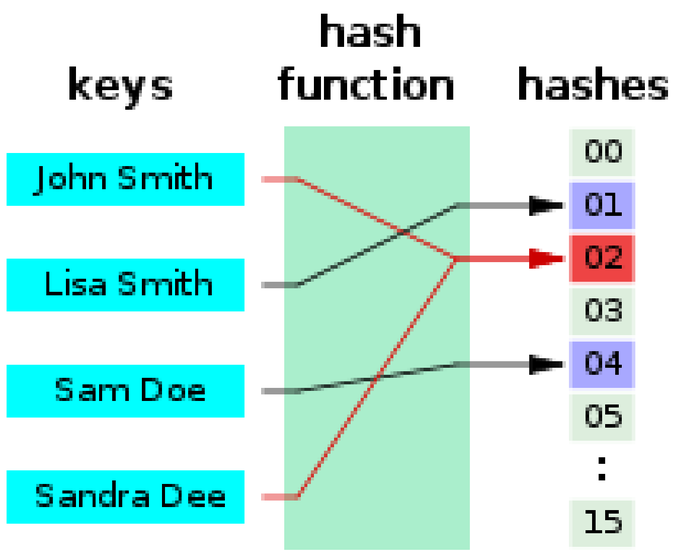
Source: Nick Williamson, “What Is A Blockchain?” (12 April 2015) - http://blog.credits.vision/what-is-a-blockchain/

Three types of document transformation

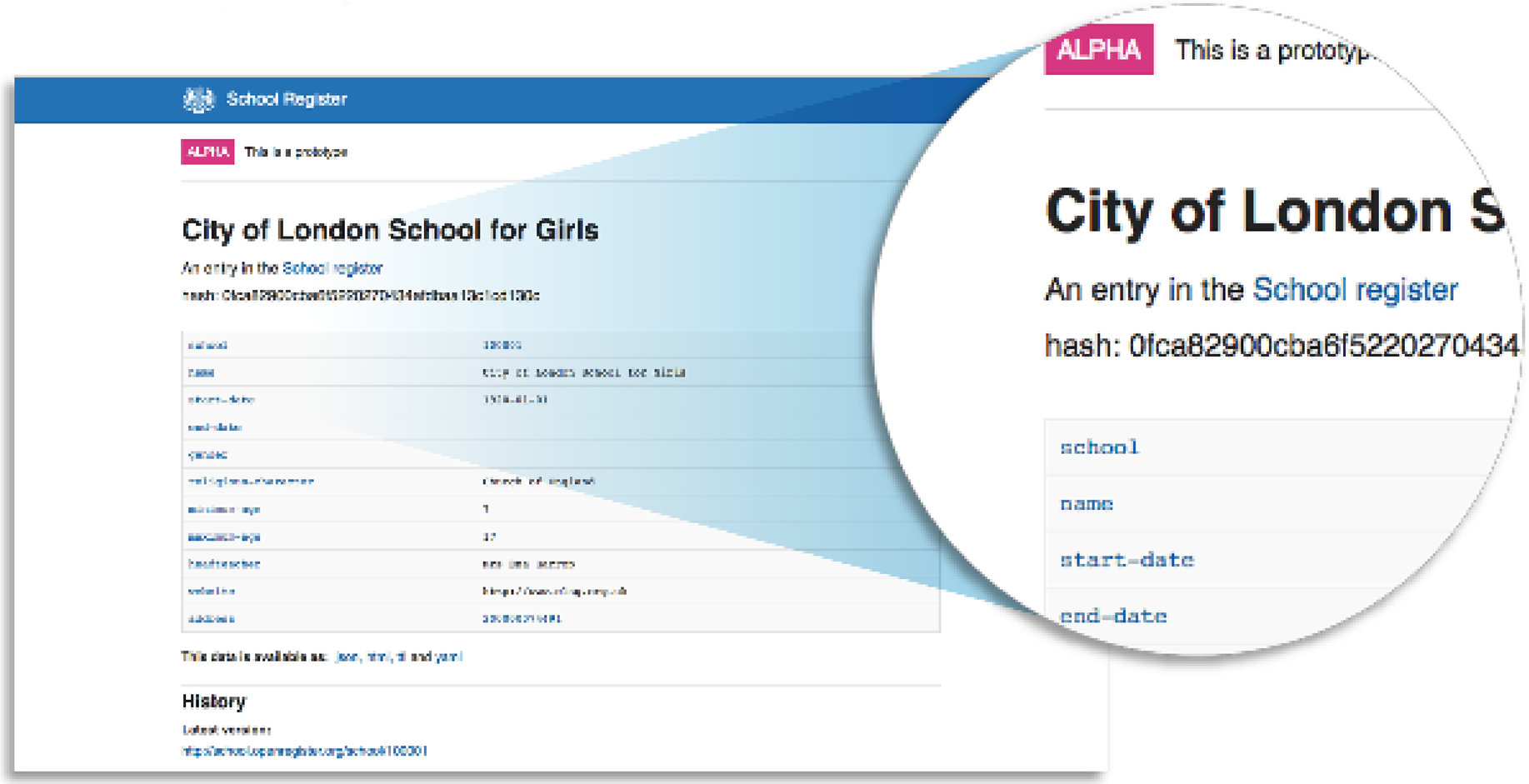
Type	Use	Result?	Reversible?
Compression	Storing and exchanging large files	Variable length	YES
Hashing	To create an empirically unique simplified representation of a file	Fixed length	NO
Encryption	To prevent unauthorized reading of a file	Variable length	YES

Simple hash function

- Hash – transform data into a set of characters of fixed length
- Used to index data in databases, and also to add extra security to encryption

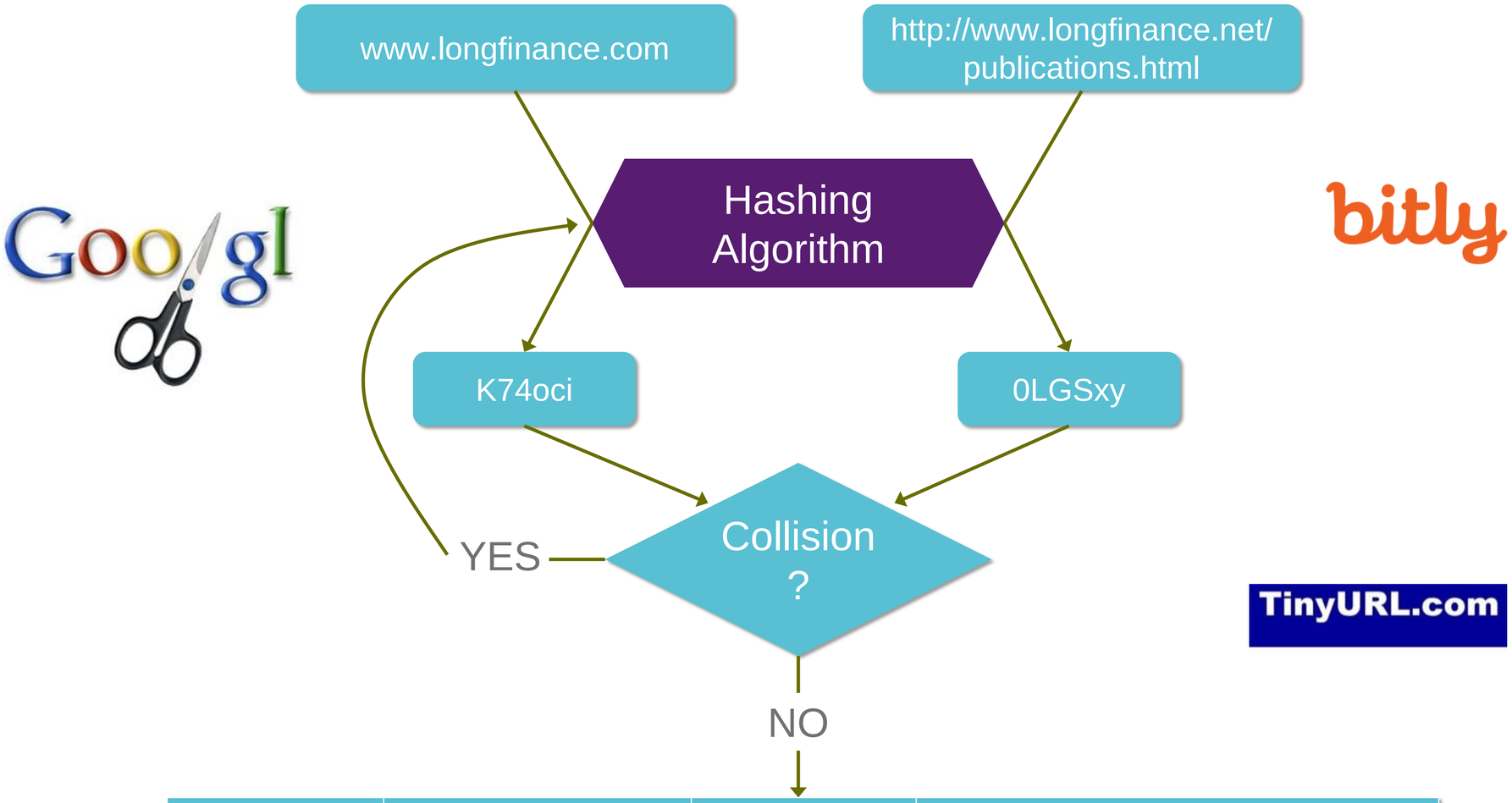


Prototype hash in a register



Source: http://media.coindesk.com/2015/09/Screenshot-of-an-entry-in-a-basic-prototype-.png

In hash’tice



GOO.GL	TinyURL	Bitly	Original URL
goo.gl/K74oci	tinyurl.com/h7ab2lh	bit.ly/211h1fj	www.longfinance.net
goo.gl/0LGSxy	tinyurl.com/jqadrh5	bit.ly/21bedZt	www.longfinance.net/publications
goo.gl/7ctZo	tinyurl.com/2c3vo6	bit.ly/1DTsoao	www.bankofengland.co.uk

Evolution of cryptography

- Early encryption examples include Egyptian Cipher in 1900 BC, the Caesar Cipher (A=D, B=E, C=F)
- 20th Century computers allowed for more secure codes and decoding, e.g., Enigma
- Symmetric key cryptography required a key to be shared physically
- 1976 Diffie-Hellman article proposed public-key cryptography, removing the need for physical exchange of keys

Encryption – Simple ciphers

Mutual Distributed Ledgers

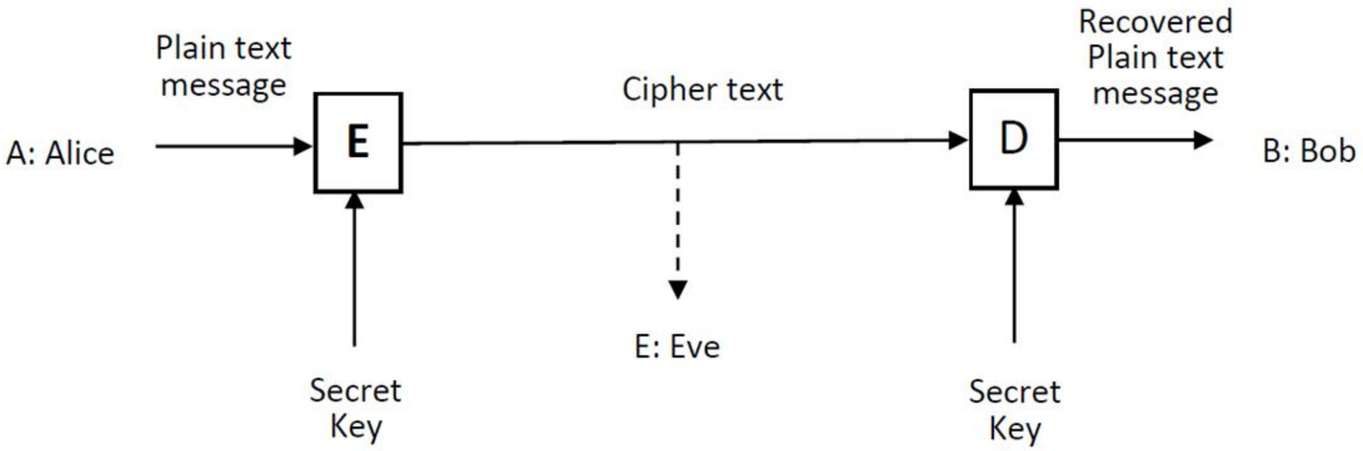
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

5 Step Shift

RZYZFQ INXYWNGZYJI QJILJWX

Encryption – Symmetric key cryptography



Example – Scrambling

At the transmitter

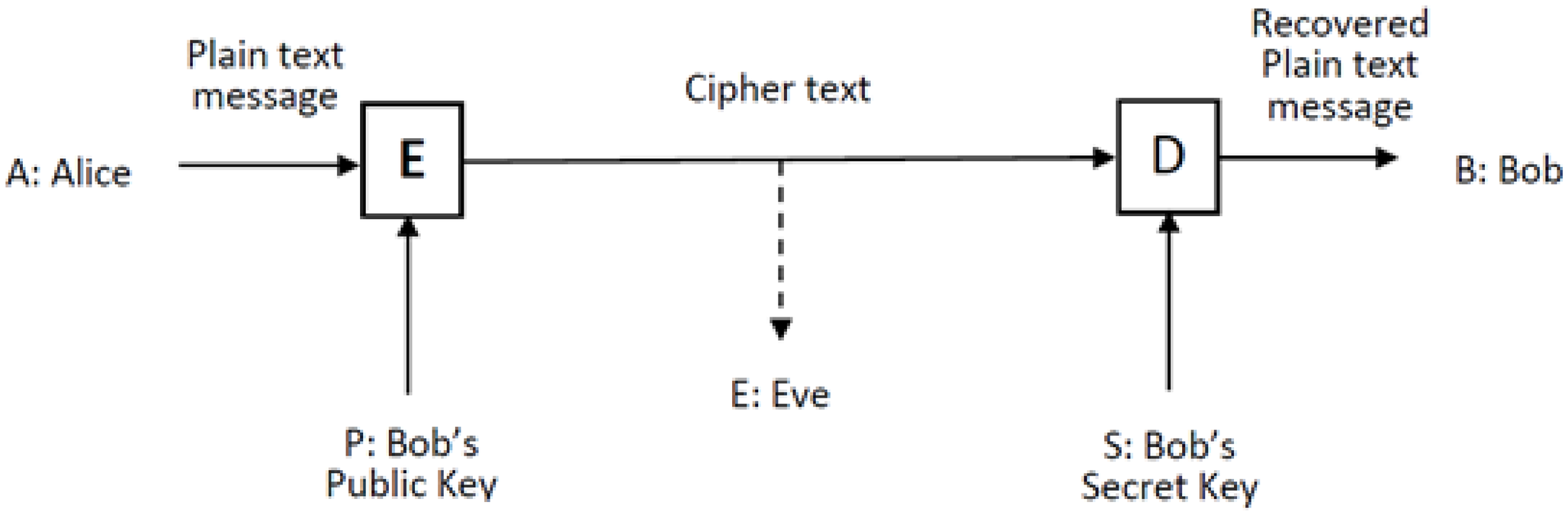
Message digits:	1 3 5 2 6 7 8
Random digits:	9 0 4 6 3 1 8
Addition gives:	0 3 9 8 9 8 6, Scrambled message

At the receiver

Scrambled message:	0 3 9 8 9 8 6
Random digits:	9 0 4 6 3 1 8
Subtraction gives:	1 3 5 2 6 7 8, Recovered 'plain text' message

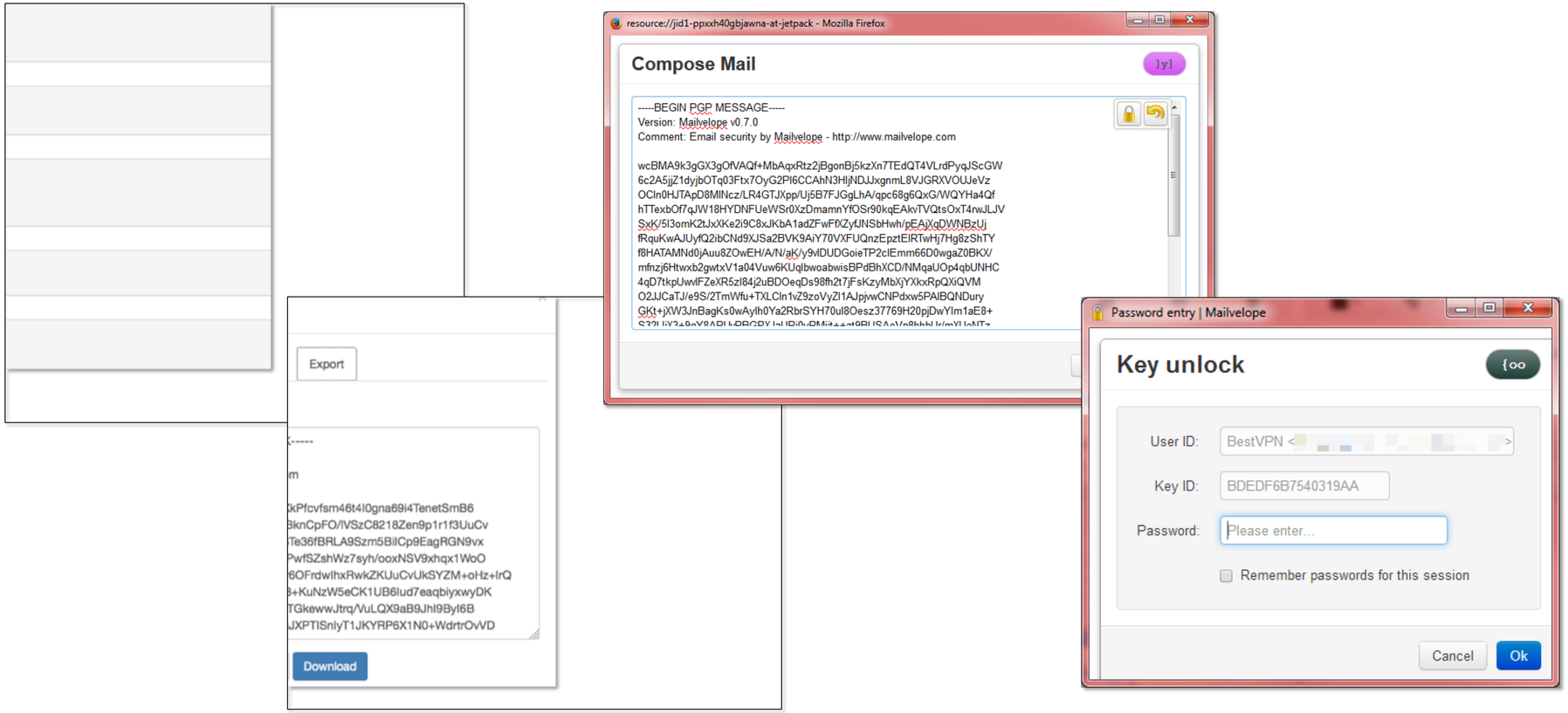
Source: http://www.gresham.ac.uk/lectures-and-events/cybersecurity-modified-rapture-sir-john-oreilly - February 2016

Public-private key cryptography



Source: http://www.gresham.ac.uk/lectures-and-events/cybersecurity-modified-rapture-sir-john-oreilly - February 2016

Public-private key in action: Mailvelope



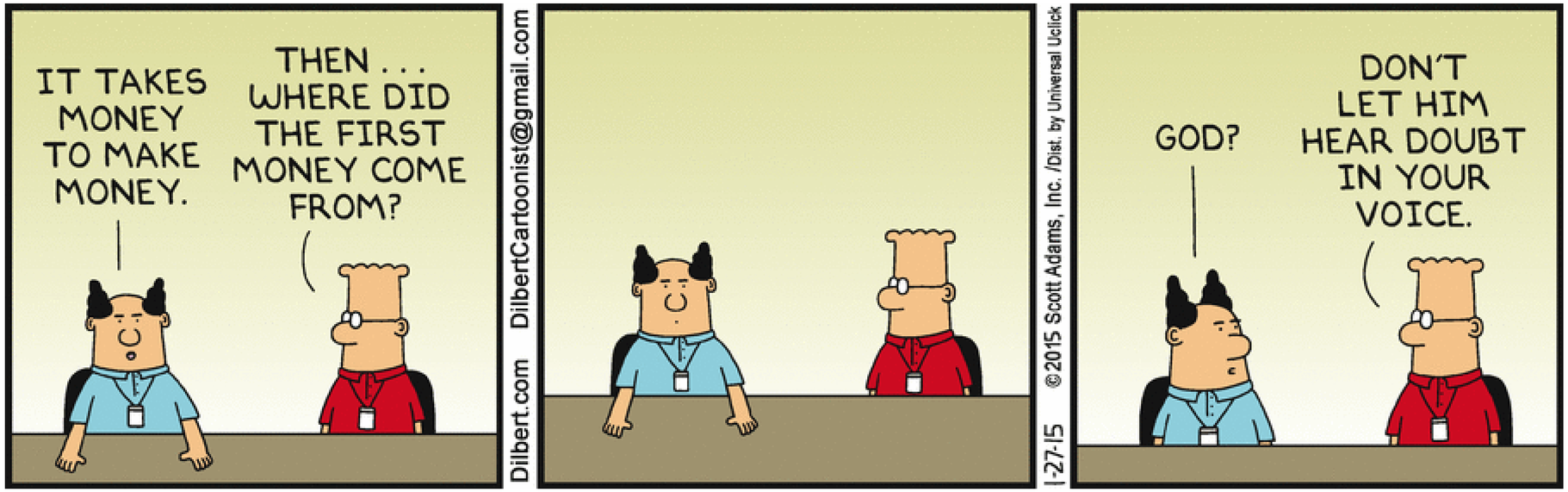
CREATE KEY

EXCHANGE KEY

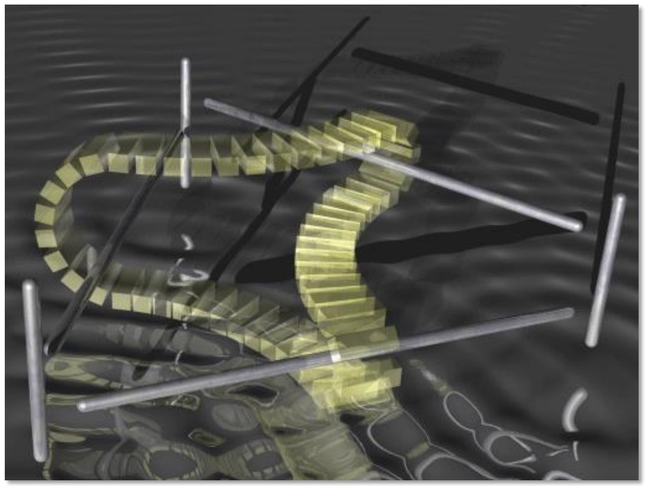
ENCRYPT EMAIL

DECRYPT EMAIL

The study of money is the root of much madness



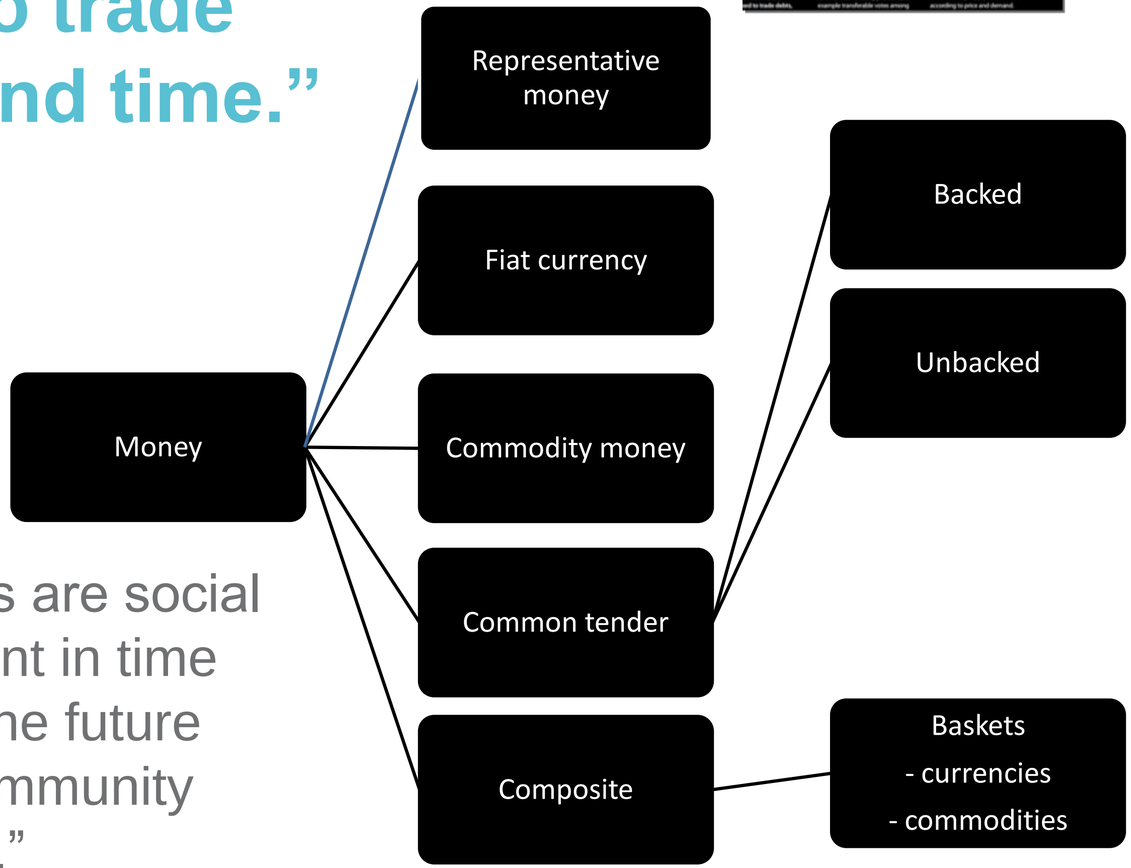
LONG FINANCE



Source: http://illusionsetc.blogspot.com/2005/08/moving-mobius-strip.html

Money as technology

“Money is a technology communities use to trade debts across space and time.”

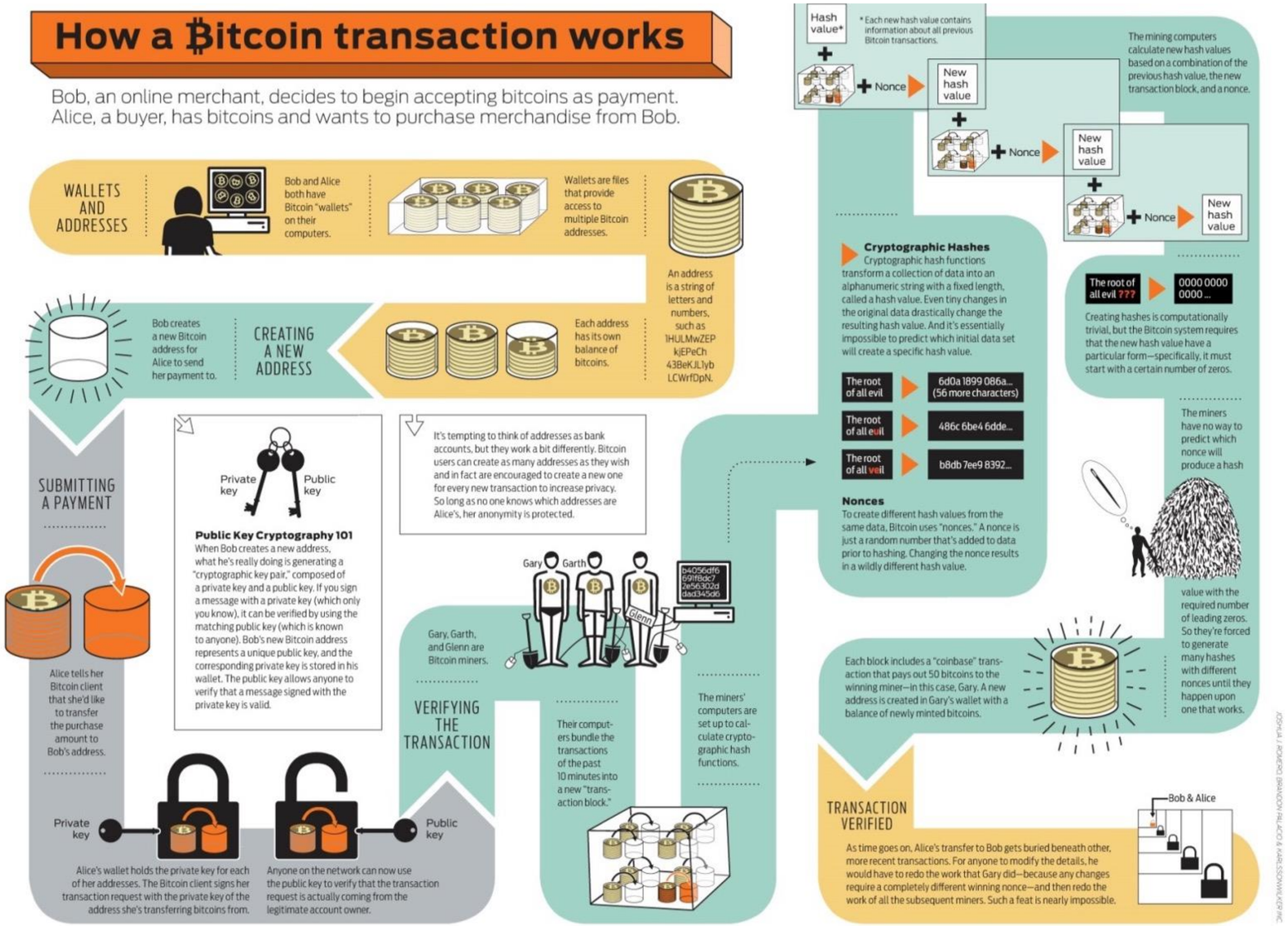


“Tokens of indebtedness are social desires frozen at a point in time – tokens depend on the future persistence of the community and its values.”

Cryptocurrencies: Money or virtual elements?

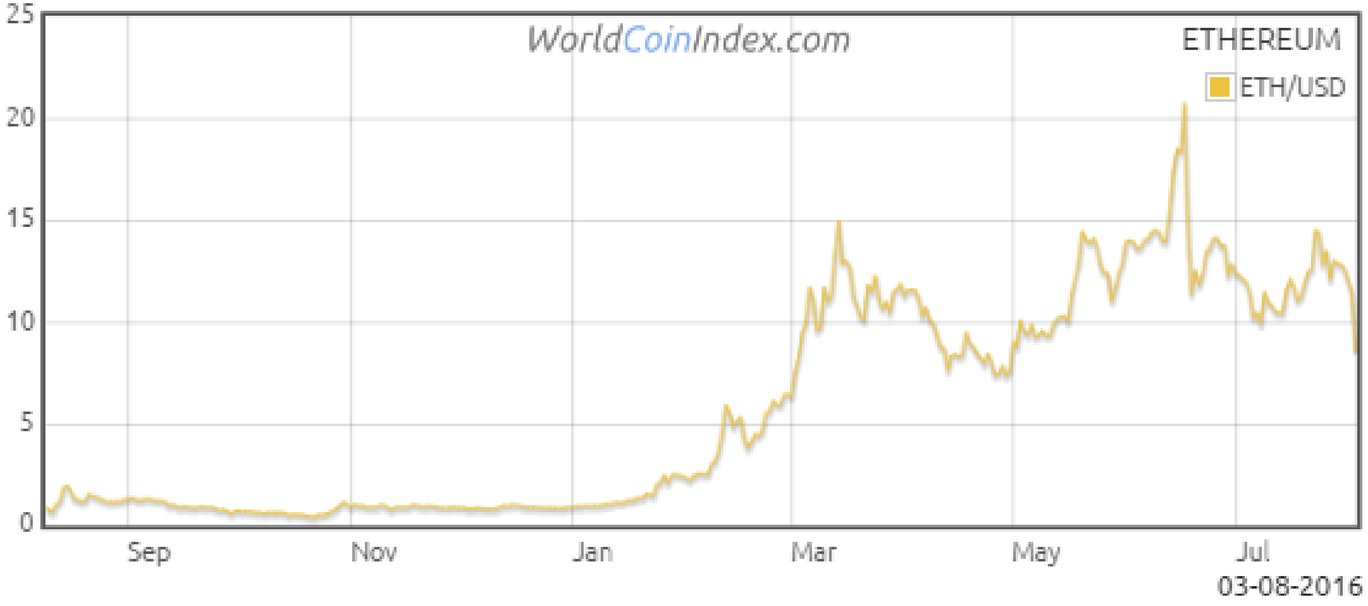
- Cryptocurrencies were invented as peer-to-peer systems for online payments that do not require a trusted central authority
- Bitcoin uses consensus in a massive peer to peer network to verify transactions

Bitcoin primer

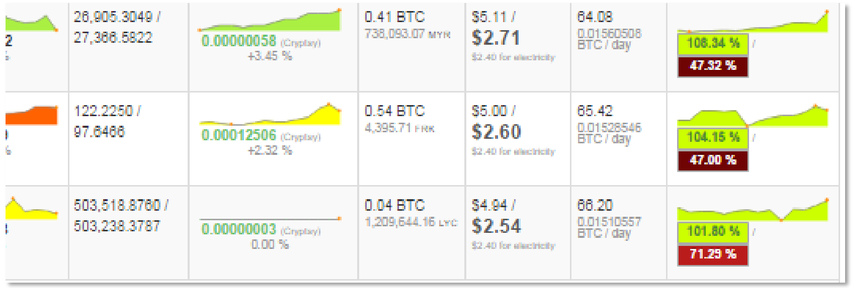


Source: Spectrum.ieee.org "How a Bitcoin Transaction Works"

Bitcoin & ethereum over time



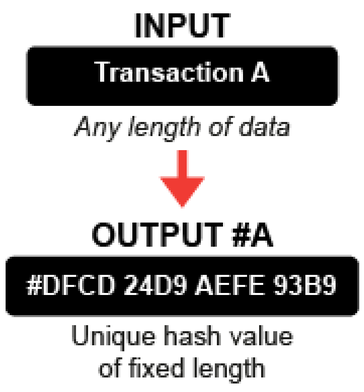
Mining is hard work – Bitcoin preponderant

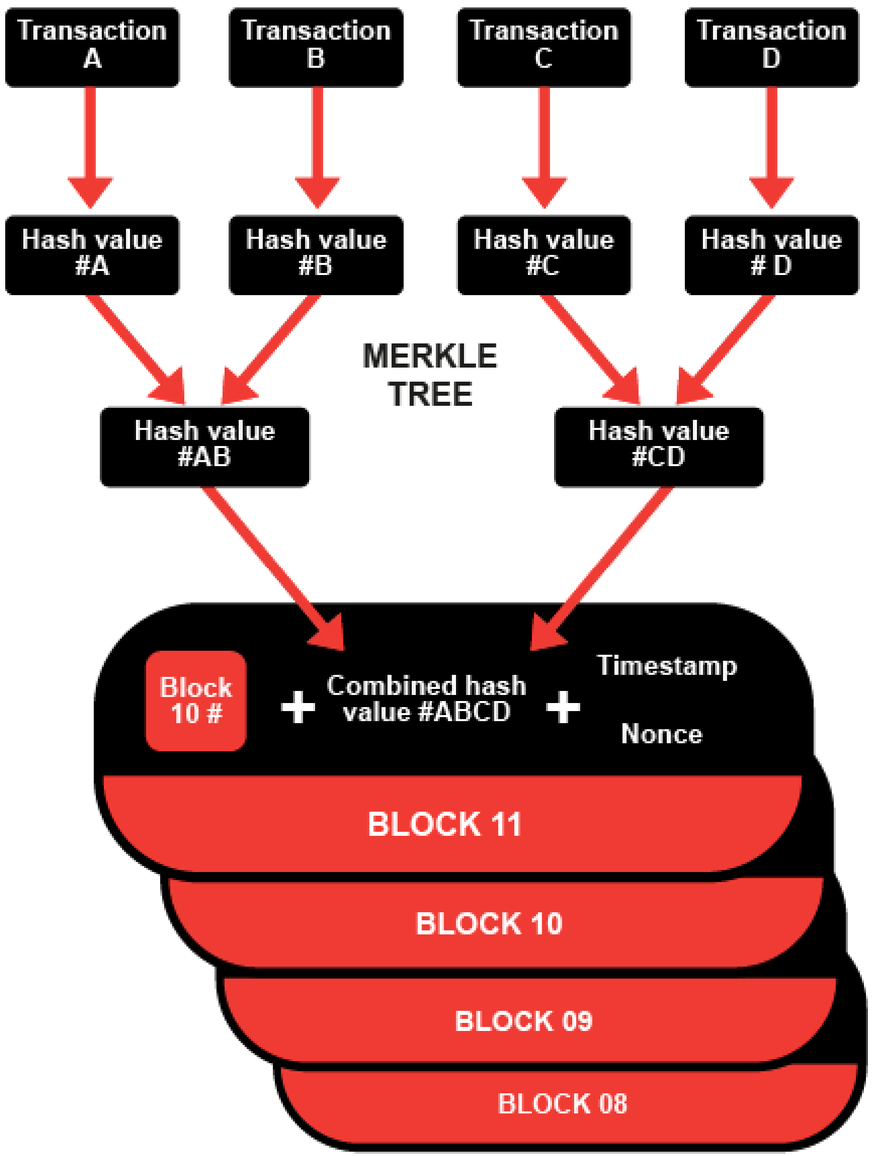


2	26,905.3049 / 27,366.5822	0.00000058 (Cryptay) +3.45 %	0.41 BTC 738,093.07 MYR	$5.11 / $2.71 $2.40 for electricity	64.08 0.01560506 BTC / day	108.34 % / 47.32 %
	122.2250 / 97.6466	0.00012506 (Cryptay) +2.32 %	0.54 BTC 4,395.71 FRK	$5.00 / $2.60 $2.40 for electricity	65.42 0.01528546 BTC / day	104.15 % / 47.00 %
	503,518.8760 / 503,238.3787	0.00000003 (Cryptay) 0.00 %	0.04 BTC 1,209,644.16 LYC	$4.94 / $2.54 $2.40 for electricity	66.20 0.01510557 BTC / day	101.80 % / 71.29 %

Source: http://www.coinwarz.com/cryptocurrency#

Overview of Blockchain





Making a hash of it…

Ledgers: Look beneath the coins

"… the potential impact of the distributed ledger may be much broader than on payment systems alone. The majority of financial assets - such as loans, bonds, stocks and derivatives - now exist only in electronic form, meaning that the financial system itself is already simply a set of digital records."

Bank of England, Quarterly Bulletin (2014, Q3)

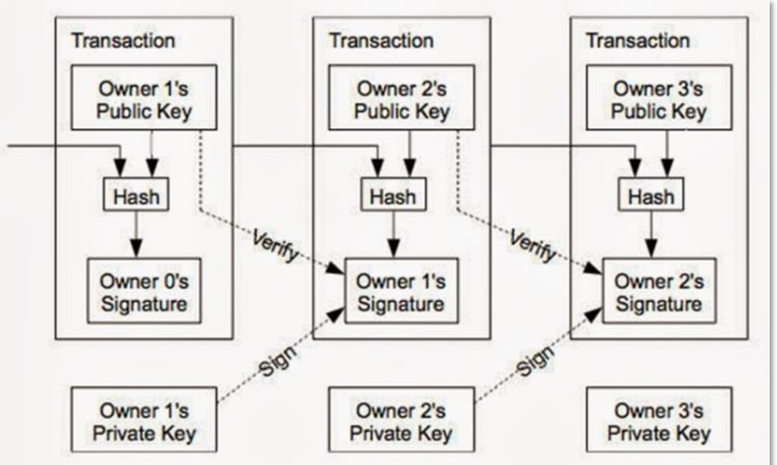


Diagram of a Bitcoin
from *Bitcoin: A Peer-to-Peer Electronic Cash System*, published in 2008 by "Satoshi Nakamoto".

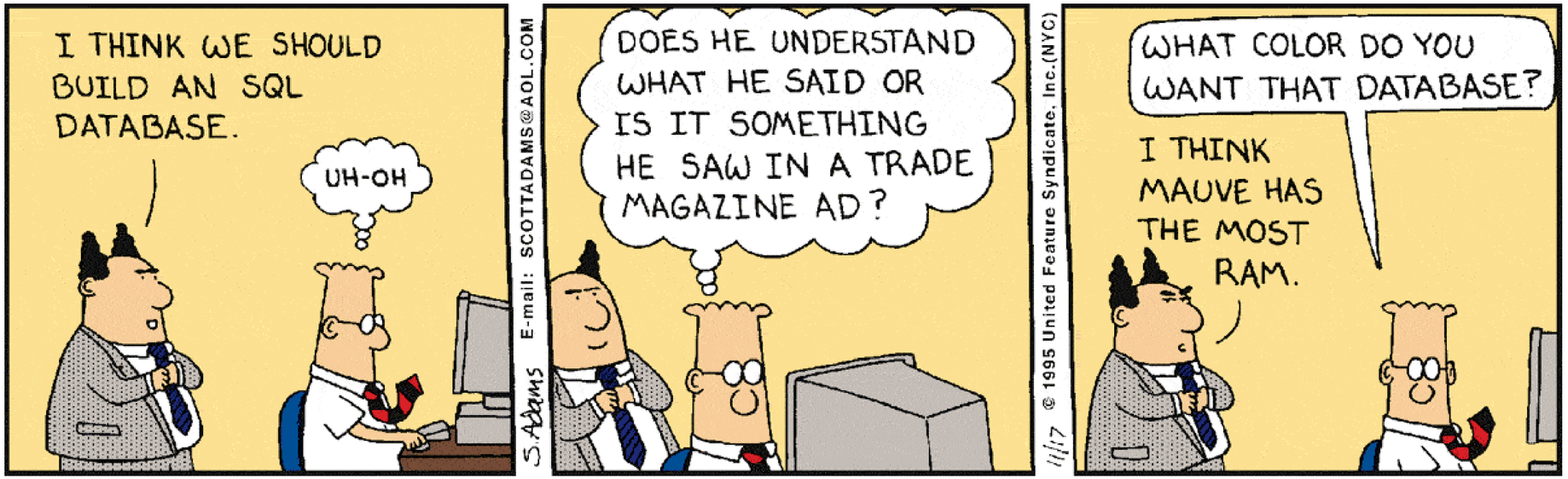
"In distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation."

Matthew Hancock & Ed Vaizey (January 2016)

Lookaheads & likelihoods

Source: Ken Tindell mashup - 14 May 2015 https://twitter.com/kentindell/status/598865133247569920

The old old new new thing…



[Internet (1976 for me), databases (Oracle, Ingres, DBII, relational/hierarchical/distributed), web (SGML, Gopher), ‘Internal Internets’ (i.e. intranets), social media (SixDegrees)…]

Source: www.dilbert.com, Friday, 17 November 1995

Terminology evolving

- Ledger – a record of transactions
- Distributed – divided among several or many, in multiple locations
- Mutual – shared in common, or owned by a community
- Mutual distributed ledger (MDL) – a record of transactions shared in common and stored in multiple locations
- Mutual distributed ledger technology – a technology that provides an immutable record of transactions shared in common and stored in multiple locations
- Blockchain – “a transaction database shared by all nodes participating in a system based on the Bitcoin protocol”

What is a central third party?

Validate – Entries

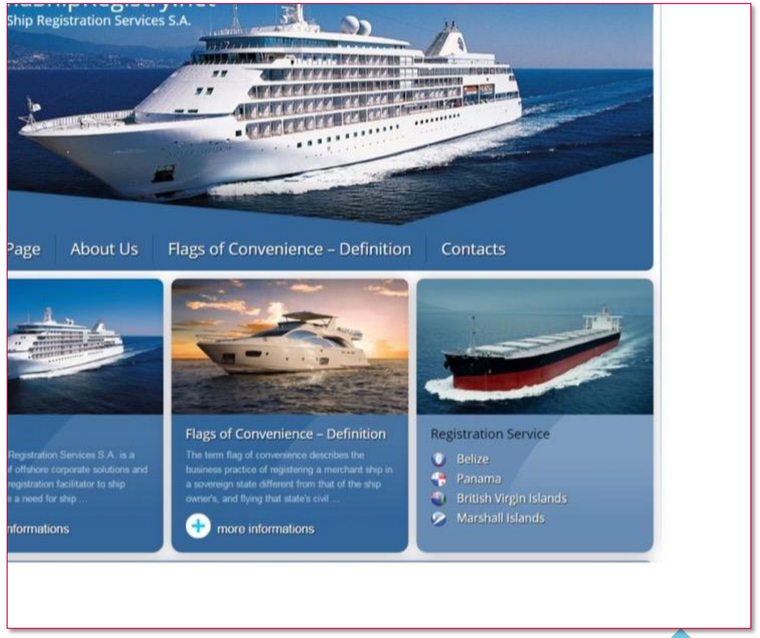
Safeguard – Transactions

Preserve – Historic record

Why does a central registry exist?

Financial services are based on ‘mistrust’ & leverage

- Validate - Sin of Commission
  – *forgery of a transaction*
- Safeguard - Sin of Deletion
  – *reversal of a transaction*
- Preserve - Sin of Omission
  – *censorship of a transaction*



Reducing natural monopolies

? Validate – “a trust model for timestamping”

✓ Safeguard – “a set of rules for updating state via blocks”

✓ Preserve – “a shared state”

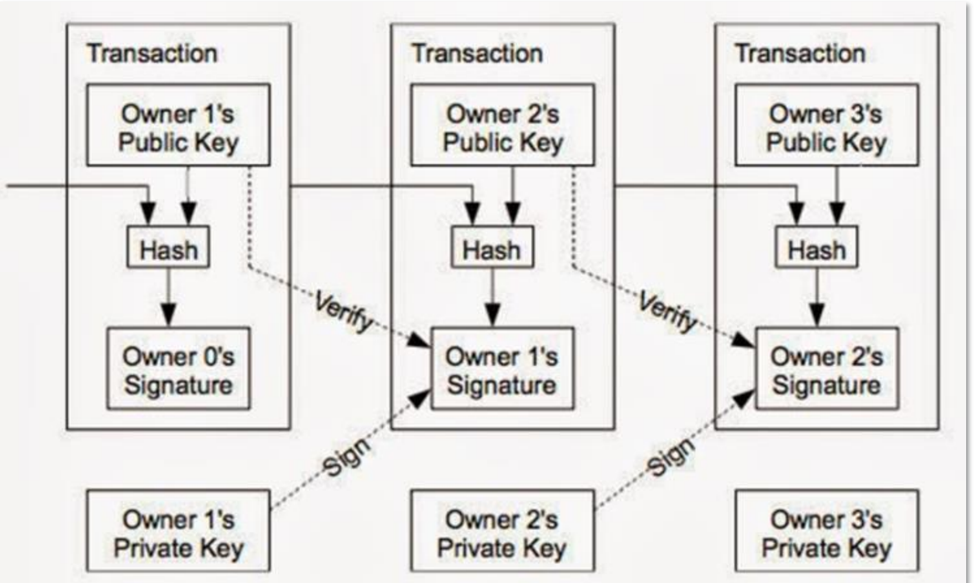
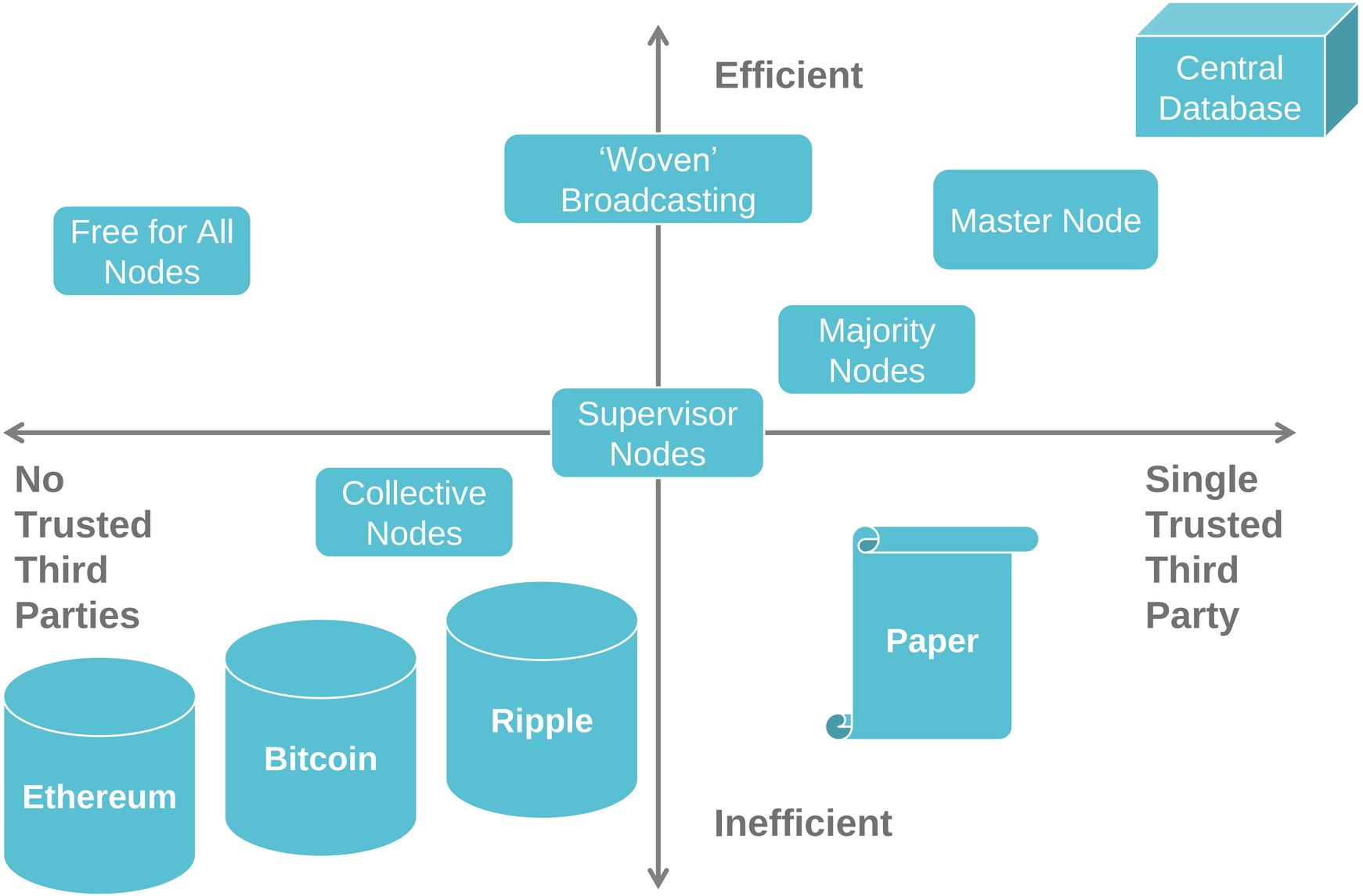
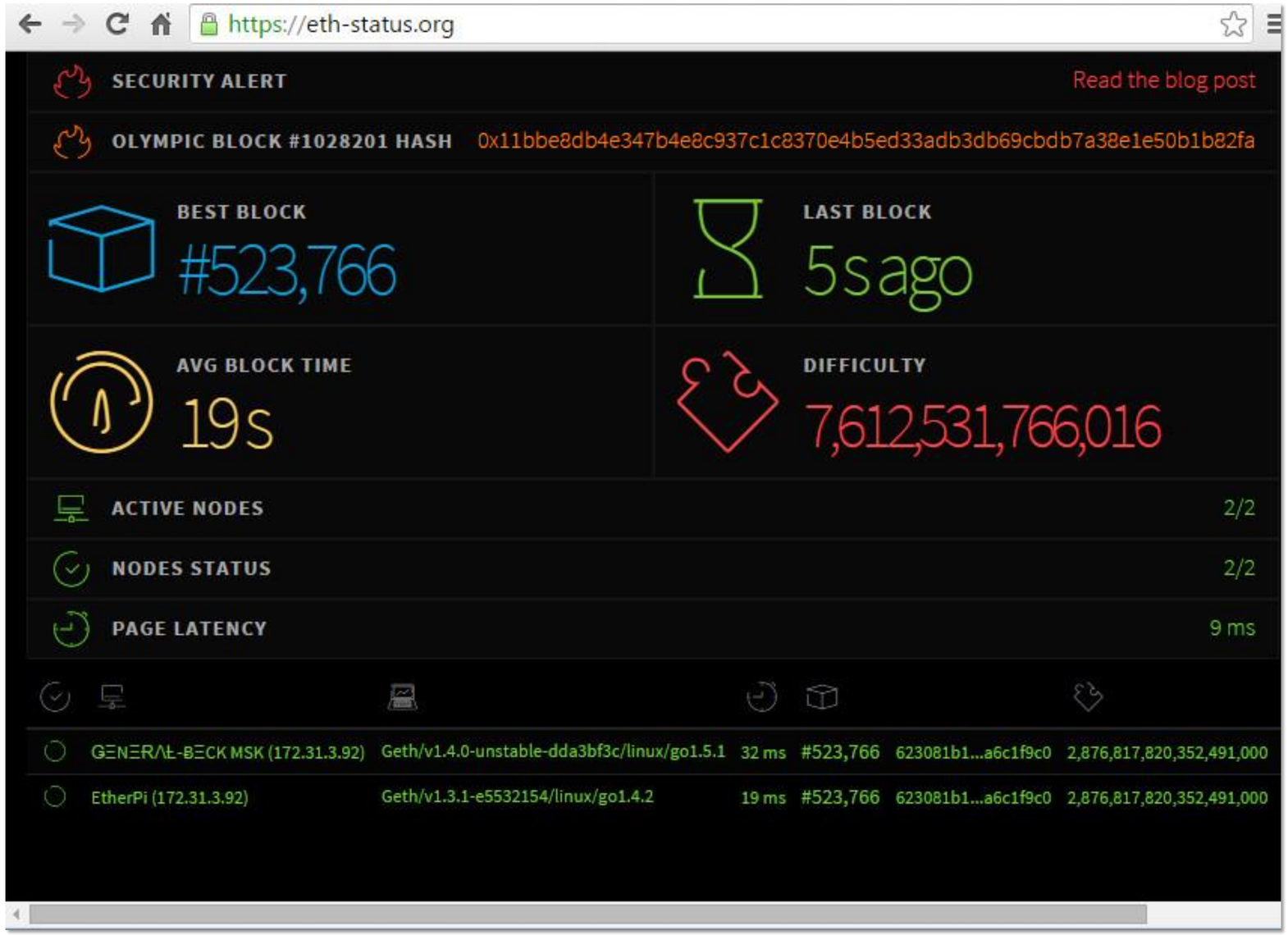


Diagram of a Bitcoin
from *Bitcoin: A Peer-to-Peer Electronic Cash System*, published in 2008 by “Satoshi Nakamoto”.

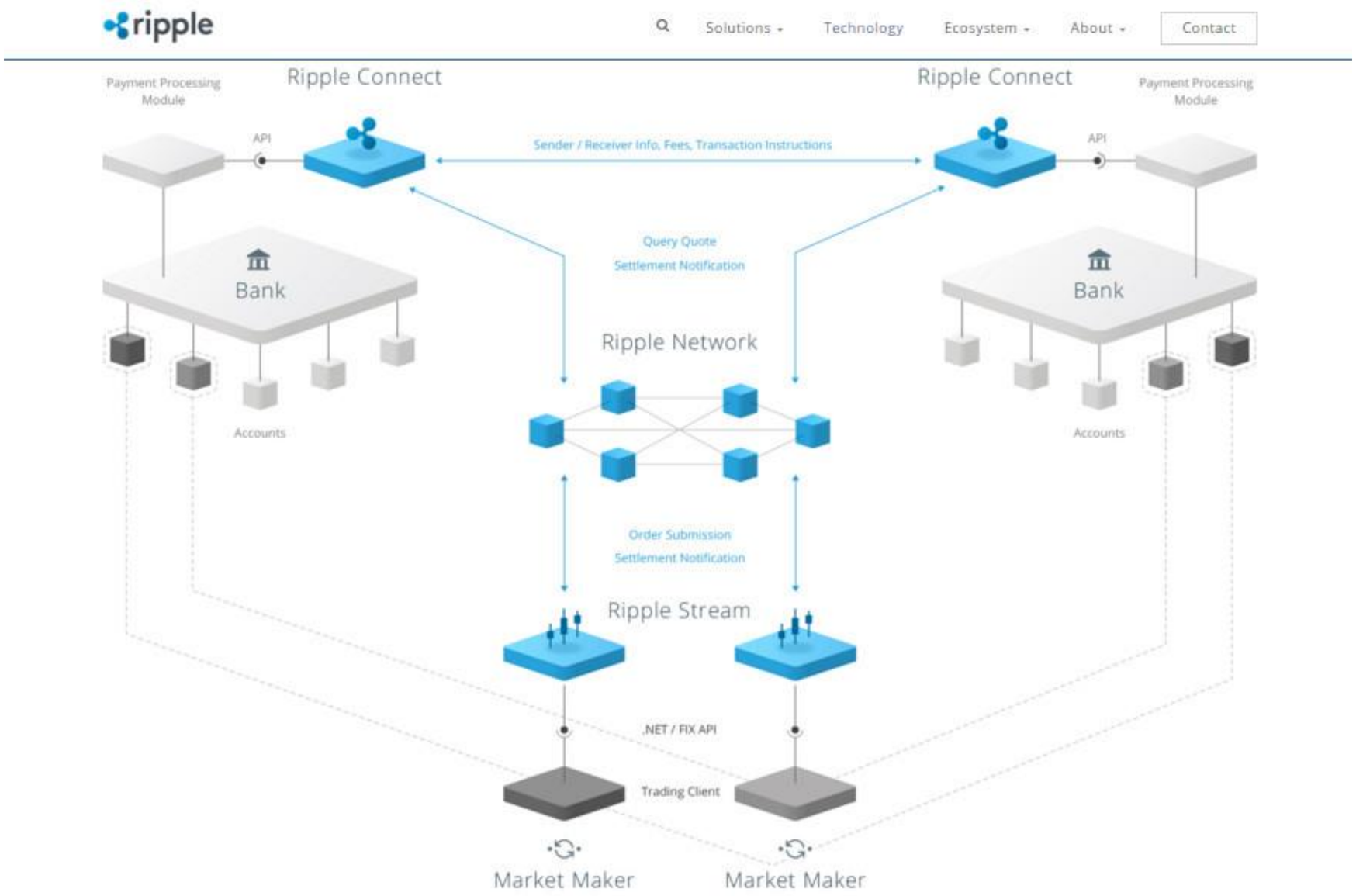
Mistrust costs coins



Example: Ethereum



Example: Ripple



Options & Outcomes

Cloud For Ledgers: Hire A Semi-Trusted Third Party!

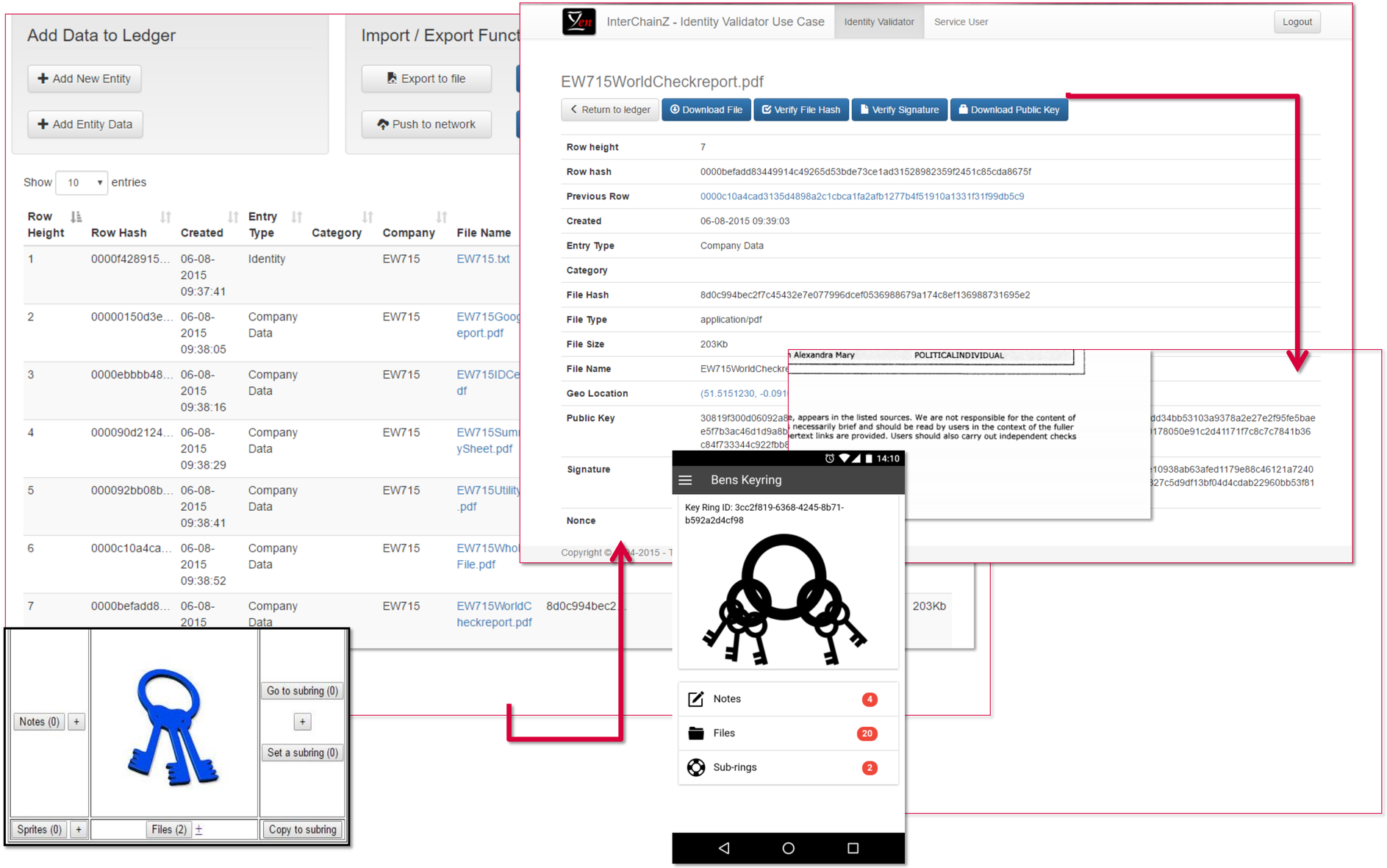
Binary Choices:

- Public versus private?
- Transparent versus opaque?
- Permissioned versus permissionless?
- True peer-to-peer or merely decentralised?
- Proof-of-work, proof-of-stake/consensus/identity/voting mechanisms, ‘agnostic’ or ‘woven’ broadcasting?

Strategic Questions:

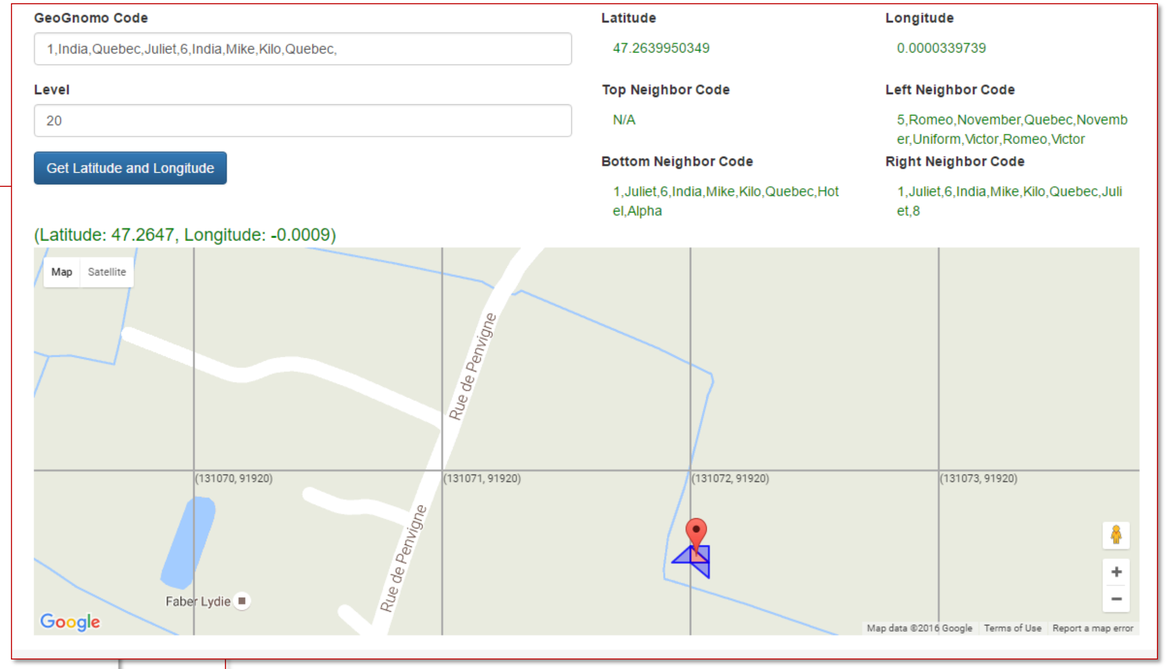
- One, few, many, or multitudes?
- Easy, middling, hard, too hard?

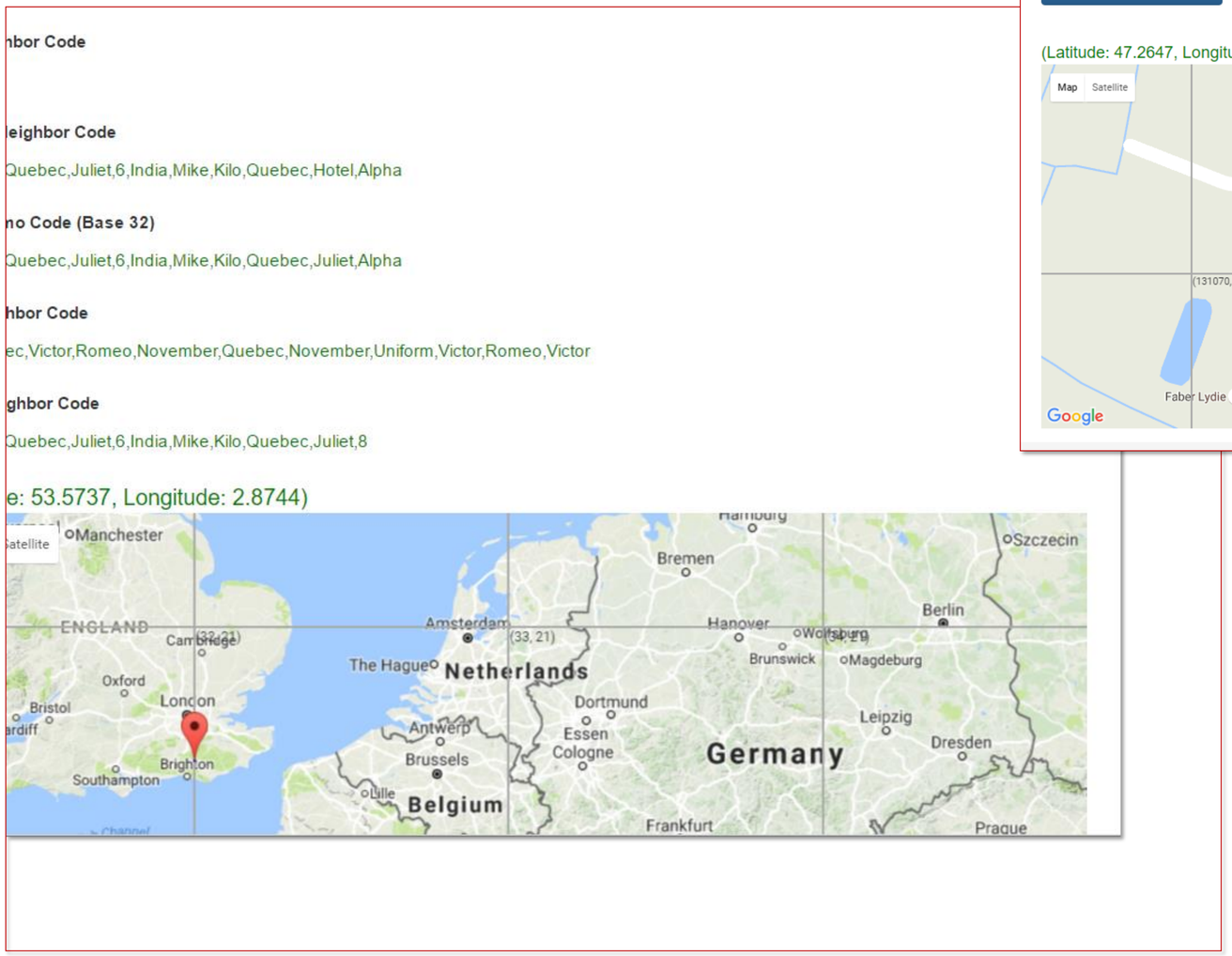
Proof-of-Concept: IDchainZ - Identity, health, qualifications



Application: Clinical trials

Application: GeoGnomo – Geostamping





Application: MetroGnomo – Timestamping & Datalogging

Application: Sharing economy broker and underwriter

vrumi

safe share

INSURANCE FOR THE SHARING ECONOMY

Current Time	Last MetroTime	Last Timestamp	Average Duration
2016-03-14 10:19:35 AM	2016-03-14 11:19:29.784195	7s ago	32s

Show 10 entries

Search:

UUID	MetroTime	RowHash	TableHash	Tag
c9b99219-bbd4-4927-99e8-ceaac929e5bc	2016-03-14 11:19:29.784195	ce997f9bd1ce9a3b84bf3cd307344184a792ce65996382bca86e6a09a9d9665e	23ae3b4a68e00c7cf5ab421ad3156867ae05cdd33ed8ebafa16946351 3dde3fa6	SafeShare: File Hash: c1c81e5dd5897ead6e215b3e02b0d1288bc5bc1a945ef26a59fdc5794da00517
08b87206-01d0-428f-668b-156d61848 82d	2016-03-14 11:19:09.434935	9986e36ba4b07ec1cddb15434cad9c990a4eab649862bc2e47f68c74fa56b9ae	d2092ed3107b830eff4fa3d92f5005ee45ee1cf3501df56b5834d9f9fe991d8	SafeShare: File Hash: 21164ebcc6aeb91b1270b109 49b13017cffdf1f937ad0e19bd2e7d376ee050f1
546609e7-d96f-42b9-bdca-4e70d4e250db	2016-03-14 11:18:59.218019	e7e3c7345edc8a45d32036920de7afe41ea192268f532978b90ec4225bc5caeb	bba25b6330c59c0f9f45a77ff9a3dd0e02c1efaedd2170796d1483fc915c53c	SafeShare: File Hash: cb91223a2bddd7f5f9a3959ebd50f2d7d65214da6366723b3b2284c0ea522fa7
1ce10457-f654-44c9-82bb-583c450fc7e7	2016-03-14 11:18:51.468576	ad083dd209d88616a50045847781565c9594823 6ecfcc008d25af31ae55d0c11	bb77776d3a09b20a820ef930f2392a2811337268 0a801b70522c5788ac9a67d76	SafeShare: File Hash: cbf1c1635f91bf2984062 1c5e31808e13c8493b50e915f92deeaf450fd25780

EVIDENCE OF INSURANCE

THIS DOCUMENT IS ISSUED AS EVIDENCE OF INSURANCE, IT DOES NOT CONSTITUTE A LEGAL CONTRACT OF INSURANCE

The Master Policyholder has procured Insurance under a Master Policy in respect of persons who are members of the Master Policyholder. This document is issued to you as evidence that your name has been added as a person insured under the Master Policy.

The coverage provided is in accordance with the terms and conditions contained in the Master Policy. The Master Policy is available for inspection upon application to the Master Policyholder.

The details that follow are those shown in the Master Policy as applicable to you. In the event of any discrepancy between the details contained in this document and those shown in the Master Policy then those shown in the Master Policy shall prevail.

Master Policy No: BW0137215 Evidence No: 33

Unique Master Reference: B1262BW0137215

1. Name and address of the Member: Ian Johnson, 1 Park Lane, London, W1 1AA

   Address of Premises: 1 Palace Mews, London, w8 6jn

2. Effective from 16th February 2016 to 1st February 2017, both days inclusive

   Operative Time — This insurance operates during the period of any booking made through the Vrumi website (being either a single booking or multiple bookings running continuously on the same day at the same property).

3. This Evidence of Insurance is underwritten with certain **UNDERWRITERS AT LLOYD'S, LONDON**. Novae Syndicates Limited

   Percentage: 100%

4. Coverage

Section one – Buildings	GBP 500,000
Section two – Content	GBP 75,000
Section three – Accident to Domestic Staff	GBP 5,000,000
Section four – Legal Liability to the Public	GBP 2,000,000

5. In the event of a claim under the Evidence of Insurance, please notify:

   Adjusting Associates LLP
   Telephone: 01443 229513
   Facsimile: 01443 229995
   Email: claims@adjustingassociates.com

   Emergency 24/7 Out of Office Number: 01724 761378

   Claims in writing should be directed to:

   Adjusting Associates LLP
   Unit 2, Sovereign Court
   Sterling Drive
   Llantrisant
   Rhondda Cynon Taff
   CF72 8LX

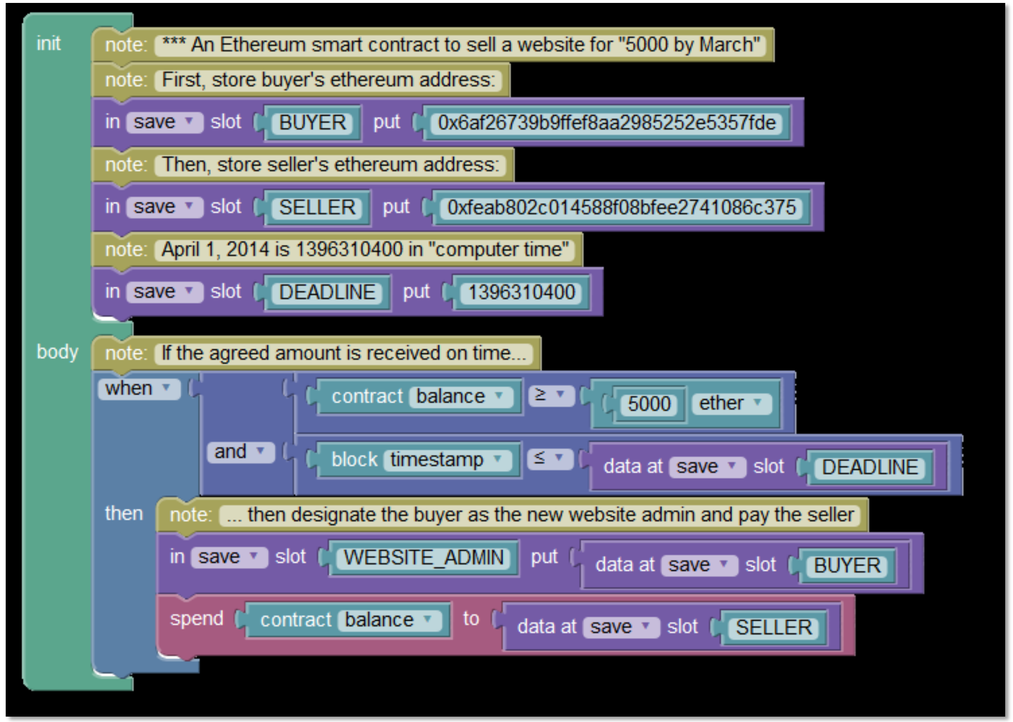
Signed and dated this 16th day of February 2016

By William Sighart (Master Policyholder)

Host details					Property details		Peroid of cover				Policy cancelled	Reason for cancellation	Premium	IPT
							From		To					
First Name	Surname	Unique Reference	Address	Poscode	Address	Postcode	Date	Time	Date	Time				9.50%
John	Smith	VR0001	123 Bank Street	EC2V 5AY	54 Woodhill Lane	W17 RQ					No		£2.00	£0.19
											Select			£-

Ledger logic & turing machines

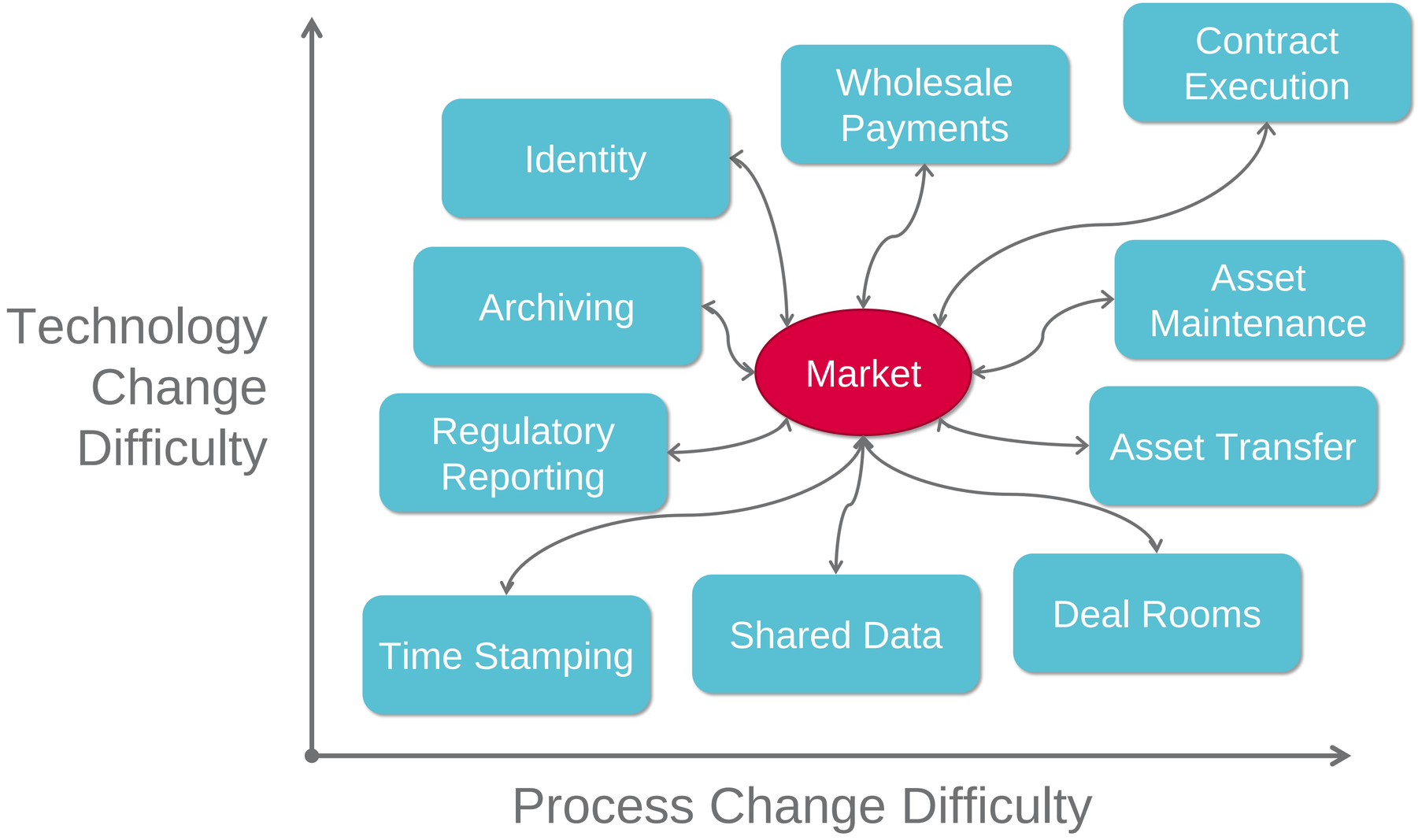
- Smart (dumb) contracts (pieces of code, aka scripts or sprites) executed when certain pre-defined conditions are met
- Decentralised autonomous organisations (DAO) – conceptual, suite of ‘smart contracts’creating autonomous entities



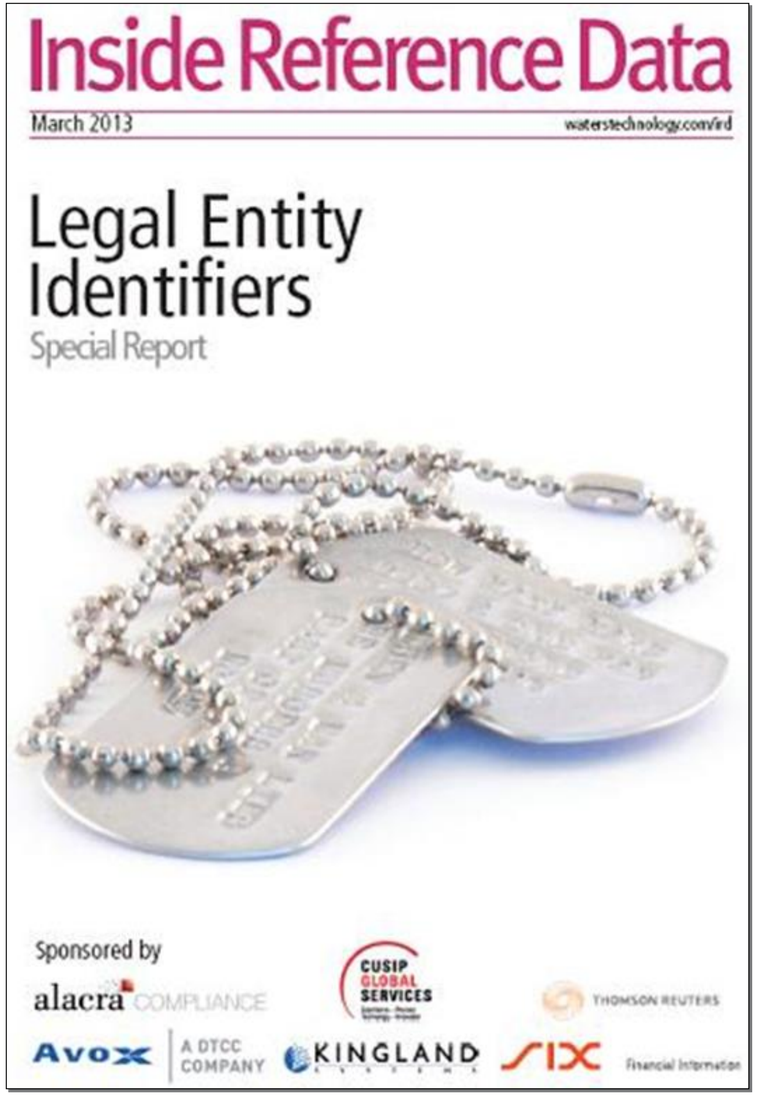
‘Forces of Nature’? ‘Sorcerers’ Apprentices’?

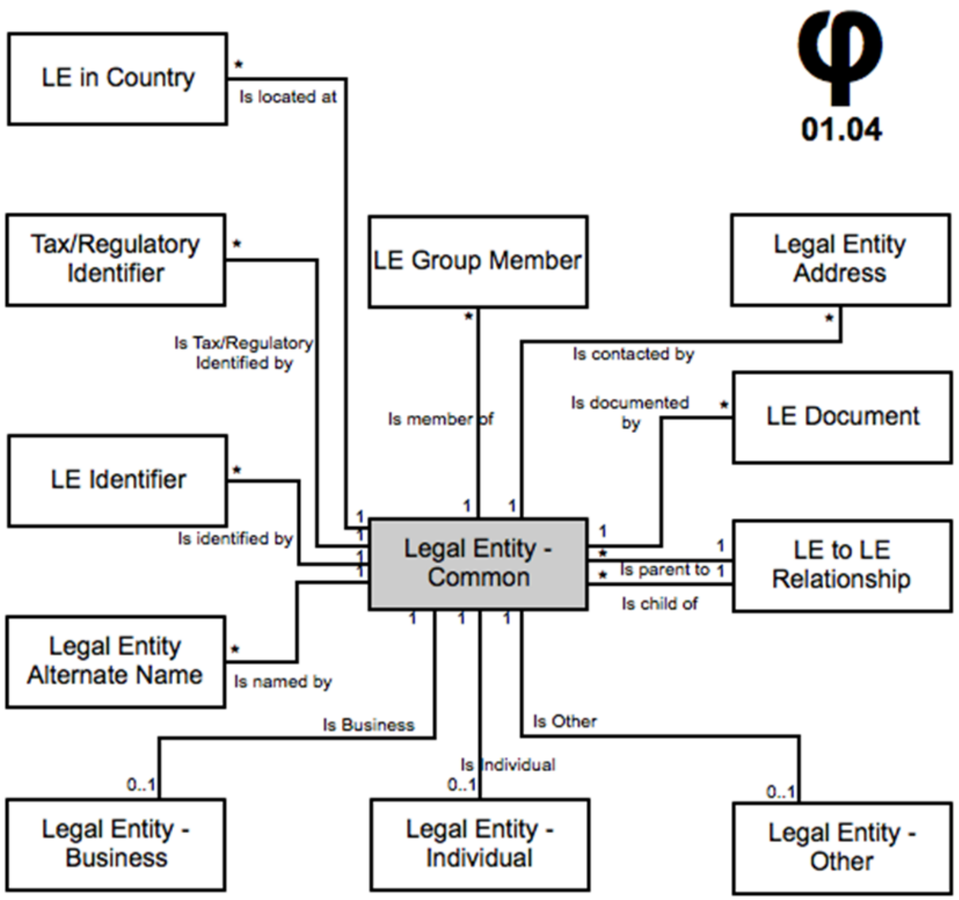
“If you have trust I shall give you trust; if you have no trust I shall take it away.”

Understanding & undertaking



Hub and spoke data





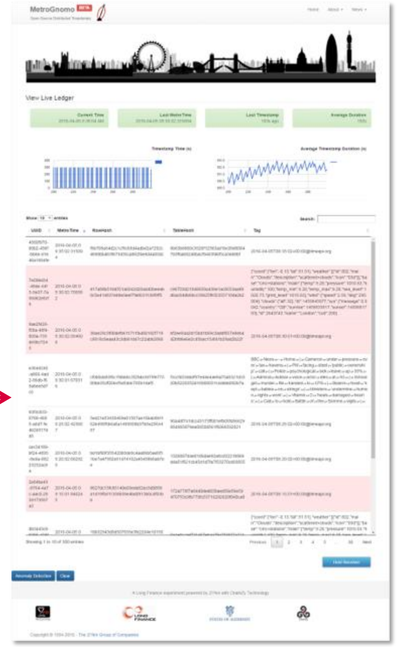
Economics matters

Factor	Bitcoin	Ethereum	ChainZy
Speed – transactions per second	7 tps	20 to 30 tps	10,000 tps + (single transmitter)
Storage	Fixed	Fixed	Variable
$/transaction	$0.10 to $2.50	$0.20 to $5.00	<$0.000001
Validation time	10 minutes	15 seconds	0.0001 second

Ongoing research

- Usable
  - Visualisation, apps, XML partial matching engines
  - Key structures, sprites (smart contracts)

- Mutual - validate
  - Validation methods – NPL timing project
  - ‘Genetic splicing’ and integrity
- Distributed - safeguard
  - Surveillance – support vector machines
  - Transmitting & receiving, high volumes, multiple transmitters



- Immutable - preserve
  - Partial data holding, long-term data storage
  - Standards – inter-governmental research project

Securing & scoring

Theme	Service	Question
Trust	Identities/Assets	Authentication
Space	Transactions	Services
Time	Debts	Value-added
Mutuality	Contracts	Common-wealth

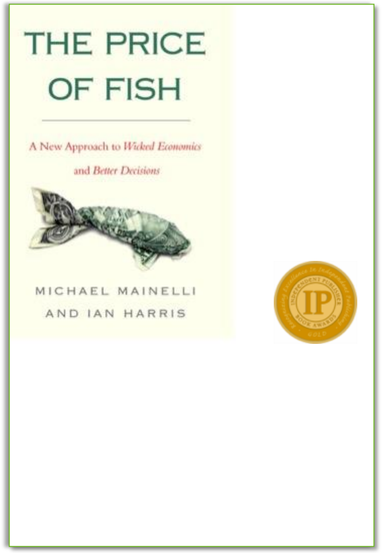
Closing thoughts?

- Mutual distributed ledgers help communities share information across time and space, less vulnerable to natural monopolies
- Mutual distributed ledgers help make better ‘contract’ utilities by:
  - Safeguarding transactions
  - Preserving transactions & data
- Mutual distributed ledger technology will displace much messaging and shared data functions
- … try one out … www.MetroGnomo.com

When would we know our commerce is working?

“Get a big picture grip on the details.”

Chao Kli Ning



Thank you!

LONG FINANCE