



© Z/Yen Group
2015

FS Club



"When would we know our financial system is working?"



The Future Of Distributed Ledgers In Finance

Professor Michael Mainelli
Executive Chairman, Z/Yen Group
michael_mainelli@zyen.com

Barclays Accelerator, London Escalator, 24 June 2015

Z/Yen Group Limited
90 Basinghall Street
London EC2V 5AY
United Kingdom
tel: +44 (20) 7562-9562
www.zyen.com





© Z/Yen Group
2015

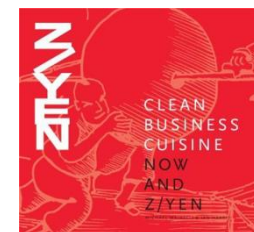
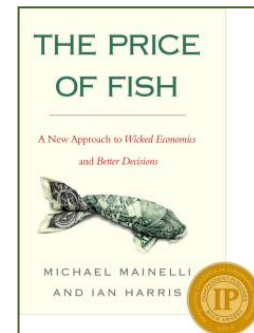
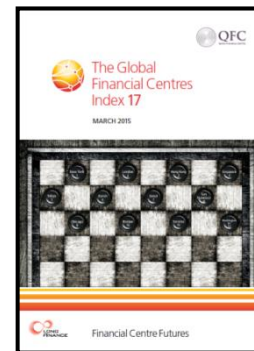
Z/Yen



The Global
Financial Centres
Index



- ◆ Special – City of London’s leading commercial think-tank
- ◆ Services – projects, strategy, expertise on demand, coaching, research, analytics, modern systems
- ◆ Sectors – technology, finance, voluntary, professional services, outsourcing



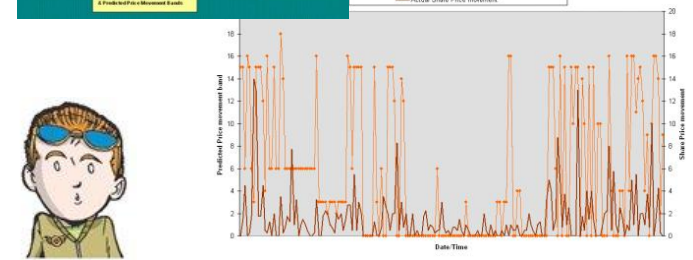
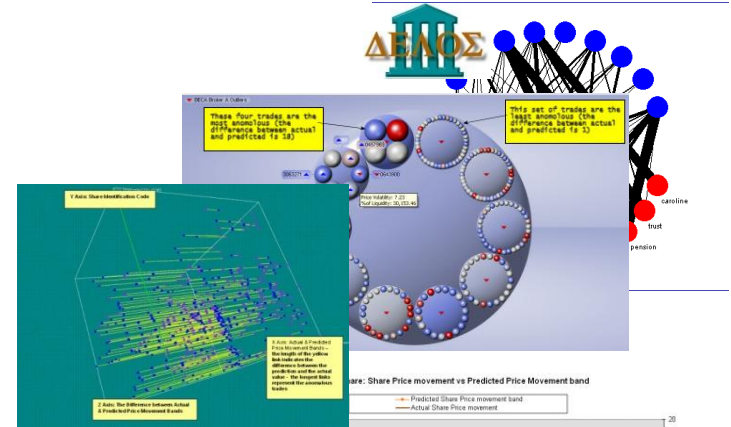
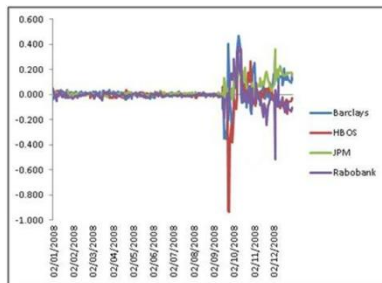
- Independent Publisher Book Awards Finance, Investment & Economics Gold Prize 2012 for ***The Price of Fish***
- British Computer Society **IT Director of the Year** 2004 for PropheZy and VizZy
- DTI **Smart Award** 2003 for PropheZy
- *Sunday Times* Book of the Week, ***Clean Business Cuisine***
- £1.9M **Foresight Challenge Award** for Financial Laboratory visualising financial risk 1997



© Z/Yen Group
2015

Z/Yen in Finance Research

- ◆ Distributed ledgers (1995-present)
- ◆ LIBOR and FX surveillance (2007-present)
- ◆ PropheZy and VizZy – automation & visualisation of compliance monitoring (2002-present)
- ◆ Prediction markets and bubbles (1998-present) – www.extzy.com
- ◆ Market intelligence – Ministry of Defence, e.g. Vision 2020 (1994-present)
- ◆ Avatars for Big Data (2010-2012)
- ◆ Financial Laboratory Club visualising risk (1997-1998)

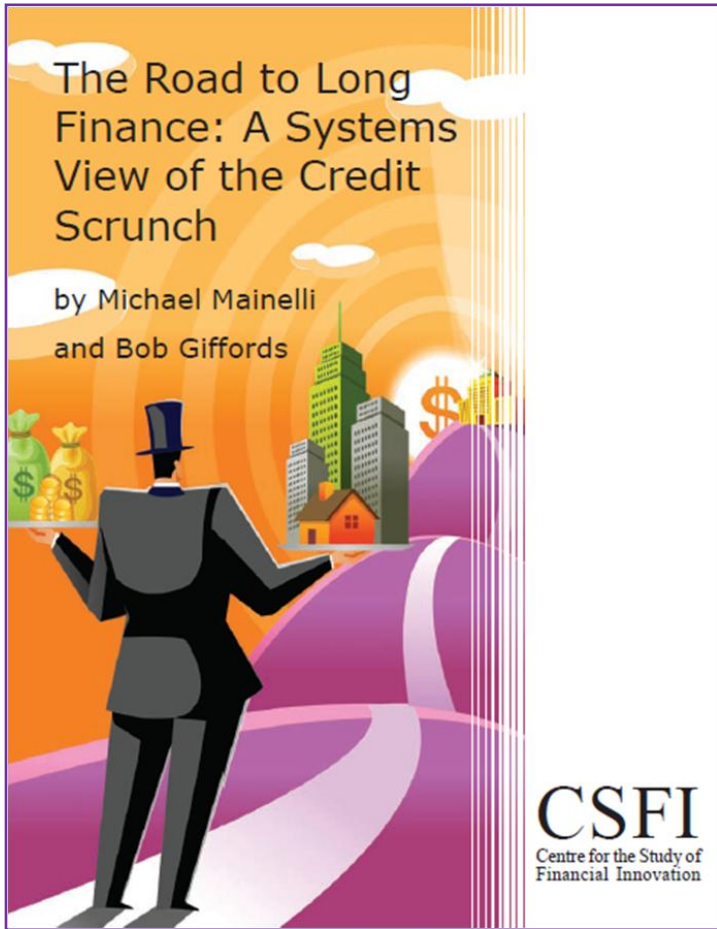


Screenshot of the ExtZy website interface. It features a navigation bar with 'Home', 'My Account', 'Find Shares', 'Community', 'Statistics', and 'Help'. The main content area includes a 'Player Rankings By...' table, a 'Welcome to ExtZy' message, a 'Market Indices' section, and a 'Case Five: United Kingdom' section with a line chart showing price and volume from 2012 to 2013. The chart highlights events like the London Olympics and Diamond Jubilee. A 'Tag Cloud' section is also visible.



© Z/Yen Group
2015

About



‘When would we know our financial system is working?’

Objectives:

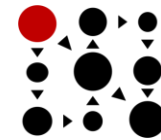
- ◆ Expand Frontiers
- ◆ Change Systems
- ◆ Deliver Services
- ◆ Build Communities



London
Accord



Financial
Centre
Futures



Meta-
Commerce



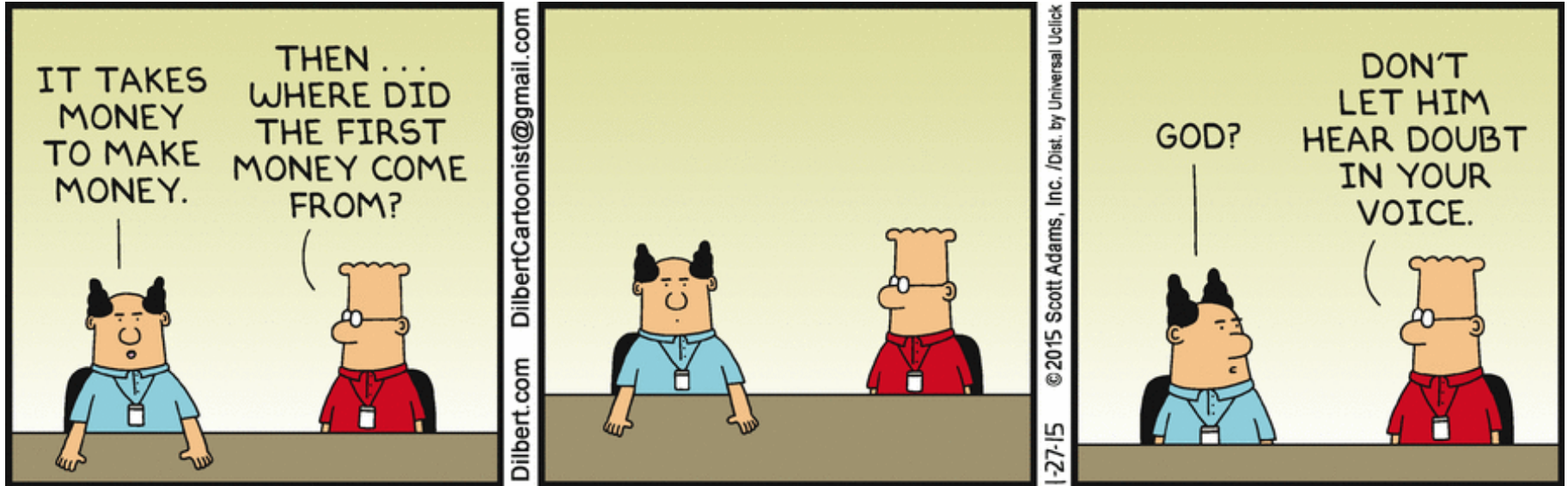
Eternal
Coin





© Z/Yen Group
2015

The Study Of Money Is The Root Of Much Madness



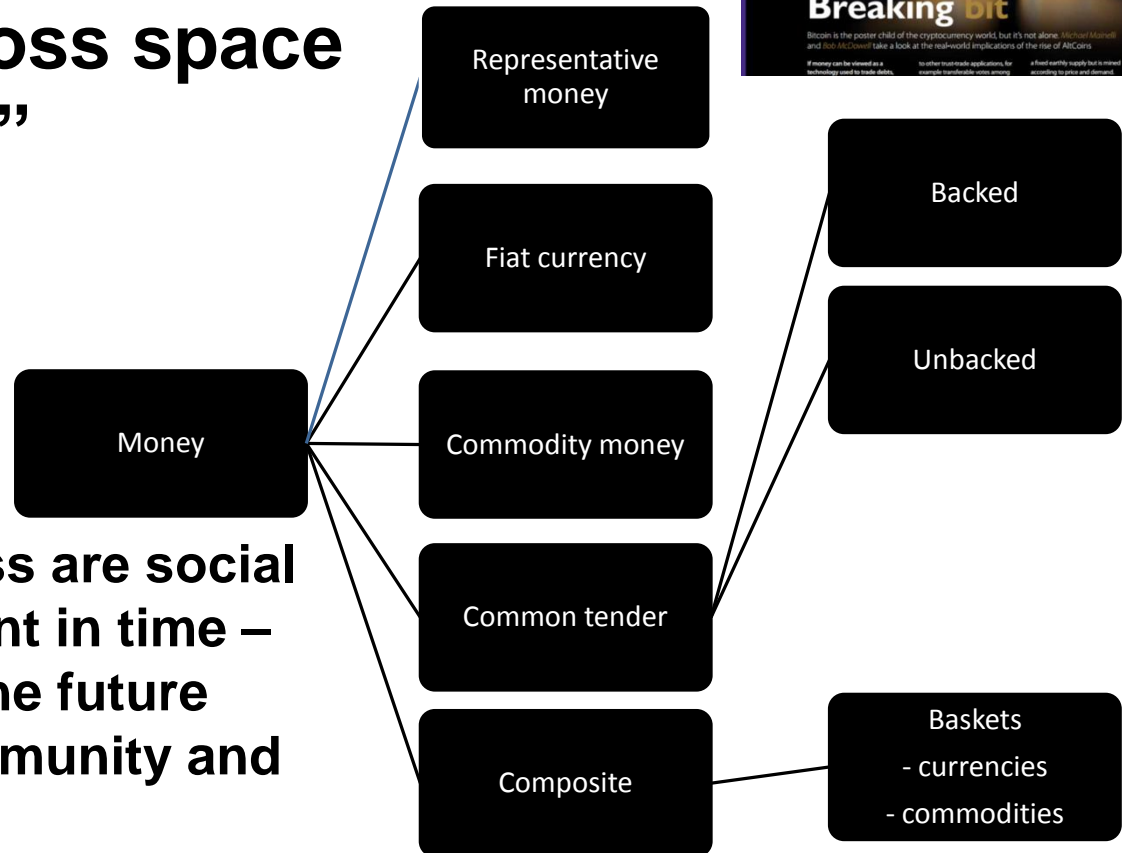
[www.dilbert.com, Thursday, 27 January 2015]



© Z/Yen Group
2015

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.”



© Z/Yen Group
2015

Why Does A Central Registry Exist?

Financial services are based on 'mistrust'

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





© Z/Yen Group
2015

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)*

“The consequences of this breakthrough [Bitcoin] are hard to overstate.”

Marc Andreessen, co-author of Mosaic, co-founder of Netscape, and Bitcoin investor

“[Virtual Currencies] may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system.”

Ben Bernanke, Chairman of the Federal Reserve USA

“Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value”

Eric Schmidt, CEO of Google

“I do think Bitcoin is the first [encrypted money] that has the potential to do something like change the world.”

Peter Thiel, Co-Founder of Paypal

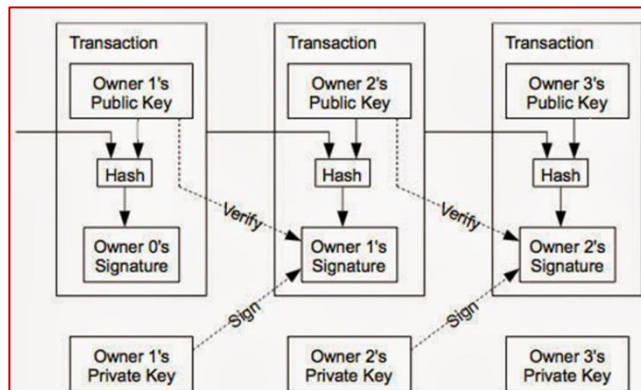


Diagram of a Bitcoin

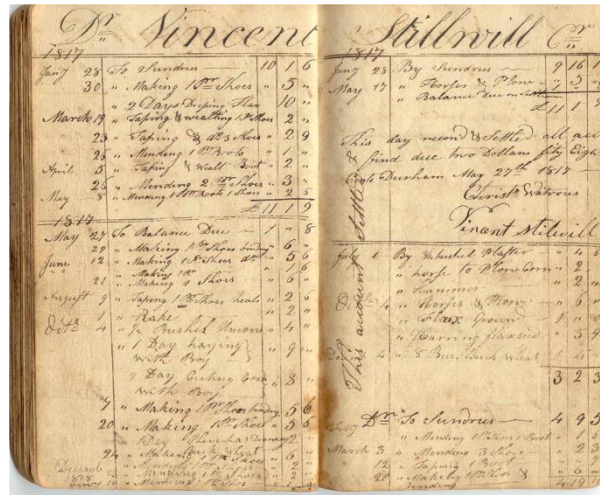
from *Bitcoin: A Peer-to-Peer Electronic Cash System*,
published in 2008 by “Satoshi Nakamoto”.



© Z/Yen Group
2015

What Is A Ledger?

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



Accounts for Demo
CASH ACCOUNT From 01/03/2003 to 29/03/2004

Date	Payee	Reference	Category	Actual (gross) Amount	Recon Balance (gross)	Admin. fund split OST net	Non OST	Sink. fund split OST net	Non OST	Balance (net)
25 MAY	Mr J Citizen	Lot 1 levy pa	Deposit	500.00	500.00	0.00	500.00	0.00	0.00	500.00
26 MAY	Local Insurance	Insurance	Ar Insurance Bu	-269.00	231.00	0.00	-269.00	0.00	0.00	231.00
31 MAY	Netbank	Govt Debit Tr	Govt Debit Tr	-2.52	228.48	0.00	-2.52	0.00	0.00	228.48
31 MAY	Netbank	Account Ser	Account Ser	-5.00	223.48	0.00	-5.00	0.00	0.00	223.48
31 MAY	Netbank	Interest	Bank Interest	0.52	224.00	0.00	0.52	0.00	0.00	224.00
3 JUN 03	Clarks Grounds	Grounds Maint	Grounds Maint	-30.00	194.00	0.00	-30.00	0.00	0.00	194.00
10 JUN 03	Electrical Engineer	Replace light	Building Maint	-22.60	171.40	0.00	-22.60	0.00	0.00	171.40
11 JUL 03	Levy credit trans	Lot 1 credit tr	Levy credit tr	0.00	171.40	0.00	-250.00	0.00	250.00	171.40
10 OCT 03	Leahy	Terror Payou	Bank Transf	1000.00	1171.40	909.09	0.00	0.00	0.00	1080.49
10 OCT 03	Fencers Upstand	Broken Pain	Fencing	-120.00	1051.40	0.00	0.00	0.00	-120.00	960.49
16 OCT 03	Mr P D Jakeson	Lot 1 levy pa	Deposit	400.00	1451.40	0.00	0.00	363.64	0.00	1324.13
6 NOV 03	Mr P D Jakeson	Lot 1 levy pa	Deposit	25.00	1476.40	0.00	0.00	22.73	0.00	1346.86
11 NOV 03	Mr P D Jakeson	Lot 1 levy pa	Deposit	5.00	1481.40	0.00	0.00	4.55	0.00	1351.41

Buttons: Edit row, Receive levy, Credit, Bill pay, Debit, Ledger, Ledger group, Statement, Reconciliation, Bank deposit, Term deposit, Strataware, Bank account

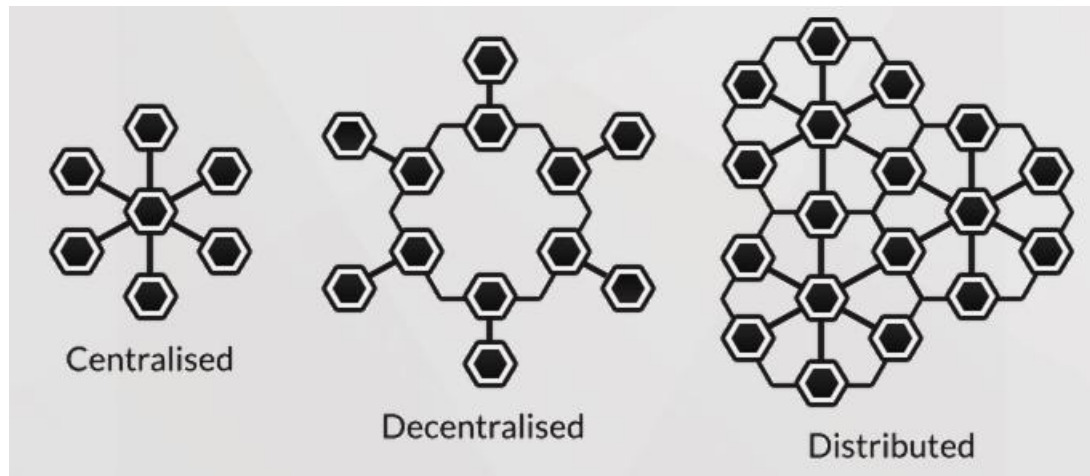


© Z/Yen Group
2015

What Does A Distributed Ledger Do?

- ◆ Validate – “a trust model for timestamping”
- ◆ Safeguard – “a set of rules for updating state via blocks”
- ◆ Preserve – “a shared state”

Persistent & Pervasive

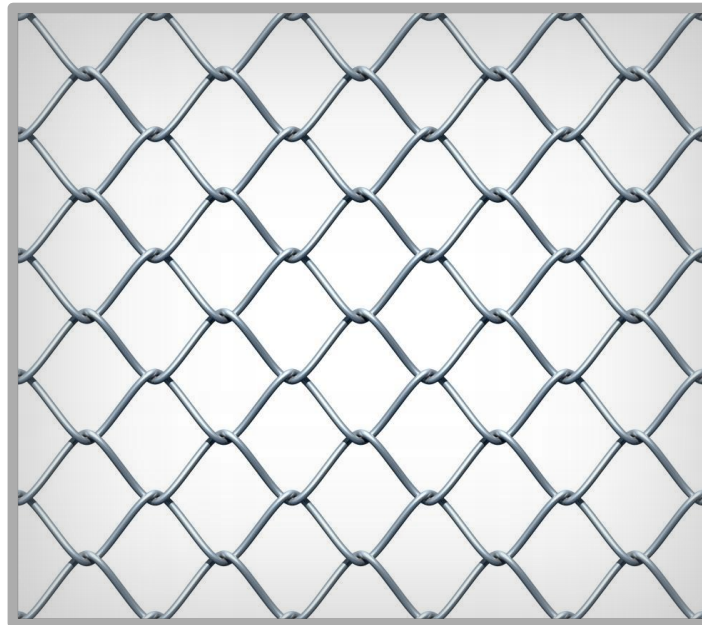




© Z/Yen Group
2015

What Are The Essential Components?

- ◆ Public-key cryptography (Diffie-Hellman circa 1976)
- ◆ Proper decentralised peer-to-peer network (Gnutella 2000)





© Z/Yen Group
2015

What's Interesting About Bitcoin's Blockchain?

Famous (infamous) distributed ledger:

- ◆ Displaces two-and-a-bit roles of trusted third parties:
 - Validate - virtual finite element* – initial entry requires high degrees of trust but then system operates on trustless basis
 - Safeguard - can't do the same transaction twice** - no double spending or transaction repudiation
 - Preserve - public history of transactions** - one unified unalterable state of the ledger at all times shared by all nodes
- ◆ Decentralised - at the extreme, no authority required to coordinate behaviour or interaction (though some close shaves)
- ◆ Distributed - robust



© Z/Yen Group
2015

The Old Old Things

- ◆ 1993 – Encrypted Open Books
- ◆ 1995 – WebDNA
- ◆ 1996 – Ricardo payment system
- ◆ 1999 – Stanford University’s CLOCKSS (Controlled Lots of Copies Keep Stuff Safe)
and LOCKSS (Lots of Copies Keep Stuff Safe) -
<http://www.lockss.org/about/history/> for archiving
- ◆ 2004 – Ripple, a consensus ledger approach to currency transaction



© Z/Yen Group
2015

Blockchains - Buzz or Hype?

- ◆ 1990 – Mondex, Digicash, Flooz, ...
- ◆ 2013 – Bitcoins – Silk Road, FBI, Alderney
- ◆ 2014 – Regulators – Jersey, FATF, ECB, State of New York, ...
- ◆ 2015 - Blockchains
 - January – IBM-Samsung
 - February – Bank of England research agenda
 - March – UK budget for standards, Barclays
 - April – UBS, BNY Mellon, Goldman Sachs
 - May – USAA, NASDAQ, Honduras land registry, Isle of Man
 - A fine (sic) of having arrived – Ripple \$700,000



© Z/Yen Group
2015

Buzz or Hype? The New New Thing



[Ken Tindell mashup - 14 May 2015 <https://twitter.com/kentindell/status/598865133247569920>]



© Z/Yen Group
2015

The Old Old New New Thing...



[www.dilbert.com, Friday, 17 November 1995]

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

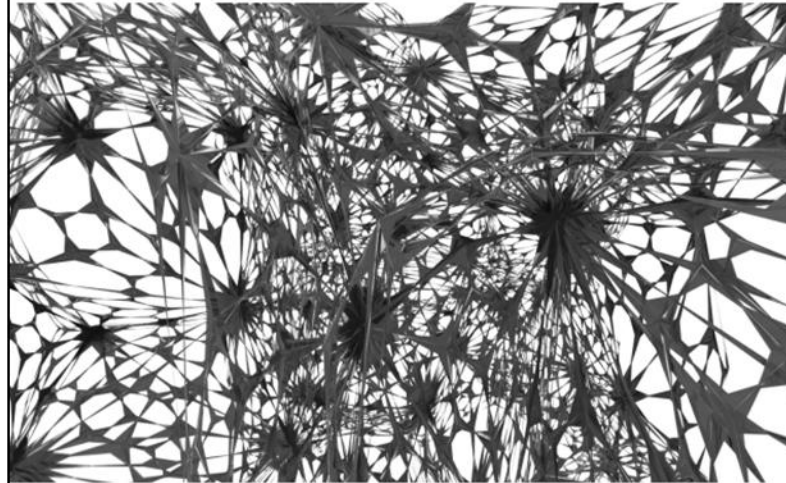


© Z/Yen Group
2015

Shared Ledgers For Shared Economy



Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance



December 2014
A Long Finance report prepared by Z/Yen Group

<http://www.longfinance.net/publications.html?id=903/>



© Z/Yen Group
2015

Taxonomic Trials

		Who do I trust to maintain a truthful record?			
		A central authority	A group of known actors	A group of actors, some known	Nobody
What is the universe of "things" I need people to agree on?	Ownership of on-platform assets	Central Bank, Commercial Bank		Ripple (XRP)	Bitcoin
	Ownership of off-platform assets	Custodian Bank	Hyperledger	Ripple (Gateways)	Colored Coins, Counterparty
	Obligations and rights arising from an agreement	Clearing House	Eris	Ripple (Codius)	Ethereum

Source: Richard Brown

[Richard Gendal Brown, "A Simple Model To Make Sense Of The Proliferation Of Distributed Ledger, Smart Contract And Cryptocurrency Projects" (19 December 2014) - <http://gendal.me/2014/12/19/a-simple-model-to-make-sense-of-the-proliferation-of-distributed-ledger-smart-contract-and-cryptocurrency-projects/>]



© Z/Yen Group
2015

Cloud For Ledgers

Hire A Trusted Third Party - Choices!

- ◆ Public versus private – is reading the ledger open to all or just to defined members of a limited community?
- ◆ Permissioned versus permissionless – are only people with permission allowed to add transactions, or can anyone attempt to add a transaction?
- ◆ Proof-of-work, proof-of-stake, consensus or identity mechanisms – how are new transactions authorised?
- ◆ True peer-to-peer or merely decentralised – are all nodes equal and performing the same tasks, or do some nodes have more power and additional tasks?



© Z/Yen Group
2015

Identity ... space, time, mutuality

What if ...

you had a portable, secure, globally available store of personal data in a blockchain? You could have all of your health records or driving history available instantly to hand on to trusted third parties. You might hand over your health record to a new doctor or to obtain a life insurance quote, or your driving history at an airport counter for a car rental insurance discount. Your personal data store might also have your biometric data, thus giving you the ability to prove at any time it is you before someone, and that data contained in the blockchain is yours.



© Z/Yen Group
2015

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.



© Z/Yen Group
2015

Ledger Logic & Turing Machines

- ◆ Smart (dumb) contracts (aka scripts) enforced when certain pre-defined conditions are met, e.g.:
 - Oracles, e.g. crop insurance smart contract coupled with ‘trusted’ weather data feed
 - Arbitrators, e.g. appointed ‘experts’, such as software development smart contract appointing software experts to test the product
- ◆ Decentralised autonomous organisations (DAO) – sophisticated, conceptual, types of ‘smart contracts’ creating autonomous entities involving both a governance system and a way for the DAO to fund and manage resources, e.g. through the sale of a service or endowment

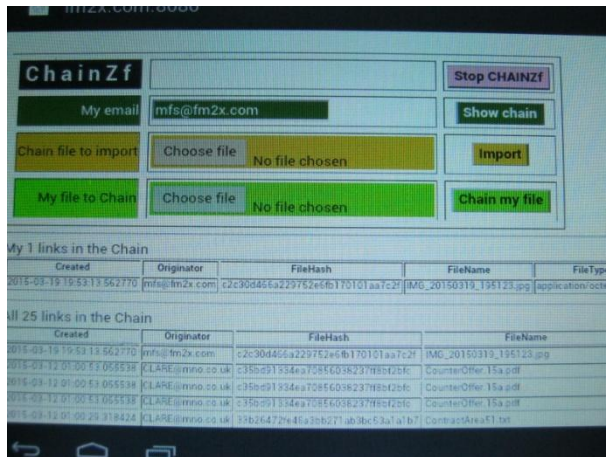
‘Forces of Nature’? ‘Sorcerers’ Apprentices’?

Long Finance koan – **“If you have trust I shall give you trust; if you have no trust I shall take it away.”**



© Z/Yen Group
2015

InterChainZ



ChainZf

My email:

Chain file to import: No file chosen

My file to Chain: No file chosen

My 0 links in the Chain

Created	Originator	FileHash	FileName	FileType	FileSize	Corresponding
---------	------------	----------	----------	----------	----------	---------------

All 4 links in the Chain

Created	Originator	FileHash	FileName	FileType	FileSize	Correspondent
2015-03-06 12:22:02.679078	smithmf@gmail.com	e0ee7cfad03c144495aa5ea1e28fa067	gdae.wmv	video/x-ms-wmv	5278176	smithmf@gmail.com
2015-03-06 12:20:04.238160	smithmf@gmail.com	68f107393d8b1bc2eda8e875a53d65dd	Character-Growth-Card.pdf	application/pdf	882901	smithmf@gmail.com
2015-03-02 11:06:08.736509	youthmind@gmail.com	8a1fec5a66c83d8bd0dce1772b721b	Self-signed SSL certificates.doc	application/octet-stream	115200	fm2x.mfs@gmail.com
2015-03-02 11:03:19.257397	fm2x.mfs@gmail.com	68911b33a7deafce2e4cea2020e55d4	Sales & Royalty Report-Jan-17-2015-to-Feb-16-2015-en_...xls	application/vnd.ms-excel	27648	fm2x.mfs@gmail.com



88c96b28-dc89-11e4-aa45-00163e05280f bid:218765812851

[Account](#) [Links](#) [Servers](#) [Menu](#) [Sign out](#)

Links (10) [+ Add New Link](#)

Linked	Account Code	Link Code	Geolocation	File	Message	FileHash	ChainHash
2015-04-09 09:56:32.202752	88c96b28-dc89-11e4-aa45-00163e05280f	a02a3b14-de9e-11e4-947a-00163e44c54d	Lat:51.4873817 Long:-0.104756999999999999	Link_File MFS.birth.certificate.front.jpg.gpg application/octet-stream 770450		2809441975d457b70c772eb23b92f1f2	c20370c9bb831cd269ac1ba373232f4b
2015-04-08 20:35:53.165718	88c96b28-dc89-11e4-aa45-00163e05280f	6d33d294-de2e-11e4-999c-00163e44c54d	doesn't work	Link_File 1428525233825.jpg image/jpeg 86217	Taken from old google phone.	5c9c4af8103add36ec2a33be891a9a2f	5423f9dfa80dbdd36ff67a60fc8a1c5
2015-04-08 19:05:23.440113	88c96b28-dc89-11e4-aa45-00163e05280f	#96879c-de21-11e4-9035-00163e05280f		Link_File 1428519859178.jpg image/jpeg 217998	Phone photo.	111630dc073b88a9f4893eeb5e0d5974	9d691a73dab1d708bb6526e268c0b875
2015-04-08 19:02:12.670317	88c96b28-dc89-11e4-aa45-00163e05280f	6fc3972c-de21-11e4-a689-00163e05280f		Link_File 1428519597253.jpg image/jpeg 233485	Sent via phone	8cdb4e78b7eba0fd5a455cac4b2aea35	8aa6f61a571c07018b9cf9913e4d3c0d
2015-04-08 18:01:23.343730	88c96b28-dc89-11e4-aa45-00163e05280f	3bf3a552-de19-11e4-be27-00163e166b38			2nd message from cpsat.info	None	982d7a41fc545fd02038609db69d142
2015-04-08 18:01:23.266822	88c96b28-dc89-11e4-aa45-00163e05280f	3c56355a-de19-11e4-b22c-00163e05280f			2nd message from chain.website	None	033605e6a588004dfa03347a8195e971
2015-04-08 18:00:34.923608	88c96b28-dc89-11e4-aa45-00163e05280f	1e2c675c-de19-11e4-8b72-00163e44c54d			2nd message fm2x.com	None	d0be1f3b0f285f84c2d2699771a6f135
2015-04-08 16:35:18.114612	88c96b28-dc89-11e4-aa45-00163e05280f	374dc55c-de0d-11e4-8445-00163e05280f			from chain.website	None	6b3ac5265849735a81a5a9cf6c8169ee
2015-04-08 16:35:07.273004	88c96b28-dc89-11e4-aa45-00163e05280f	2c9f3226-de0d-11e4-ad09-00163e166b38			from cpsat.info	None	a4eb455b5344a19f663c5b5c06f236b1
2015-04-08 16:35:04.707580	88c96b28-dc89-11e4-aa45-00163e05280f	2ecd8926-de0d-11e4-8b7d-00163e44c54d			From fm2x.com	None	4dfd2f0c59561054689a0c648faab5b1



© Z/Yen Group
2015

InterChainz Research

- ◆ Taxonomies
- ◆ Use Cases
- ◆ Multiple chains – identity, transaction, contents (dust, flakes, nuggets, nodules, ...)
- ◆ Persistence – sleeved models, economic/energy decay rates, ‘gradual compression’ (courtesy Frederic Vander Elst)
- ◆ Pervasion – robustness
- ◆ Trusted third party models
- ◆ Speed, volume, bandwidth

Result – matrix of options with pros & cons


***“If we knew what we were doing,
it wouldn’t be called research, would it?”***



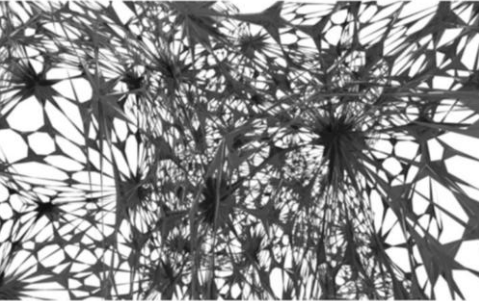
© Z/Yen Group
2015

The Long-Term?

Theme	Service	Question
Trust	Identities	authentication
Space	Transactions	services
Time	Debts	value-added
Mutuality	Contracts	common-wealth



Chain Of A Lifetime:
How Blockchain Technology
Might Transform Personal Insurance



December 2014
A Long Finance report prepared by Z/Yen Group

The Pembury Tavern
90 Amhurst Road
London E8 1JH
Tel. 020 8986 8597

Milton Pegasus (4.1% ABV) pint £3.00
Subtotal £3.00
Bitcoin 0.0474 £3.00

Individual Pubs Limited
Pegasus House
Pembroke Avenue
Waterbeach
Cambridge
CB25 9PY

VAT reg no. 783 9983 50
A: £2.50 net, £0.50 VAT @
20.0% Total £3.00

Receipt number 721636
2013-06-25

SPECIAL REPORT



Breaking bit

Bitcoin is the poster child of the cryptocurrency world, but it's not alone. *Michael Mainelli* and *Bob McDowell* take a look at the real-world implications of the rise of AltCoins

If money can be viewed as a technology used to trade debts, to other trust-trade applications, for example transferable votes among a fixed earthly supply but is mined according to price and demand.



© Z/Yen Group
2015

Discussion

- ◆ Regulate - governance & management standards, technical performance
- ◆ Use - trade reporting, 'too big to fail', account portability
- ◆ Encourage – new services, e.g. regulatory 'validation'

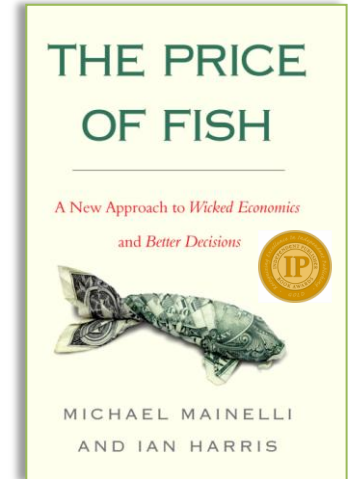


© Z/Yen Group
2015

When Would We Know Our Commerce Is Working?



“Get a big picture grip on the details.”
Chao Kli Ning



Thank you!

