InterChainZ

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

LONG FINANCE

Sharing Ledgers For Sharing Economies

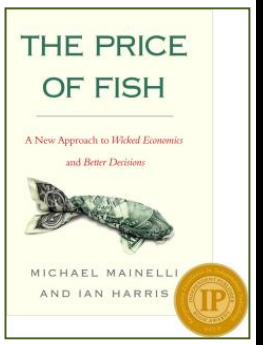
Learning from InterChainZ Project

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

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

Z/Yen

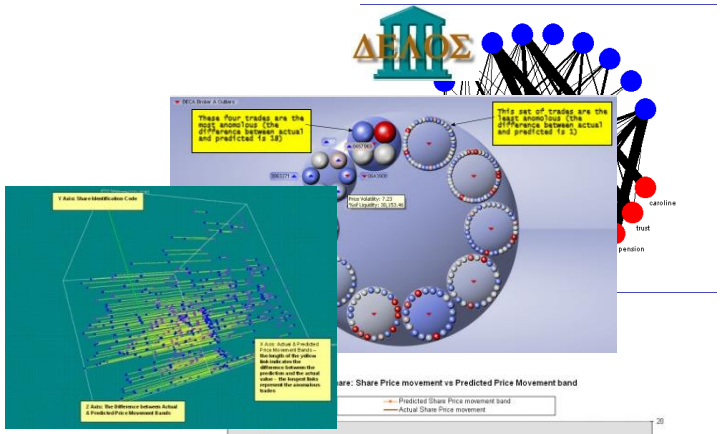
- Special – City of London's leading commercial think-tank
- Services – projects, strategy, expertise on demand, coaching, research, analytics, modern systems
- Sectors – technology, finance, voluntary, professional services, outsourcing

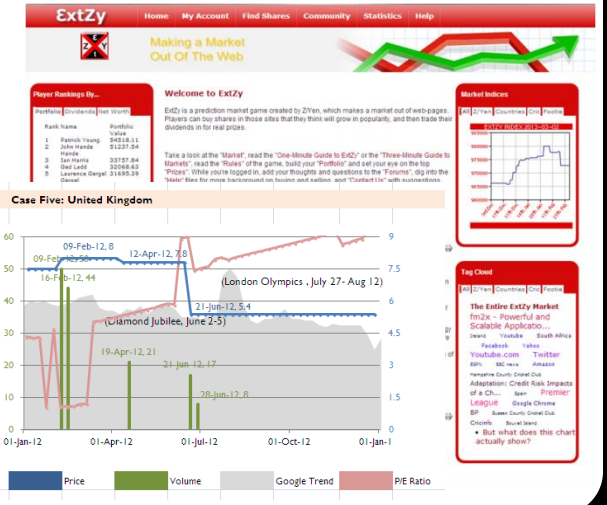


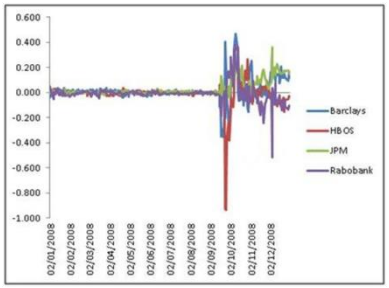
- Independent Publisher Book Awards Finance, Investment & Economics Gold Prize 2012 for ***The Price of Fish***
- British Computer Society **IT Director of the Year** 2004 for PropheZy and VizZy
- DTI **Smart Award** 2003 for PropheZy
- *Sunday Times* Book of the Week***, Clean Business Cuisine***
-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

Z/Yen in Finance Research

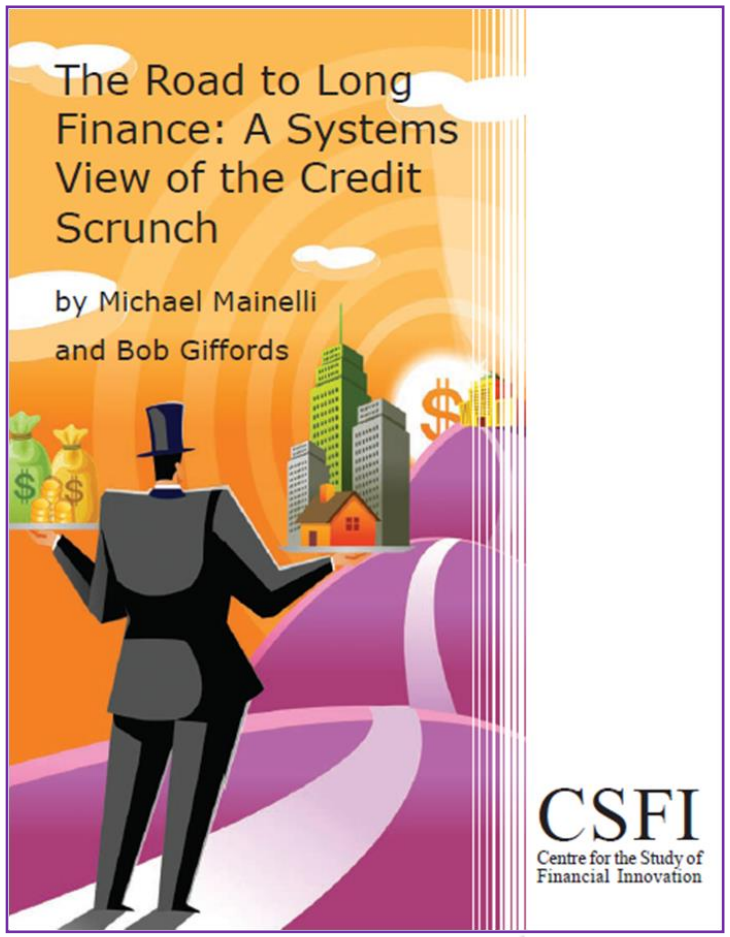
- Distributed ledgers (1995-present)
- LIBOR and FX surveillance (2007-present)
- PropheZy and VizZy – automation & visualisation of compliance monitoring (2002-present)
- Prediction markets and bubbles (1998-present) – www.extzy.com
- Market intelligence – Ministry of Defence, e.g. Vision 2020 (1994-present)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







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

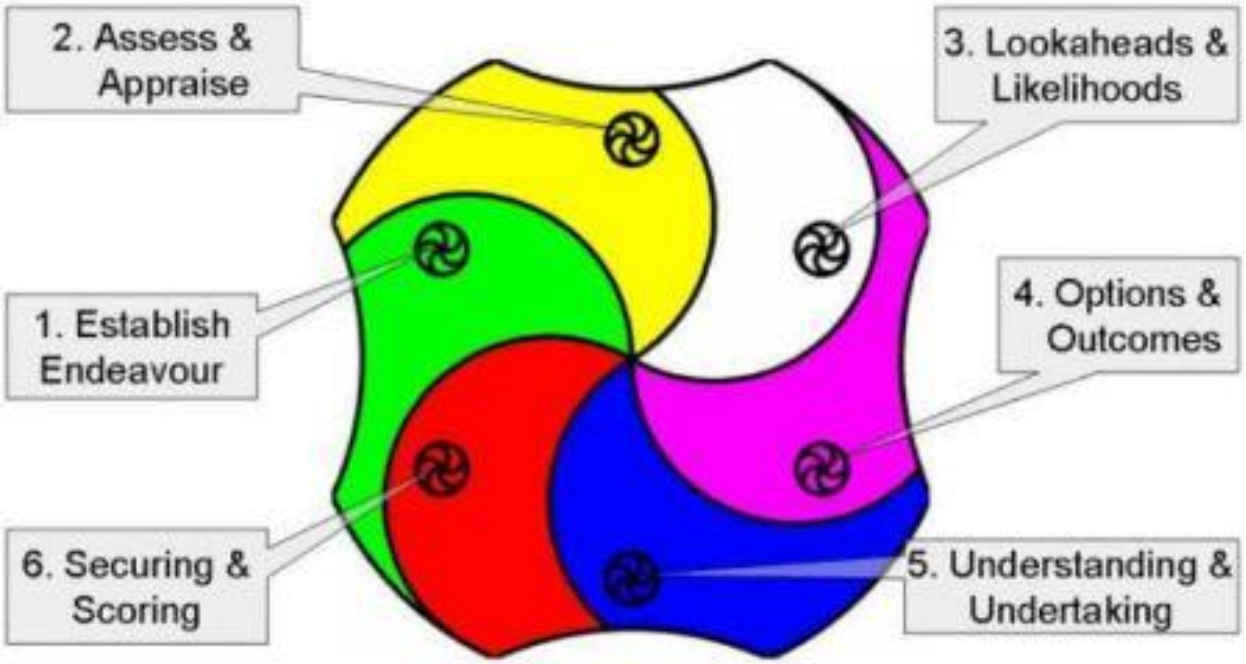
Gresham College Founded 1597

City of London

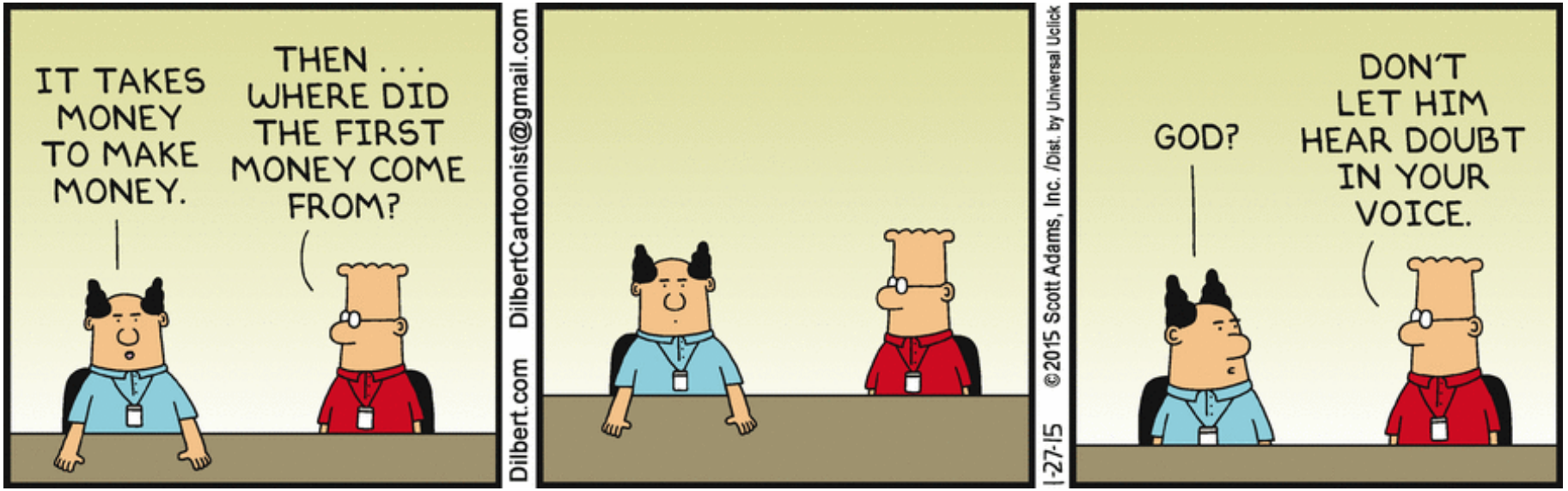
InterChainZ Consortium Partners

Partner	Description	Contact
DueDil	We are the business information provider for the UK and Ireland. It's an easy way to access millions of official company and company director documents online. We have collected and connected 20 years of financial history, contact information, corporate structures, director timelines and litigations.	www.duedil.com
PwC	Our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at PwC.com.	www.pwc.com
Suncorp	Suncorp Group includes leading general insurance, banking, life insurance and superannuation brands in Australia and New Zealand. The Group has 15,000 employees and relationships with nine million customers. We are a Top 20 ASX-listed company with $96 billion in assets. These products have the potential to reach 92% of Australians. We deliver products and services to personal customers, small and medium sized businesses, as well as corporate clients.	www.suncorp.com.au

InterChainZ Project Approach and Methodology: Z/EALOUS



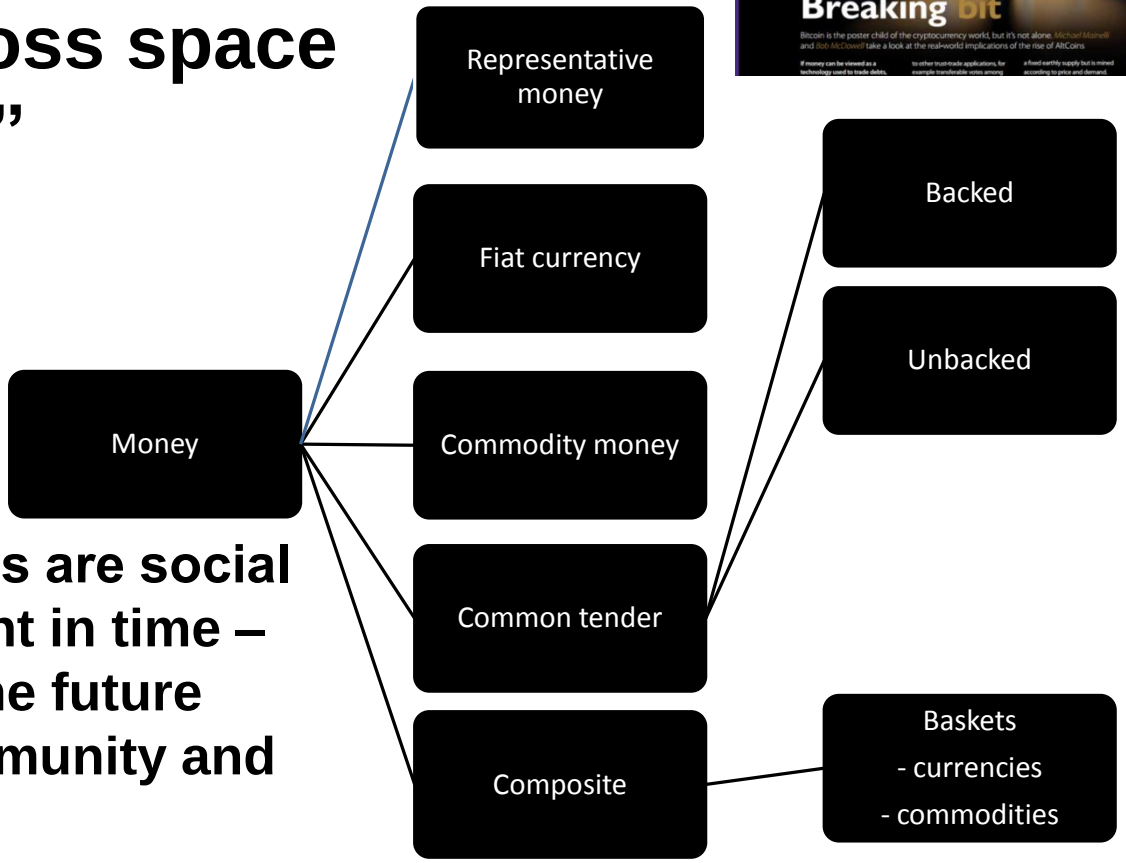
The Study Of Money Is The Root Of Much Madness



[www.dilbert.com, Thursday, 27 January 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.”

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

[Robert Sams, "Blockchain Finance" (March 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)

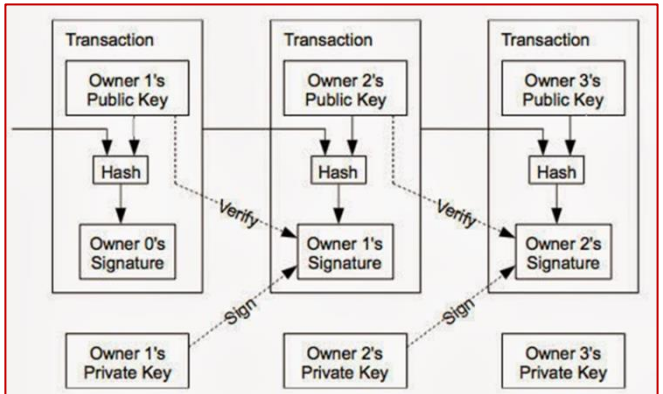


Diagram of a Bitcoin
from *Bitcoin: A Peer-to-Peer Electronic Cash System*, published in 2008 by "Satoshi Nakamoto".

"The consequences of this breakthrough [Bitcoin] are hard to overstate."
Marc Andreesen, co-author of Mosaic, co-founder of Netscape, and Bitcoin investor

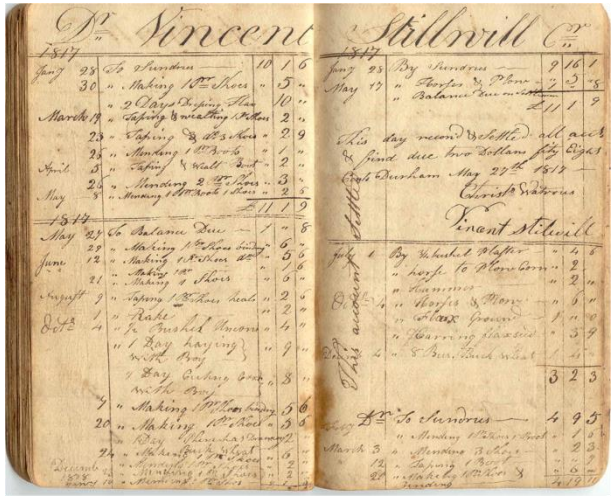
"[Virtual Currencies] may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system."
Ben Bernanke, Chairman of the Federal Reserve USA

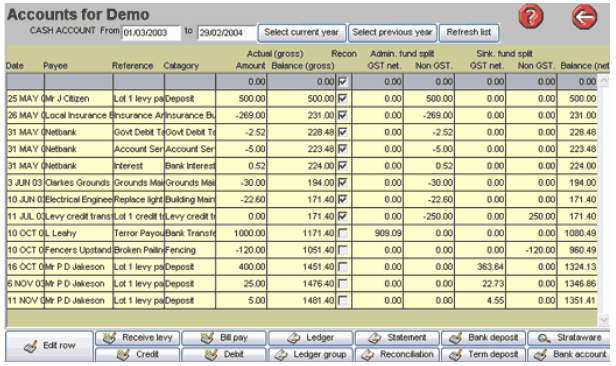
"Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value"
Eric Schmidt, CEO of Google

"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

What Is A Ledger?

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

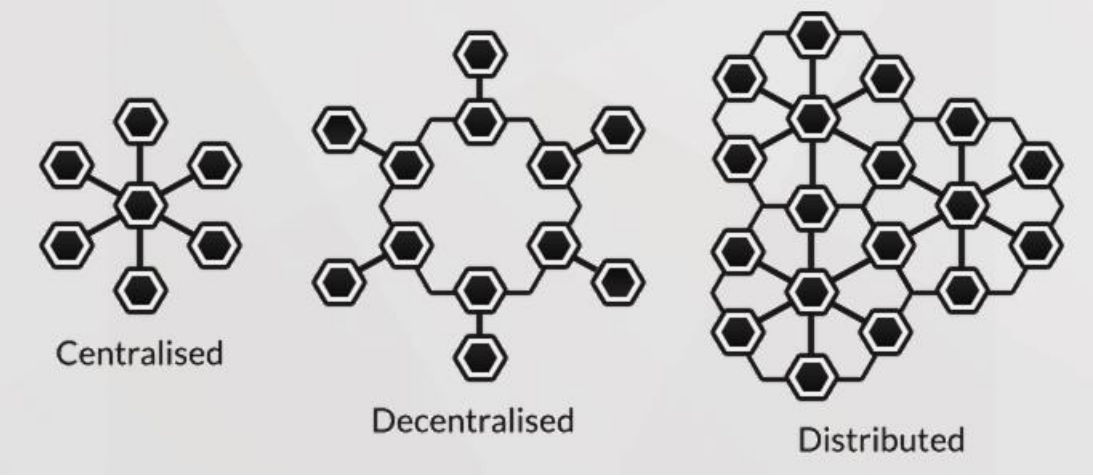




What Does A Distributed Ledger Do?

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

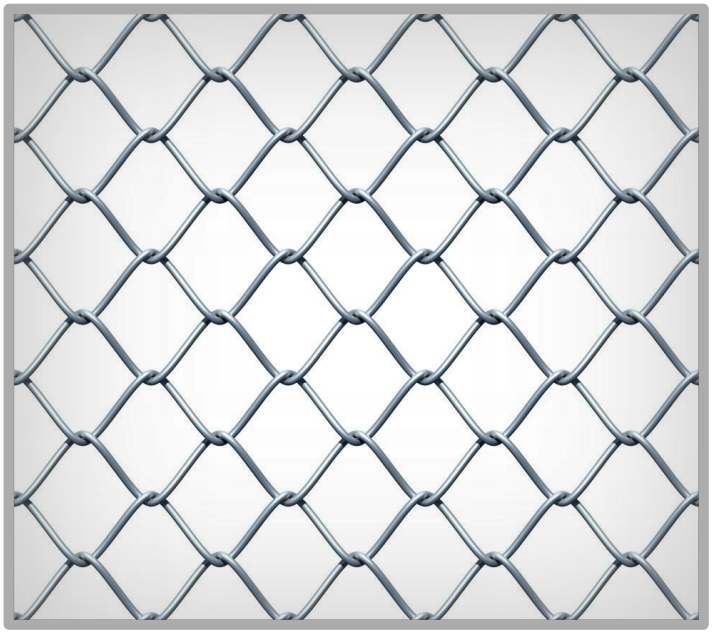
Persistent & Pervasive



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

What Are The Essential Components?

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



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

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

Blockchains - Buzz or Hype?

- 1990 – Mondex, Digicash, Flooz, … Wei-Dai b-money 1998
- 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
  - May - A fine (sic) of having arrived – Ripple $700,000
  - August - Sign of the Tines – Bitcoin forking hell

Buzz or Hype? The New New Thing

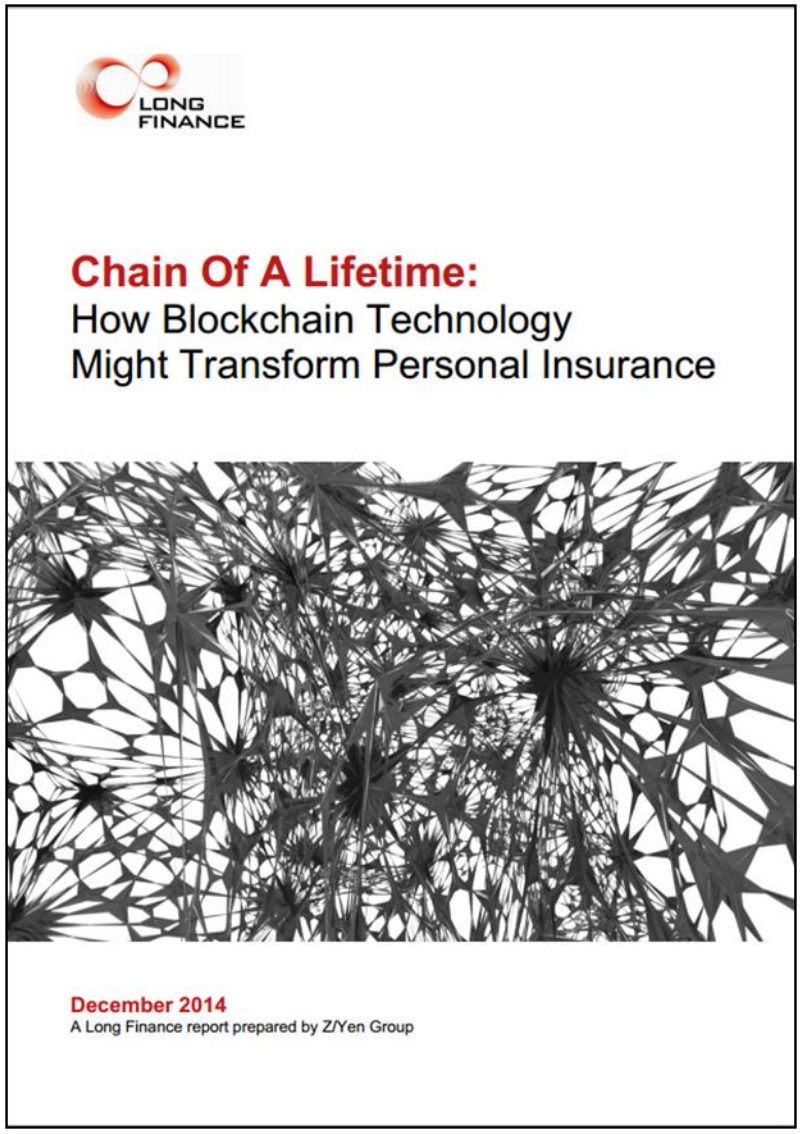
[Ken Tindell mashup - 14 May 2015 https://twitter.com/kentindell/status/598865133247569920]

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)…]

Shared Ledgers For Shared Economy



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

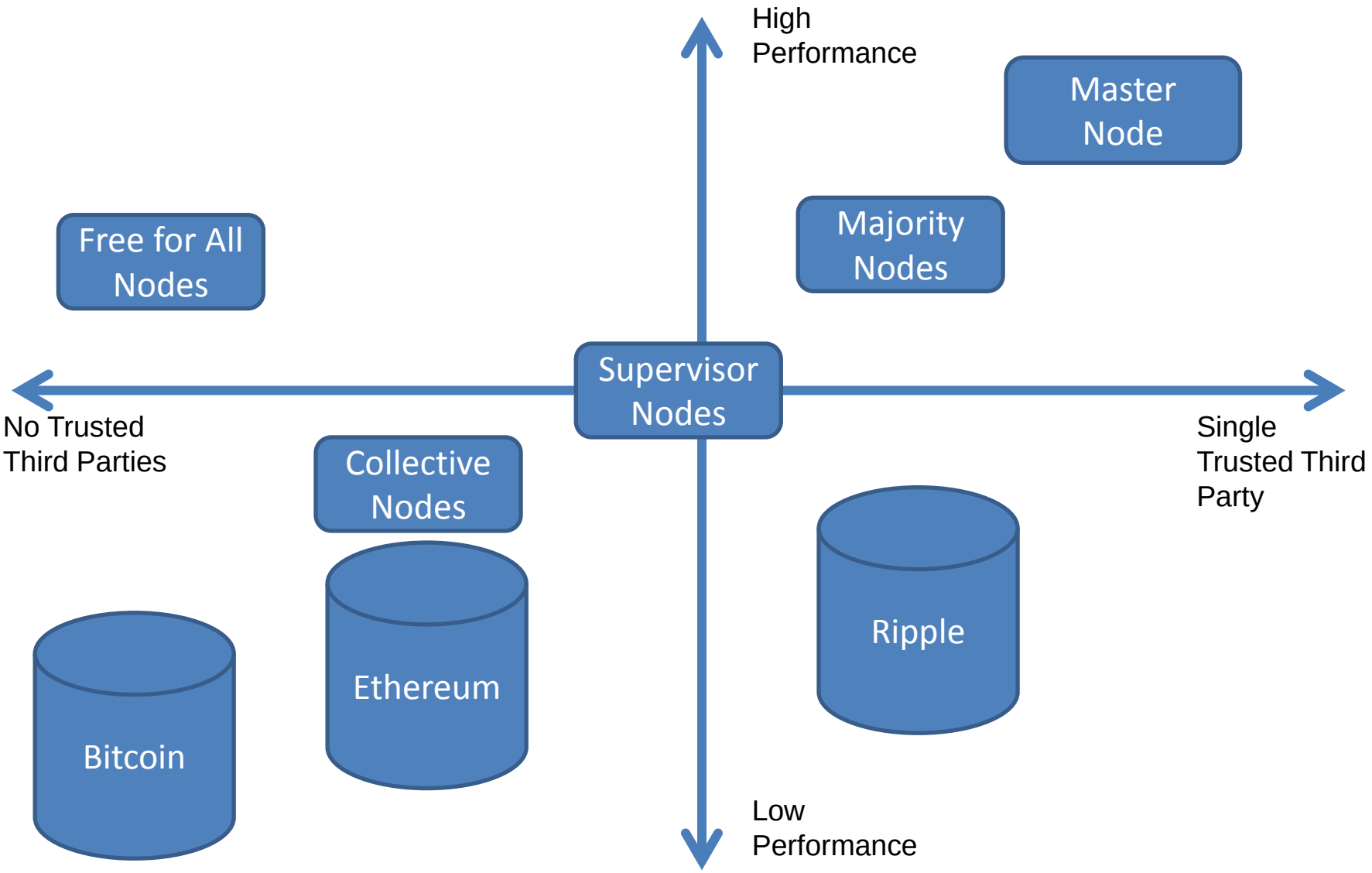
Taxonomic Trials

		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

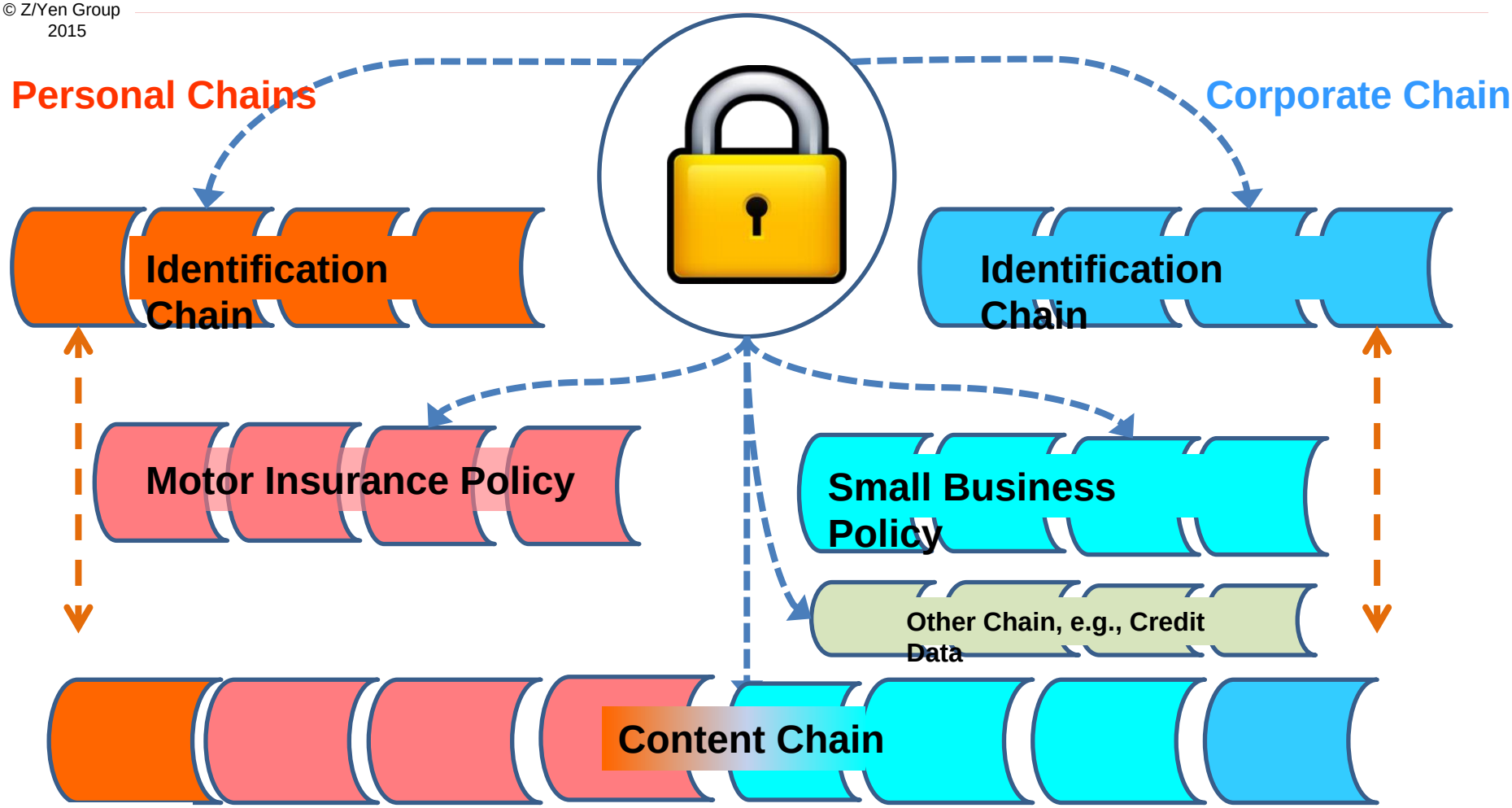
Source: Richard Brown

[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/]

InterChainZ Evaluation



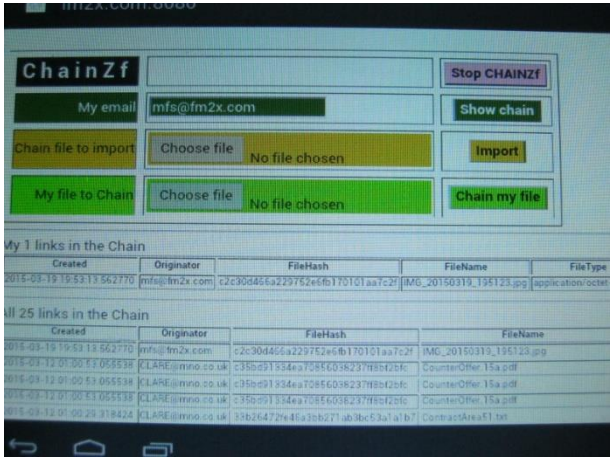
InterChainZ in Pictures



Types of keys

- Chain creator " I have added data"
- Chain Co-Validator "I have confirmed the data"
- Chain Viewer "I need to view all or part of the chain"

InterChainZ



ChainZf | Stop CHAINZf
My email: ben_morris@zyen.com | Show chain
Chain file to import: Choose File | No file chosen | Import
My file to Chain: Choose File | No file chosen | Chain my file
Export my Chain

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	youthinmind@gmail.com	8a1fec5a66c83d8bed0ddce1772b721b	Self-signed SSL certificates.doc	application/octet-stream	115200	fm2x.mfs@gmail.com
2015-03-02 11:03:19.257397	fm2x.mfs@gmail.com	68911b33a7deacfe2e4ceea2020e55d4	Sales & Royalty Report-Jan-17-2015-to-Feb-16-2015-en_US..xls	application/vnd.ms-excel	27648	fm2x.mfs@gmail.com

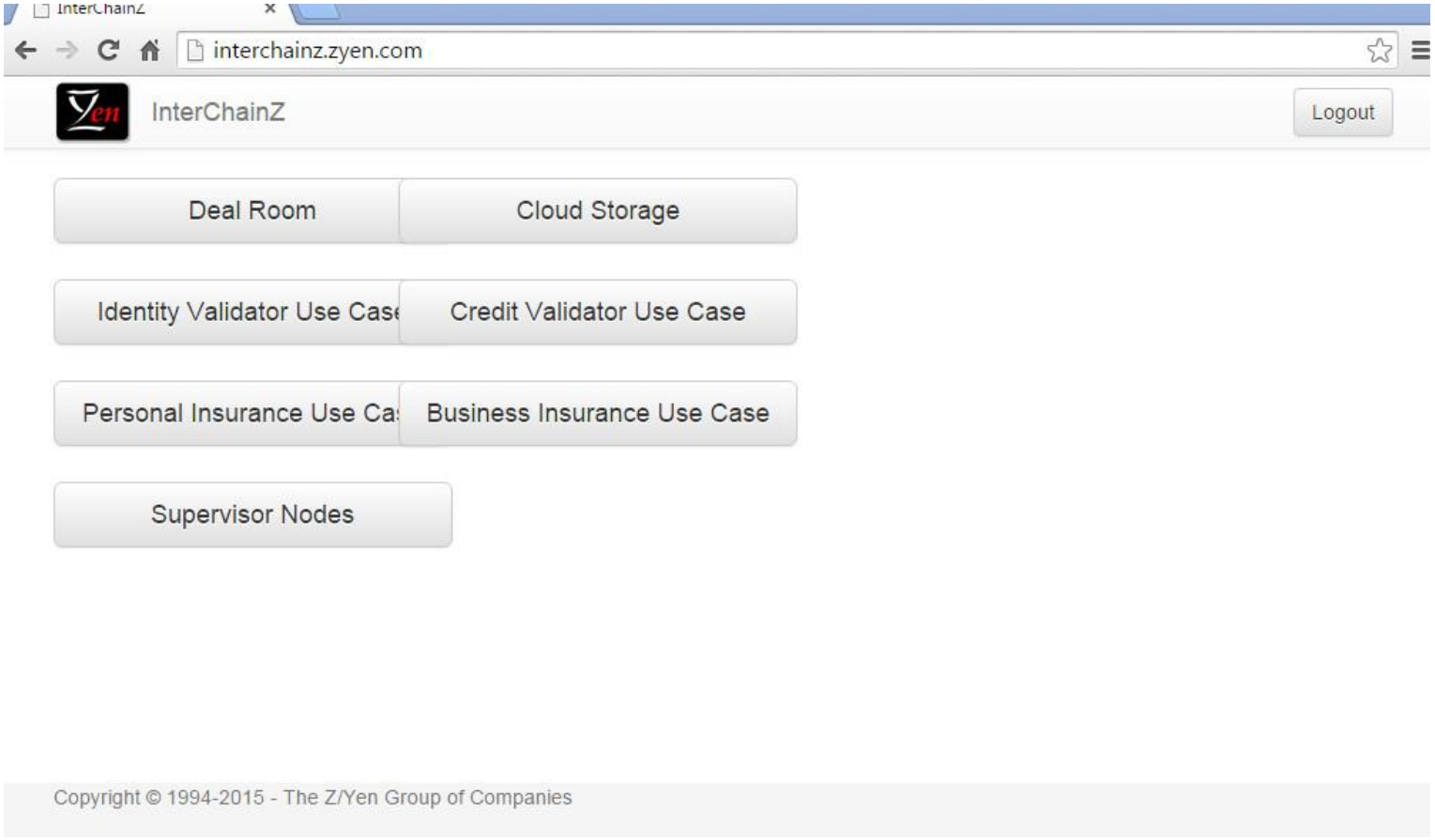
88c96b28-dc89-11e4-aa45-00163e05280f bid:218765812851

Account | Links | Servers | Menu | Sign out

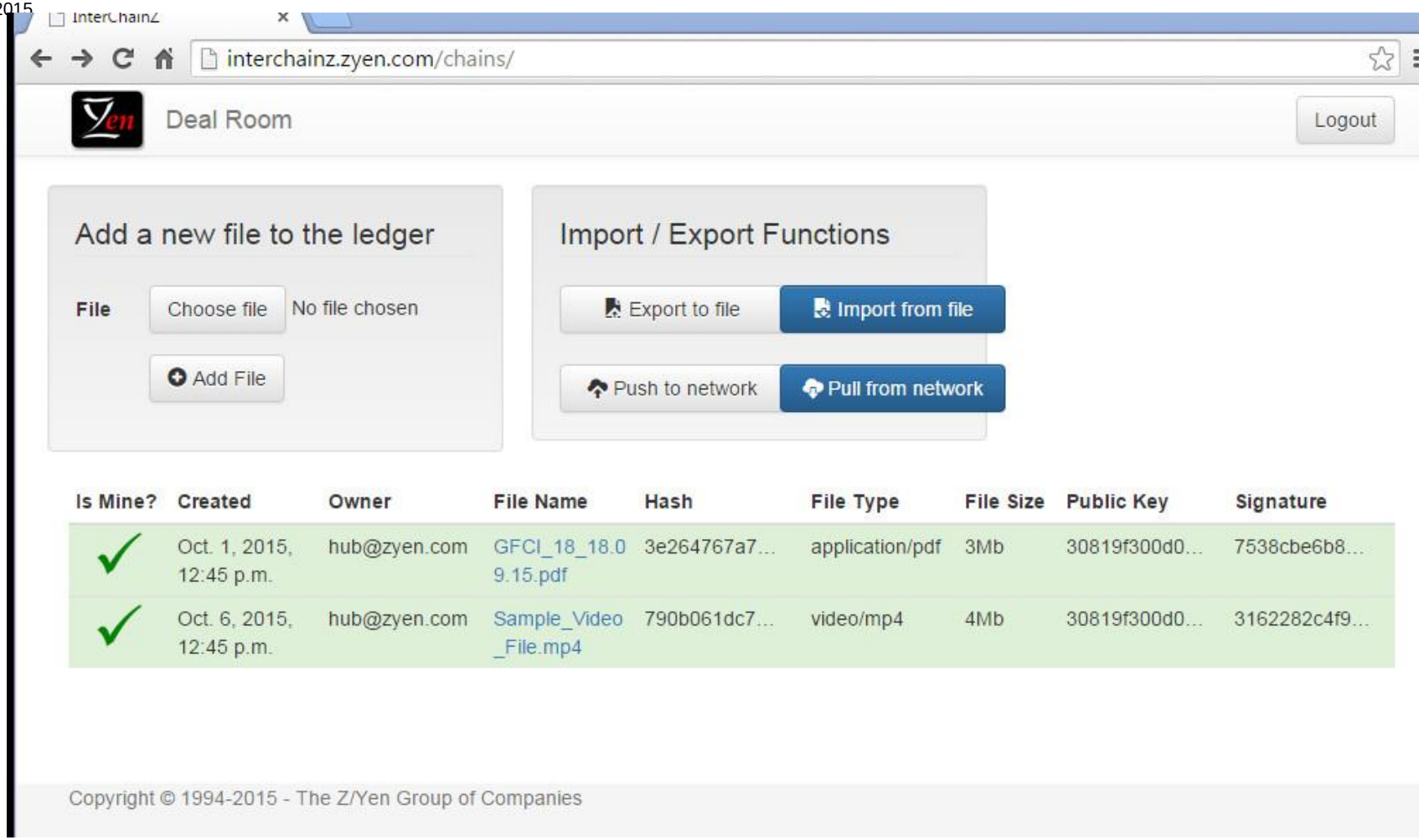
Links (10) + Add New Link

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:-0.10475699999999999	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.	5c9c4af8103add36ec2a33be891a9fa2	5423f9dfa80ddbdd36ff67a60fc8a1c5
2015-04-08 19:05:23.440113	88c96b28-dc89-11e4-aa45-00163e05280f	ff96879c-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	982d7a41cfc545fd02038609db69d142
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

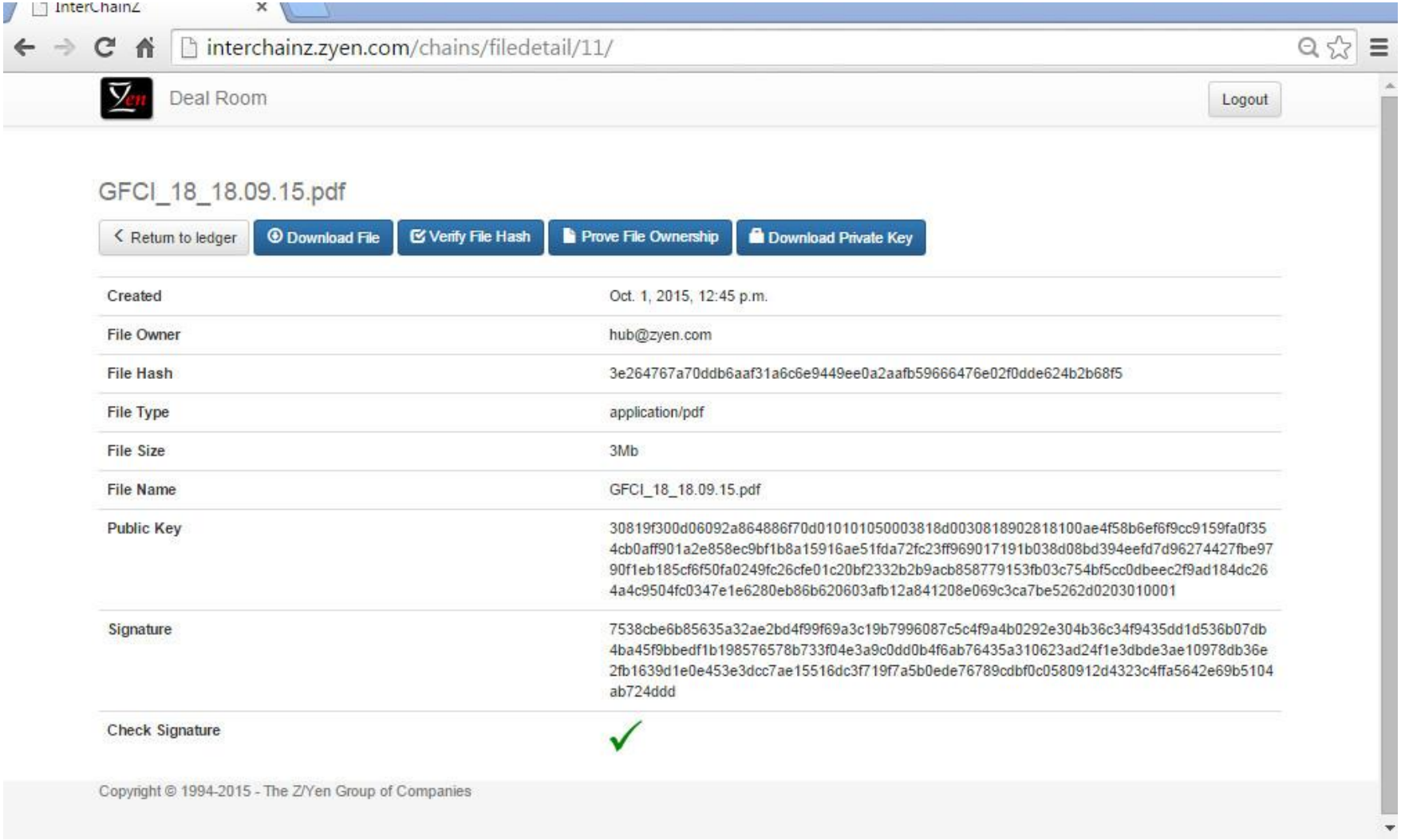
InterChainZ Log In Screen



InterChainZ Deal Room



InterChainZ File Detail



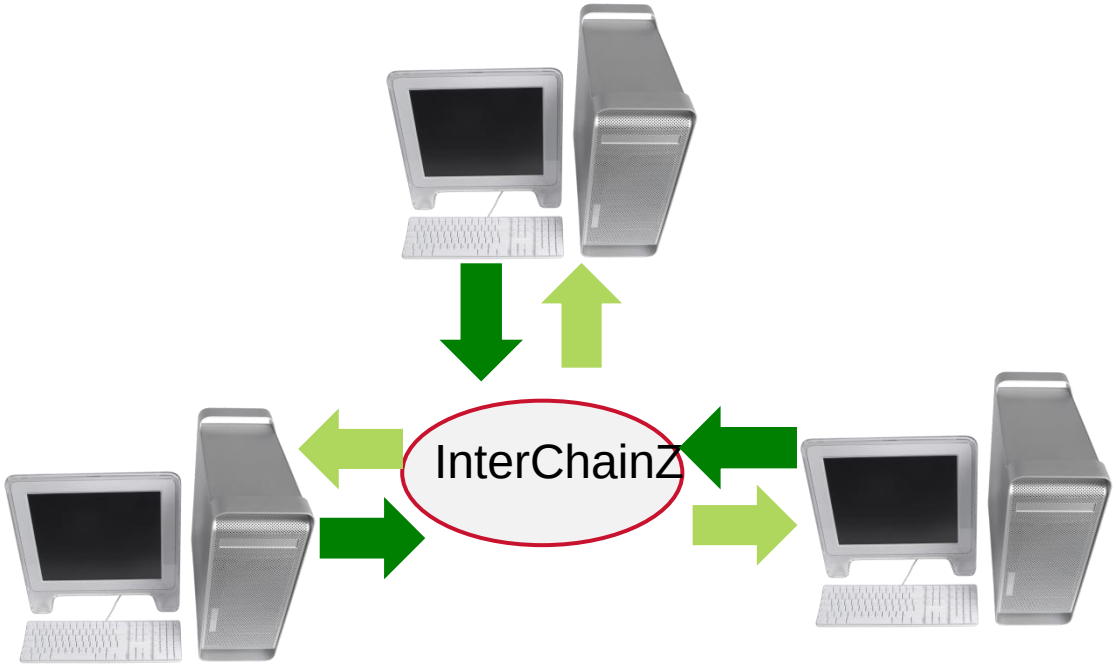
Thoughts on Chain Options: Number of Chains

Option	How it works	Potential Benefits	Potential Risks	Further Thoughts
Single Chain	All content, transaction and identification information is held on one chain	• Straightforward data structure, easy to implement and to search • Distribution – all data distributed throughout the chain thus reducing risk of data loss from small number of nodes	• Volume – as chain grows it will require large storage capacity • Performance – likely to impede speed of searches and access • Regulatory – potential lack of oversight over sensitive personal information	Useful for demonstration purposes and for smaller private chains
Dual Chains	Separate transaction-content chain and identification chain	• Maintains a simple link between data and content • Allows for more options for storing sensitive content, e.g., in standalone chain infrastructure, or in traditional storage, e.g., local servers • Lower volume of identification chain reducing storage requirements and improving performance • Facilitate giving access to subsets of data	• Slightly more complex structure requires security for both chains and links • Regulators and customers may require additional audits to confirm links in place	Need to develop protocols for linking data on chains and retrieving data from content chain
Many Chains	Separate content chain, identification chain and transactions chains	• As for Dual chains, also allows an individual to link to different chains in different networks for different types of transactions, e.g., an insurance chain and a credit chain	• Increasingly complex structures may be harder to control • Requires excellent data sharing protocols to validate data links to different chains networks	Business case for additional complexity needs development, may be a longer term option

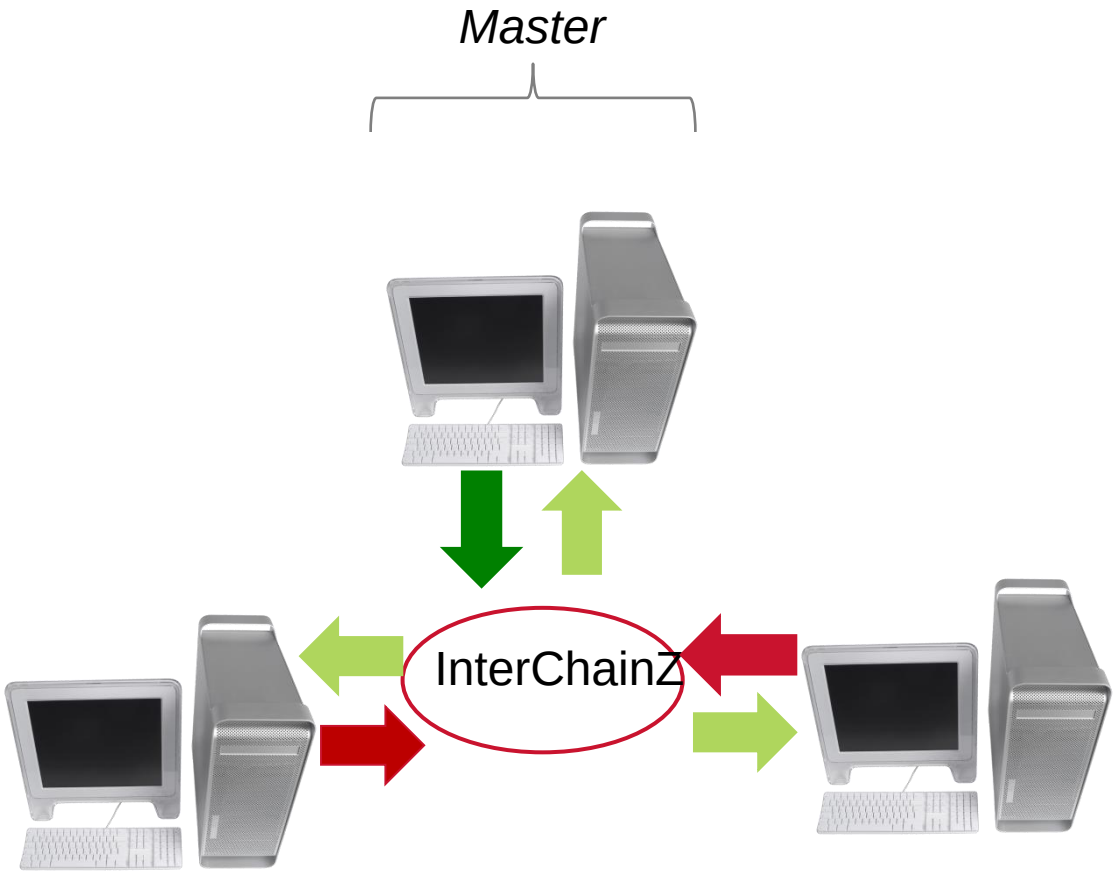
Thoughts on Chain Options: Node Architecture

Option	How it works	Potential Benefits	Potential Risks	Further Thoughts
Master	Specific Node must approve all entries	• Central ability t o control ledger • Straightforward to update approval rules • Increased speed of entry to ledger as no need to wait for other nodes to be live • Simple to implement	• Single point of failure – ledgers cannot function without it • Remain reliant on single trusted third party	See Cloud Storage Demo for Example
Supervisor	A number of specific nodes must approve all entries	• Relatively straightforward to update approval rules • Moderate speed of entry as only waiting for specific nodes	• Remain reliant on specific nodes being live • More complex implementation – need to agree supervisors and fall backs	See Supervisor Nodes Demo for example
Majority	51% or more of nodes must approve all entries	• Not dependent on specific nodes to be available	• More complex to implement – e.g., to calculate how many nodes are live at any time	To be developed
Collective	All nodes must approve all entries	• Increased certainty over entries – no partial approval allowed	• Requires all nodes to be live at all times • Likely to impact performance while waiting for 100% approval	To be developed
Free for All	Any member of network can add to chain	• Simple to maintain and implement • Relatively high performance • Does not require specific nodes to be live	• Lack of control over data entry	See client use case demos

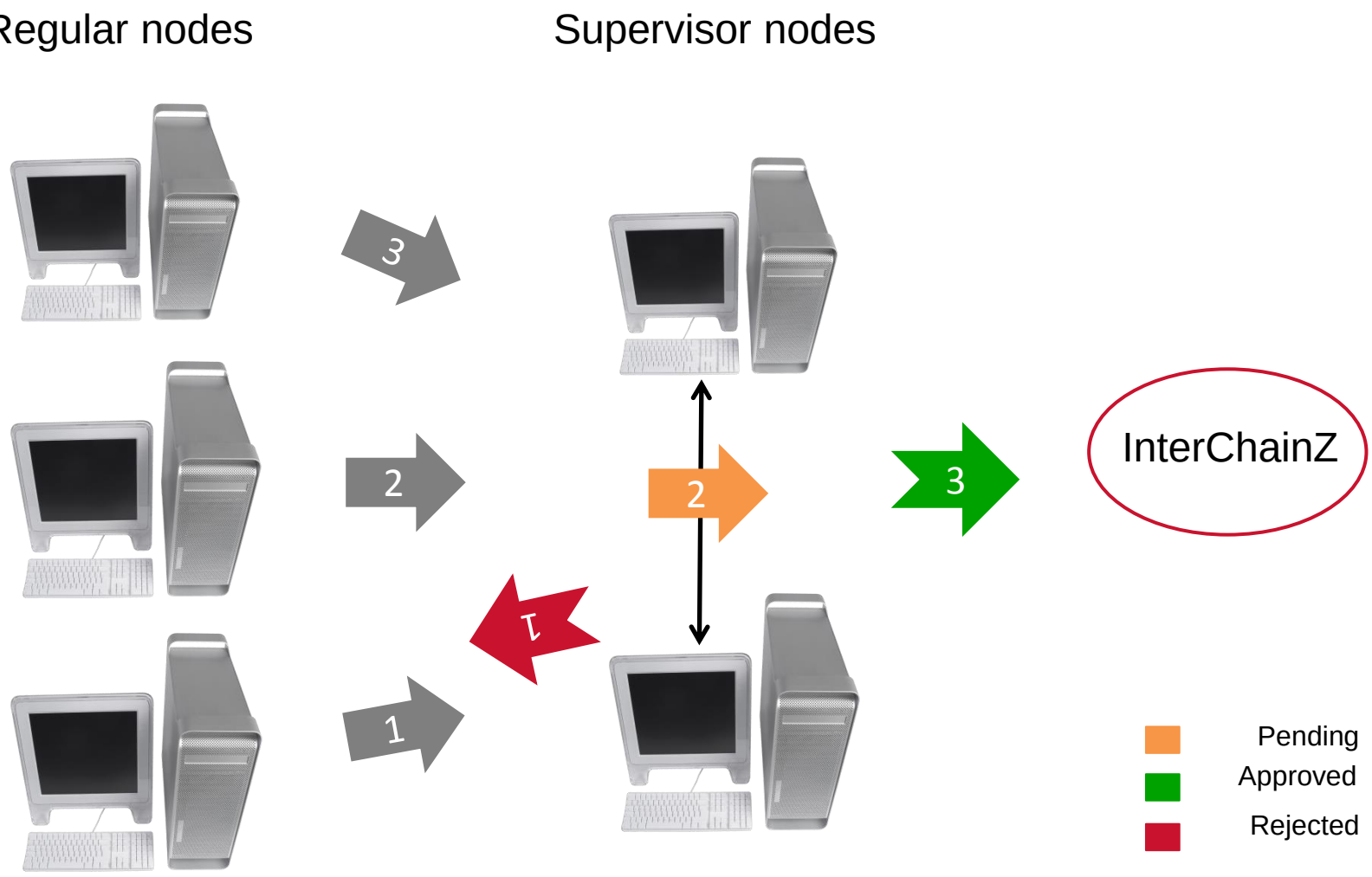
All Nodes Architecture



Master Node Architecture



Supervisor Nodes Architecture



Possible Size Requirements – Static Data

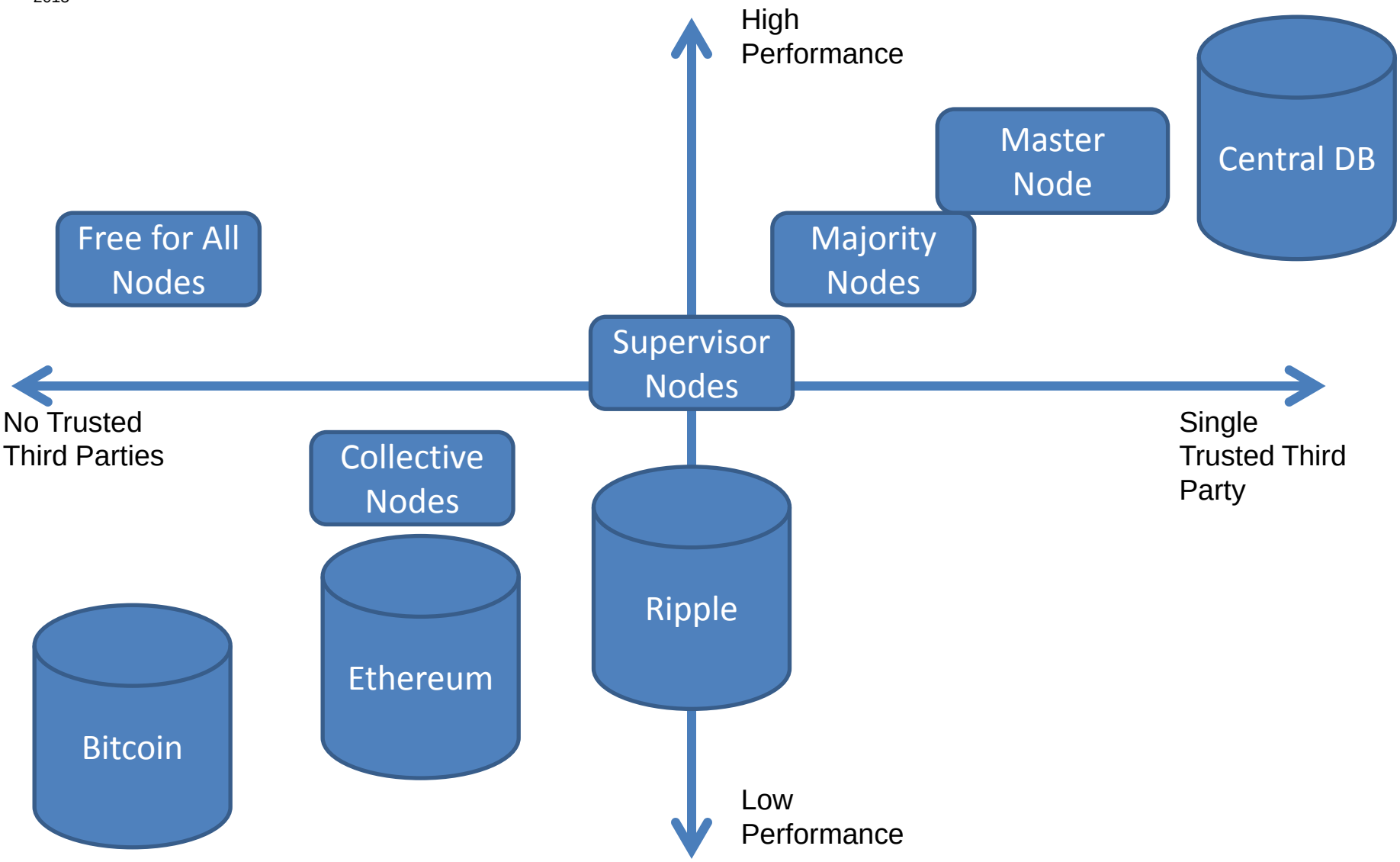
File Sizes/ Number of Nodes	1 Client: 750KB	100 Clients: 75MB	500 Clients: 375 MB	1000 Clients: 750 MB	10000 Clients: 7.5GB
2	1.5 MB	150 MB	750 MB	1.5 GB	15 GB
5	3.75 MB	375 MB	1.875 GB	3.75 GB	37.5GB
100	75 MB	7.5 GB	37.5 GB	75 GB	750GB
500	375MB	37.5 GB	187.5 GB	375 GB	3.75 TB

Possible Size Requirements – Cloud Storage Cost Estimate

File Sizes/ Number of Nodes	1 Client: 750KB	100 Clients: 75MB	500 Clients: 375 MB	1000 Clients: 750 MB	10000 Clients: 7.5GB
500	375MB < £1 per month	37.5 GB £1.35 per month	187.5 GB £6.75 per month	375 GB £13.50 per month	3.75 TB: £135 per month

Number of Read/ Write Operations Per month	10000 Clients: 500,000
Potential Cost @ 0.0022p per 100,000 per month	0.01p

InterChainZ Evaluation



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?

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.

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.

Ledger Logic & Turing Machines

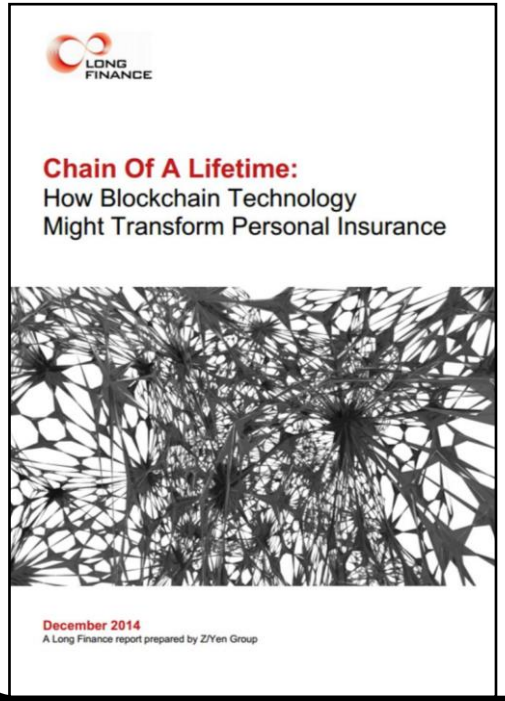
- Smart (dumb) contracts (aka scripts) enforced when certain pre-defined conditions are met, e.g.:
  - Oracles, e.g. crop insurance smart contract coupled with 'trusted' weather data feed
  - Arbitrators, e.g. appointed 'experts', such as software development smart contract appointing software experts 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."**

The Long-Term?

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



Discussion

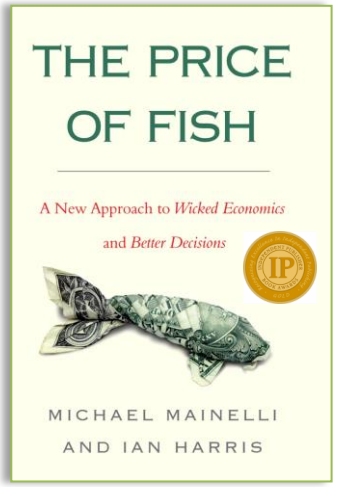
- Regulate - governance & management standards, technical performance
- Use - trade reporting, ‘too big to fail’, account portability
- Encourage – new services, e.g. regulatory ‘validation’

Next Steps: IntereXchainZ

- Facilities for automated creation of new mutual distributed ledgers;
- Management and control features;
- Integrity proofing;
- Market functions;
- Usability and ergonomics;
- Exchange functions;
- Data taxonomies, encryption levels and tracking;
- Content Hash-Addressable Storage Market (C#ASM);
- Documentation of regulatory standards.

When Would We Know Our Commerce Is Working?

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



Thank you!

LONG FINANCE