

An open source research programme for Smart Ledgers and new technologies



Information Rules Smart Ledgers & Permissions

Long Finance Webinar

Thursday, 06 December 2018, 15:00 to 15:30

(presentation starts at 15:01)

Z/Yen Group Limited
41 Lothbury
London EC2R 7HG
United Kingdom
tel: +44 (20) 7562-9562
www.zyen.com



Introduction



James Pitcher
Programme Director
Z/Yen Group

james_pitcher@zyen.com

Agenda

15:00 – 15:05	Welcome & Introduction
15:05 – 15:20	Presentation
15:20 – 15:25	Questions
15:25 – 15:30	Concluding Remarks

Report

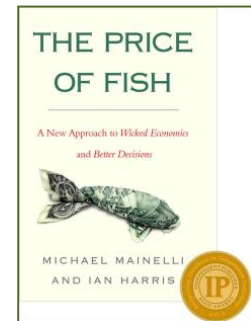
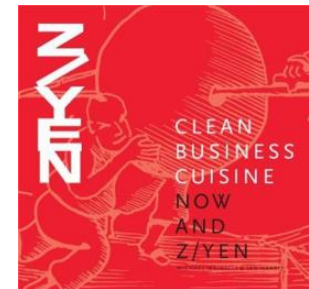


Read the report [here](#).



- ◆ **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





Distributed Futures Programme



We work in partnership with many stakeholders to learn together and build the vital infrastructure needed to make Smart Ledgers a success.

Our research is structured around four themes:

- ◆ Societal
- ◆ Technological
- ◆ Economic
- ◆ Political

Directed at four outcomes:

- ◆ Expanding frontiers
- ◆ Changing systems
- ◆ Delivering services
- ◆ Building communities



Sponsored By

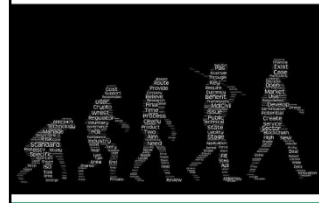








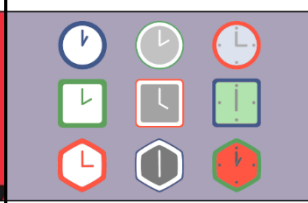
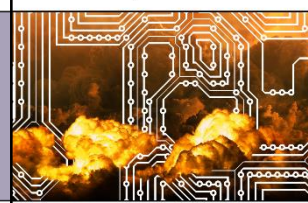
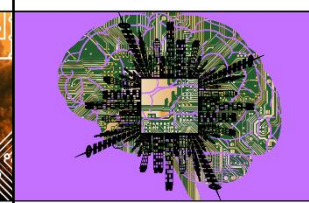

CARDANO
FOUNDATION



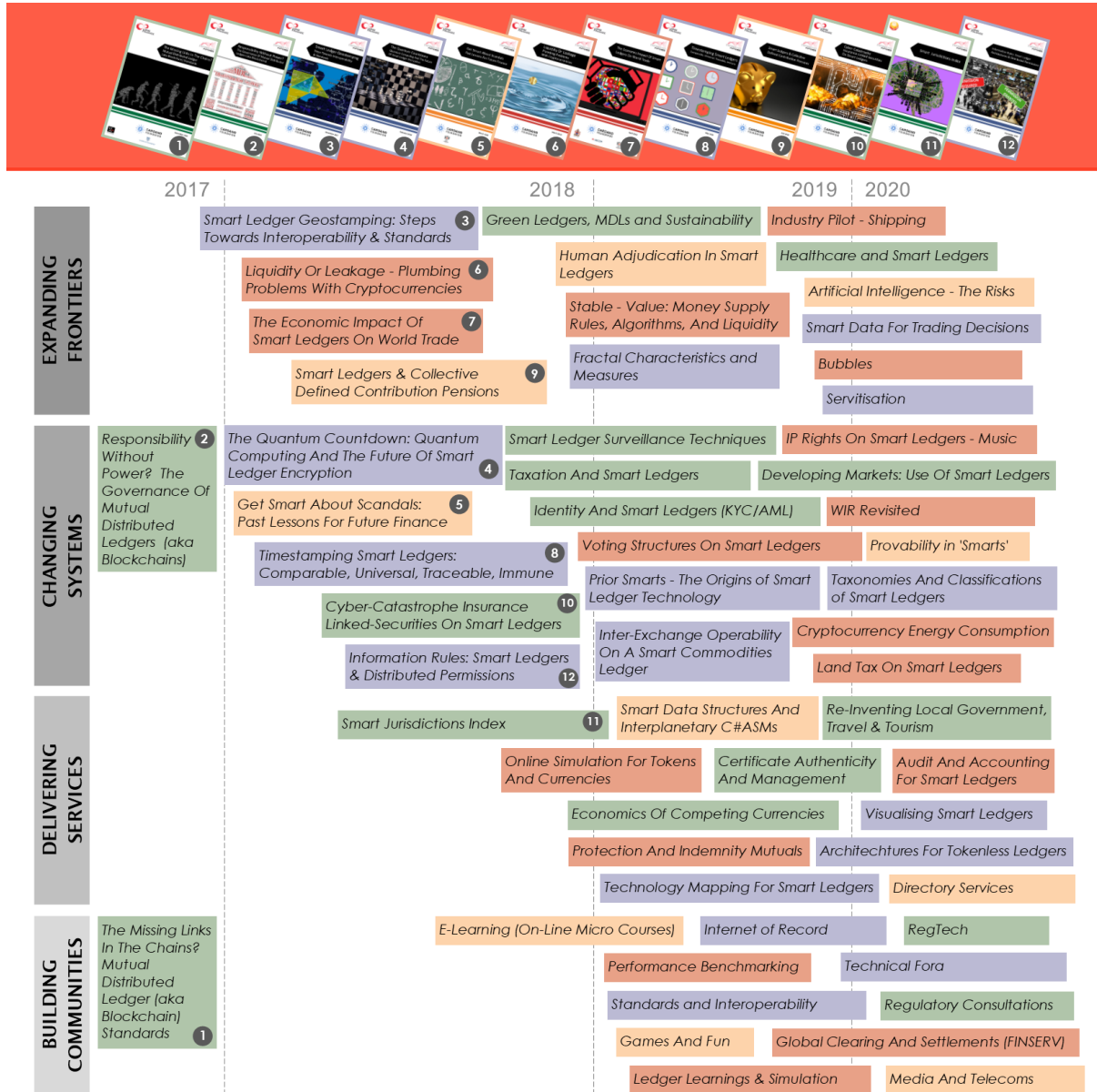
The Z/zen Group

Distributed Futures Research

 <p>The Missing Links In The Chains? Mutual Distributed Ledger (aka Blockchain) Standards</p> <p>November 2016</p> <p>CARDANO FOUNDATION STATES OF ALABAMA pwc</p>	 <p>Responsibility Without Power? The Governance Of Mutual Distributed Ledgers (aka Blockchains)</p> <p>July 2016</p> <p>CARDANO FOUNDATION</p>	 <p>Smart Ledger Geostamping Steps Towards Interoperability & Standards</p> <p>December 2017</p> <p>CARDANO FOUNDATION</p>	 <p>The Quantum Countdown Quantum Computing And The Future Of Smart Ledger Encryption</p> <p>February 2018</p> <p>CARDANO FOUNDATION</p>	 <p>Get Smart About Scandals Past Lessons For Future Finance</p> <p>March 2018</p> <p>CARDANO FOUNDATION</p>	 <p>Liquidity Or Leakage Plumbing Problems With Cryptocurrencies</p> <p>March 2018</p> <p>CARDANO FOUNDATION</p>
---	---	--	---	--	--

 <p>The Economic Impact Of Smart Ledgers On World Trade</p> <p>April 2018</p> <p>CARDANO FOUNDATION</p>	 <p>Timestamping Smart Ledgers Comparable, Universal, Traceable, Immune</p> <p>May 2018</p> <p>CARDANO FOUNDATION</p>	 <p>Cyber-Catastrophe Insurance-Linked Securities On Smart Ledgers</p> <p>November 2018</p> <p>CARDANO FOUNDATION</p>	 <p>Smart Jurisdictions Index</p> <p>November 2018</p> <p>CARDANO FOUNDATION</p>	 <p>Information Rules: Smart Ledger Architectures & Distributed Permissions</p> <p>November 2018</p> <p>CARDANO FOUNDATION</p>
--	--	---	---	---

Timeline



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”
- ◆ **smart ledger** – MDL with embedded, executable code

Smart Ledgers Hold Immense Promise

Financial Instruments, Records, Models		Public Records		Private, Semi-Private/Semi-Public		Physical Keys, Intellectual Property, Other Records	
Currencies	Derivatives	Land & Property Titles	Vehicle Registries	Contracts	ID	Home Key	Hotel Key
Commodities	Insurance Policies	Shipping Registries	Satellite Registries	Signature	Will	Office Key	Car Key
Trading Records	Private and Public Equities	Business License	Business Ownership Records	Trust	Escrow	Deposit Box Key	Mail Box Key
Certificates of Deposit	Bonds	Incorporation / Dissolution Records	Regulatory Records	Other Classifiable Data	High School / University Degrees	Internet Of Things	Copyrights & Patents
Voting Rights (Financial Services)	Credit Data	Criminal Records	Passport	Professional Qualifications	Certifications	Licenses	Digital Rights Management
Collateral Management	Client Monies Segregation	Birth / Death Certificates	Voting ID	Human Resources Records	Medical Records	Trademarks	Proof Of Authenticity / Authorship
Mortgage / Loan Records	Crowd-Funding	Health & Safety Inspections	Tax Returns	Accounting Records	Business Transaction Records	Cultural Events	Historical Events
P2P Lending	Microfinance	Building & Other Types Of Permits	Court Records	Locational Data	Genome & DNA	Documentaries	Big Data
Account Portability	Airmiles / Corporate Tokens	Government / Listed Companies	Accounts & Annual Reports	Arbitration	Genealogy Trees	SIM Cards	Archives

Report Walkthrough

Information Rules: Smart Ledgers & Permissions



Maury Shenk

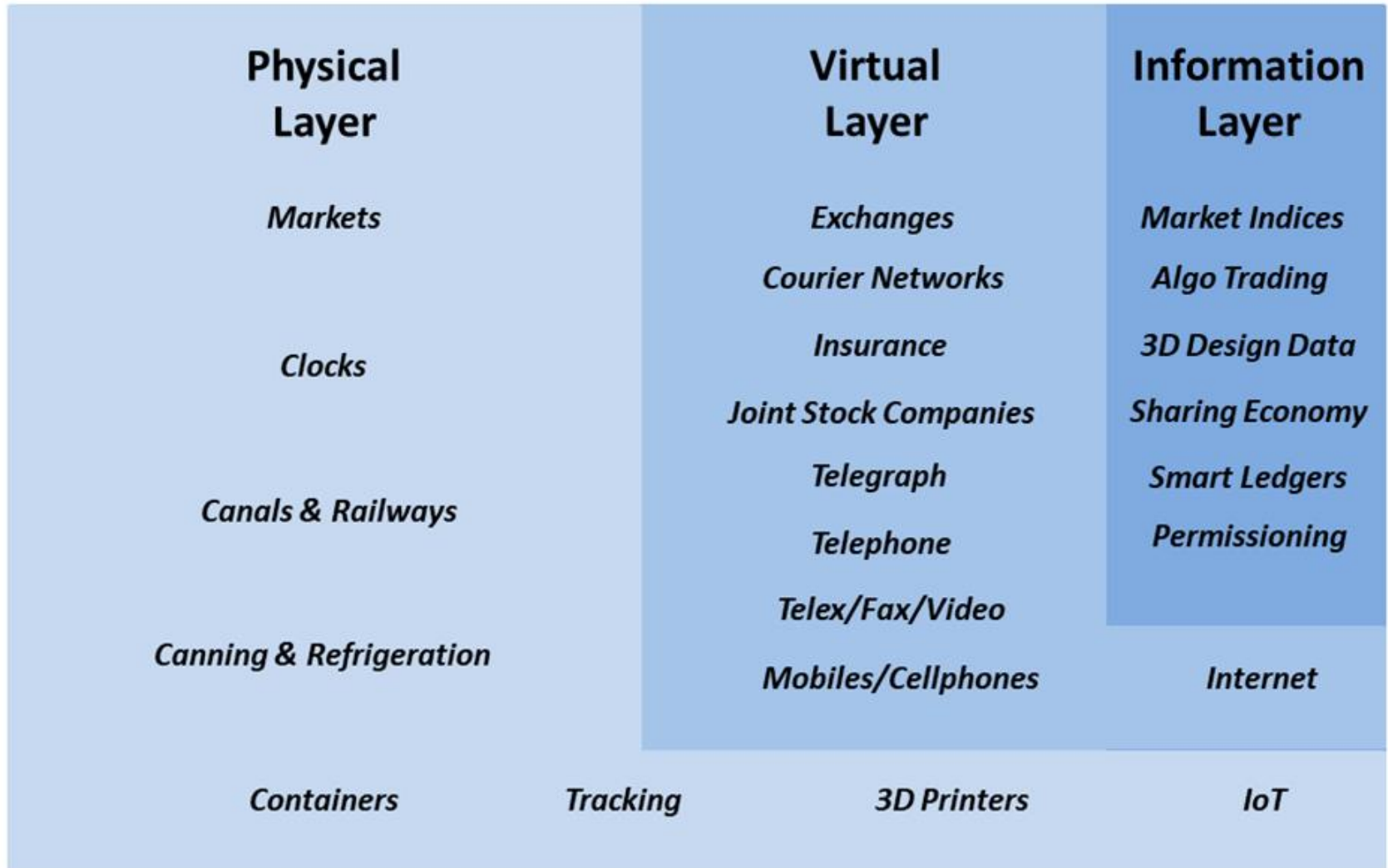
*Maury Shenk, Managing
Director, Lily Innovation*

Why We Need a Permissions Framework

- ◆ Permission (or not) to use digital / online resources is at the core of our information economy
- ◆ But there are major holes in existing frameworks
 - No widely-accepted standards
 - Major cybersecurity issues as more devices come online (e.g. IoT)
 - Difficulty of implementing concepts of “may” and “should” (or not) on Boolean devices
- ◆ Need to move beyond access control



Three Market Layers



Examples of Market Layers

- ◆ **Physical layer:** actual exchange
- ◆ **Virtual layer:** communications about exchange
- ◆ **Information layer:** metadata about exchange



Choosing a Permissions Framework

◆ Criteria

- Precision – ability to accurately convey permissions
- Breadth – ability to convey any permission
- Applicability – comprehensibility and practicality for real-world markets

◆ Candidates

- Access control
 - Standard for computer systems
 - Comes in many flavors – e.g. access control list, role-based, attribute-based
- Differential privacy – conveying information while avoiding disclosure of personal information
- Deontic logic – formal logic of “may” and “ought”

Deontic Logic in Practice (for Identity)

What a Human Hears	High-Level Proposition	Propositional Variables	Deontic Proposition
You are an authorised user of this computer system	Person X may access resource R	$AR_X = X$ accesses resource R	$P(AR_X)$
If you are in the finance department, you may access the accounting system	If person X belongs to group G, she may access resource R	$AR_X = X$ accesses resource R $G = \text{group } G$	$\text{If } X \in G \rightarrow P(AR_X)$
Would Mr. Jones please go to the ticketing desk	If recipient of message is person X, she should take action A	$U = \text{recipient of message}$ $A_X = X$ takes action A	$\text{If } U = X \rightarrow O(A_U)$ $\text{If } U = X \rightarrow O(A_X)$
Sorry, no admittance for under 18s	If person X is under age K, she may not access resource R	$K_X = \text{age of } X$ $AR_X = X$ accesses resource R	$\text{If } K_X < 18$ $\rightarrow \neg P(AR_X)$
No ID, no entry	If person X cannot prove she is over age K, she may not access resource R	$K_X = \text{age of } X$ $ID_X = \text{identification documents in } X\text{'s possession}$ $AR_X = X$ accesses resource R	$\text{If } (K_X > 18) \neg \vdash ID_X$ $\rightarrow \neg P(AR_X)$

Structure Of A New Permission Architecture

Privacy	Consumer Financial	Securities Trading	Travel	Government Services	E-Commerce	...
Logical Access Control				Physical Access Control		
Domain-Specific Permission Libraries						
Deontic Logic API						
Deontic Logic Translation Engine						
Smart Ledgers – Internet of Record						
TCP/IP – Internet of Communications						
Underlying Computing Operating System (e.g., Linux, iOS, MacOS, Windows)						

Why and How Smart Ledgers?

- ◆ Advantages over centralised solutions
 - Inherently distributed
 - Open architectures are common / understood
- ◆ Technical challenges
 - Functions to manage technical complexity – requires an advanced, “third generation” architecture
 - Implementing deontic logic on a Boolean computer
- ◆ Legal challenges
 - Differ by jurisdiction (e.g. Europe, US, China, India)
 - Tensions between GDPR and Smart Ledgers (e.g. erasure, repeated processing) are surmountable

Information Rules

Smart Ledgers & Permissions

Questions

Concluding Remarks



James Pitcher
Programme Director
Z/Yen Group

james_pitcher@zyen.com

When Would We Know Our Commerce Is Working?



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

Thank you!

