Distributed Futures

An open source research programme for Smart Ledgers and new technologies

The Quantum Countdown:

Quantum Computing and the Future of Smart Ledger Encryption

Tuesday, 20 February 2018, London

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

Sponsored By

CARDANO FOUNDATION

LONG FINANCE

The Z/Yen Group

Agenda

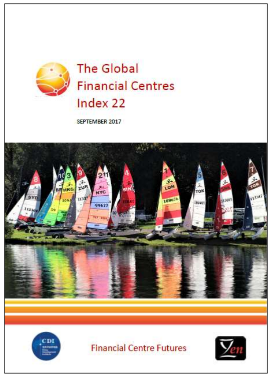
08:45 – 09:00	**Registration**
09:00 – 09:05	**Welcome** *Bob McDowall, Cardano Foundation*
09:05 – 09:30	**Introduction and Background** *Michael Mainelli, Executive Chairman, Z/Yen Group*
09:30 – 10:00	**The Quantum Countdown: Report Walkthrough** *Maury Shenk, Managing Director, Lily Innovation*
10:00 – 10:40	**Panel Discussion** ♦ True area for Smart Ledger risk ♦ Modelling of response time for the PQC Problem ♦ Policy-making and advocacy ♦ Insurance
10.40 – 10:45	**Summary**
10:45	**Formal Close**

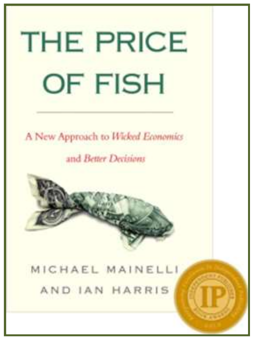
Z/Yen

LONG FINANCE

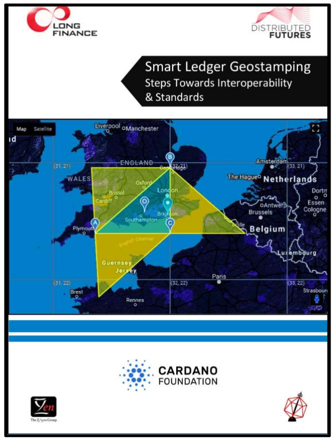
Global Green Finance Index

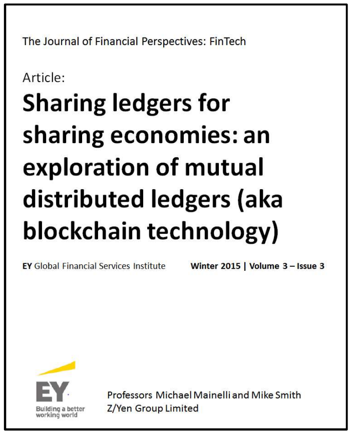
- ♦ Special – City of London’s leading commercial think-tank
- ♦ Services – projects, strategy, expertise on demand, coaching, research, analytics, modern systems
- ♦ Sectors – technology, finance, voluntary, professional services, outsourcing
  - ➢ Independent Publisher Book Awards Finance, Investment & 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 £aboratory visualising financial risk 1997




THE PRICE OF FISH
A New Approach to Wicked Economics and Better Decisions
MICHAEL MAINELLI AND IAN HARRIS

Smart Ledger Research

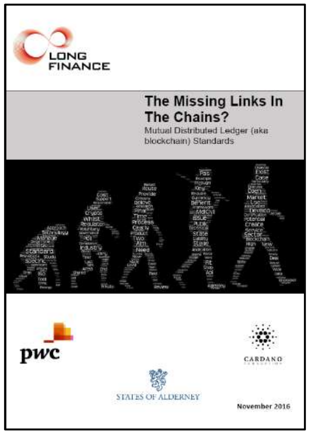

Smart Ledger Geostamping
Steps Towards Interoperability
& Standards


The Journal of Financial Perspectives: FinTech

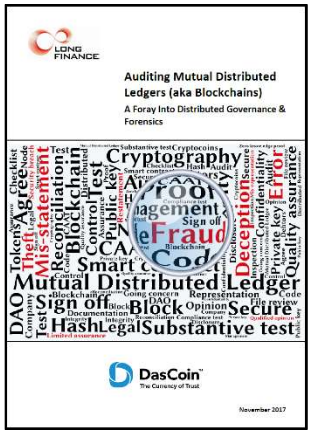
Article:
Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)

EY Global Financial Services Institute — **Winter 2015 | Volume 3 – Issue 3**

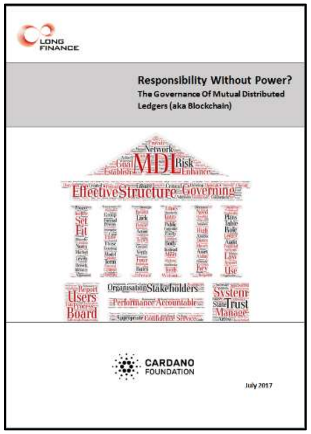
Professors Michael Mainelli and Mike Smith
Z/Yen Group Limited


The Missing Links In The Chains?
Mutual Distributed Ledger (aka blockchain) Standards

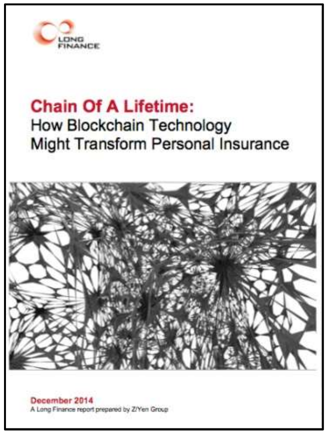
November 2016


Auditing Mutual Distributed Ledgers (aka Blockchains)
A Foray Into Distributed Governance & Forensics

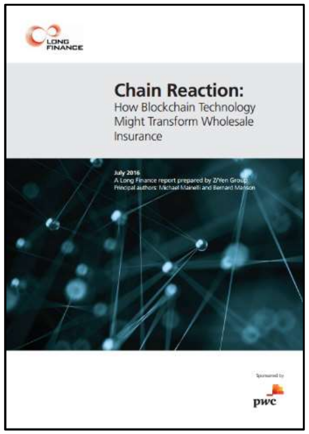
November 2017


Responsibility Without Power?
The Governance Of Mutual Distributed Ledgers (aka Blockchain)

July 2017

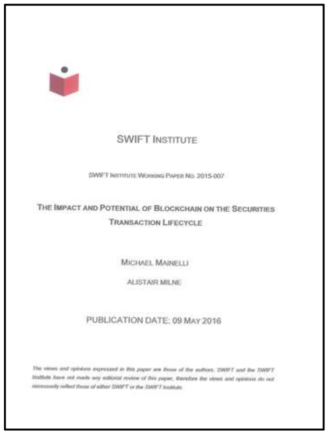

Chain Of A Lifetime:
How Blockchain Technology
Might Transform Personal Insurance

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


Chain Reaction:
How Blockchain Technology Might Transform Wholesale Insurance

July 2016
A Long Finance report prepared by Z/Yen Group
Principal authors: Michael Mainelli and Bernard Manson

Sponsored by


SWIFT INSTITUTE

SWIFT INSTITUTE WORKING PAPER NO. 2015-007

THE IMPACT AND POTENTIAL OF BLOCKCHAIN ON THE SECURITIES TRANSACTION LIFECYCLE

MICHAEL MAINELLI

ALISTAIR MILNE

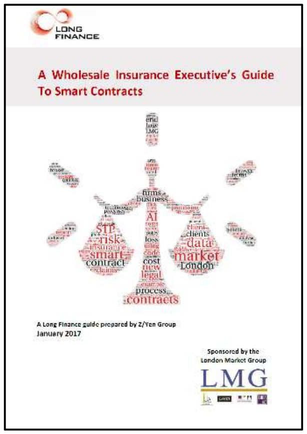
PUBLICATION DATE: 09 MAY 2016

The views and opinions expressed in this paper are those of the authors. SWIFT and the SWIFT Institute have not made any editorial review of this paper, therefore the views and opinions do not necessarily reflect those of either SWIFT or the SWIFT Institute.

From Slips To Smart Contracts
Intelligent Technology
In The London Wholesale Insurance Market

A Long Finance report prepared by Z/Yen Group
January 2017

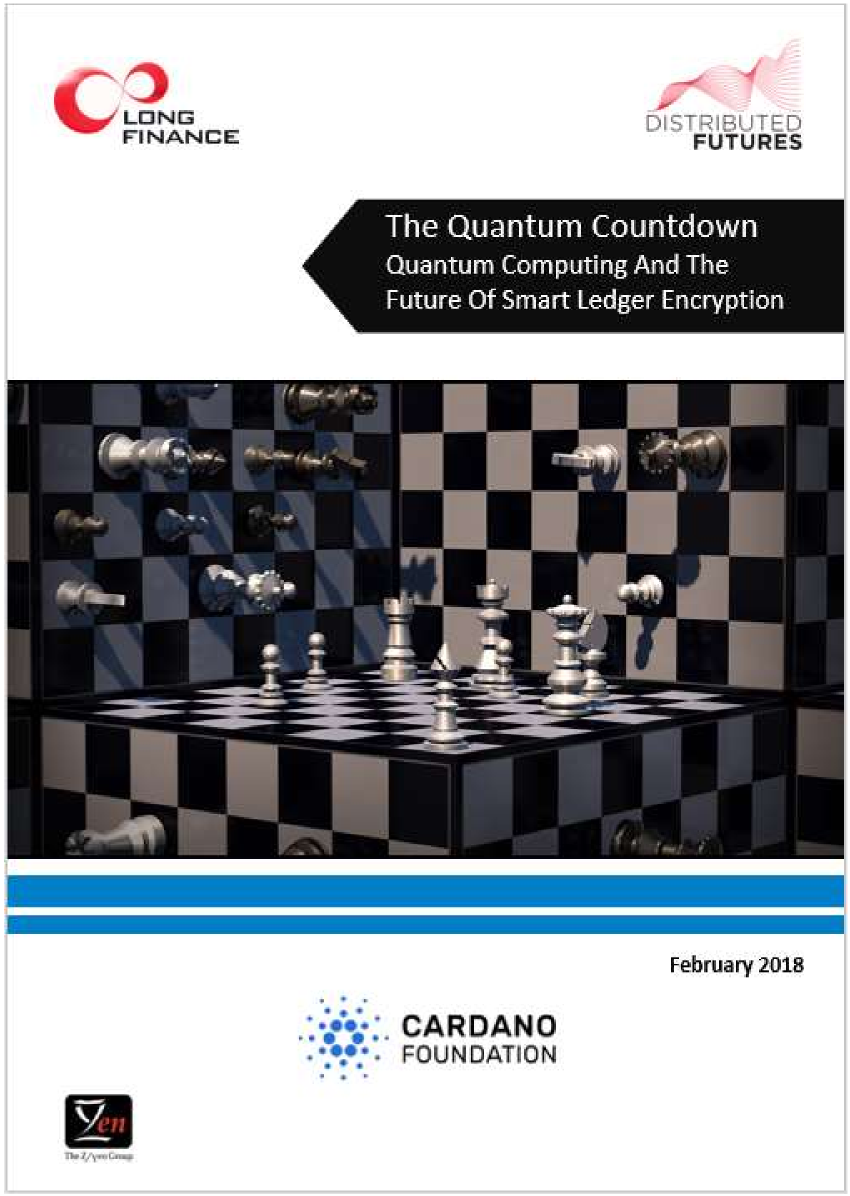
Sponsored by the
London Market Group


A Wholesale Insurance Executive's Guide To Smart Contracts

A Long Finance guide prepared by Z/Yen Group
January 2017

Sponsored by the
London Market Group

Draft Report



LONG FINANCE

DISTRIBUTED FUTURES

The Quantum Countdown

Quantum Computing And The Future Of Smart Ledger Encryption

February 2018

CARDANO FOUNDATION

The Z/Yen Group

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:

- Society
- Technology
- Economics
- Politics

And it’s directed at four outcomes:

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

DISTRIBUTED FUTURES

Project Balance & Sequencing

🟥 Not Started | 🟧 Planning | 🟩 Underway | 🟦 Completed

	SOCIAL	TECHNOLOGICAL	ECONOMIC	POLITICAL
EXPANDING FRONTIERS	🟩 Smart Ledgers/World Trade 🟩 Pensions 🟧 Human Adjudication	🟦 Smart Ledger Geostamping 🟧 Fractal Characteristics	🟩 Liquidity 🟩 Economic Impact of SL's 🟧 Money Suppy Rules 🟥 Industry Pilot - Shipping	🟧 Green Ledgers
CHANGING SYSTEMS	🟥 Provability in 'Smarts' 🟩 Past Financial Scandals	🟩 The Quantum Countdown 🟩 Timestamping 🟥 Commodities Lerdgers 🟥 GDPR & Permissioning Logic	🟧 Voting Structures 🟥 IP Rights - Music 🟥 Crypto Energy Comsumption	🟧 Cyber-Catastrophe ILS 🟧 Surveillance Techniques 🟥 Taxation
DELIVERING SERVICES	🟥 Interplanetary C#ASMs 🟥 Directory Services	🟥 Visualising Smart Ledgers 🟥 Tokenless Architecture	🟧 Online Token Simulation 🟥 Audit & Accounting 🟥 Protection & Indemnity	🟧 Competing Currencies
BUILDING COMMUNITIES	🟩 E-Learning/Micro courses 🟥 Games & Fun	🟥 Standards/Interoperability 🟥 Technical Fora	🟥 Ledger Learning/Simulation 🟥 Performance Benchmarking	🟥 RegTech 🟥 Regulatory Consultations

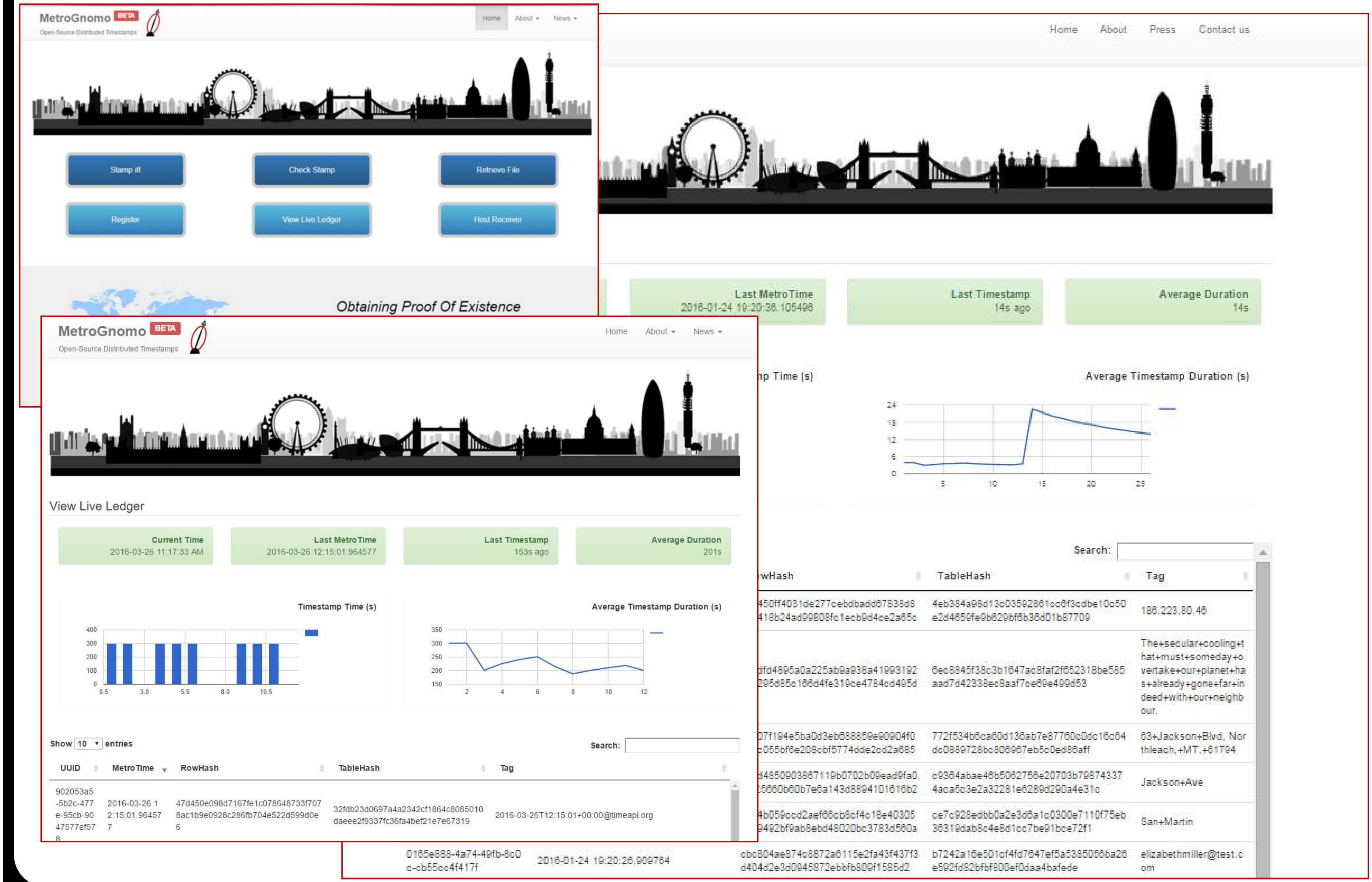
Terminology Evolving

- **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

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, clinical trials, 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, geostamping, etc.

Application:
MetroGnomo – Timestamping & Datalogging



MetroGnomo BETA
Open-Source Distributed Timestamps

Last MetroTime	Last Timestamp	Average Duration
2016-01-24 19:20:36.105496	14s ago	14s

Search:

		wHash	TableHash	Tag
		450ff4031de277cebdbadd67838d8 418b24ad99808fc1ecb9d4ce2a65c	4eb384a98d13c0359286 1cc6f3cdbe10c50 e2d4659fe9b629bf6b36d01b87709	186.223.80.46
		dfd4895a0a225ab9a938a41993192 295d85c166d4fe319ce4784cd495d	6ec8845f38c3b1647ac8faf2f652318be585 aad7d42338ec8aaf7ce69e499d53	The+secular+cooling+that+must+someday+overtake+our+planet+has+already+gone+far+indeed+with+our+neighbour.
		07f194e5ba0d3eb688859e909 04f0 c055bf6e208cbf5774dde2cd2a685	772f534b6ca60d136ab7e87760c0dc16c64 dc0889728bc808967eb5c0ed86aff	63+Jackson+Blvd, Northleach,+MT,+61794
		d4850903867119b0702b09ead9fa0 25660b60b7e6a143d8894101616b2	c9364abae46b5062756e20703b79874337 4aca5c3e2a32281e6289d290a4e31c	Jackson+Ave
		4b059ccd2aef66cb8cf4c18e40305 9492bf9ab8ebd48020bc3783d560a	ce7c928edbb0a2e3d6a1c0300e7110f75eb 36319dab8c4e8d1cc7be91bce72f1	San+Martin
0165e888-4a74-49fb-8c0c-cb55cc4f417f	2016-01-24 19:20:26.909764	cbc804ae874c8872a6115e2fa43f437f3 d404d2e3d0945872ebbfb809f1585d2	b7242a16e501cf4fd7647ef5a5385056ba26 e592fd82bfbf800ef0daa4bafede	elizabethmiller@test.com

MetroGnomo BETA
Open-Source Distributed Timestamps

View Live Ledger

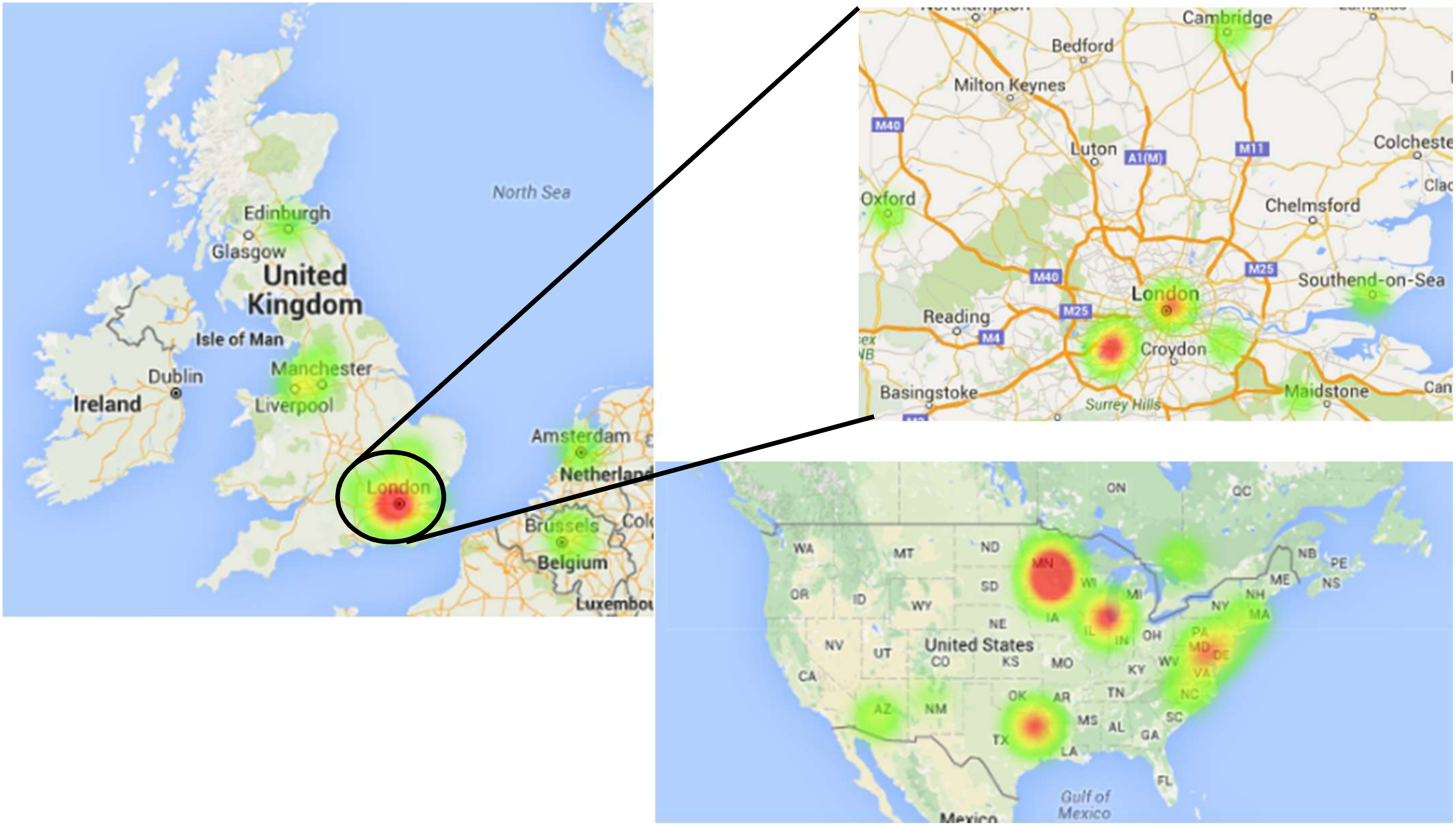
Current Time	Last MetroTime	Last Timestamp	Average Duration
2016-03-26 11:17:33 AM	2016-03-26 12:15:01.964577	153s ago	201s

Show 10 ▾ entries

Search:

UUID	MetroTime	RowHash	TableHash	Tag
902053a5-5b2c-477e-95cb-9047577ef578	2016-03-26 12:15:01.964577	47d450e098d7167fe1c078648733f7078ac1b9e0928c286fb704e522d599d0e6	32fdb23d0697a4a2342cf1864c8085010daeee2f9337fc36fa4bef21e7e67319	2016-03-26T12:15:01+00:00@timeapi.org

Application: Clinical Trials



The Quantum Countdown:

Quantum Computing and the Future of Smart Ledger Encryption

Maury Shenk

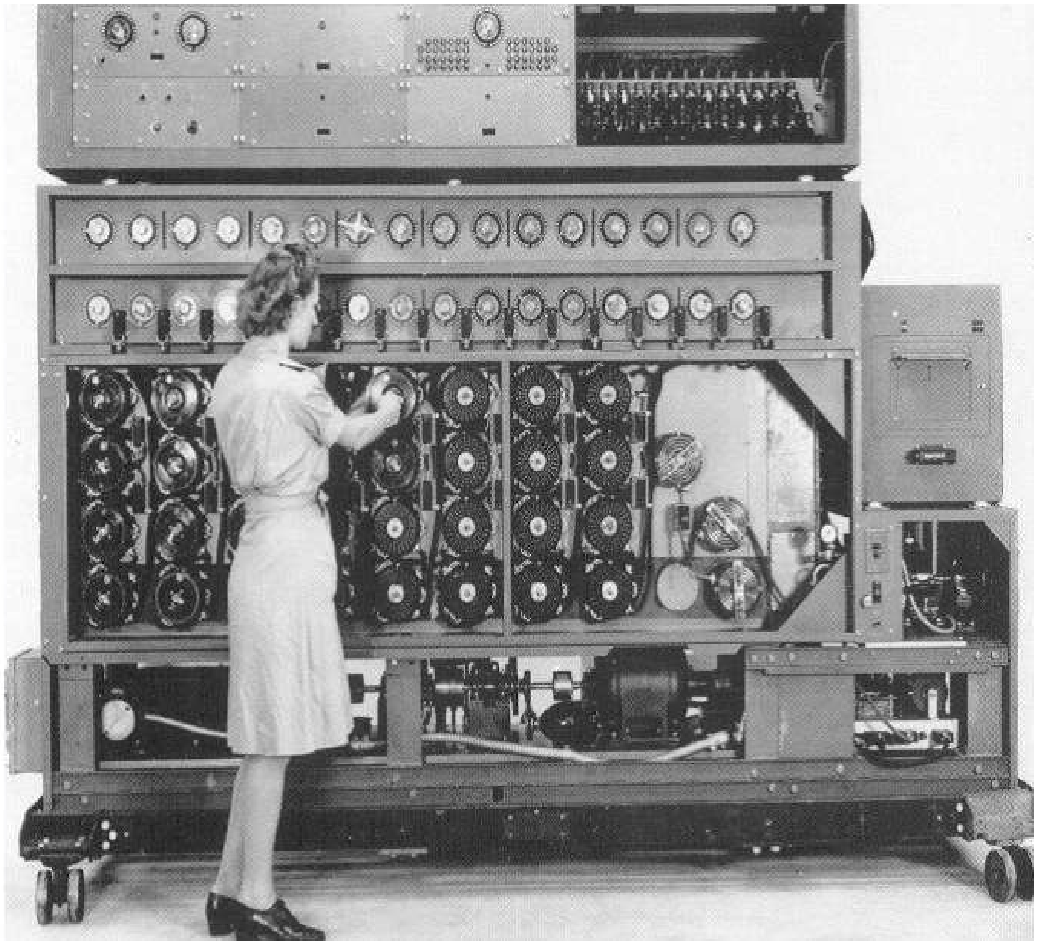
Managing Director, Lily Innovation

The Post-Quantum Cryptography Problem

3 ***Large-scale*** 2 ***quantum computers*** would pose 4 ***a serious threat*** to the security of 1 ***public key cryptography***

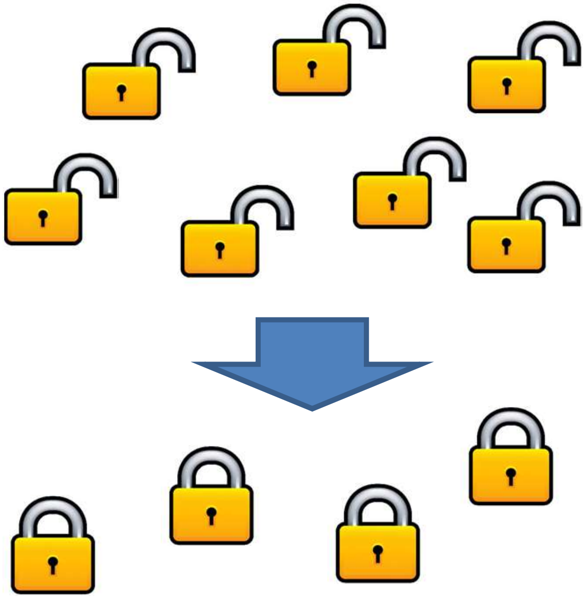
So 6 ***what should affected entities do***, and 5 ***when***?

Symmetric Cryptography



Public Key Cryptography

- Uses public and private keys for each communication, avoiding need for key exchange
- Based on problems that are "hard" in one direction (*eg* knapsack problem or integer factorisation)
- Used for Smart Ledger digital signature



Technique	Sender Uses	Recipient Uses	Why It Works
Public key secure communication	Recipient's public key	Recipient's private key	Only recipient (using her private key) can read messages encrypted with her public key
Public key digital signature	Sender's private key	Sender's public key	Only sender can sign with her private key, and recipient can use the sender's public key to confirm signature

The Post-Quantum Cryptography Problem

③ ***Large-scale*** ② ***quantum computers***

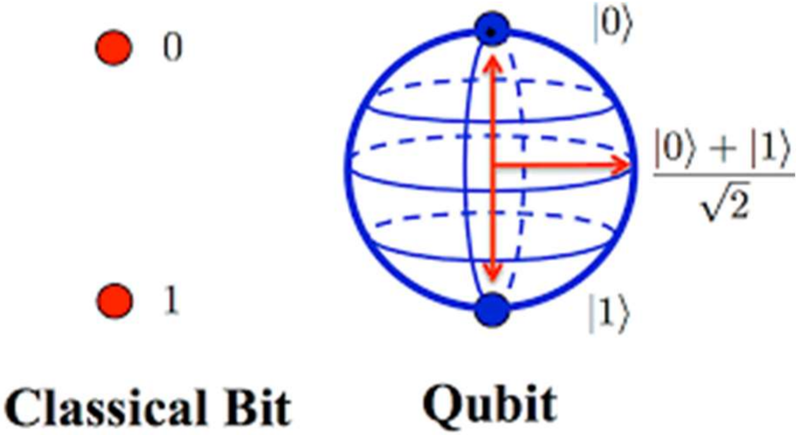
would pose ④ ***a serious threat*** to the

security of ① ***public key cryptography***

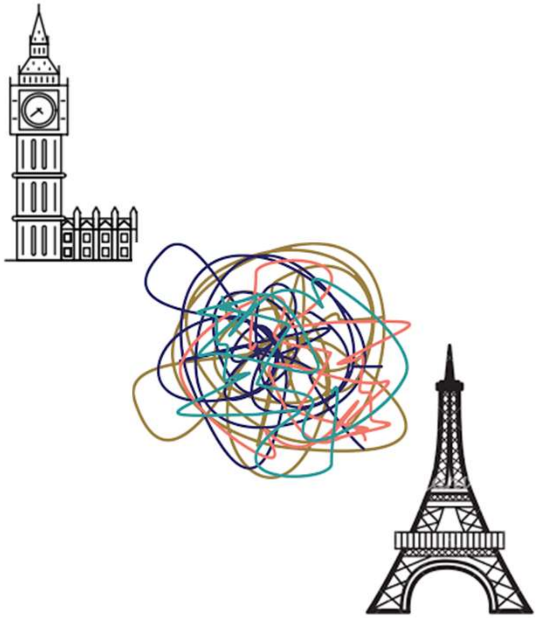
So ⑥ ***what should affected entities do***,

and ⑤ ***when***?

Quantum Phenomena



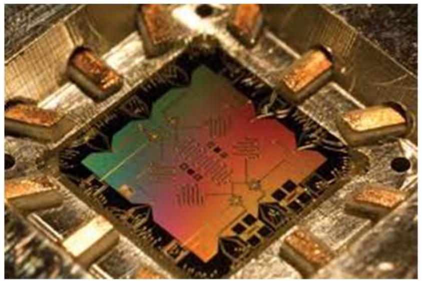
Superposition

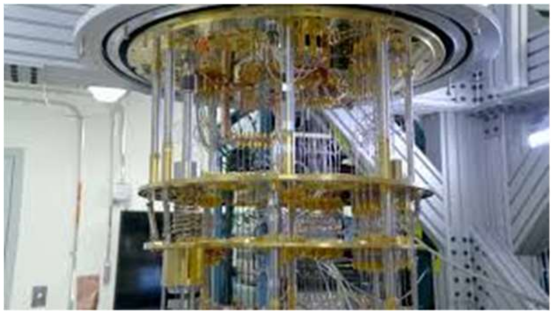


Entanglement

Quantum Computers

- Proposed by Richard Feynman in 1981
- Progress with entangled qubits
  - 1998 – 2
  - 2011 – 14
  - 2017/2018 – 17 (IBM, Intel), 50 (IBM), 49 (Intel, Google)
- Physical qubits (the numbers above)
  - Low-temperature devices showing quantum effects
  - Decoherence – currently after ~ 90 microseconds
- Logical qubits (do not exist yet)
  - Stable computing devices
  - 10,000+ physical qubits required for one logical qubit
  - 3000-5000 logical qubits required to attack current public key cryptography





The Post-Quantum Cryptography Problem

3 ***Large-scale*** 2 ***quantum computers*** would pose 4 ***a serious threat*** to the security of 1 ***public key cryptography***

So 6 ***what should affected entities do***, and 5 ***when***?

The Quantum Threat

- The new math!
- Shor’s algorithm
  - Discovered in 1994 at Bell Laboratories
  - Would allow a sufficiently powerful quantum computer to solve quickly the hard problems underlying the most common public key cryptography algorithms (including RSA, ECDSA, Diffie-Hellman)
    - RSA is commonly used for securing web connections
    - ECDSA is standard algorithm for blockchain signatures
    - “Sufficiently powerful” means about 3000-5000 logical qubits for RSA-2048
  - Prompted increased interest in quantum computers
- Grover’s algorithm
  - Discovered in 1996 at Bell Laboratories
  - Provides quadratic speed-up for attacking symmetric cryptography and hash algorithms
  - Hash algorithms (particularly SHA-256) are key for blockchain
- But there are good alternatives that avoid these threats

The Post-Quantum Cryptography Problem

③***Large-scale*** ②***quantum computers***

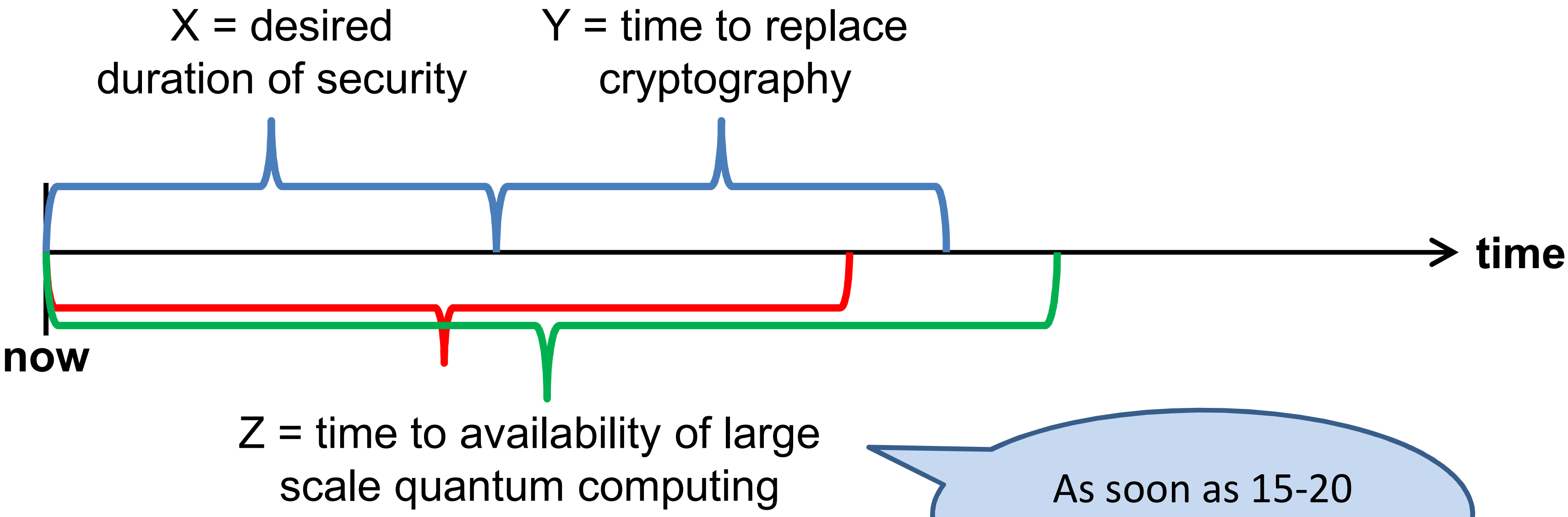
would pose ④***a serious threat*** to the

security of ①***public key cryptography***

So ⑥***what should affected entities do***,

and ⑤***when***?

The Mosca Inequality


X = desired duration of security
Y = time to replace cryptography
time
now
Z = time to availability of large scale quantum computing

As soon as 15-20 years?

- For each system:
  - If X + Y < Z, there is time to act
  - If X + Y > Z, it may already be too late to entirely avoid the post-quantum cryptography problem
- Some systems may fall into the second category – particular issue for blockchain / Smart Ledgers, where X is very large

DISTRIBUTED FUTURES

The Post-Quantum Cryptography Problem

3 ***Large-scale*** 2 ***quantum computers***

would pose 4 ***a serious threat*** to the

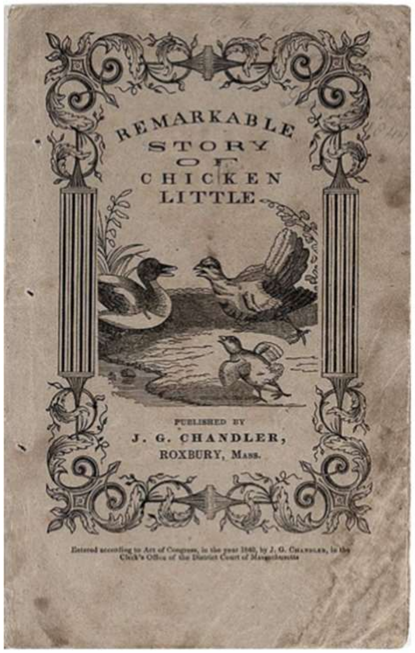
security of 1 ***public key cryptography***

So 6 ***what should affected entities do***,

and 5 ***when***?

Don’t Panic

- Is this like the Y2K problem? – no certain deadline
- Maybe more like climate change? – uncertainty as to timing and impacts



REMARKABLE
STORY
OF
CHICKEN
LITTLE.

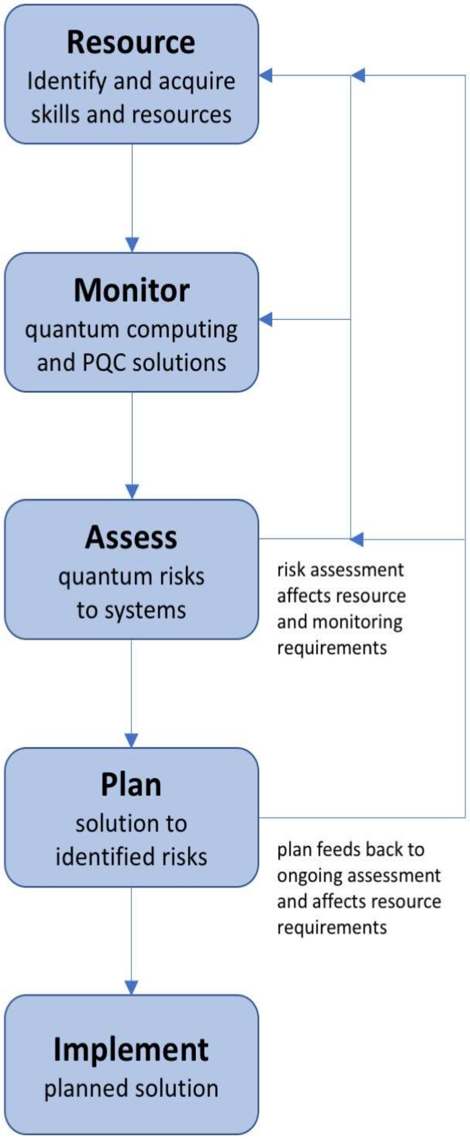
PUBLISHED BY
J. G. CHANDLER,
ROXBURY, Mass.

Entered according to Act of Congress, in the year 1840, by J. G. Chandler, in the Clerk's Office of the District Court of Massachusetts

Good Solutions Exist or Are Coming

- EU PQCRYPTO recommendations (2015)
- US National Institute of Standards and Technology competition (2016 - around 2022)
- Promising families of quantum-resistant algorithms
  - Lattice
  - Signature-based
  - Code-based
  - Multivariate
  - Supersingular elliptic curve isogeny

A Programme of Action



Resource
Identify and acquire skills and resources

Monitor
quantum computing and PQC solutions

Assess
quantum risks to systems

risk assessment affects resource and monitoring requirements

Plan
solution to identified risks

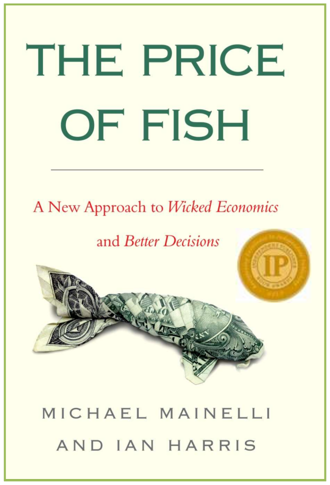
plan feeds back to ongoing assessment and affects resource requirements

Implement
planned solution

- ♦ An obvious conclusion?
  - ➢ New systems should be quantum resistant from the start, to avoid risks (and costs of re-engineering)
  - ➢ But many Smart Ledgers and other new systems are not taking this approach, including because most familiar / off-the-shelf components are not quantum-resistant

When Would We Know Our Commerce Is Working?

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



THE PRICE OF FISH

A New Approach to *Wicked Economics* and *Better Decisions*

MICHAEL MAINELLI AND IAN HARRIS

Thank you!