The Quantum Countdown

Quantum Computing And The Future Of Smart Ledger Encryption

Long Finance Webinar

Wednesday, 01 August 2018, 15:00 to 15:30 BST

(presentation starts at 15:02)

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

@longfinance

Sponsored By

CARDANO FOUNDATION

Agenda

15:02 – 15:05 Introduction

15:05 – 15:25 Presentation

15:25 – 15:30 Concluding Remarks

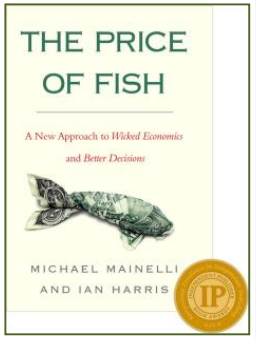
Introduction

James Pitcher
Programme Director
Z/Yen Group

james_pitcher@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

Distributed Futures Programme

An open source research programme for Smart Ledgers and new technologies.

Our research is structured around four themes:

- Society
- Technology
- Economics
- Politics

And is directed at four outcomes:

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

www.distributedfutures.net

Presentation

Maury Shenk

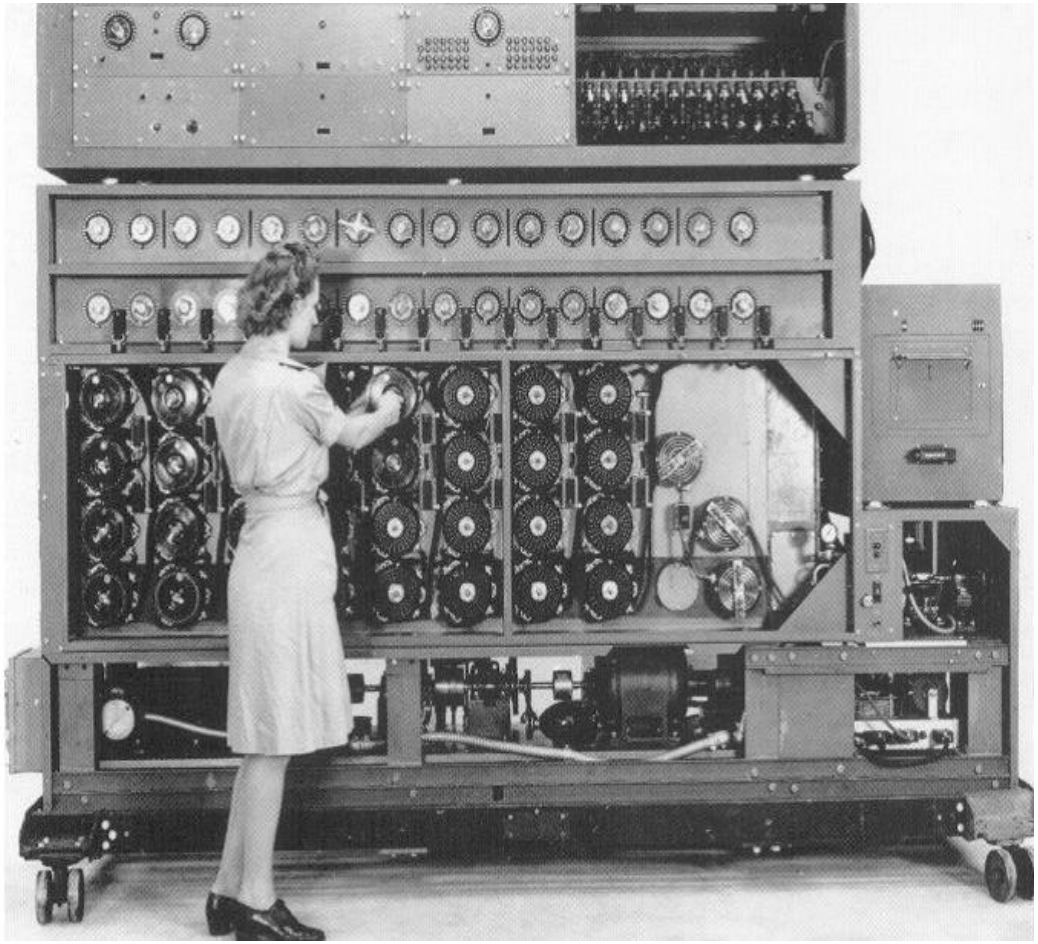
Maury Shenk
Managing Director
Lily Innovation

The Post-Quantum Cryptography Problem

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

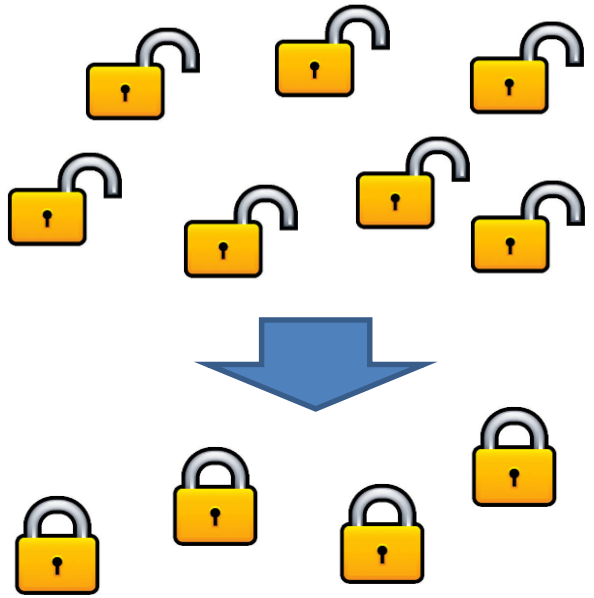
So ***what should affected entities do***, and ***when***?

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



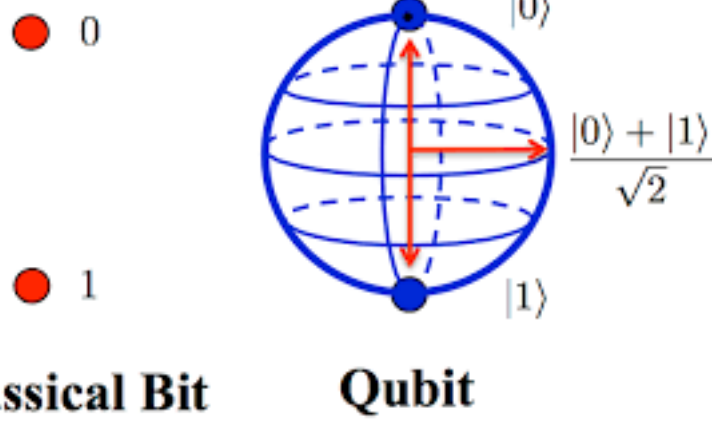
Technique	Sender Uses	Recipient Uses	Why It Works
Public key secure communication	Recipient’s public key	Recipient’s private key	Only recipient (using her private key) can read messages encrypted with her public key
Public key digital signature	Sender’s private key	Sender’s public key	Only sender can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

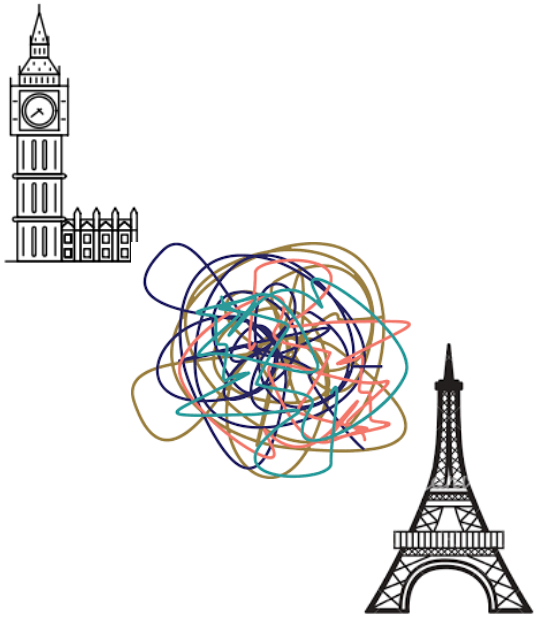
The Post-Quantum Cryptography Problem

3 2
Large-scale 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



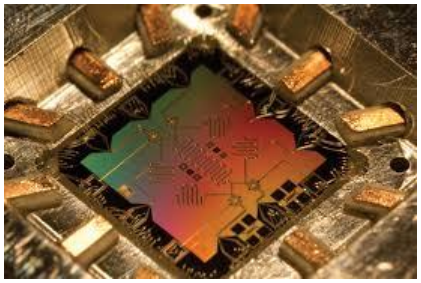


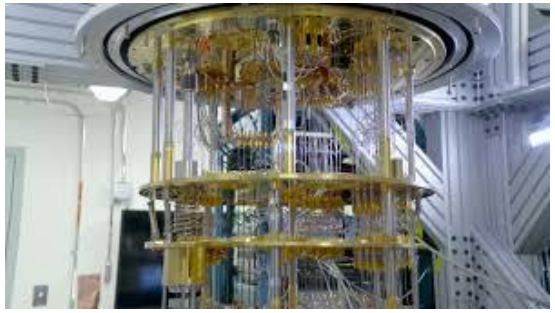
Superposition

Entanglement

Quantum Computers

- Proposed by Richard Feynman in 1981
- Progress with entangled qubits
  - 1998 – 2
  - 2011 – 14
  - 2018 – 72 (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 2
Large-scale 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

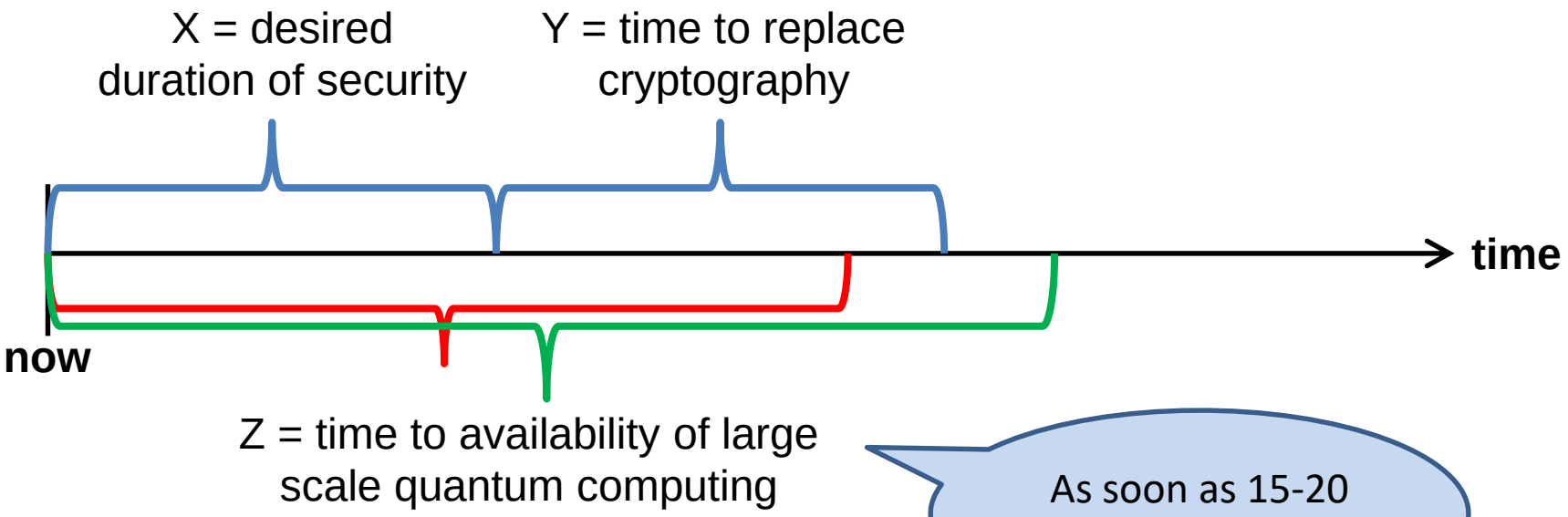
- The new math!
- Shor's algorithm
  - Discovered in 1994 at Bell Laboratories
  - Would allow a sufficiently powerful quantum computer to solve quickly the hard problems underlying the most common public key cryptography algorithms (including RSA, ECDSA, Diffie-Hellman)
    - RSA is commonly used for 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 2
Large-scale 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



- 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

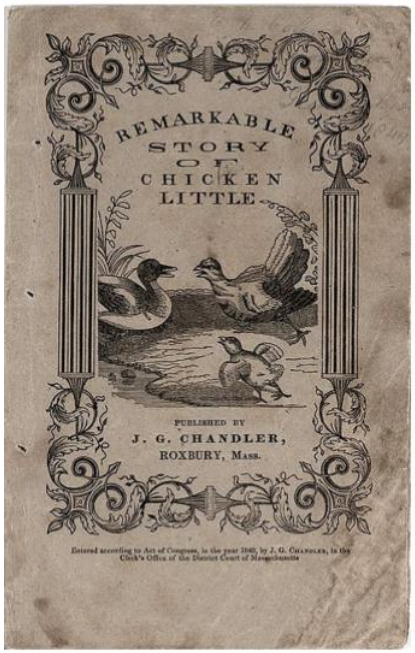
The Post-Quantum Cryptography Problem

3 2
Large-scale 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

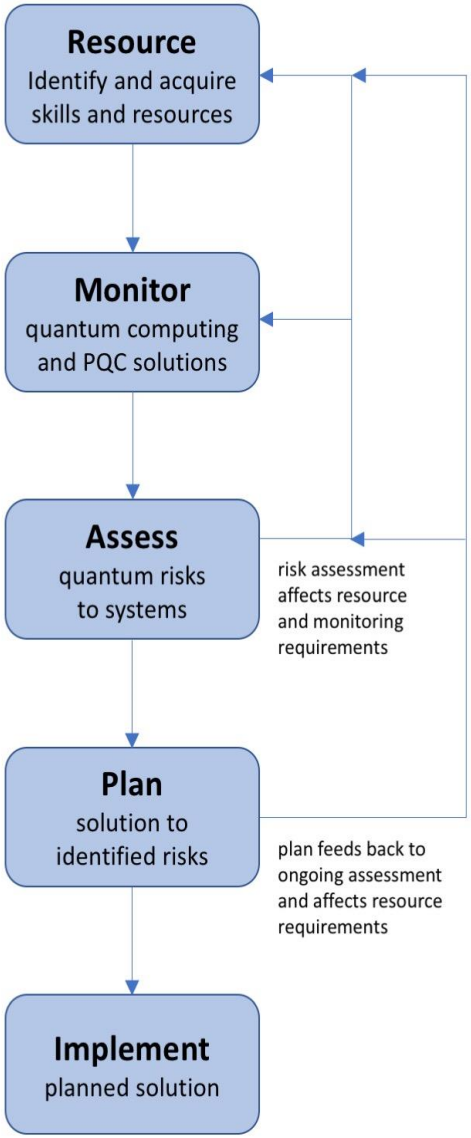
- Is this like the Y2K problem? – no certain deadline
- Maybe more like climate change? – uncertainty as to timing and impacts



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



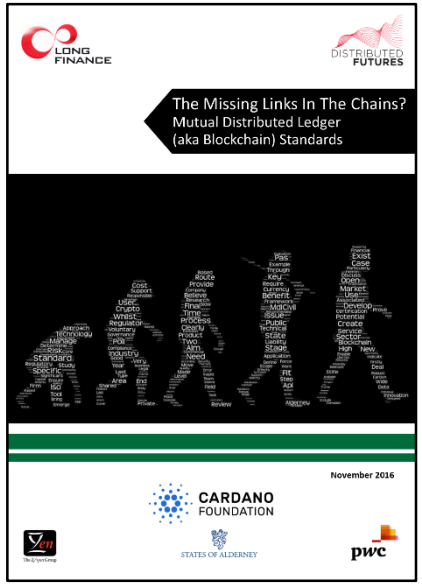
- An obvious conclusion?
  - New systems should be quantum resistant from the start, to avoid risks (and costs of re-engineering)
  - But many Smart Ledgers and other new systems are not taking this approach, including because most familiar / off-the-shelf components are not quantum-resistant

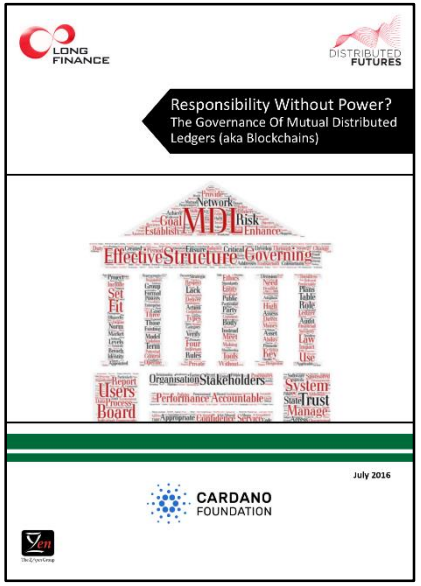
Concluding Remarks

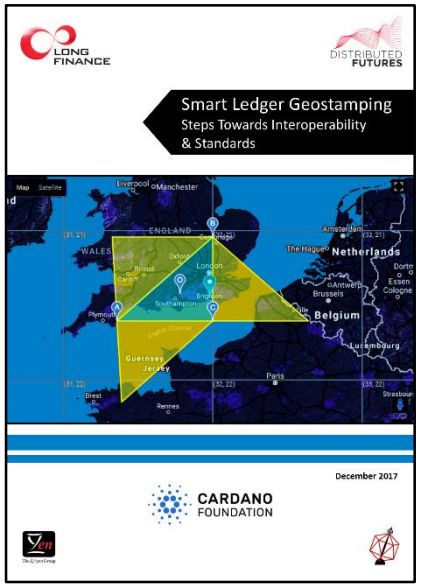
James Pitcher
Programme Director
Z/Yen Group

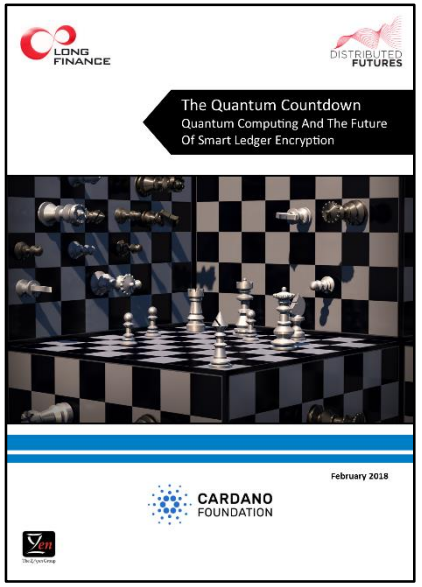
james_pitcher@zyen.com

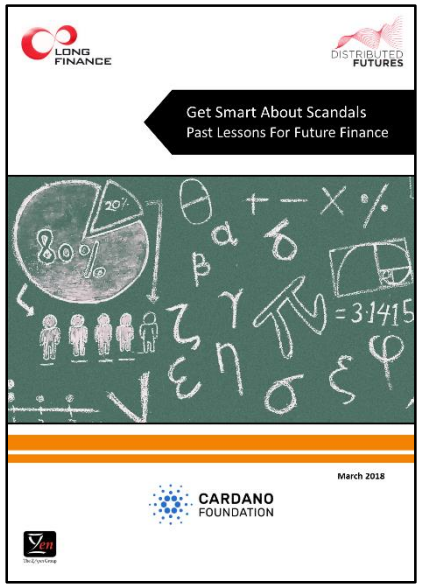
Distributed Futures Research

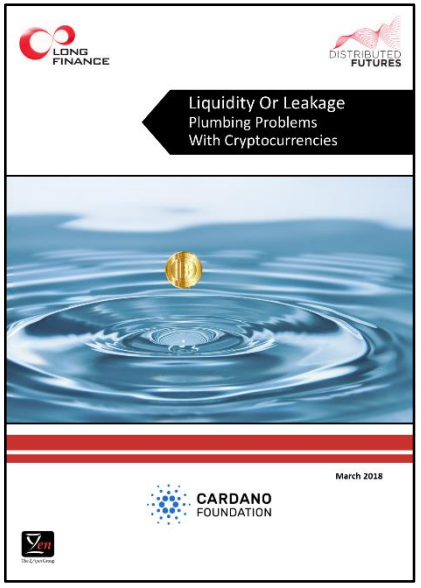


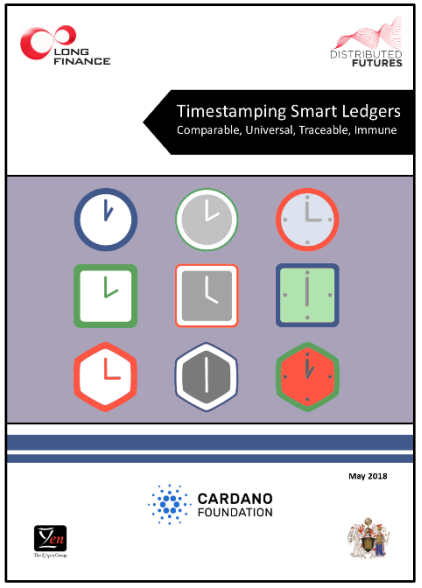




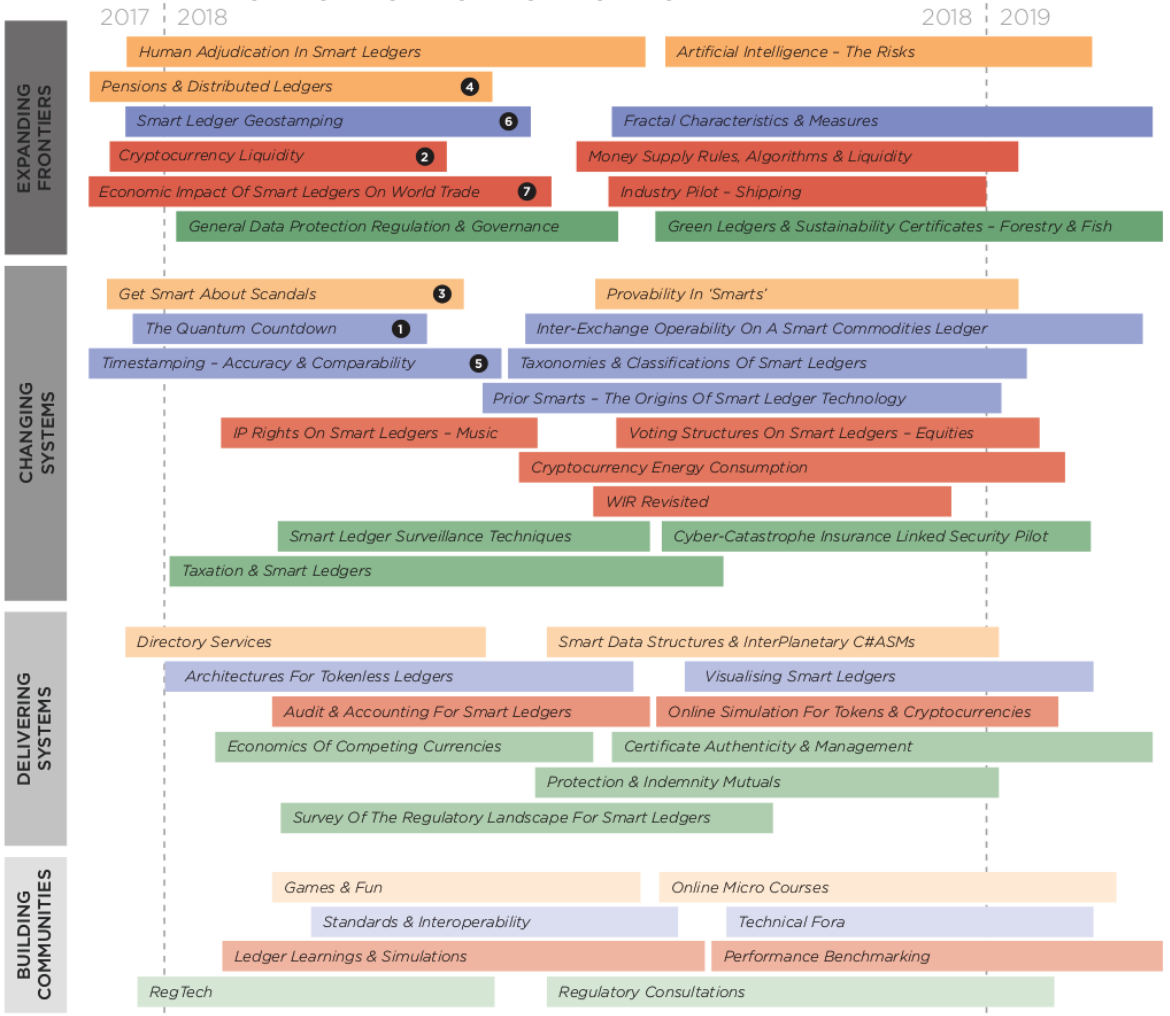








Timeline


2017
2018
2018
2019
EXPANDING FRONTIERS
CHANGING SYSTEMS
DELIVERING SYSTEMS
BUILDING COMMUNITIES
Human Adjudication In Smart Ledgers
Artificial Intelligence – The Risks
Pensions & Distributed Ledgers 4
Smart Ledger Geostamping 6
Fractal Characteristics & Measures
Cryptocurrency Liquidity 2
Money Supply Rules, Algorithms & Liquidity
Economic Impact Of Smart Ledgers On World Trade 7
Industry Pilot – Shipping
General Data Protection Regulation & Governance
Green Ledgers & Sustainability Certificates – Forestry & Fish
Get Smart About Scandals 3
Provability In 'Smarts'
The Quantum Countdown 1
Inter-Exchange Operability On A Smart Commodities Ledger
Timestamping – Accuracy & Comparability 5
Taxonomies & Classifications Of Smart Ledgers
Prior Smarts – The Origins Of Smart Ledger Technology
IP Rights On Smart Ledgers – Music
Voting Structures On Smart Ledgers – Equities
Cryptocurrency Energy Consumption
WIR Revisited
Smart Ledger Surveillance Techniques
Cyber-Catastrophe Insurance Linked Security Pilot
Taxation & Smart Ledgers
Directory Services
Smart Data Structures & InterPlanetary C#ASMs
Architectures For Tokenless Ledgers
Visualising Smart Ledgers
Audit & Accounting For Smart Ledgers
Online Simulation For Tokens & Cryptocurrencies
Economics Of Competing Currencies
Certificate Authenticity & Management
Protection & Indemnity Mutuals
Survey Of The Regulatory Landscape For Smart Ledgers
Games & Fun
Online Micro Courses
Standards & Interoperability
Technical Fora
Ledger Learnings & Simulations
Performance Benchmarking
RegTech
Regulatory Consultations

Next Steps

- Distributed Futures – www.distributedfutures.net
- Cardano Foundation - https://cardanofoundation.org/
- Long Finance - www.longfinance.net

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

Thank you!