FS Club

LONG FINANCE

The Quantum Threat (& Opportunity) To Financial Services

Thursday, 18 July 2019

85 Gresham Street,

City Of London

The Financial Services Club

Wi-Fi Username: Meeting Room Wifi
Password: Londonguestwifi

@FSClub

@ZYenResearch

A Word From Our Chair

Michael Mainelli
Co-Chairman
FS Club

Event Sponsors:

FS Club

LONG FINANCE

The Financial Services Club

Established 2004

Networking, debates and speakers you don't usually meet elsewhere

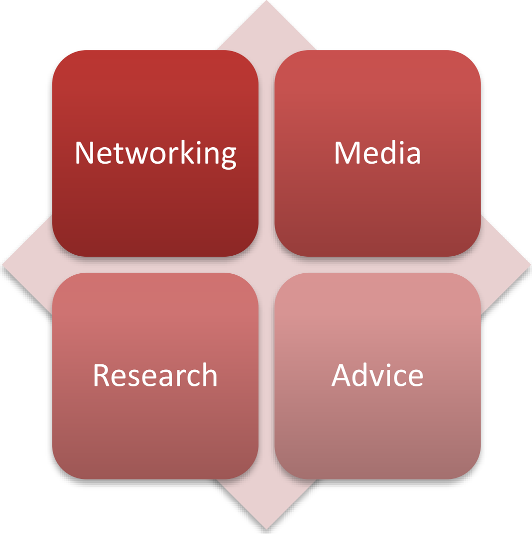
Chatham House Rule

www.thefinanser.com
www.fsclub.net

What FS Club & Long Finance Do

Financial Services Club Meetings
Sponsored Events
Breakfast, Lunch
and Dinner
Roundtables

Daily Newsletter
Daily Blog
Social Media
White Papers
Speaking



Primary Research
Secondary Research
Quantitative and Qualitative

Workshops
Strategic Planning
Market and Business Development

Events…

FS Club
Smart Centres Index:
The Environment For The
Development Of New Technology

Gresham's Law

Z/Yen Group

Data Foundations

Integrity Innovation Partnership Excellence
International listing & trading venues of choice
Capital Markets Innovations:
Institutional Trading Liquidity
Dr Robert Barnes, Chartered FCSI
Global Head of Primary Markets & CEO Turquoise

News, Bulletins, Blog…

FS Club

LONG FINANCE

Financial Services Club The number ONE networking group for senior executives in financial services.

<

Corporate Actions: The Case Of The Missing Billions

Sander Eijkenduijn, CFO Scorpeo LLC
Andy Agathangelou, Founder, Transparency Task Force

Wednesday, 04 September 2019 18:00

Launch Of Global Financial Centres Index 26, Seoul

Monday, 09 September 2019

>

5355
Readership

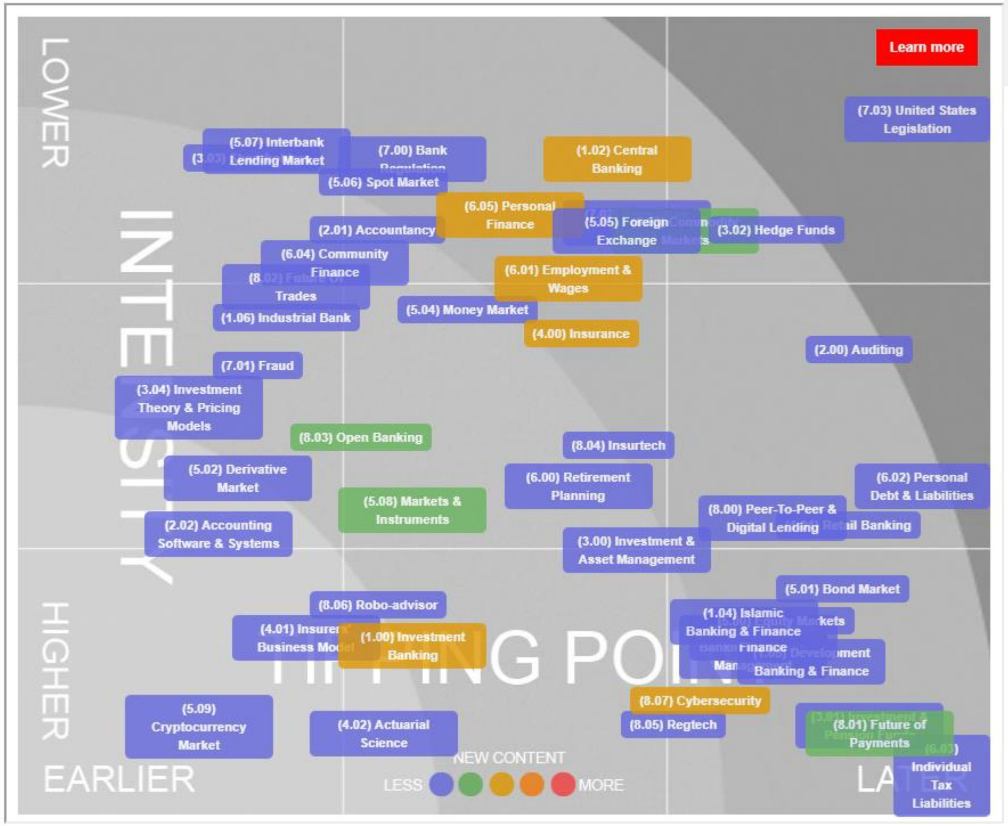
261
Events held

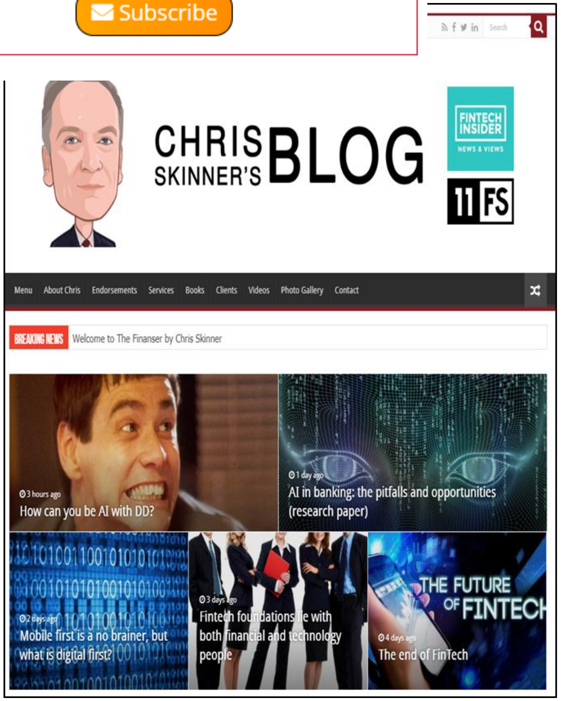
Become a member

Get the FREE daily breaking news, blog, events and features via email

Subscribe

Financial Services Club Perspectives





Welcome to The Finanser by Chris Skinner

3 hours ago
How can you be AI with DD?

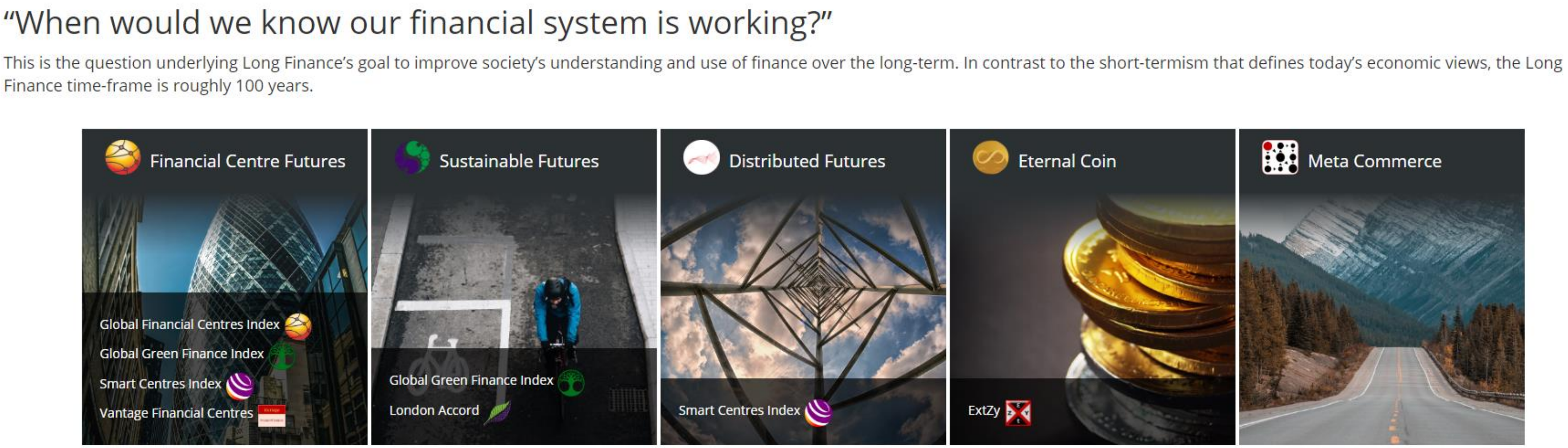
1 day ago
AI in banking: the pitfalls and opportunities (research paper)

2 days ago
Mobile first is a no brainer, but what is digital first?

3 days ago
Fintech foundations lie with both financial and technology people

4 days ago
The end of FinTech

What Long Finance Does



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

This is the question underlying Long Finance's goal to improve society's understanding and use of finance over the long-term. In contrast to the short-termism that defines today's economic views, the Long Finance time-frame is roughly 100 years.

Financial Centre Futures

- Global Financial Centres Index
- Global Green Finance Index
- Smart Centres Index
- Vantage Financial Centres

Sustainable Futures

- Global Green Finance Index
- London Accord

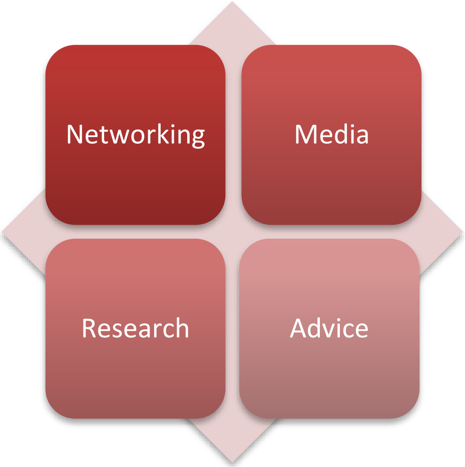
Distributed Futures

- Smart Centres Index

Eternal Coin

- ExtZy

Meta Commerce



Networking

Media

Research

Advice

FS Club

Recent Research

LONG FINANCE

The Global Green Finance Index 3

March 2019

MAVA

The Global Financial Centres Index 25

MARCH 2019

Financial Centre Futures

LONG FINANCE

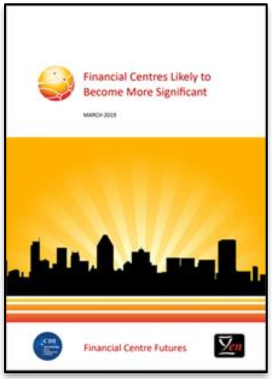
DISTRIBUTED FUTURES

To Be, To Have, To Know

Smart Ledgers & Identity Authentication

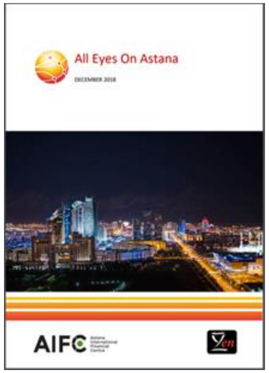
February 2019

CARDANO FOUNDATION


Financial Centres Likely to Become More Significant

MARCH 2019

Financial Centre Futures


All Eyes On Astana

DECEMBER 2018

AIFC

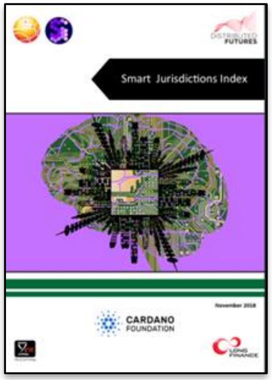
LONG FINANCE

DISTRIBUTED FUTURES

Information Rules: Smart Ledger Architectures & Distributed Permissions

November 2018

CARDANO FOUNDATION


DISTRIBUTED FUTURES

Smart Jurisdictions Index

November 2018

CARDANO FOUNDATION

LONG FINANCE

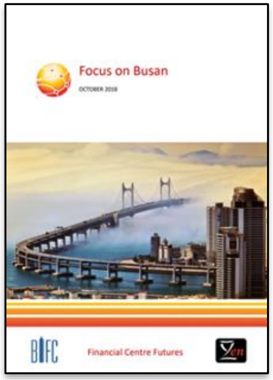
LONG FINANCE

DISTRIBUTED FUTURES

Cyber-Catastrophe Insurance-Linked Securities On Smart Ledgers

November 2018

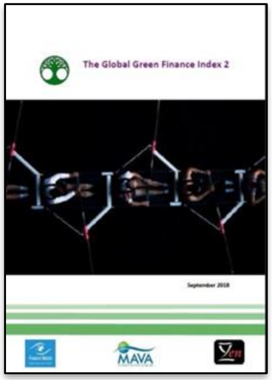
CARDANO FOUNDATION


Focus on Busan

OCTOBER 2018

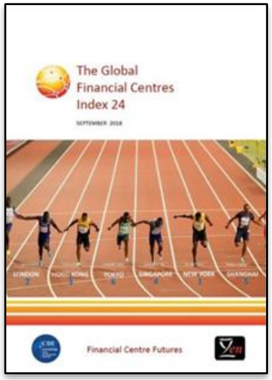
BIFC

Financial Centre Futures


The Global Green Finance Index 2

September 2018

MAVA


The Global Financial Centres Index 24

SEPTEMBER 2018

Financial Centre Futures

China's Financial Center Index (CDI CFCI 10)

Shenzhen, China

2018 September

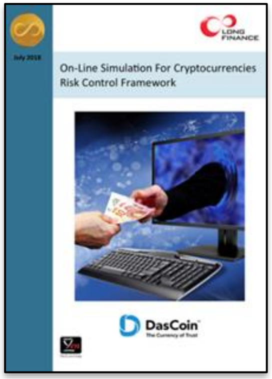
LONG FINANCE

DISTRIBUTED FUTURES

Smart Ledgers & Collective Defined Contribution Pensions

July 2018

CARDANO FOUNDATION

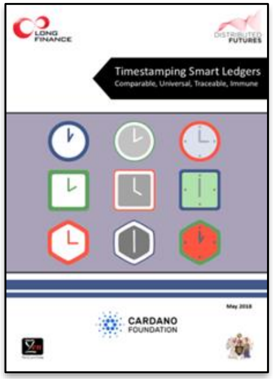

July 2018

LONG FINANCE

On-Line Simulation For Cryptocurrencies Risk Control Framework

DasCoin

The Currency of Trust


LONG FINANCE

DISTRIBUTED FUTURES

Timestamping Smart Ledgers

Comparable, Universal, Traceable, Immune

May 2018

CARDANO FOUNDATION

LONG FINANCE

DISTRIBUTED FUTURES

The Economic Impact Of Smart Ledgers On World Trade

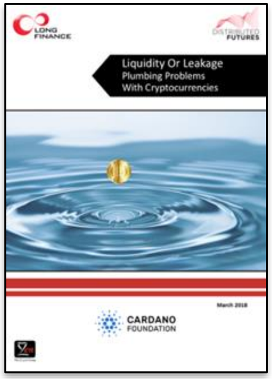
April 2018

CARDANO FOUNDATION

The Global Financial Centres Index 23

MARCH 2018

Financial Centre Futures


LONG FINANCE

DISTRIBUTED FUTURES

Liquidity Or Leakage

Plumbing Problems With Cryptocurrencies

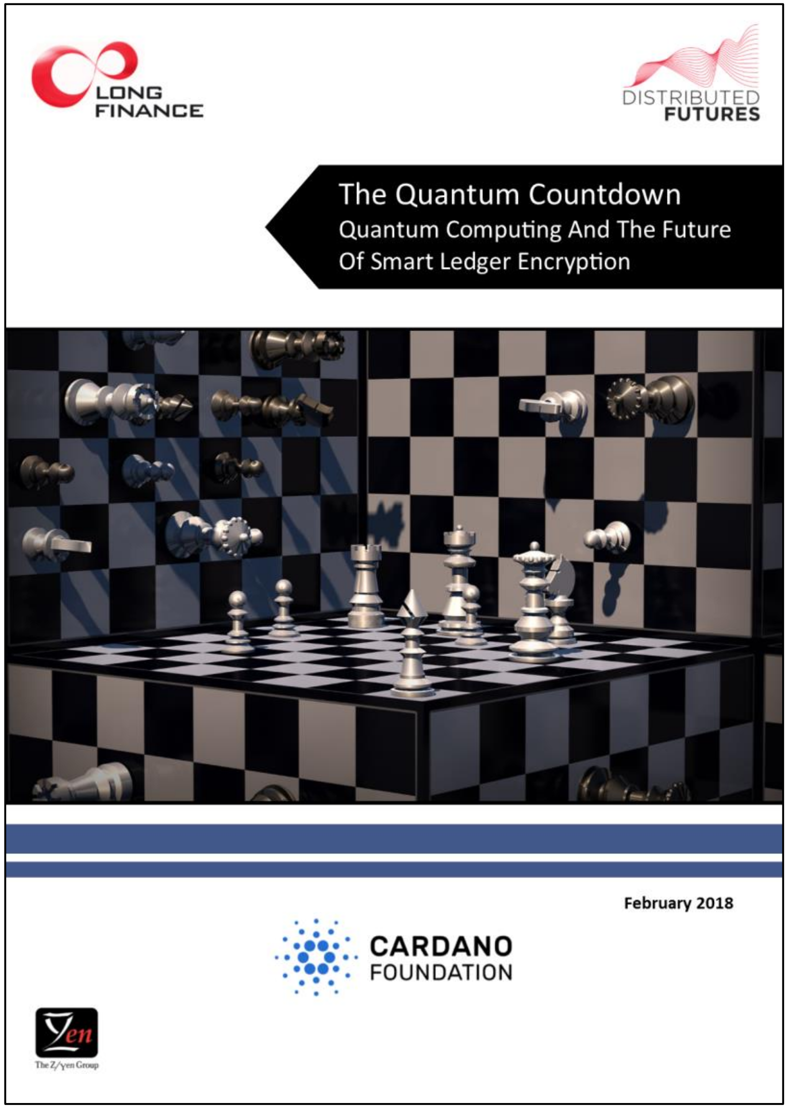
March 2018

CARDANO FOUNDATION

FS Club

Our 2018 Report

LONG FINANCE



LONG FINANCE

DISTRIBUTED FUTURES

The Quantum Countdown

Quantum Computing And The Future Of Smart Ledger Encryption

February 2018

CARDANO FOUNDATION

Zen
The Z/Yen Group

Read The Report Here: https://www.zyen.com/media/documents/Quantum_Countdown.pdf

The Quantum Threat…

Maury Shenk
Managing Director
Lily Innovation

@FSClub

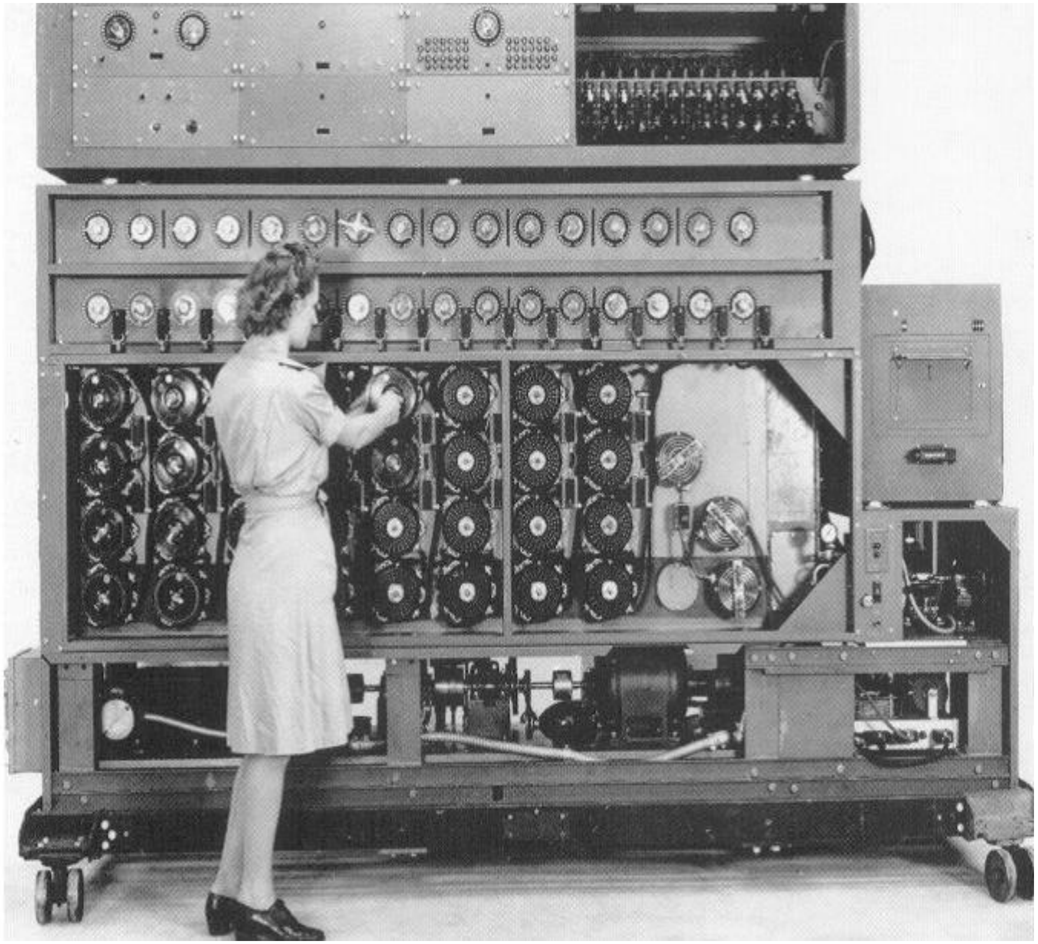
@ZYenResearch

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***

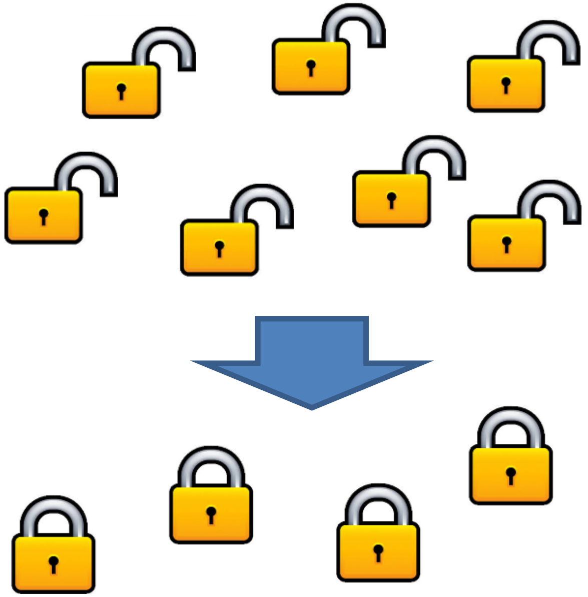
So [6] ***what should affected entities do***, and [5] ***when***?

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)
- Secures many aspects of electronic communications and authentication



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***

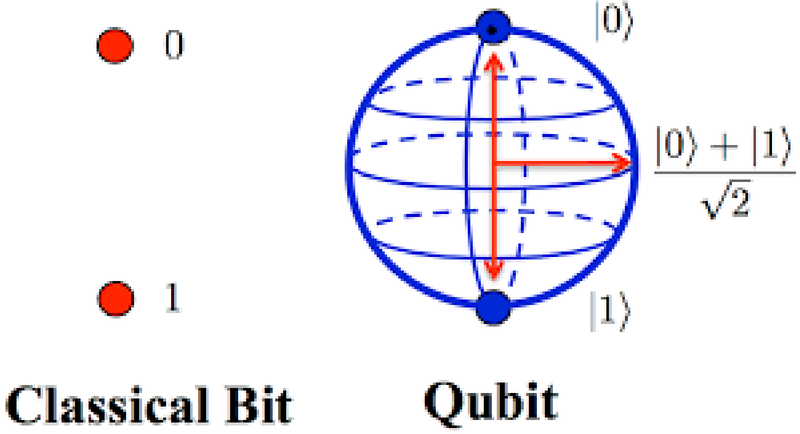
would pose ④ ***a serious threat*** to the

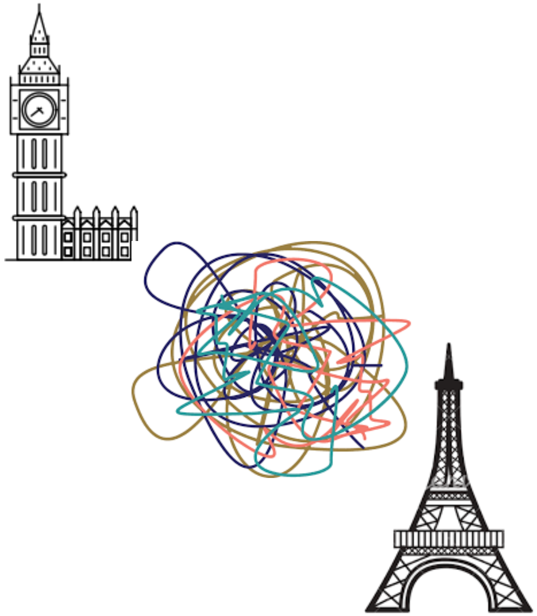
security of ① ***public key cryptography***

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

and ⑤ ***when***?

Quantum Phenomena



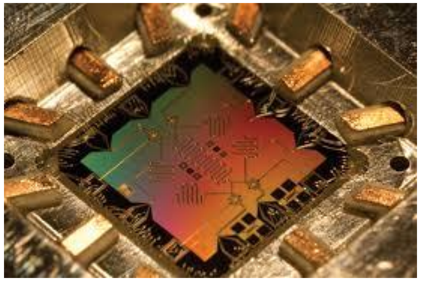


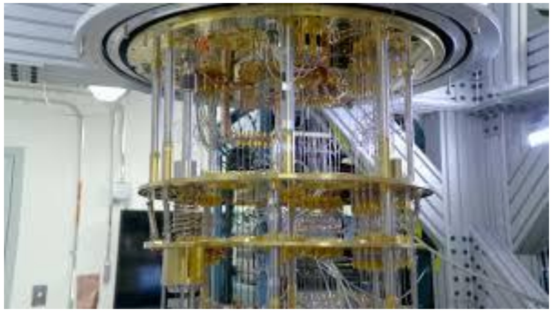
Superposition

Entanglement

Quantum Computers

- Proposed by Richard Feynman in 1981
- Progress with entangled qubits
  - 1998 – 2 (Oxford)
  - 2011 – 14 (academics in Austria and Canada)
  - 2018 – 72 (Google)
- Physical qubits (the numbers above)
  - Low-temperature devices showing quantum effects
  - Decoherence – ~100 microseconds for operational quantum computers
- Logical qubits (do not exist yet)
  - Stable computing devices
  - ~1000 - 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

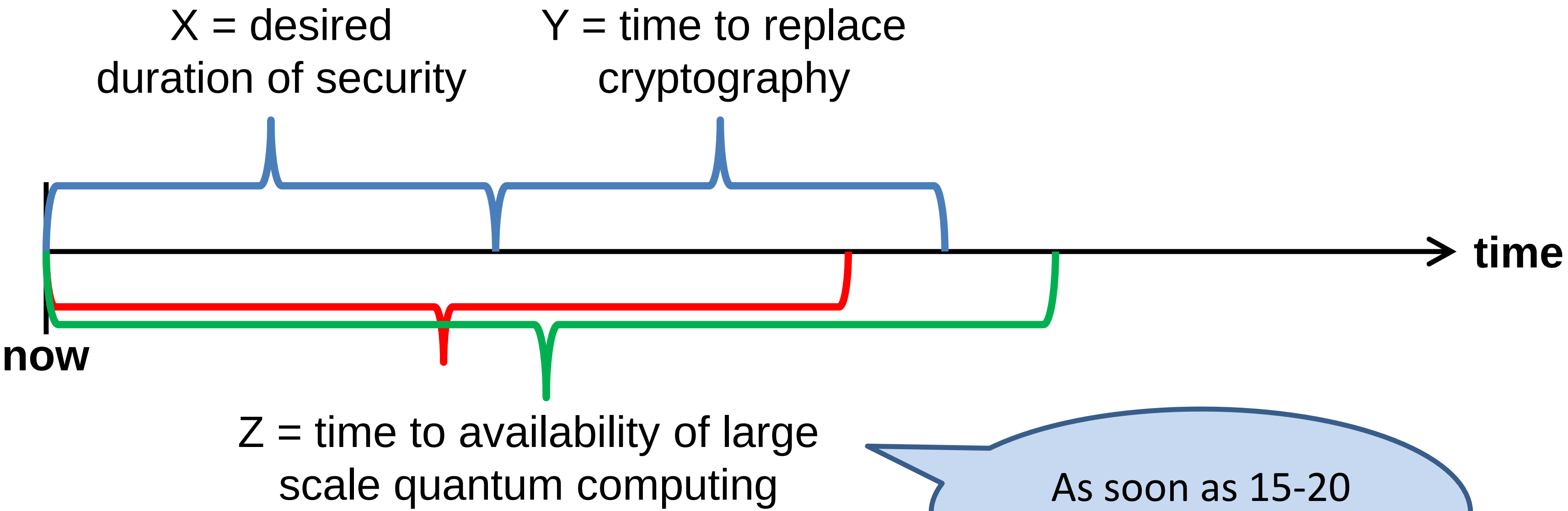
- The new math!
- Shor's algorithm
  - Discovered in 1994 at Bell Laboratories
  - Would allow a sufficiently powerful quantum computer to solve quickly the hard problems underlying the most common public key cryptography algorithms (including RSA, ECDSA, Diffie-Hellman)
    - RSA is commonly used for 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 (used for authentication, including on blockchains)
- 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, especially where X is very large – e.g. blockchain / Smart Ledgers, life insurance, bonds

The Post-Quantum Cryptography Problem

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

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

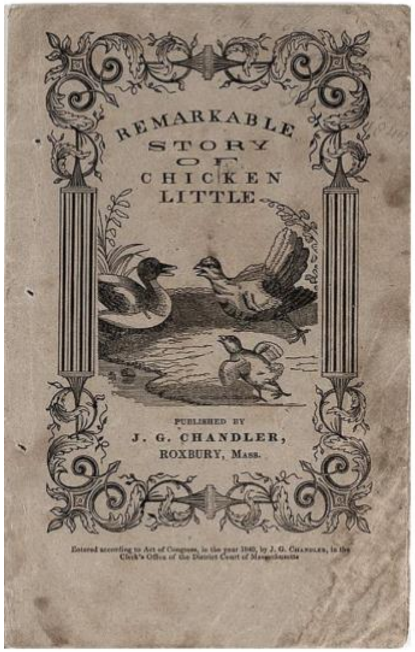
security of [1] ***public key cryptography***

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

and [5] ***when***?

Don’t Panic

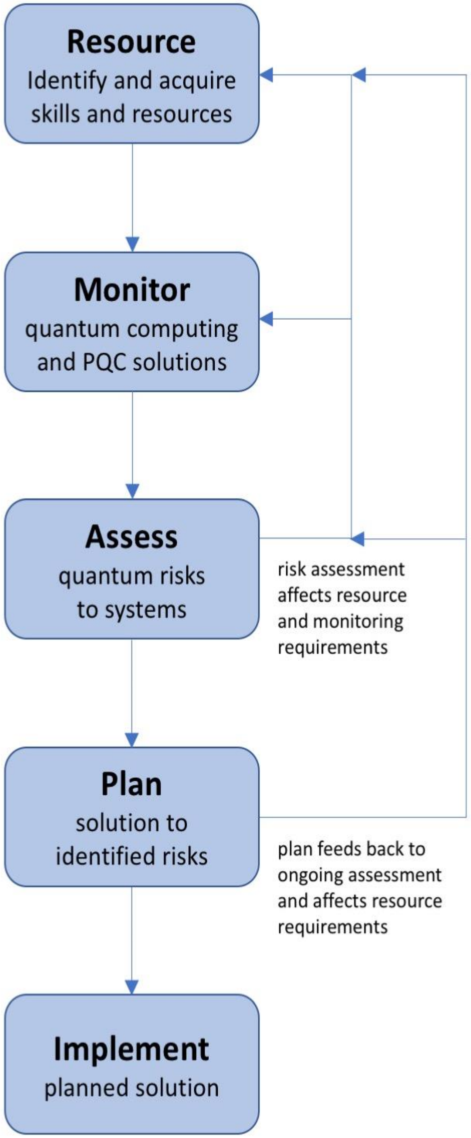
- Is this like the Y2K problem? – but no certain deadline
- Maybe more like climate change? – uncertainty as to timing and impacts



Good Solutions Exist or Are Coming

- EU PQCRYPTO recommendations (2015)
- US National Institute of Standards and Technology competition (launched 2016)
  - 69 Round 1 submissions in early 2018
  - Round 2 candidates announced Feb. 2019 – 17 public key confidentiality algorithms and 9 digital signature algorithms
  - Originally expected to conclude 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 new systems are not taking this approach, including because most familiar / off-the-shelf components are not quantum-resistant

The Quantum Threat…

Panel Discussion

Maury Shenk
Managing Director
Lily Innovation

Michael Mainelli
Co-Chairman
FS Club

Henry Price
Imperial College
London

Questions, Comments & Answers(?)

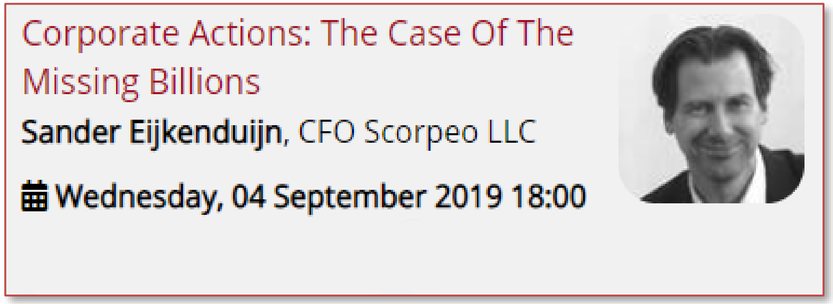
FS Club

LONG FINANCE

Forthcoming Events...

Building Robust Investment Strategies

Andrew Craig, Founder, Plain English Finance
Roderick Collins, Director, Solent Systematic Investment Strategies
Wednesday, 14 August 2019 12:00



Corporate Actions: The Case Of The Missing Billions

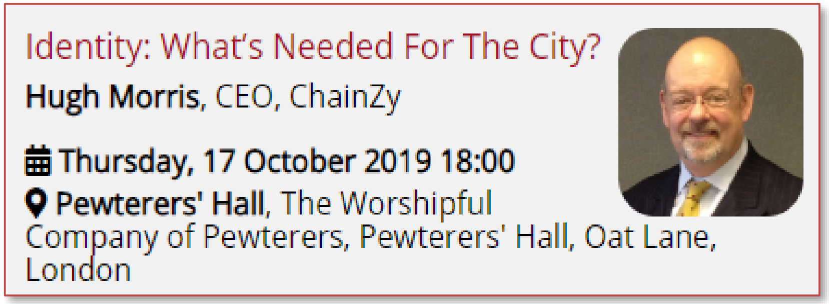
Sander Eijkenduijn, CFO Scorpeo LLC

📅 **Wednesday, 04 September 2019 18:00**

Central Bank Independence & The Future Of The Euro

Professor Panicos Demetriades

📅 **Thursday, 03 October 2019 18:00**
📍 **Pewterers' Hall**, The Worshipful Company of Pewterers, Pewterers' Hall, Oat Lane, London



Identity: What's Needed For The City?

Hugh Morris, CEO, ChainZy

📅 **Thursday, 17 October 2019 18:00**
📍 **Pewterers' Hall**, The Worshipful Company of Pewterers, Pewterers' Hall, Oat Lane, London

FS Club

LONG FINANCE

Thank You!

BT

Invest Northern Ireland

@FSClub

@ZYenResearch