

Disclaimer: please note that the following represents the personal views of the speaker and is not the official position of equensWorldline or its subsidiaries or of its clients and partners

## Making Tea on the Blockchain

FS Club

© equensWorldline - For internal use

**equensWorldline**

### Michael Salmony

#### Personal Background

- ▶ Computer Science  
PhD in Computer + Networks = New Media
- ▶ International Business  
Transformation of Industries through Technology
- ▶ Banking  
New Services / New Processes
- ▶ Payments  
Innovations, Regulation, Digital Strategy



2

**equensWorldline**

### 1st Multi-Media Internet Application?



The Cambridge Coffee Pot  
160.000 hits per year

3

**equensWorldline**

### BoE's Haldane suggests ditching cash for cryptocurrency

18 September 2015 | 5719 views | 1



The Bank of England's chief economist has floated the prospect of abolishing paper cash and replacing it with a state-backed digital currency as a way of facilitating negative interest rates.

4

**equensWorldline**

### How Blockchain Could Help Kanye Use Facebook To Get Out Of Debt - And Solve Facebook's Video Problem

He has spent a year working out how blockchain – the technology on which the cryptocurrency Bitcoin is based – can be used to solve humanity's biggest problems, from crime and corruption to deforestation and over-fishing.



Making the following Billion dollar companies obsolete

the blockchain will help you verify if the robot is telling you the truth or not.

The Blockchain Would Have Saved Lehman Brothers  
Forbes / Opinion

MundoBitcoin @MundoBitcoin  
It's happening. #Bitcoin offers refugees blockchain IDs and bitcoin debit cards (bt.uk/A006P7)

Gaurav Rana @GauravRana  
btimes.co.uk/decentralised-... #SyrianRefugees #BlockchainID #Bitcoin

CryptoCoinTalk @cryptocointalk  
#Bitcoin Offers #Refugees #Bitcoin Debit Cards - cryptocointalk.com/topic/42597-bit-... #altcoin via @cryptocointalk #BTC #XBT #finance #fintech

RajeevDM @rajeevdm  
#BGLFession-@MyBitcoin #CEO @SusanneOnline claims #Bitcoin is world's 1st #VirtualNation pic.twitter.com/3AP133a1

Innovate Your State @IYS\_Org

Blockchain is the kill switch for fraud  
11 May 2016 | 2:01 pm | 98

Brian Donegan, Head of Operations, eBusiness, ICT Development, Isle of Man Government, speaks about applications of blockchain other than within financial services, and how secure it really is.

5 equensWorldline

### What we always promise to do


Overall context

- Customer comes first
- Technology enables

.....

#### Have Business Problem

Cybercrime, Cost of X-border payment, Open Banking, Cash, Identity, Tsunami of Regulation, T&Cs, Wearables, IoT, Margins, Security, GDPR, Big Data, Third Parties, Customer Loyalty, Automation, Bank Crises, Use of Branches, ...



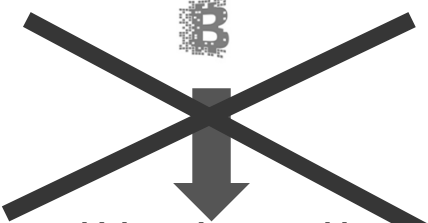
Which Technology solves ???

6 equensWorldline


### What we repeatedly actually do: A Solution looking for a Problem

.....

#### Have Technology



Which Business Problem shall we apply this to ???



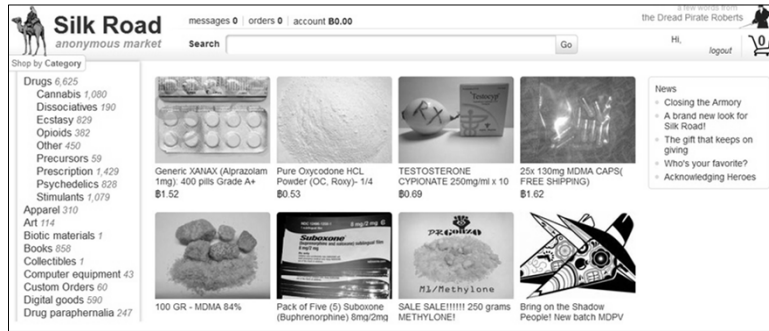
7 equensWorldline

.....

Does Blockchain have the potential to be a truly disruptive technology ?

8 equensWorldline

### Solves Problem for Drug Dealers



9

equensWorldline

### Of interest to non-capitalistic idealists Anti-“centric” Anarchists

**Advantages:**

Allows users to easily access a ride-sharing program that:

- Is decentralized
- Doesn't require fiat currency
- Isn't capitalistic like Uber or Lyft



- and thousands of conference organisers, consultants, media/journalists, ...
- and venture capitalists, speculators, ...

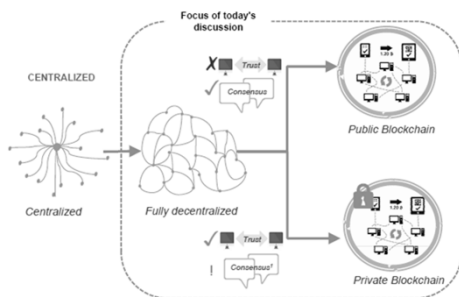
Of interest to banks and users ?

Our agenda

10

equensWorldline

### EPC Workshop December 2015



11

equensWorldline

### Distributed Systems with 30years' Experience


Telephone system, Internet, eMail, Netflix, Airline booking, MMORPG, Visa etc



12

equensWorldline

.....

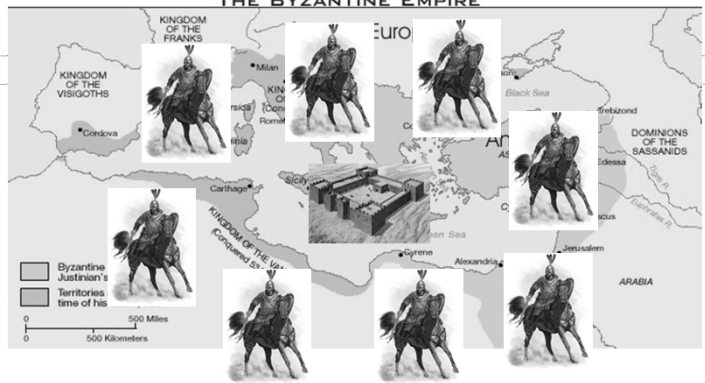


"A real computer science breakthrough. This is a problem that we've been trying to solve in computer science since the early 1980s. How to prevent the double spending problem."

Ben Horowitz 4bn\$ number 1 venture capital firm (Facebook, Twitter, ...)

13 **equensWorldline**

.....



► Reaching consensus in a distributed, faulty system without central control

14 **equensWorldline**

.....

### The Byzantine Generals Problem

LESLIE LAMPFORT, ROBERT SHOSTAK, and MARSHALL PEASE  
SRI International © 1982 ACM

► "Practical Byzantine Fault Tolerance" algorithm with high-performance processing thousands of requests per second with sub-millisecond increases in latency + Java library etc. available for decades

Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

15 **equensWorldline**

.....

### This problem has been solved since the 1980s

► **Paxos** is a family of protocols for solving consensus in a network of unreliable processors. Consensus is the process of agreeing on one result among a group of participants. This problem becomes difficult when the participants or their communication medium may experience failures.

Operating Systems Editor R. Stockton Gaines  
**Time, Clocks, and the Ordering of Events in a Distributed System**  
Leslie Lamport  
Massachusetts Computer Associates, Inc.  
first published 1978

first published 1985

first published 1989

The Fischer Lynch Paterson impossibility result (FLP) states that a deterministic asynchronous consensus system can have at **most two of** the following three properties:  
- safety (results are **valid** and identical at all nodes),  
- guaranteed **termination** or liveness (nodes that don't fail always produce a result),  
- and **fault tolerance** (the system can survive the failure of one node at any point).

This is a proven result

16 **equensWorldline**

### Speaking from personal background in computer algorithms



17

equensWorldline

### Technically - does not work well

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshi@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. ! escrow mechanisms could easily be implemented to protect buyers.

**4. Proof-of-Work**

- 1) New transactions are broadcast to all nodes. !
- 2) Each node collects new transactions into a block. !
- 3) Each node works on finding a difficult proof-of-work for its block. ! The average work required is exponential. !
- 4) When a node finds a proof-of-work, it broadcasts the block to all nodes. !

**10. Privacy**

A new key pair should be used for each transaction to keep them ! from being linked to a common owner. Some linking is still unavoidable. !

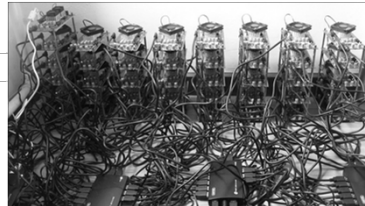
**11. Calculations**

An attacker can only try to change one of his own transactions to take back money he recently spent. We can calculate the probability. !

18

equensWorldline

11,598,666,437 MW/h



19

equensWorldline

### High claims on Scalability

Aiming well beyond Niche Solutions

### Ex-Google engineer bids to fix core banking

14 July 2016

“... solved the greatest challenge ... how to replace core banking systems

banks ... hampered by underlying software written decades ago ... answer is Vault OS, core banking software created for the cloud which uses private blockchain-style technology and has cryptographic ledgers for watertight security... 50-strong team ... its OS is completely flexible and handles any standard banking functions or business models ... it employs smart contracts and machine learning ... banks can scale to millions of customers... banks can determine their exact financial position at any moment. ...implementation of capital-adequacy standards such as Basel III automatic .... fixes broken banking and will be the engine for the banks of tomorrow”

20

equensWorldline



.....

**Payments** = instruments, compliance, regulation, dispute management, scheme, reach, brand, scale, KYC, commercial model, merchant services, availability, investigation, governance, guarantees, liquidity, collateral, SLAs, refund procedures, reconciliation, data standards, fraud support, limits, ROI, screening, funding, risk management, invoicing, QoS, business rules, ...

---

25 equensWorldline

### The appeal of decentral control

.....

Leap over censorship  
Escape total surveillance

Freenet is a peer-to-peer platform for censorship-resistant communication and publishing. Browse websites, post on forums, and publish files within Freenet with strong privacy protections.

---

26 equensWorldline

### Governance without Central Entity ?

.....

- ▶ If I have a problem who do I call ?
- ▶ Who decides who can join the scheme ?
- ▶ Who resolves conflict ?
- ▶ Who evolves the system ?
- ▶ ...

---

27 equensWorldline

### Eliminating Cental Entities

By creating new ones

Banks embrace Ripple and move beyond testing to real-world transactions

.....

- ▶ Goal: slash the time and cost of cross-border settlement
- ▶ Method: ditch the traditional, sluggish model of using local currency accounts with correspondent banks

- ▶ Instead, money is converted into the native Ripple currency, XRP

▶ "Using blockchain the first financial institution in Canada to complete an overseas payment in a matter of seconds. **Without blockchain, that transaction would have taken two to six business days**"

---

28 equensWorldline

### The Economist



When financial firms do business with each other, the hard work of synchronising their internal ledgers can take several days, which ties up capital and increases risk.

29

equensWorldline

### What BUSINESS use may come out of all this algorithm discussion ?

- ▶ More modern IT-know-how in banking ?
  - Not rely on consultants, media hype
  - Understand systems : distribution, scalability, security, ...



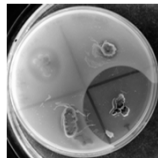
30

equensWorldline

### Geeks and Suits don't interact



Wau at the 17C3



31

equensWorldline

### What BUSINESS use may come out of all this algorithm discussion ?

- ▶ More modern IT-know-how in banking ?
  - Not rely on consultants
  - Understand systems : distribution, scalability, security, ...

- ▶ Established models are being challenged through BC discussion – good !
- ▶ BC discussion unleashes will, money, priority for change – good !

32

equensWorldline



### Many models do deserve to be challenged

---




Figure 2: Capital markets today

- ▶ Santander/Oliver Wyman report:
- ▶ inefficiencies in global collateral management market are costing banks \$4 billion p.a..




Figure 3: Capital markets in 2025

- ▶ "distributed ledger technology could **reduce banks' infrastructure costs** attributable to cross-border payments, securities trading and regulatory compliance **by between \$15-20 billion per annum** by 2022."
- ▶ "Uptake of distributed ledgers will remove **\$110 billion** in costs for the global financial services industry over the next three years" [McKinsey]

**equensWorldline**

### How to deal with the good scenarios

---

The pattern we repeatedly see:

- ▶ a) **We need to improve**
  - Global collateral mgmt
  - Lehmann
  - X-Border Payments
  - Post-trade securities
  - Cash reduction
  - Identity
  - Domestic Heating control
  - ...
- ▶ b) **Blockchain is the answer**

## Probably **Yes!**

## Probably **No**

**equensWorldline**

---

**Improvement here is**  
(not lack of technology)

**a matter of *will*, priorities, investment**

**equensWorldline**

### Blockchain is the magic keyword that unlocks **will, money, priority, ...**

---

if I call this project a blockchain, we'll get funding for it

It has to have blockchain in the title to get published and be accepted at conference


... if you included the word "blockchain" on your resumé it earns you 2x premium

**equensWorldline**

### Some things can only be explained psychologically

BC not such a big topic in Music/Media/Telco/Airline/...

---



37 equensWorldline

### BC as Catalyst for Improvement

---

► **PwC:**

- „maybe the solution doesn't involve Blockchain at all, but Blockchain has encouraged the leap to a solution"

► **DZ Bank:**

- „Selbst wenn am Ende ganz andere technische Lösungen zum Einsatz kommen, so wäre die Blockchain doch gleichsam der Katalysator gewesen"
- „Selbst wenn der Hype um die Blockchain nur das Ergebnis hätte, dass diese Technologie als Katalysator für Diskussionen über Lösungen jenseits der eingefahrenen Wege diene, so wäre dies mehr als begrüßenswert und würde die Europäische Finanzbranche einen grossen Schritt in Richtung Zukunft bringen"

38 equensWorldline

### #Blockwash - When is a blockchain not a blockchain

Where the smart money is going

---

► **Ripple**

- „Interledger: not blockchain but "a principle of getting different networks to connect"

► **R3** (consortium of 42 of the world's largest banks)

- „Scaling and interoperability a concern "
- „Doesn't follow that blockchain is the solution"
- „Corda: not really a blockchain"
- A blockchain "inspired" platform
- "Supports "a variety of consensus mechanisms"
- use "industry standard tools"

How do we make a shared ledger?

We might use a blockchain, we might not

Mobile-friendly - Apr 5, 2016 - Consortium startup R3CEV today announced it is working on a distributed ledger that might otherwise be considered a blockchain, but which the company made perfectly clear is anything but.

Bitcoin.com  
R3CEV Unveils Corda, But 'Is Not Building a Blockchain'  
By Jamie Redman - April 6, 2016

► **Intel** (Kelly Olson, director Intel distributed ledger technology group)

- "except in niches ("drugs") distributed ledger technologies (blockchains) "probably" won't replace either cash or everyday retail payments"
- "fundamental shift to decentralized endpoints is a security challenge"
- "There's no clear way to add that to the blockchain today without adding a centralized factor"
- "totally inappropriate for enterprise adoption - security, scalability, privacy"
- "lots of projects out there called BC, that aren't"

Morgan Stanley report dampens distributed ledger hype

39 equensWorldline

---


$$\frac{|1 - e^{2\pi i \frac{mr b}{q}}|}{|1 - e^{2\pi i \frac{r b}{q}}|} = \frac{|\sin(\pi m r b / q)|}{|\sin(\pi r b / q)|}$$

40 equensWorldline

.....  
**Shor's Factoring Algorithm**

**5.1 Factoring**

Probably the most important quantum algorithm so far is Shor's factoring algorithm [81]. It can find a factor of a composite number  $N$  in roughly  $(\log N)^2$  steps, which is polynomial in the length  $\log N$  of the input. On the other hand, there is no known classical (deterministic or randomized) algorithm that can factor  $N$  in polynomial time. The best known classical randomized algorithms run in time roughly

$$(\log N)^2 (\log \log N)^2 \log \log \log N$$

where  $\alpha = 1/3$  for a heuristic upper bound [61] and  $\alpha = 1/2$  for a rigorous upper bound [62]. In fact, much of modern cryptography is based on the conjecture that no fast classical factoring algorithm exists [77]. All this cryptography (for example RSA) would be broken if Shor's algorithm could be physically realized. In terms of complexity classes: factoring (rather, the decision problem equivalent to it) is provably in **BQP** but is not known to be in **BPP**. If indeed factoring is not in **BPP**, then the quantum computer would be the first counterexample to the "strong" Church-Turing thesis, which states that all "reasonable" models of computation are polynomially equivalent

.....  
**Summary and Recommendations**

- ▶ There are *many* technology developments
  - AI, Biometrics, Big Data, DLT, Wearables, BLE, NFC, Beacon, QR, Quantum, B2B AR, Cloud, Watson, HBP, Elliptic curves, XBRL, API, VR, Tokenisation, Oauth, Voice control/ident, ...
  
- ▶ Understand key facts and impact, work with serious partners, do pilots, shout about it
  - Don't get caught in hype fuelled by investors, media, consultants
  
- ▶ Prioritise *business* issues
  - Decide which have pressing business problems (x-border post-trade securities?)
  - Solve using suitable (scalable, compliant, ...) technology
    - may be BC, may not - business stays technology agnostic
  
- ▶ Leverage drive in industry to make things better
  - New business (with money unlocked by BC debate)
  
- ▶ Make up your own mind !

.....  
**The Future: Making Coffee on the Blockchain**



**The Cambridge Coffee Pot**  
**160.000 hits per year**

.....  
**Thanks**

For more information please contact:  
 Michael Salmony  
 Executive Adviser  
 T +49 172 6 86 71 63  
 michael.salmony@equens.com

equensWorldline is an expert leader in e-payment services and a registered trademark of Worldline. Confidential information owned by equensWorldline, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from equensWorldline.  
 © equensWorldline - For internal use