Blockchain Technology: The Next Big Thing?

Professor Michael Mainelli

@mrmainelli
michael_mainelli@zyen.com

29 March 2016
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
Z/Yen in Finance Research

♦ Distributed ledgers (1995-present)
♦ LIBOR and FX surveillance (2007-present)
♦ PropheZy and VizZy – automation & visualisation of compliance monitoring (2002-present)
♦ Market intelligence – Ministry of Defence, e.g. Vision 2020 (1994-present)
♦ Avatars for Big Data (2010-2012)
The Study Of Money Is The Root Of Much Madness

www.longfinance.net

[www.dilbert.com, Thursday, 27 January 2015]

How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

**WALLETS AND ADDRESSES**

Bob and Alice both have Bitcoin "wallets" on their computers.

**Creating a New Address**

Bob creates a new Bitcoin address for Alice to send her payment to.

**Submitting a Payment**

Alice is her Bitcoin client that she will use to transfer the purchase amount to Bob’s address.

**Verifying the Transaction**

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

**Cryptographic Hashes**

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it’s essentially impossible to predict which initial data set will create a specific hash value.

**Nonces**

To create different hash values from the same data, Bitcoin users use "nonces." A nonce is just a random number that’s added to data prior to hashing. Changing the nonce results in a wildly different hash value.

**The miners’ computers are set up to calculate cryptographic hash functions.**

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner. In this case, Gary. A new address is created in Gary’s wallet with a balance of newly minted bitcoins.

**The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they’re forced to generate many hashes with different nonces until they happen upon one that works.**

**Spectrum.ieee.org “How a Bitcoin Transaction Works”**
“... the potential impact of the distributed ledger may be much broader than on payment systems alone. The majority of financial assets — such as loans, bonds, stocks and derivatives — now exist only in electronic form, meaning that the financial system itself is already simply a set of digital records.”

*Bank of England, Quarterly Bulletin (2014, Q3)*
“In distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation.”
Matthew Hancock & Ed Vaizey (January 2016)
### Possibly Distributively Ledgerable

<table>
<thead>
<tr>
<th>Area</th>
<th>Possible Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial instruments, records, models</td>
<td>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 &amp; corporate tokens, etc.</td>
</tr>
<tr>
<td>Public records</td>
<td>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.</td>
</tr>
<tr>
<td>Private records</td>
<td>Contracts, ID, signature, will, trust, escrow, any other type of classifiable personal data (e.g. physical details, date of birth, taste) etc.</td>
</tr>
<tr>
<td>Semi-private/semi-public records</td>
<td>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, etc.</td>
</tr>
<tr>
<td>Physical keys</td>
<td>Key to home, hotel, office, car, locker, deposit box, mail box, Internet of Things, etc.</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>Copyrights, licenses, patents, digital rights management of music, rights management of intellectual property such as patents or trademarks, proof of authenticity or authorship, etc.</td>
</tr>
<tr>
<td>Other records</td>
<td>Cultural, historical events, documentary (e.g. video, photos, audio), (big) data (weather, temperatures, traffic), SIM cards, archives, geostamping, etc.</td>
</tr>
</tbody>
</table>
Why Does A Central Registry Exist?

Financial services are based on ‘mistrust’ & leverage

♦ Validate - Sin of Commission – forgery of a transaction

♦ Safeguard - Sin of Deletion – reversal of a transaction

♦ Preserve - Sin of Omission – censorship of a transaction

[Robert Sams, "Blockchain Finance" (March 2015)]
What Does A Distributed Ledger Do?

♦ Validates – “a trust model for timestamping”
♦ Safeguards – “a set of rules for updating state via blocks”
♦ Preserves – “a shared state”

Persistent & Pervasive

Terms Defined

♦ **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”
Buzz or Hype? The New New Thing

[Ken Tindell mashup - 14 May 2015 https://twitter.com/kentindell/status/598865133247569920]
The Old Old New New Thing…

I THINK WE SHOULD BUILD AN SQL DATABASE.

DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?

WHAT COLOR DO YOU WANT THAT DATABASE?

I THINK MAUVE HAS THE MOST RAM.

[www.dilbert.com, Friday, 17 November 1995]

[Internet (1976 for me), databases (Oracle, Ingres, DBII, relational/hierarchical/distributed), web (SGML, Gopher), ‘Internal Internets’ (i.e. intranets), social media (SixDegrees)...]
Buzz Or Hype - Old Old Things?

- 1976 – Diffie-Hellman & Merkle (also RSA)
- 1990 – Mondex, Digicash, Flooz
- 1993 – Encrypted Open Books
- 1995 – Z/Yen Stacks, WebDNA
- 1996 – Ricardo payment system
- 1999 – LOCKSS & CLOCKSS
- 2000 – Gnutella
- 2004 – Ripple
- 2007 – Estonia
- 2009 – Bitcoin
- 2013 – Silk Road, FBI, Alderney coin
- 2016 – UK government, Blythe Masters DAH, R3, SafeShare Insurance, CLEAR, …
Mistrust Costs Coins

Supervisor Nodes

Efficient

- ‘Woven’ Broadcasting
- Master Node

Inefficient

- No Trusted Third Parties
- Collective Nodes

Free for All Nodes

Central Database

Single Trusted Third Party

Bitcoin

Ethereum

Ripple

Paper

Collective Nodes
Logically One, Physically Many

- Identity systems – PwC KYC Centre of Excellence
- Wholesale insurance ‘deal rooms’
- Retail insurance – motor, home, small business
- Credit validation and scoring
- Clinical trials
- Timestamping – MetroGnomo.com with States of Alderney
InterChainZ & IntereXchainZ

- Personal chains
  - Identification chain
  - Motor insurance policy
  - Content chain
- Corporate chains
  - Identification chain
  - Small business policy
  - Other chain, e.g., credit data

Different keys for the locks
# Identity

## InterChainZ - Identity Validator Use Case

**Add Data to Ledger**
- Add New Entity
- Add Entity Data

**Import / Export Functions**
- Export to file
- Push to network

### Show 10 entries

<table>
<thead>
<tr>
<th>Row Height</th>
<th>Row Hash</th>
<th>Created</th>
<th>Entry Type</th>
<th>Category</th>
<th>Company</th>
<th>File Name</th>
<th>File Hash</th>
<th>File Size</th>
<th>Geo Location</th>
<th>Public Key</th>
<th>Signature</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00004288315</td>
<td>06-06-2015 09:37:41</td>
<td>Identity</td>
<td>EW715</td>
<td>EW715</td>
<td>EW715Identity.pdf</td>
<td>7bf7ec5d9d7e7a077f6563a967</td>
<td>20KB</td>
<td></td>
<td>7c30f5d325642fda968987c3</td>
<td>0e50c0a90f3688677a</td>
<td>4 False Positive Hits found: All discounted based on name enumberate, One Exact Match - Queen of England (Q)</td>
</tr>
<tr>
<td>2</td>
<td>00000150d3e</td>
<td>06-06-2015 09:30:05</td>
<td>Company Data</td>
<td>EW715</td>
<td>EW715</td>
<td>EW715CompanyData</td>
<td>7bf7ec5d9d7e7a077f6563a967</td>
<td>20KB</td>
<td></td>
<td>7c30f5d325642fda968987c3</td>
<td>0e50c0a90f3688677a</td>
<td>4 False Positive Hits found: All discounted based on name enumberate, One Exact Match - Queen of England (Q)</td>
</tr>
<tr>
<td>3</td>
<td>00000ebeb48</td>
<td>06-06-2015 09:38:16</td>
<td>Company Data</td>
<td>EW715</td>
<td>EW715</td>
<td>EW715CompanyData</td>
<td>7bf7ec5d9d7e7a077f6563a967</td>
<td>20KB</td>
<td></td>
<td>7c30f5d325642fda968987c3</td>
<td>0e50c0a90f3688677a</td>
<td>4 False Positive Hits found: All discounted based on name enumberate, One Exact Match - Queen of England (Q)</td>
</tr>
<tr>
<td>4</td>
<td>000005d2124</td>
<td>06-06-2015 09:38:29</td>
<td>Company Data</td>
<td>EW715</td>
<td>EW715</td>
<td>EW715CompanyData</td>
<td>7bf7ec5d9d7e7a077f6563a967</td>
<td>20KB</td>
<td></td>
<td>7c30f5d325642fda968987c3</td>
<td>0e50c0a90f3688677a</td>
<td>4 False Positive Hits found: All discounted based on name enumberate, One Exact Match - Queen of England (Q)</td>
</tr>
<tr>
<td>5</td>
<td>000092bc0b8</td>
<td>06-06-2015 09:30:41</td>
<td>Company Data</td>
<td>EW715</td>
<td>EW715</td>
<td>EW715CompanyData</td>
<td>7bf7ec5d9d7e7a077f6563a967</td>
<td>20KB</td>
<td></td>
<td>7c30f5d325642fda968987c3</td>
<td>0e50c0a90f3688677a</td>
<td>4 False Positive Hits found: All discounted based on name enumberate, One Exact Match - Queen of England (Q)</td>
</tr>
<tr>
<td>6</td>
<td>0000c10a4ca</td>
<td>06-06-2015 09:38:52</td>
<td>Company Data</td>
<td>EW715</td>
<td>EW715</td>
<td>EW715WholeFile.pdf</td>
<td>7bf7ec5d9d7e7a077f6563a967</td>
<td>20KB</td>
<td></td>
<td>7c30f5d325642fda968987c3</td>
<td>0e50c0a90f3688677a</td>
<td>4 False Positive Hits found: All discounted based on name enumberate, One Exact Match - Queen of England (Q)</td>
</tr>
<tr>
<td>7</td>
<td>0000befadd8</td>
<td>06-06-2015 09:35:33</td>
<td>Company Data</td>
<td>EW715</td>
<td>EW715</td>
<td>EW715WorldCheckreport.pdf</td>
<td>7bf7ec5d9d7e7a077f6563a967</td>
<td>20KB</td>
<td></td>
<td>7c30f5d325642fda968987c3</td>
<td>0e50c0a90f3688677a</td>
<td>4 False Positive Hits found: All discounted based on name enumberate, One Exact Match - Queen of England (Q)</td>
</tr>
</tbody>
</table>

**Please note**
- (1) General Legal Notice
- (2) Category Legal Notice
- (3) Reported Link Legal Notice

**Comment:**
- 4 False Positive Hits found: All discounted based on name enumberate, One Exact Match - Queen of England (Q)

**Usernames:**
- henry4703

**Printed:**
- 16-08-2013 10:06 UTC

**NAME:**
- Elizabeth Windsor

**MODE:**
- Part Match

**LAURENCE**
- Anne Elizabeth Alice Louise
- Individual

**MONTBATTEN WINDSOR**
- Louise
- Individual

**MONTBATTEN-WINDSOR**
- Searie Elizabeth Mary
- Individual

**DOLLY**
- Alexandra
- Individual

**WINSTON**
- Elizabeth Alexandra Mary
- Political/Criminal

**1) General Legal Notice**
- All information identified or correlated in this profile appears in the listed sources. We are not responsible for the content of any part sites or sources. Information contained is necessarily brief and should be read by users in the context of the full details available in the external sources to which hyperlinks are provided. Users should carry out independent checks in order to verify the information correlated.

**2) Category Legal Notice**
- Category is based on information contained in the sources provided.
## Insurance - ACORD Messaging

### Add Data to Ledger
- Add New Entity
- Add Entity Data

### Import / Export Functions
- Export to file
- Import from file
- Push to network
- Pull from network

### LEDGER

<table>
<thead>
<tr>
<th>Row Height</th>
<th>Row Hash</th>
<th>Created</th>
<th>Entry Type</th>
<th>Company</th>
<th>File Name</th>
<th>File Hash</th>
<th>Encrypted?</th>
<th>File Type</th>
<th>File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>0000439b3b...</td>
<td>15-12-2015 18:43:05</td>
<td>Company Data</td>
<td>RC Smith Insurance</td>
<td>Vehicle or Equipment Certificate of Insurance.pdf</td>
<td>10498t7f15...</td>
<td>✓</td>
<td>application/pdf</td>
<td>15Kb</td>
</tr>
<tr>
<td>12</td>
<td>00005cbb10a...</td>
<td>15-12-2015 18:43:25</td>
<td>Company Data</td>
<td>RC Smith Insurance</td>
<td>Florida Personal Auto Application.pdf</td>
<td>0t2c81e5d5...</td>
<td>✓</td>
<td>application/pdf</td>
<td>16Kb</td>
</tr>
<tr>
<td>13</td>
<td>0000967c8d...</td>
<td>15-12-2015 18:44:28</td>
<td>Company Data</td>
<td>RC Smith Insurance</td>
<td>Vehicle or Equipment Certificate of Insurance.pdf</td>
<td>10498t7f15...</td>
<td>✓</td>
<td>application/pdf</td>
<td>15Kb</td>
</tr>
<tr>
<td>14</td>
<td>0000998c12...</td>
<td>15-12-2015 18:45:10</td>
<td>Company Data</td>
<td>RC Smith Insurance</td>
<td>Florida Auto Insurance Identification Card.pdf</td>
<td>cbf1c1635f...</td>
<td>✓</td>
<td>application/pdf</td>
<td>3Kb</td>
</tr>
<tr>
<td>15</td>
<td>00008ae2fa...</td>
<td>15-12-2015 18:46:18</td>
<td>Company Data</td>
<td>RC Smith Insurance</td>
<td>Florida Insurance Supplement, Credit Report Disclosure Information (DCI)</td>
<td>600d008ad8...</td>
<td>✓</td>
<td>application/pdf</td>
<td>8Kb</td>
</tr>
</tbody>
</table>
Current Operating Model
Coverholder & Service Company – Key Interactions

Key:
- Inefficient process
- Sub-optimal process
- Efficient process
- Process sequence

1. Risk query, claims, Policy etc.
   - Client (can be in or out of territory)

2. Risk, premium, claim information; premium and claims payments Referrals and responses
   - Local / Placing / Producing Broker*
   - *In some territories these can be onshore
   - Coverholder / Service Company (TPA for some claims)

3. Agreement Process
   - Approved Broker

4. Bureau Submission
   - London Market Carrier(s)

5. Regulatory Information (Lloyd’s only)

6. Reporting Data

7. Tax and Regulatory Reporting
   - Central Settlement

8. Syndicate Returns (Lloyd’s only)

9. LDR

10. Lloyd’s

11. Various reports

12. Regulators and Tax Authorities

13. Lloyd’s International Offices

14. Reporting Data

15. Regulators and Tax Authorities

16. Lloyd’s

17. Various reports

18. Regulators and Tax Authorities

NB: Relates to Lloyd’s business only. This diagram does not include known issues such as: oversight, approval, audits and complaints

Justification for RAG status
1) Multiple data formats
2) Negative Londonisms, e.g. Declaration, onerous data requirements
3) Paper usage, photocopying and scanning, duplication
4) Negative Londonisms, e.g. LPANS, Bureau queries
5) Manual mismatch clearing, data duplication
5a) ACORD XML
6) Lack of structured data, no written data or ‘Net of RI’
7) Lack of structured data. Three days to settle monies
8) Lack of structured data, duplication across carriers
9) and 10) Lack of audit trail and granularity, signed data only

* In some territories these can be onshore.
Target Operating Model (TOM)
London Market – Key Interactions

- **Policy Holder**: Risk query, claims, Policy
- **Local Broker**: E.g. Quote request, Declaration, Claims Advice
- **Regional Broker**: Premium Payment
- **Surplus Lines Broker**: Endorsements etc.

**Optional Channels**
- **Local Broker**
- **Regional Broker**
- **Surplus Lines Broker**

**Approved Broker**
- **Approved Broker**: Direct Policy, Claims Advice, Premium Payment, Endorsements etc.

**Service Hub**
- **Message Hub (TMEL)**
- **Customer Interactions**: Customer Services, Broker Services
- **e-Placing Services**: Data services, Structure Data Capture
- **Document Repository**: Claims Services, Data services
- **Carrier Services**: Data services, Bureau Services

**Non Service Hub Activities**
- **London Market Carrier(s)**
- **London Market Companies**
- **IUA Companies**

**Data feeds**
- **ACORD XML**

**Lloyd's**
- **Data feed**

**Regulators and Tax Authorities**
- **Data feeds**

**Justification for RAG status**
1) 2) Easier access to central services
3) Placing avoiding paper with single contract version and no re-keying of data; enhance trading floors
4) and 5) Easier access to central services (ACORD) to avoid duplicative processes and rekeying data
6) Data provided to Lloyd's and IUA in ACORD XML for consistency, audit trail and automated reporting
7) Written as well as signed data provided to regulators, full audit trail

**NB:** Brokers primarily interact with broker and market services, NOT carrier or Hub services

* Encourage Data Standards adoption, don’t enforce a new Londonism

**Key:**
- Red: Inefficient process
- Orange: Sub-optimal process
- Green: Efficient process
- Blue: Process sequence
<table>
<thead>
<tr>
<th>First Name</th>
<th>Surname</th>
<th>Unique Reference</th>
<th>Address</th>
<th>Postcode</th>
<th>First Name</th>
<th>Surname</th>
<th>Unique Reference</th>
<th>Address</th>
<th>Postcode</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td>Smith</td>
<td>VR0001</td>
<td>123 Bank Street</td>
<td>EC2V 5AY</td>
<td>John</td>
<td>Smith</td>
<td>VR0001</td>
<td>54 Woodhill Lane</td>
<td>W17 RO</td>
</tr>
</tbody>
</table>

EVIDENCE OF INSURANCE

This Document is issued as Evidence of Insurance, it does not constitute a legal contract of insurance.

The Master Policyholder has procured insurance under a Master Policy in respect of persons who are members of the Master Policyholder. This document is issued to you as evidence that your name has been added as a person insured under the Master Policy.

The coverage provided is in accordance with the terms and conditions contained in the Master Policy. The Master Policy is available for inspection upon application to the Master Policyholder.

The details that follow are those shown in the Master Policy as applicable to you. In the event of any discrepancy between the details shown in this document and those shown in the Master Policy then those shown in the Master Policy shall prevail.

Master Policy No: 5W01/37215
Unique Master Reference: B20029W01/37215

1. Name and address of the Member: John Johnson, 1 Park House, London, W1 1AA.
Address of Premises: 1 Palace West, London, W1 1AA.

2. Effective from 14th February 2016 to 14th February 2017, both days inclusive.

Operational Time: The insurance operates during the period of any booking made through the Vrumi website (being either a single booking or multiple bookings running continuously on the same day at the same property).

3. This Evidence of Insurance is underwritten with certain Underwriters at Lloyd's, London. Niven Syndicates Limited.
Per cent: 150%.

4. Coverage:
- Section One – Buildings: GBP 95,000
- Section One – Contents: GBP 25,000
- Section Two – Accidental Damage: GBP 5,000
- Section Three – Legal Liability to the Public: GBP 2,000

5. In the event of a claim under the Evidence of Insurance, please notify:
Advising Associates LLP
Tel: 0141 202 0519
Fax: 0141 226 5115
Email: claims@advisingassociates.com

Claims in writing should be directed to:
Advising Associates LLP
Unit 2, Station Road, Solihull
Email: claims@advisingassociates.com

Emergency 24/7 Out of Office Number: 01794 381301

Signed and dated the 15th day of February 2016

[Signature] (Master Policyholder)
Process versus Technology

Technology Change Difficulty

- Identity
- Archiving
- Regulatory Reporting
- Timestamping
- Shared Data
- Deal Rooms
- Asset Transfer
- Asset Maintenance
- Contract Execution
- Wholesale Payments
- Market

Process Change Difficulty
Mutual distributed ledgers help make better ‘contract’ utilities by providing:

- shared ‘preserved’ data
- shared ‘safeguarded’ transactions

Mutual distributed ledger technology will displace much messaging and shared data functions

… try one out … www.MetroGnomo.com
"Get a big picture grip on the details."

Thank you!

When Would We Know Our Commerce Is Working?
Basic Copyright Notice & Disclaimer

©2016 This presentation is copyright protected. All rights reserved. You may download or print out a hard copy for your private or internal use. You are not permitted to create any modifications or derivatives of this presentation without the prior written permission of the copyright owner.

This presentation is for information purposes only and contains non-binding indications. Any opinions or views expressed are of the author and do not necessarily represent those of Swiss Re. Swiss Re makes no warranties or representations as to the accuracy, comprehensiveness, timeliness or suitability of this presentation for a particular purpose. Anyone shall at its own risk interpret and employ this presentation without relying on it in isolation. In no event will Swiss Re be liable for any loss or damages of any kind, including any direct, indirect or consequential damages, arising out of or in connection with the use of this presentation.