What Blockchain Means for Financial Risk Management

GARP Webcast Series

Adam Stradling
Blockchain Entrepreneur

On24 Tech Tips

• Make sure your speakers are on
• Hit F5 any time your console freezes
• For a LIVE event you should be hearing music now
• Use the “Ask a Question” feature to report issues
• Webcast starts at the top of the hour
Adam Stradling, Blockchain Entrepreneur

- During 2011 and 2012, I cofounded and operated Bitcoin.com
- Since then I’ve been involved in a number of other bitcoin/blockchain startups
- Originated from the financial risk management and technology world
- Worked with the financial risk management advisory group at EY, among other similar companies

https://www.linkedin.com/in/adamstradling
Risk Management and Blockchain

What does blockchain mean for financial risk management?
Industry Survey – Risk Reductions

DISTRIBUTED LEDGER TECHNOLOGY BENEFITS

Which of the following do you believe distributed ledger technology could help reduce?1

- Settlement Risk: 84%
- Settlement Time: 84%
- Counterparty Risk: 74%
- Custodial Risk: 57%
- Capital Cost: 45%
- Systemic Risk: 34%
- Market Risk: 31%
- Other: 12%

Other than payments and digital currency, what area / products could most benefit from the technology?2

- OTC Derivatives: 62%
- Private Stock: 54%
- Repo: 54%
- Syndicated Loans: 48%
- Other: 16%

1. Based on 58 respondents in 2015.

Presentation Agenda

• Short introduction to Blockchain Technology

• What blockchain means for financial risk management
  • Settlement Risk – Clearing and settlement using blockchains
  • Emergent “Blockchain Risks” – the new risks arising from blockchains
  • OTC Derivatives and Counterparty Risk – Smart contracts and swaps
  • Other Applications to Risk Management – Short review and survey

• Conclusion and Next Steps: A unique proposal for risk managers
Introduction To Blockchain Technology
How Does Bitcoin Work?

Let’s look at Bitcoin, best explained through this video:

https://www.youtube.com/watch?v=l9jOJk30eQs
### Consensus Computing Technology Stack

<table>
<thead>
<tr>
<th></th>
<th><strong>Bitcoin</strong></th>
<th><strong>Crypto 2.0</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td>The data: ledger of bitcoin transactions and amounts</td>
<td><strong>General Business Processes:</strong> The data: securities, bonds, escrows, voting, many other applications</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td><strong>Scripting Language:</strong> Single application, digital signatures – ECDSA</td>
<td><strong>Operating System:</strong> Turing complete, new crypto like new sig types, multi-sig, many more</td>
</tr>
<tr>
<td><strong>Blockchain</strong></td>
<td><strong>Consensus Process:</strong> Voting process: Proof of Work, SHA256</td>
<td><strong>Consensus Process:</strong> Voting process: Proof of Stake, Consensus, Scrypt, many others</td>
</tr>
</tbody>
</table>
Learning Resources

• Detailed technical video on how Bitcoin works (22 minutes): https://www.youtube.com/watch?v=Lx9zgZCMqXE

• Satoshi’s original paper: https://bitcoin.org/bitcoin.pdf

• The Ultimate List of Bitcoin and Blockchain Whitepapers: http://startupmanagement.org/2014/12/16/the-ultimate-list-of-bitcoin-and-blockchain-white-papers/
Settlement On The Blockchain
The Idea and Its Pioneers

Original Idea

Use the Bitcoin’s transaction processing and security infrastructure to build ledgers for other assets

Settlement – The OP_Return

Each Bitcoin transaction contains an open data field called the OP_Return.

<table>
<thead>
<tr>
<th>Block</th>
<th>Transaction ID</th>
<th>OP_RETURN metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>333394</td>
<td>bebb21c7bbd8a7d267b4be36b0f43eea3fe0c7ba245c4fc161deb9a126a1fe7</td>
<td>&quot;??Beyond(^_^)<a href="mailto:Gender@ISTScare.org">Gender@ISTScare.org</a>??&quot;WQwiARliCh5CZvlvmQoXI9eKUdlbmsRlkBJU1RTY2FyZS5vcmcaA6a28590c080112220a1e4265796f6e64285e5f5e2947656e64657242671a00 (raw)</td>
</tr>
<tr>
<td>333390</td>
<td>fa89bf48f4b2187673ab64f5e0f7d7a4649bf24d161eeea47d3f19e35bbb309676</td>
<td>&quot;OA???d?u=<a href="https://cpr.sm/rmcVXv9c5b">https://cpr.sm/rmcVXv9c5b</a> (Open Assets)T0EBAAFkG3U9aHR0cHM6Ly9jcHluc20vcm1jVh2OWM1Yg== (base64 encoded)6a224f41010001641b753d687470733a2f2f6370722e736d2f726d</td>
</tr>
</tbody>
</table>
| 333388 | 173ae8d9bc09bad166bf80bc9fc2ada1e573cb51a54b10da6c6201c4a119652 | "???590c.org(^_^)Taichung@TW????????WQwiARliChg10TBlm9yZheX14vVGFpY2h1bmdAVFcQ3g8aA6vN6a28590c080112220a18353930632e6f7267285e5f5e295461696363abcdef (raw)"
Settlement – Embedded Meta Data

Meta Data Embedded in A Bitcoin Transaction

Source: http://omnichest.info/lookuptx.aspx?txid=4b083367a540e57eb4e3136c6a2ea167b5bd126deaf6bfaf3f0037300b8c2d21
Settlement – Embedded Consensus Protocols

This is the first ledger (parsed by the distributed ledger – it knows nothing about the embedded data)

This is the second ledger (parsed by the Symbiont smart contract server)

Source: http://symbiont.io/uncategorized/what-is-embedded-consensus/
## Settlement – Assets Creation and Transfer

Assets created and sent through these networks

<table>
<thead>
<tr>
<th>Tx_Index</th>
<th>Block</th>
<th>Age</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>11831060</td>
<td>394793</td>
<td>10 mins ago</td>
<td>1GmbusLpguNIVS3...</td>
<td>Send (1DwlaFKuTImUqfUCx... received 0 BITCRYSTALS)</td>
</tr>
<tr>
<td>11831059</td>
<td>394793</td>
<td>10 mins ago</td>
<td>1AeqgtHedfA2yVX...</td>
<td>Send (14d2p5LTEAcoTHC... received 0.9 GEMZ)</td>
</tr>
<tr>
<td>11831058</td>
<td>394793</td>
<td>10 mins ago</td>
<td>1ANa1glJ1EKUmQ...</td>
<td>Send (13VLpxG8UEqdiWm... received 9.47 XCP)</td>
</tr>
<tr>
<td>11831057</td>
<td>394793</td>
<td>10 mins ago</td>
<td>1GmbusLpguNIVS3...</td>
<td>Send (1DwlaFKuTImUqfUCx... received 1547.11864407 BITCRYSTALS)</td>
</tr>
<tr>
<td>11831056</td>
<td>394792</td>
<td>38 mins ago</td>
<td>1JdylAW6huTkXnk...</td>
<td>Broadcast BLOCKSCAN VERIFY-ADDRESS u9yv6frdmqr1val</td>
</tr>
<tr>
<td>11831055</td>
<td>394791</td>
<td>1 hour 4 mins ago</td>
<td>1DwlaFKuTImUqfUCx...</td>
<td>Send (1Au07L34aLMr4rsD... received 0.0284116 SJCX)</td>
</tr>
<tr>
<td>11831054</td>
<td>394791</td>
<td>1 hour 4 mins ago</td>
<td>1AtYnMAHfJfG9TU...</td>
<td>Send (1GmbusLpguNIVS3... received 1547.11864407 BITCRYSTALS)</td>
</tr>
<tr>
<td>11831053</td>
<td>394789</td>
<td>1 hour 21 mins ago</td>
<td>1Zl8LysKvFmxEb...</td>
<td>Send (1LTBCy8dhKhzNNZ... received 2075.42150129 LTBCOIN)</td>
</tr>
<tr>
<td>11831052</td>
<td>394789</td>
<td>1 hour 21 mins ago</td>
<td>1KPCVvPVcoDkwW...</td>
<td>Send (1LTBCy8dhKhzNNZ... received 2155.28605926 LTBCOIN)</td>
</tr>
</tbody>
</table>

Tokens represent ownership in an asset (mostly user created assets)

## Settlement - Businesses, Projects, News

<table>
<thead>
<tr>
<th>Business / Project</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symbiont</td>
<td><a href="http://symbiont.io/">http://symbiont.io/</a></td>
</tr>
<tr>
<td>Coinprism / Open Assets</td>
<td><a href="https://www.coinprism.com/">https://www.coinprism.com/</a></td>
</tr>
<tr>
<td>Omnilayer</td>
<td><a href="http://www.omnilayer.org/">http://www.omnilayer.org/</a></td>
</tr>
<tr>
<td>Blockchain Clearing Corp</td>
<td><a href="http://blockchainclearing.com/">http://blockchainclearing.com/</a></td>
</tr>
<tr>
<td>TZero</td>
<td><a href="https://t0.com/">https://t0.com/</a></td>
</tr>
<tr>
<td>Digital Asset Holdings</td>
<td><a href="http://digitalasset.com/">http://digitalasset.com/</a></td>
</tr>
<tr>
<td>Clearmatics</td>
<td><a href="http://www.clearmatics.com/">http://www.clearmatics.com/</a></td>
</tr>
<tr>
<td>Setl</td>
<td><a href="https://www.setl.io/">https://www.setl.io/</a></td>
</tr>
<tr>
<td>BankChain</td>
<td><a href="https://www.bankchain.com/">https://www.bankchain.com/</a></td>
</tr>
<tr>
<td>Counterparty</td>
<td><a href="http://counterparty.io/">http://counterparty.io/</a></td>
</tr>
</tbody>
</table>

### Relevant news


Settlement - Risk Implications

“*The trade is the settlement*”, Patrick Byrne, CEO of TZero

Risk reduction:
- structural risk due to possible gross settlement of securities
- counterparty risk – reduce or eliminate clearing houses or other intermediaries
- capital risk due to reduced settlement periods

Costs reduction:
- necessary internal controls
- reconciliation burden

Increased security:
- Hard crypto, e.g. Public/Private key infrastructure
- Immutable, standardized, authenticated transaction records
Not all the companies/projects are using the Bitcoin blockchain

Approaches using Bitcoin have been criticized

Introducing “Emergent Blockchain Risks”
Emergent Blockchain Risks
Emergent Risks – Criticisms of Bitcoin

• **Privacy/Confidentiality** – Bitcoin blockchain is inherently “transparent”, only pseudo-anonymity

• **Compliance** – Anonymous validators/miners existing in potentially sanctioned regions

• **Scalability and Cost** – technical barriers to scaling, cost of Proof of Work

• **Settlement Finality** - “Probabilistic” settlement vs legal finality

• **Miners Incentive** - Top heavy incentive because of exogenous value

• **Decentralization** - State of Bitcoin decentralization
Idea

“Turn off” different features of public blockchains

- **Restrict Access** - for reading or writing information to the chain, hence “permissioned”, and thus gives a form of privacy

- **Identification** - of validators and users

- **Consensus algorithm** – increase speed and scalability, security features, and many other reasons

- **Source Code** - closed or partially open, as opposed to fully open
Emergent Risks – Security by Sharing

If we:

- close source
- control access
- change consensus process
- identify all participants

A standard database and technology stack? An intranet?

Required security depends on the specific business process

Emergent Risks - Ecosystem

Ecosystem evolving across private, semi-public, and fully public

What to choose and why?
Emergent Risks – The Trust Spectrum

Who do I need to trust and what am I trusting them about?

<table>
<thead>
<tr>
<th>Ownership of on-platform assets</th>
<th>Ownership of off-platform assets</th>
<th>Obligations and rights arising from an agreement</th>
<th>Who do I trust to maintain a truthful record?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Bank, Commercial Bank</td>
<td>Custodian Bank</td>
<td>Clearing House</td>
<td>A central authority</td>
</tr>
<tr>
<td>A group of known actors</td>
<td>Hyperledger</td>
<td>Eris</td>
<td>A group of known actors</td>
</tr>
<tr>
<td>A group of actors, some known</td>
<td>Ripple (Gateways)</td>
<td>Ripple (Codius)</td>
<td>A group of actors, some known</td>
</tr>
<tr>
<td>Nobody</td>
<td>Bitcoin</td>
<td>Colored Coins, Counterparty</td>
<td>Nobody</td>
</tr>
<tr>
<td>Ethereum</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Blockchain is Risk Technology

Blockchains are a Financial Risk Management Technology

Application of established financial risk management principles – and, the creation of new principles – to assess the economic value that blockchain technologies can have on different lines of business.
A smart-contract is an event-driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger.

Source: [http://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/](http://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/)
Smart Contracts – Swap Example

1. **Hedger**
   - Sell Index
   - Buy USD

2. **Trader**
   - Buy Index
   - Sell USD

3. **Swap Term Sheet** *in CODE*
   - Payment Frequency, Day Count, Reset Frequency, Maturity, Tenor, etc.

4. **Crypto Collateral**

5. **Multi-Signature Escrow**:
   - Collateral, margin, settlement via trustless bitcoin escrow

6. **D. Ledger**
7. **Oracle: Index Data**
Smart Contract Swap – Problem?

What’s the problem for financial institutions?

No fiat crypto currencies, yet

No agreed upon blockchain, yet

“Fedcoin”: A government issued digital currency and blockchain

http://andolfatto.blogspot.com/2015/02/fedcoin-on-desirability-of-government.html

“SettlementCoin” by UBS: a digital fiat redeemable with UBS


Institutional Blockchain by R3: private distributed ledger for institutions


“PBOCoin”: China just announced its intention to build its own digital currency

## Derivatives - Projects and Businesses

<table>
<thead>
<tr>
<th>Resources</th>
<th>Website</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirror</td>
<td><a href="https://www.mirror.co/">https://www.mirror.co/</a></td>
<td>Tagline: We're building a global OTC trading and hedging platform.</td>
</tr>
<tr>
<td>Clearmatics</td>
<td><a href="http://www.clearnatics.com/">http://www.clearnatics.com/</a></td>
<td>Tagline: Clearmatics is developing the next-generation clearing machines for financial OTC markets</td>
</tr>
<tr>
<td>TeraExchange</td>
<td><a href="http://www.teraexchange.com/overview.html">http://www.teraexchange.com/overview.html</a></td>
<td>TeraExchange will help market participants meet globally recognized regulatory goals in the OTC derivatives markets</td>
</tr>
<tr>
<td>Ethereum</td>
<td><a href="https://ethereum.github.io/solidit/">https://ethereum.github.io/solidit/</a></td>
<td>Working cryptoswap video: <a href="https://www.youtube.com/watch?v=LHCAU5dJ3Mk">https://www.youtube.com/watch?v=LHCAU5dJ3Mk</a></td>
</tr>
<tr>
<td>Most Banks</td>
<td>Most of the banks are experimenting with derivatives constructs</td>
<td></td>
</tr>
</tbody>
</table>
What are the implications for financial risk management?

Pre Dodd-Frank: Bilateral

Reduce/eliminate processes, overhead, and risks associated with the central clearing operation.

Post Dodd-Frank: Mandatory Central

Real-time monitoring and audit capabilities for regulators: system is inherently transparent and accountable.

Greater security, flexibility, and cost savings for entities that are non-centrally cleared; reduces intermediation.
Other Topics and Risk Applications
## Other Topics and Risk Applications

### Blockchain Based Audit, Accounting, and Operational Risk:
- Record keeping and audit
- PKI infrastructure and ownership
- Other smart contract
- Cyber security

### Product Review of Blockchain Clearing and Settlement Solutions:
- 30+ companies/projects with solutions
- Securities, derivatives, repo, syn loan, etc

### Detailed Analysis of Emergent Blockchains Risks:
- Consensus protocol risk analysis
- Classification and taxonomy
- Political risks
- Cyber security

### Cutting Edge of Blockchain Technology:
- Publicly Private Blockchains
- Privacy Preserving Cryptosystems
- Scalability solutions
Create an open consortium of financial risk professionals to study the effects of blockchain technology on their profession.

For anyone who would be interested, please email craig.collins@garp.com.
Satoshi Might Agree

Blockchains are a Financial Risk Management Technology

Genesis Block

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

Source: http://bit.ly/1PoeDU3
Creating a culture of risk awareness®

Global Association of Risk Professionals

111 Town Square Place
14th Floor
Jersey City, New Jersey 07310
U.S.A.
+ 1 201.719.7210

2nd Floor
Bengal Wing
9A Devonshire Square
London, EC2M 4YN
U.K.
+ 44 (0) 20 7397 9630

www.garp.org

About GARP | The Global Association of Risk Professionals (GARP) is a not-for-profit global membership organization dedicated to preparing professionals and organizations to make better informed risk decisions. Membership represents over 150,000 risk management practitioners and researchers from banks, investment management firms, government agencies, academic institutions, and corporations from more than 195 countries and territories. GARP administers the Financial Risk Manager (FRM®) and the Energy Risk Professional (ERP®) exams; certifications recognized by risk professionals worldwide. GARP also helps advance the role of risk management via comprehensive professional education and training for professionals of all levels. www.garp.org

© 2015 Global Association of Risk Professionals. All rights reserved.