Blockchain Breakout Session

Digital Money Symposium
26 January 2016
What is a Blockchain?

A blockchain is a distributed ledger database that uses a cryptographic network to provide a single source of truth.
A blockchain allows untrusting parties with common interests to co-create a permanent, unchangeable and transparent record of exchange and processing without relying on a central authority.
Why is it significant?

• If the **Internet** is a disruptive platform designed to facilitate the **dissemination of information**…..

• …then **Blockchain Technology** is a disruptive platform designed to facilitate the **exchange of value**.
What are the implications?

Disintermediation
- Enables direct ownership and transfer of digital assets without need for an intermediary

Speed & Efficiency
- Faster settlement on a relatively cost effective and efficient network

Automation
- Programmability enables automation of capabilities on the ledger (e.g. smart contracts)

Certainty
- Provides irrefutable proof of existence, proof of process and proof of provenance
Blockchain is bigger than Bitcoin

Blockchains are platforms upon which various applications can be built, well beyond currencies.
Example of Relevance of Blockchain in Banking

Blockchain's distributed ledger model has potential to take steps, time and cost out of financial flows

Financial Intermediaries (Today)

- Requires trusted, centralized intermediaries
- Batch clearing and settlement
- Higher fees and costly infrastructure

Financial Protocol (Emerging)

- No (or fewer) intermediaries required
- Near real-time processing and management
- Lower fees and reduced infrastructure cost
Wide range of contemporary blockchain technologies

Source: Richard Brown, R3
What are smart contracts?

Smart contracts are cryptographically-assured executable business logic that can move value.
Evolution from cyber-libertarian hobby into the mainstream
Growing interest in blockchain

VENTURE CAPITAL ACTIVITY IN BLOCKCHAIN IS ESCALATING

$1BN

$99MM

2013

Global Startup Funding

2015

Google searches

bitcoin

blockchain

Imperial College London
Poll Results

(30 Respondents)
Blockchain Use Cases
Proof of ownership and a marketplace for sales and purchase of digital assets
Company: MyPowers
Enables authenticity of a review through trustworthy endorsements for employee peer review
Company: TRST.im
Decentralized prediction platform for the share markets, politics etc
Company: Augur
Decentralized patient records management
Company: BitHealth (Healthcare IT)
Points based value transfer for ride sharing
Company: Lab2Mox
Digital security trading: ownership and transfer
Companies: Symbiont, Mirror, Spritze, Secure Assets, Birrshares, Coins-e, equityBts, DkMarkets, MUNA
Digitization of documents/contracts and proof of ownership for transfers
Company: Cols (Colored Coins)
Decentralized storage using a network of computers on blockchain
Company: Storj
Decentralized IoT
Home automation: Chimera-icn.io
Industries: Film
t
Provides digital identity that protects consumer privacy
Companies: Shi Card, Uniquid
Escrow/Custodian service
Companies: PlayCoin, Bitplay
A smart contract IT portal executing order fulfillment in ecommerce/manufacturing
Company: UbMS
Digital assets: Improves anti-counterfeit measures
Consumer electronics, Automotive, Degree Verification
Companies: The Real McCoy, ChainLink, Company Degree Of Trust, Other companies: Everpass, BlockVerify
Provides digital identity that protects consumer privacy
Companies: Onename, Q nome
Customer identification: Trustsplan
Elections Voting: Follow My Vote
Enables authenticity of a review
Companies: The World Table
Helps users engage, share reputation and collect feedback
Company: Asimov
Decentralized internet and computing resources to every home and business
Company: ePlug
Digitizing company incorporations, transfer of equity/ownership and governance
Company: Otonomos
From 'Let's Talk Payments
“Whilst it is true that virtually ANY application COULD store its data on a blockchain, it is not true that ANY application WOULD WANT to do this.”

Research grant reviewer, January 2016
Poll Responses on Most Promising Use Cases

- Low-friction low-cost cross-border payments
- Digital legal tender
- Replacing traditional payment schemes
- Corporate action automation
- Exchange of assets with superfast settlement
- Know your customer (KYC)
- Sharing of personal data in innovative distributed and secure ways (e.g. health records)
- Ensuring integrity of code and systems
- Auditing services
- IoT (esp. with Smart Contracts)
- Provenance (e.g. of used cars)
Blockchain Financial Use Cases

**Currency and Payments**
- P2P (including Merchant Wallets)
- Remittances
- Merchant Processing
- B2B, B2C
- Networks & Consortia

**Other Areas of Interest**
- Trade
- Markets and Securities
- AML & Compliance
- Digital Identity
Blockchain Use Cases

Non-financial
Verify Degree

SUCCESS

Qualification verified by Imperial College London

Transaction details
Confirmed by Bitcoin network.

Verify the Existence of NDA Contract: Widget Manufacturing Consultation

View independent proof that the contract has been signed and recorded in a trusted public ledger.

Step 1: Choose a Contract Type (One-Way NDA)
Step 2: Name the parties to the contract, and agree upon the basic outline of the contract
Step 3: Negotiate the detailed terms of your contract, with full version control
Step 4: Sign the final agreed version of your contract
Step 5: Receive proof of signing and verify what has been signed

View Proof of Contract Existence

See your contract hash and signatures recorded on a trusted public ledger.

Your contract has been recorded in the form of a transaction in the Bitcoin Blockchain. The Blockchain is an immutable public ledger, which means it is transparent and easily verifiable through multiple independent sources, and it is not possible to alter or change transaction records.

Therefore, proof of existence of your contract is permanently stored on the Blockchain.

The transaction identification number of your contract is:

b6f1c84693a29040264a6912810c5d7941dec35a2b89eb0e14c18d8

Imperial College Centre for Cryptocurrency Research and Engineering
Blockchain Implementation
Considerations
## Poll results: Biggest Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Number of Respondents</th>
<th>Percentage of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding the most appropriate use cases</td>
<td>16</td>
<td>53%</td>
</tr>
<tr>
<td>Developing an ecosystem</td>
<td>16</td>
<td>53%</td>
</tr>
<tr>
<td>Selecting and implementing an appropriate technology</td>
<td>7</td>
<td>23%</td>
</tr>
<tr>
<td>Security/privacy issues</td>
<td>6</td>
<td>20%</td>
</tr>
<tr>
<td>Scalability</td>
<td>3</td>
<td>10%</td>
</tr>
</tbody>
</table>

**Additional challenges identified:**
Legal/Regulatory (2), Stability/resilience of platform/provider (2), Engagement (1)
Timeframe to Production

- 10 years or more: 13%
- 5-9 years: 10%
- 2-4 years: 50%
- Within 1 year: 14%
- We are using it already: 3%
- No answer: 13%

Dominant Emerging Platform

- Bitcoin: 7%
- Ethereum (Smart Contracts): 20%
- OpenChain (Side Chains): 10%
- Other: 10%
- Don't know: 63%

Other: Credits (10%), Hyperledger R3 (3%)
Challenges to blockchain adoption

• Determining optimal blockchain use cases
• Requires building an ecosystem/network of participants
• Technology is not yet industrial grade
• Requires integration into legacy systems or migration of current tech
• Requires fundamental business process redesign
• Will require adaptation of some regulatory and legal frameworks
• Unless asset remains digital, full benefit of blockchain cannot be fully realized
Comments
Your experiences
Q&A

Contacts: morgan.mckenney@citi.com and wjk@imperial.ac.uk