Lunch Session 3: Blockchain and cryptocurrencies – all you need to know

Wednesday, September 26
12:30-14:00
• Ari Laakkonen, AIPPI (Moderator)

• Fraser Rowand, Rowand LLP
• John Lee, Bunz
• Paolo Cioppa, R3
• Calum Smyth, Barclays
Fraser Rowand, Rowand LLP

John Lee, Bunz

Paolo Cioppa, R3

Calum Smyth, Barclays
Themes

• Blockchains are not just cryptocurrencies
• Blockchains already involve entire industry sectors
• Blockchains enable security measures where otherwise could be complex to implement
• Fraser Rowand, Rowand LLP
• John Lee, Bunz
• Paolo Cioppa, R3
• Calum Smyth, Barclays
Blockchain Primer
Blockchain Primer

HASH FUNCTION

Text → Hash Function → AD89F2A3

Different Text → Hash Function → 893BD85C

PUBLIC-PRIVATE KEY PAIRS

Private key → Key Generator → Public Key

ONE WAY ONLY!
Blockchain Primer

Transactions

Inputs
- Fraser’s coins
- Fraser’s signature

Outputs
- Payable to Ari’s account
- Conditions on withdrawal

- Pointer to UTXO
- Unlocking script

- Output address
- Locking script
Blockchain Primer

Block N

Header

Transaction
Transaction
Transaction
Transaction
Transaction
Transaction
Transaction
Transaction
Transaction
Transaction
Transaction
Blockchain Primer

Block N

Header

Hash

Block N+1

Header

Hash

Block N+2

Header
Blockchain Primer

• “Emergent Consensus”
• Decentralized and Trustless
• Independent verification by nodes that transactions and newly mined blocks are legitimate
Blockchain Primer
Blockchain Primer

- Mining Nodes compete to create next block
- Proof-of-Work
- “Difficulty” – Hash of block header must be lower than a target number
- Miners adjust “nonce” in header and re-try until they succeed, or a valid new block is produced by another miner
- Successful miner earns fees and new coins
Blockchain Primer

• Ongoing innovations in blockchain
  – Unlocking scripts & smart contracts
  – Split keys
  – Non-cryptocurrency blockchain applications

• New models – how does consensus emerge? What is the economic/game theory that secures the network?
• Fraser Rowand, Rowand LLP
• **John Lee, Bunz**
• Paolo Cioppa, R3
• Calum Smyth, Barclays
Blockchain Community and Understanding of IP
Smart contracts

• Introduced by Ethereum; Smart contracts holds the ability to decentralize computing

• Every Token, Asset, Functions are a type of smart contract
Variety in Blockchain Ecosystem

Protocols
- ZCASH
- Qtum
- DASH
- Bitcoin
- CARDANO FOUNDATION
- Cardano
- Dash
- Ripple
- Litecoin
- Ethereum
- Cosmos
- Aion
- Polkadot
- Lightining Network
- EOS
- ZEPPLEIN
- NEO
- RSK
- Raiden
- Plasma
- IOTA

Tools
- uPort
- Basecoin
- STAKI
- Civic
- Evernym
- Kin
- Factom
- Decentraland
- Factom
- Estonian

Value Exchange
- Sia
- Golem
- 1
- Factom
- Dmarket
- Gnosis

Specialized Usage
Definition of Blockchain/DLT

Decentralized*
*Except for PoA and private chain

Immutable*
*Except Ethereum EIP Process to recover funds

Transparency*
*Except you can track wallet ID’s across multiple transactions

Smart Contract*
*Except not all DLT or Blockchain allow for smart contracts

No Central Failure points*
*Except most protocols are not resistant to Quantum attacks

Defining Blockchain and DLT is dependent upon your audience
Blockchain Community

• Blockchain and DLT community is in itself distributed and unique
• Each community has their own ethos and development/Education path
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as intermediaries of trust between parties engaged in economic payments. While the system works well enough and has grown over the years, it still suffers from the inherent weaknesses of the trust-based model. Completely non-reversible transactions are not realistic, since financial institutions cannot prevent mediating disputes. The cost of mediating these transactions is high, limiting the practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of the ability to make non-reversible payments for non-reversible services. With the possible exception of those in need for fast spans, merchants must be wary of their customers, handling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person using physical currency, but no mechanism exists to make payments over a communications channel without a trusted third party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impossible to reverse would protect sellers from fraud, and reduce economic mechanisms can be improved to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed transaction server to generate computational proof of ownership and order of events. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Introduction

With obvious inherent connections to the Internet's e-commerce, these systems were adapted to other domains, such as in technology initiatives to onboard to the existing technological systems of the world. The authors demonstrated through the use of the Bitcoin, Ethereum, and other similar cryptocurrencies. These developments have been adopted to different industries, such as in the creation of new, high-value currencies. For this reason, a simple understanding of the underlying technology is necessary to understand the potential of blockchain. In this case, we provide an overview of an application that we hope will make blockchain adoption a reality.

3. Driving Factors

There are many factors that can significantly impact the adoption rates of new technologies. However, the factors that seem to have the most significant impact are the following:

- Technical feasibility: The technology must be technically viable and usable.
- Economic viability: The technology must be economically viable for users.
- Social acceptability: The technology must be socially acceptable to users.
- Environmental impact: The technology must be environmentally friendly.
- Security: The technology must be secure and reliable.

The factors that impact the adoption rates of blockchain technologies are many and complex. It is important to consider all of these factors when planning the implementation of new technologies.
Licenses

- ERC/EIP process – de facto Public Ethereum’s standardization process

- Licenses
  - Bitcoin: MIT
  - Ethereum: ??? (exploring MIT, MPL, LGPL)
  - Ethereum Clients: Varying levels of GLP
  - Hyperledger: Apache 2.0
  - R3’s Corda: Apache 2.0
Community Expertise
IP potential

http://cipher.ai/blockchain-patents-control-technology/
Thank you
• Fraser Rowand, Rowand LLP
• John Lee, Bunz
• **Paolo Cioppa, R3**
• Calum Smyth, Barclays
2018 AIPPI World Congress

SEPTEMBER 2018
The Problem?

Industries are forced into a cost trap (not just banks)

- Legacy infrastructure is leading to an increase in IT expenditure
- Reconciliation and dispute resolution are leaving firms with vast inefficiencies
- Clearing and settlement that rely on third parties and record loans and securities, are forcing unavoidable cost implications on the industry
- Trade processes are slow, manual, cumbersome and expose risk

Expensive legacy technology and inefficient business processes are a problem not just faced by banks – blockchain technology can be leveraged by many other industries to realize similar efficiencies

The impact:

Projected IT spend by banks globally in 2017
$215bn

Global annual banking operating costs
$2.6tr
The Solution

Blockchain will provide one version of the truth

CENTRALIZED AND DECENTRALIZED LEDGERS

Highly fragmented data and increased risk

Transactions take days to confirm and validate. Trade data is stored locally by each party and tied directly to a transaction.

Regulatory reporting is complex, tedious and suffers from human error.

All transactions are controlled by a single centralized asset ledger, meaning risk exposure is tied to one single entity.

DISTRIBUTED LEDGERS

Data is complete, consistent, timely, accurate, and widely available between parties relevant to a transaction.

Transactions will be executed exactly as the protocol commands, removing the need for a trusted third party and additional action to meet regulatory requirements via smart contracts.

Blockchain does not have a central point of failure, ensuring higher security.

Simplified reconciliation and near real-time validation.
A Powerful Vision for the Future: Instantaneous, Secured, Error-Free Data Enabled by Blockchain Technology

Blockchain technology offers the opportunity for companies to profit handsomely by helping redesign global business:

Current State of the Financial Services Marketplace
- Highly fragmented and increased risk
- Trade data stored locally by each party to a transaction
- Transactions take days to confirm and validate
- Regulatory reporting is tedious and suffers from human error

Envisioned Future State Powered by Blockchain
- Unified by one, interoperable ledger
- Reduced systemic, counterparty and security risk
- Simplified reconciliation and near real-time validation
- Improved regulatory reporting = less regulatory capital
- Once-in-a-generation opportunity to transform the economics of transaction processing between regulated financial institutions through drastic cost reduction and massive improvements in capital allocation
Section 01

Introducing R3
Stage 1: Our members led us to research the role of blockchain in financial services

Developing an acute understanding

• R3 was founded through a realization that blockchain could be transformative for the operational challenges within financial services
• First R3 roundtable was attended by eight banks in Sept 2014 to understand the appetite within financial services
• 1st proof of concept delivered for FX settlement on blockchain
• R3 became the formal advisor to 42 bank members in Nov 2015
• R3 launched the Architecture Working Group, Product/Use Case Working Group, and Regulatory Working Group to drive understanding
R3: Leading A Global Ecosystem in Blockchain Innovation

<table>
<thead>
<tr>
<th>R3’s 100+ Members</th>
<th>Includes global financial institutions &amp; companies in banking, insurance, real estate, and asset management</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ultimate end users and beneficiaries of applications built on Corda, R3’s members drive application development in the R3 Incubator/Accelerator</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R3’s 200+ Partners</th>
<th>Includes enterprise tech. companies and software vendors such as Microsoft, Intel, Amazon, Oracle, Accenture, and Finastra</th>
</tr>
</thead>
<tbody>
<tr>
<td>R3’s partners help develop blockchain applications on Corda and assist in their go-to-market and operation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R3’s 40+ Shareholders</th>
<th>R3’s biggest members and customers bought into the company’s record-breaking Series A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many of the world’s largest financial institutions now have a vested interest in the success of the Corda platform</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R3’s 20+ Member Regulators</th>
<th>Includes banking/market supervisors in global financial centers like Singapore, Hong Kong, &amp; Abu Dhabi</th>
</tr>
</thead>
<tbody>
<tr>
<td>By including regulators in product development, new applications identify regulatory requirements early in their development lifecycle</td>
<td></td>
</tr>
</tbody>
</table>

Corda’s two-sided network of Users and Builders has grown exponentially over the last two years. Corda provides blockchain developers with a powerful platform to launch their applications and capture blockchain’s lucrative network effects.
The R3 Member Network

Regulators:
20+ Regulators and Central bank members including:
• HKMA
• AMF Montreal
• Abu Dhabi Global Markets

Partners:
100+ partners which includes system integrators & advisory, independent software vendors, Infrastructure/technology partners and network service providers
Stage 2: The Creation of Corda

Enterprise grade blockchain built from the ground up

- An audit of blockchains proved nothing could stand up to the complexity, regulatory demands and rigor needed for financial services
- Corda was made public in April 2016, and open-source in November 2016
- Additionally over 50 members joined the original 42 bank members
- R3 research team completes experiments in areas including payments, digital fiat currencies, KYC, reference data, syndicated loans, Trade Finance (Open Account and Doc Trade) and derivatives
- Corda Version 1 shipped October 2017 promising API stability
- Corda Version 2 Shipped November 2017
- Corda Version 3 shipped March 2018 promising additional wire stability
- R3 Corda Enterprise went live in June 2018

Corda is uniquely architected for privacy, interoperability and immutability
Illustrative CorDapp / Project Portfolio

<table>
<thead>
<tr>
<th><strong>Incubator</strong></th>
<th><strong>Accelerator</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ChainThat – Insurance Accounting &amp; Settlement</td>
<td>LenderComm – Syndicated Lending (Finastra)</td>
</tr>
<tr>
<td>Confidential – Mortgage Loan Servicing</td>
<td>Digital Assets</td>
</tr>
<tr>
<td>Indigo – Individual Self-Sovereign Identity (Sovrin)</td>
<td>Digital Assets</td>
</tr>
<tr>
<td>Janus – Asset-backed Securitization</td>
<td>Digital Identity</td>
</tr>
<tr>
<td>LEIA II – Corporate Identity &amp; KYC (Synechron)</td>
<td>Digital Identity</td>
</tr>
<tr>
<td>Lionrock – Currency on Ledger (HKMA)</td>
<td>Digital Cash</td>
</tr>
<tr>
<td>Sibi – Workers’ Comp. Processing (Cognizant)</td>
<td>Insurance</td>
</tr>
<tr>
<td>Pedigree – Private Company Share Issuance on Ledger</td>
<td>Digital Assets</td>
</tr>
<tr>
<td>CommodDT – Natural resources workflow reconciliation</td>
<td>Trade Finance</td>
</tr>
<tr>
<td>42 – Club loan syndication, workflow, reconciliation</td>
<td>Digital Assets</td>
</tr>
<tr>
<td>Confidential – Central Bank Digital Currency (2x Sovereignties)</td>
<td>Digital Cash</td>
</tr>
</tbody>
</table>

+10 other earlier stage projects

<table>
<thead>
<tr>
<th><strong>Accelerator</strong></th>
<th><strong>Accelerator</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>LenderComm – Syndicated Lending (Finastra)</td>
<td>Digital Assets</td>
</tr>
<tr>
<td>Bravo – HQLA Liquidity Provision (HQLA*)</td>
<td>Digital Assets</td>
</tr>
<tr>
<td>Maison – Regulatory Reporting</td>
<td>Digital Assets</td>
</tr>
<tr>
<td>Marco Polo – Open Account TF (TradeIX)</td>
<td>Trade Finance</td>
</tr>
<tr>
<td>SIA – Consortium Network for Invoice Financing</td>
<td>Trade Finance</td>
</tr>
<tr>
<td>Threadbo II – FX Settlement (Calypso)</td>
<td>Digital Assets</td>
</tr>
<tr>
<td>Voltron X – Letters of Credit on Ledger</td>
<td>Trade Finance</td>
</tr>
<tr>
<td>B3i – Major insurance consortium efficiency project</td>
<td>Insurance</td>
</tr>
<tr>
<td>InsurWave (EY / Guardtime) – Maritime Insurance</td>
<td>Insurance</td>
</tr>
</tbody>
</table>

+30 non R3-led partner pilots in production
Corda

Immutability
Records stored in a cryptographic manner assures lineage and evidence of tampering

Mutual verification
Shared facts are agreed upon by a variety of consensus mechanisms

Security & Privacy
Transaction information is propagated only to relevant nodes to ensure strict data privacy, whilst maintaining the assurance of validity and uniqueness

Easy Integration
Re-use existing developer skills and make integration with bank systems easy and safe. Contracts can be coded in modern, standard languages like Java

Consistent Shared Facts on Ledger
Records of shared facts including financial agreements are consistent across entities, only with those party to the transactions

Smart Contracts
Business Logic is encapsulated and executes in a deterministic, tamper evident manner

Interoperability
Corda retains this privacy but allows any node to transact without creating islands of assets or liquidity issues

Transparency
Consensus achieved at individual deal level, rather than system level. Supports a variety of consensus mechanisms
**Broadcast Blockchain**

<table>
<thead>
<tr>
<th>Bank A’s Ledger</th>
<th>Bank B’s Ledger</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Fact</td>
</tr>
<tr>
<td>1</td>
<td>Bank A pays B $5.</td>
</tr>
<tr>
<td>2</td>
<td>Bank B purchases bond X from issuing bank A.</td>
</tr>
<tr>
<td>3</td>
<td>Bank C purchases bond X from bank B.</td>
</tr>
<tr>
<td>4</td>
<td>Bank C enters a credit default swap with bank D.</td>
</tr>
<tr>
<td>5</td>
<td>Bank D owes bank B $10.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bank C’s Ledger</th>
<th>Bank D’s Ledger</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Fact</td>
</tr>
<tr>
<td>1</td>
<td>Bank A pays B $5.</td>
</tr>
<tr>
<td>2</td>
<td>Bank B purchases bond X from issuing bank A.</td>
</tr>
<tr>
<td>3</td>
<td>Bank C purchases bond X from bank B.</td>
</tr>
<tr>
<td>4</td>
<td>Bank C enters a credit default swap with bank D.</td>
</tr>
<tr>
<td>5</td>
<td>Bank D owes bank B $10.</td>
</tr>
</tbody>
</table>

**Corda**

<table>
<thead>
<tr>
<th>Bank A’s Ledger</th>
<th>Bank B’s Ledger</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Fact</td>
</tr>
<tr>
<td>1</td>
<td>Bank A pays B $5.</td>
</tr>
<tr>
<td>2</td>
<td>Bank B purchases bond X from issuing bank A.</td>
</tr>
<tr>
<td>3</td>
<td>Bank C purchases bond X from bank B.</td>
</tr>
<tr>
<td>4</td>
<td>Bank C enters a credit default swap with bank D.</td>
</tr>
<tr>
<td>5</td>
<td>Bank D owes bank B $10.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bank C’s Ledger</th>
<th>Bank D’s Ledger</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Fact</td>
</tr>
<tr>
<td>1</td>
<td>Bank A pays B $5.</td>
</tr>
<tr>
<td>2</td>
<td>Bank B purchases bond X from issuing bank A.</td>
</tr>
<tr>
<td>3</td>
<td>Bank C purchases bond X from bank B.</td>
</tr>
<tr>
<td>4</td>
<td>Bank C enters a credit default swap with Bank D.</td>
</tr>
<tr>
<td>5</td>
<td>Bank D owes bank B $10.</td>
</tr>
</tbody>
</table>

Blockchains do not need to share data with all parties
The Corda Ledger

The ledger from each peer’s point of view is the union of all intersections with other network peers

ALICE = {1, 7}

BOB = {1, 7, 6, 5}

CARL = {9, 4, 6, 5, 2, 3}

DEMI = {2, 3, 8}

ED = {9, 4, 8, 3}
Anatomy of a bilateral ledger

- There is no “central ledger”
- Each network peer maintains a separate vault of facts
- Facts can be thought of a row in a table
- All peers to a shared fact store identical copies
- Not all on-ledger facts have to be shared with other peers

<table>
<thead>
<tr>
<th>Id</th>
<th>Fact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>“Much consensus”</td>
</tr>
<tr>
<td>7</td>
<td>“So bilateral”</td>
</tr>
<tr>
<td>11</td>
<td>“Wow ledger”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Id</th>
<th>Fact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>“Much consensus”</td>
</tr>
<tr>
<td>6</td>
<td>“Very fact”</td>
</tr>
<tr>
<td>7</td>
<td>“So bilateral”</td>
</tr>
<tr>
<td>5</td>
<td>“amaze network”</td>
</tr>
</tbody>
</table>
Agreements as represented on Corda

**Contract Code**
- Issue
  - rule #1 (code)
- Pay
  - rule #1 (code)
  - rule #2 (code)

**Legal Prose**
ISSUER:____ and OWNER:____ agree that ISSUER owes ASSET:____
QUANTITY:____ to OWNER, redeemable on demand under the following circumstances

**Parties to this Agreement**

**State of Cash Agreement**
- Contract Code Reference
- Legal Prose Reference
- Whereas:
  - Issuer: Barclays Bank PLC
  - Issue Date: 1 Jan 2016
- Amount: 100
- Currency: USD
- Owner: XYZ Shipping Ltd

**Smart Contract Templates**

**Attachment Service for Document Storage**
Corda controls the evolution of agreements

The “agreement” in this example is the agreement between the issuer and the owner, which evolves, as the state gets updated.
To avoid the double spend issue (whereby a single input state is spent twice), Corda will use a pluggable uniqueness service: the notary. This will sign each proposed transaction to confirm it has not been spent already. The transaction is then confirmed.
Interaction Between Lawyers and Corda

**Varying timeframes**

<table>
<thead>
<tr>
<th>Short Term</th>
<th>Medium Term</th>
<th>Long Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Advising clients regarding structure of a DLT network (i.e. allocating liability)</td>
<td>• Ensuring that the correct legal prose is coded (and only to the extent necessary)</td>
<td>• Working with developers to create bespoke coded smart contracts</td>
</tr>
<tr>
<td>• Ensure compliance with regulations (i.e. data security, data privacy)</td>
<td>• Reviewing smart contracts in sandbox environments to ensure they perform correctly</td>
<td></td>
</tr>
<tr>
<td>• Review network agreements</td>
<td>• Entering the correct legal prose into the correct fields during negotiation (see Barclay’s Smart Contract Template presentation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Start developing smart contract templates and contributing to a template library</td>
<td></td>
</tr>
</tbody>
</table>
Thank You
• Fraser Rowand, Rowand LLP
• John Lee, Bunz
• Paolo Cioppa, R3
• Calum Smyth, Barclays
Calum Smyth

Cryptocurrencies & the Blockchain Patent Landscape
Cryptocurrencies in numbers

- 1,320: 2018 cryptos
- $0.06: 2010 Bitcoin
- $19k: 2017 Bitcoin
- 73 TWh: 2017 power consumption
- $18 bn: H1 '18 value
- 706 ICOs: 2018 cryptos
Story of a Revolution

- Encrypted electronic cash – 1990s
- Problem: digital copying & double spending
- 2008 – Satoshi Nakamoto published Bitcoin paper
- Cyberphunk philosophy & distributed control
- 2011 - Silk Road, dark web, drugs and weapons
- The first Initial Coin Offering 2013
- “I’m Satoshi Nakamoto” – Craig Wright 2016
- 2017 & hyper-volatility
- Altcoins & regulatory questions
How it works - Bitcoin

- 10 mins
- 21m BC
- 16x10^{18}
- 12.5 BC
- Alt-coins
Pitfalls

- Energy Consumption
- Security
- Speed
- Consumer Protection
- Volatility
Initial Coin Offerings (ICO\textsc{\textregistered}s)

- Raising funds for DLT company or project
- No shares - investors buy ‘tokens’ that are then traded
- Token is a right to use end product when complete
- Speculative?
- Pump & Dump
- Regulation & securities
Patent landscape

- Filings start: 2014
- Filings to date: 3,653
- Families >1 grant: 222
- Estimated prosecution cost to date: $30m
Total DLT families

Pending & Granted

CoInplug: 61
IBM: 59
Alibaba: 50
Bank of America: 39
Beijing Rui: 31
nChain: 29
MasterCard: 27
Hangzhou Fuzamei: 24
Jiangsu Tongfudun: 23
China United: 21
Bubi Beijing: 20
Cloudminds Shenzhen: 19
Hangzhou Yumphant: 18
Cognitive Scale: 16
Nokia: 16
Remaining 732 organisations

2,004
Global companies – US grants

$2.4 million spent in obtaining granted US patents
Future trends?
Thanks for your attention!