A primer on blockchain technology and its applications

Adrien Treccani, Ph.D.

Swissquote Conference 2017
Finance in a nutshell

Transfer of value
Electronic transfer (one bank)
Electronic transfer (two banks)

How to make sure consolidated accounting is correct / no fraud?
Electronic clearing

Clearing agency

Holds commercial banks’ deposits

Central bank

-1000

-1000

+1000

Commercial banks' deposits
Complex system

Potential frictions
Cost
Latency
Errors
Credit risk
Blockchain motivation

“Blockchain could reduce banks’ infrastructure costs by US$15 – 20 billion per annum by 2022.” Santander Report

Peer-to-peer payment
- Inexpensive
- Fast
- Atomic

Internet
Blockchain motivation (cont’d)

Centralized network
- High barrier-to-entry
- Pyramidal governance
- Oligopolies
- Subject to politics

Distributed network
- Frictionless entry
- Democratic governance
- Global access
- Algorithmic validation
Bitcoin network

Distributed payment network
Globally available
No central authority (e.g., no bank)
Consensus-based “democracy”

Key numbers
• 20M users
• 4 tx/s
• $250M/day
• ~30 min settlement

Use case I: Bankless merchant
Use case II: Remittance
Bitcoin currency

No stabilization policy
Strict 21M cap on bitcoin supply
Deflationary monetary policy

Key numbers
- $100.0B+ market cap
- $7000 ATH price
- 150K merchants

Double spending problem

How to avoid users spending the same money twice?
Double spending solution (centralized)

I have canceled your second order.

Don’t ever try again to spend more than you have at my expense.
Double spending (distributed)

**Challenge**

- No central authority
- No chronology
- No trust between users

*How to reach an agreement (consensus) on which transactions to validate/ignore?*
Blockchain *trust machine*
Traceability

Real-time example
Blockchain storage

**Distributed persistence**

Users maintain full copy of the blockchain
- Entire history of transactions
- High redundancy
- Peer-to-peer, public network

**Key numbers**
- 5000+ copies
- 140Gb of data
- 280M txs
### One-slide cryptography fast-track

<table>
<thead>
<tr>
<th>Traditional finance</th>
<th>Bitcoin ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account ID</strong></td>
<td><strong>Address</strong></td>
</tr>
<tr>
<td><em>receive payments</em></td>
<td><em>1BvBMSEYstWetqTFn5Au4m4...</em></td>
</tr>
<tr>
<td>IBAN number</td>
<td></td>
</tr>
<tr>
<td>GB87BARC20658244971655</td>
<td></td>
</tr>
<tr>
<td><strong>Credentials</strong></td>
<td><strong>Private key</strong></td>
</tr>
<tr>
<td><em>spend money</em></td>
<td><em>5Kb8kLf9zgWQnogidDA76MzPLgT...</em></td>
</tr>
<tr>
<td>Card + PIN code + nice smile</td>
<td>Use your secret PIN and smile to your banker</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td><strong>Digital signature</strong></td>
</tr>
<tr>
<td><em>prove ownership</em></td>
<td><em>Use private key to prove ownership of address</em></td>
</tr>
<tr>
<td>Bank statement</td>
<td></td>
</tr>
<tr>
<td>Ask your banker for a bank statement</td>
<td></td>
</tr>
</tbody>
</table>
Payment processing

1. Create transaction
   with destination address

2. Digitally sign tx
   with private key

3. Broadcast tx
   to other network participants

4. Wait for inclusion in blockchain
   By whom ??
Ledger consensus
Miners
Proof-of-work

**Stupid but complex problem**
Miners need to solve proof-of-work problem
- Required for insertion of new block
- Extremely computationally intensive
- Special hardware + electricity costs

**Bitcoin reward for new blocks**
Miners are rewarded with bitcoins
- Freshly created bitcoins (inflation)
- Transaction fees
Network security

2011/10/08 02:00
Hash Rate TH/s: 11
Buy bitcoins

e.g. bitstamp.net or coinbase.com
Power consumption

Mining: 350 megawatts and growing (abt consumptions of 290,000 US homes)
Beyond bitcoin currency
And beyond payment... programmable money

"Code is law"

**Ambition**

Replace lawyers by software engineers
Replace courts by autonomous software
Smart contract

Transactions
send value to contract

Events
send information to contract

Transactions
send value from contract

Events
send information from contract

Logic
State
Use case: Multi-signature account

<table>
<thead>
<tr>
<th>Logic</th>
<th>Allow withdraw if and only if</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. CEO orders withdraw, or</td>
</tr>
<tr>
<td></td>
<td>2. 2 out of 3 assistants order</td>
</tr>
<tr>
<td></td>
<td>withdraw and volume smaller</td>
</tr>
<tr>
<td></td>
<td>than 1M a day</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Balance of the contract</td>
</tr>
<tr>
<td></td>
<td>• Authorized assistants</td>
</tr>
<tr>
<td></td>
<td>• Amount withdrawn in last 24h</td>
</tr>
</tbody>
</table>

Multi-signature account logic includes:

1. CEO orders withdraw, or
2. 2 out of 3 assistants order withdraw and volume smaller than 1M a day

Key elements:

- Multi-signature
- CEO
- Assistants
- Balance of the contract
- Authorized assistants
- Amount withdrawn in last 24h
Smart contract platform
Case study: The DAO

“Do smart contracts remove all form of risk?”
Case study: The DAO
Case study: The DAO

THE DAO IS CODE.

GET DAO TOKENS
Case study: The DAO
Discussion

For further discussion: treccani@metaco.com

- The challenge of storing cryptocurrencies
- What about central-bank-issued digital currencies?