Blockchain(s) and Potential Impacts on Reconciliation

ECB OMG Meeting, 20. Sep. 2018
Dr. Udo Milkau, Chief Digital Officer, Transaction Banking
DZ BANK AG, Frankfurt
Why?

BLOCKCHAIN DEPLOYMENTS TO SAVE BANKS MORE THAN $27BN ANNUALLY BY 2030

*On-chain Settlement Costs to Fall by 11% Compared With Current Levels*

Hampshire, UK – 1st August 2018: A new study from Juniper Research has found that blockchain deployments will enable banks to realise savings on cross-border settlement transactions of more than $27 billion by the end of 2030, reducing costs by more than 11% per on-chain transaction.

According to the research, *The Future of Blockchain: Key Vertical Opportunities & Deployment Strategies 2018-2030*, banks that integrate blockchain will achieve cost reductions not just in payment processing and reconciliation, but in treasury operations and compliance. Indeed, the research argued that in compliance, automation of identity/money-laundering checks, allied to capability of the blockchain to verify the digital identity of an individual, should enable savings of up to 50% of the existing costs base within a few years.

However, the research cautioned that the need to parallel-run blockchain-based services with legacy systems would mean that savings would not be realised for several years after initial deployment, with annual cost reductions not reaching $1 billion per annum until 2024.

Blockchain Myths: Trust, Truth, Revolution, and the Best Money Ever

Impossibility of Distributed Consensus vs. Game-theoretical Synchronisation in “Bitcoin” (with assumptions and limitation, of course)

Fischer, Lynch and Paterson (1985)

Impossibility of Distributed Consensus with One Faulty Process

MICHAEL J. FISCHER
Yale University, New Haven, Connecticut

NANCY A. LYNCH
Massachusetts Institute of Technology, Cambridge, Massachusetts

AND

MICHAEL S. PATERSON
University of Warwick, Coventry, England

Abstract. The consensus problem involves an asynchronous system of processes, some of which may be unreliable. The problem is for the reliable processes to agree on a binary value. In this paper, it is shown that every protocol for this problem has the possibility of nontermination, even with only one faulty process. By way of contrast, solutions are known for the synchronous case, the “Byzantine Generals” problem.

Source: Journal of the Association for Computing Machinery, Vol. 32, No. 2, April 1985, pp. 374-382
There is not THE blockchain ...
## Blockchain in Reality: Efficiency, Decentralization, Finality, and Security

<table>
<thead>
<tr>
<th></th>
<th>Efficiency</th>
<th>Decentralization</th>
<th>Finality</th>
<th>Cyber Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bitcoin</strong></td>
<td>No by design: proof-of-work has to be inefficient by design</td>
<td>Not in reality: onion-like structure w. rent-seeking minors</td>
<td>No by design: eventual consistency (probabilistic approach in a repeated game)</td>
<td>Not more: 51% attacks on two minor coins*** were successful in May 2018</td>
</tr>
<tr>
<td><strong>IOTA</strong></td>
<td>unclear (?)</td>
<td>No: central “Coordinator” (to be trusted by participants)</td>
<td>No: no finality (endless tree of validations)</td>
<td>No: validation by participants open for Sybil attacks</td>
</tr>
<tr>
<td><strong>Resilience</strong></td>
<td>Yes: limited number of participants, but redundancy</td>
<td>No by design: private Distributed Ledgers require central facilities</td>
<td>Yes: final confirmation by designated nodes</td>
<td>Yes: BFT as established tool for cyber resilience</td>
</tr>
</tbody>
</table>

* DAG: Directed Acyclic Graph; ** Byzantine Fault Tolerance; *** on Bitcoin Gold and on Monacoin
Agenda: Practical Applications of the Tool-set “Blockchain” / DLT

1. Legacy and General Problem: Synchronisation

2. Atomic Protocols (replacing unidirectional “teletype” messages)

3. Integrated Settlement (direct final transfer; see also TIPS)

4. Consensus about Future Actions ("Smart Contracts", i.e. Scripts)

5. The Question of Operating Models: bilateral, distributed, centralised?
1. The Legacy of Unidirectional Protocols: the good, old teletype …
1. Challenges of Missing Synchonisation (illustrative and simplified)

A) Reconciliation

Front-office

Execution (e.g. by a electronic trading venue)

CCP

Back-office (legal sub-ledger)

General ledger (“IFRS”)

Valuation of Collaterals (based on internal models)

Account

B) Confirmation(s)

Trade Repository

Back-office (legal sub-ledger)

General ledger (“IFRS”)

Valuation of Collaterals (based on internal models)

Account

C) Transperancy

Collateralisation (CCP or bilateral)

D) Methodologies

Payments
2. Atomic Protocols = message + confirmation + time out (in case of problems)

---

**Ripple InterLedger Protocol (ILP)**

**SEPA Instant Payments + TIPS**

3. Synchronised Settlement versus DvP

Ripple InterLedger Protocol (ILP)

- Bilateral Agreement with Finality
  - Public Clearing, Collateral Mgmt. and Repository
  - General Ledger
  - General Ledger

SEPA Instant Payments + TIPS

- TIPS with direct link to (existing) liquidity in TARGET2

3. Synchronised Settlement … @ Project Ubin 2.0

Source: www.mas.gov.sg
4. Consensus about of Future Actions …

A Protocol based on “Smart Contracts”

Bilateral Agreement with Finality

Public Clearing, Collateral Mgmt. and Repository

General Ledger General Ledger

Agreement (illustrative)

A. Header:
   - Counterparty A: xxx …
   - Counterparty b: yyy …
   - Nominal: $$$ …

B. Payments:
   - Cashflow (i) … (x)
   - Charges / Fees

C. Triggers/Actions:
   - If – then - else …

D. Collateral:
   - Method of calculation …
   - Input … (“Oracles”)

E. Options (Put, Call, etc.):
   - On message_of_A …

…

X. General clauses:
   - legal text …

Z. Default:
   - Definition xxx …
4. … but Missing Standards and Diverging Objectives …

Various Languages and Templates:

- ISDA Common Domain Model / C. Clack et al. "Smart Contract Templates"
- Axoni’s AxLang / Scala
- Corda Smart Contracts (Contract Catalogue Templates)
- Digital Asset Modeling Language (DAML)
- Nivaura’s Legal Markup Language (LML)
- OASIS LegalXML
- ConsenSys’ OpenLaw Markup Language
- … et cetera

Diverging Objectives, what a “Smart Contract” Script should represent:

- Description of a “contract“ (agreement including all events during the life cycle)
- Description of a process/workflow (e.g. issuance of an instrument)
- Description of a “market” (participants with different roles and responsibilities)
- … and other concepts
5. … and the Question of Operating Models: bilateral, distributed, centralised?

- **Bilateral Messages / Atomic Protocol**
  - "Scheme"

- **Distributed Ledger with Nodes**
  - "Initiative"

- **Central (Cloud) Platform**
  - "Utility"

Governance with a central body for rules & regulation, future development, on-boarding, dispute management et cetera.
A Conclusion

As we approach the time of year for retrospectives and predictions, I find myself thinking a lot about the evolution of distributed ledgers in financial services. The past year has been instructive in shedding light on the future trajectory of the technology. …

This past year also brought more rational expectations over the technology's current capacity to achieve the scale and processing power needed for large-scale solutions. …

… the industry has come to the realization that blockchain's potential isn't limitless and as companies focus on the nuts-and-bolts of development, applications need to demonstrate sufficient ROI and client value …

We've learned what works and what doesn't. We've seen the technology's limitations. And we understand that it is still very much a work in progress. …

… the technology simply doesn't have the scale or capacity to match the robust processing engines that underpin the US capital markets today …

But we also recognize that there will likely be many blockchain applications in use before it is ready to become the standard in a market as big as the US equities markets. …