# 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

DZ BANK
Die Initiativbank

# Why?

JUNIPER RESEARCH

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

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

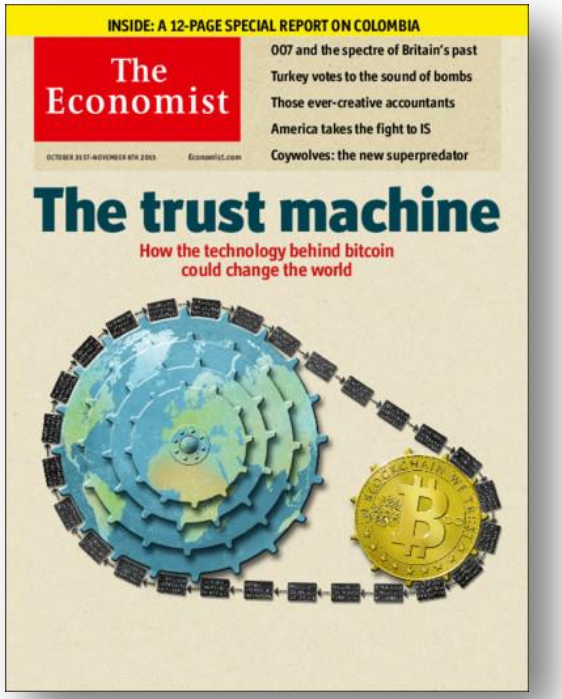
Hampshire, UK – 1st August 2018: A new study from Juniper Research has found that blockchain deployments will enable banks to realise savings on cross-border settlement transactions of more than $27 billion by the end of 2030, reducing costs by more than 11% per on-chain transaction.

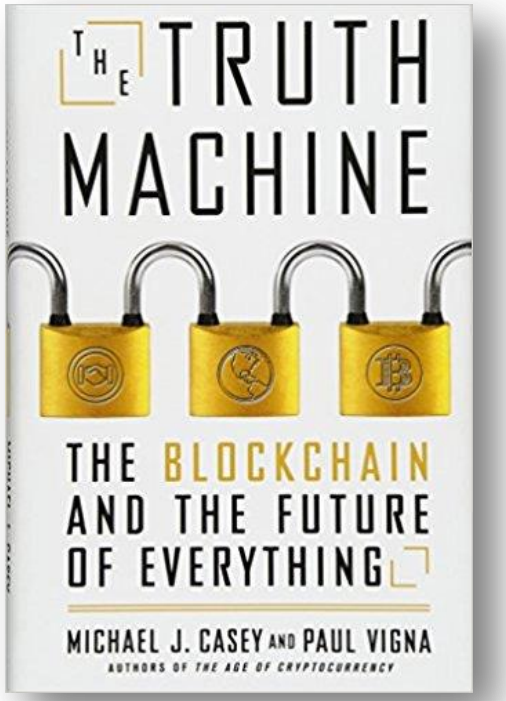
According to the research, The Future of Blockchain: Key Vertical Opportunities & Deployment Strategies 2018-2030, banks that integrate blockchain will achieve cost reductions not just in payment processing and reconciliation, but in treasury operations and compliance. Indeed, the research argued that 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.

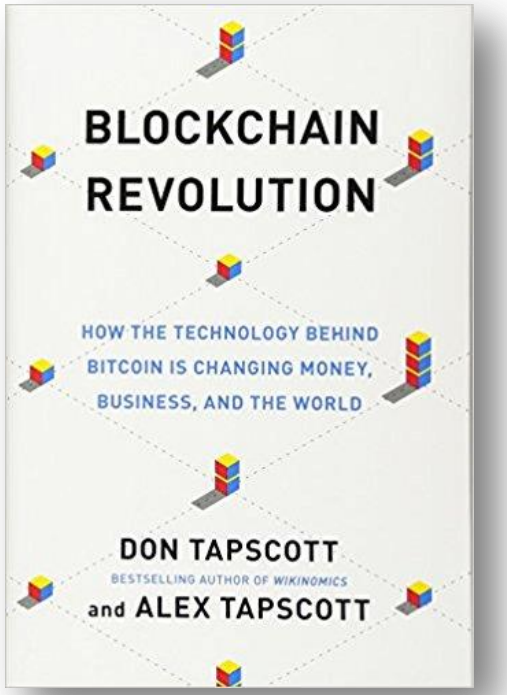
However, the research cautioned that the need to parallel-run blockchain-based services with legacy systems would mean that savings would not be realised for several years after initial deployment, with annual cost reductions not reaching $1 billion per annum until 2024.

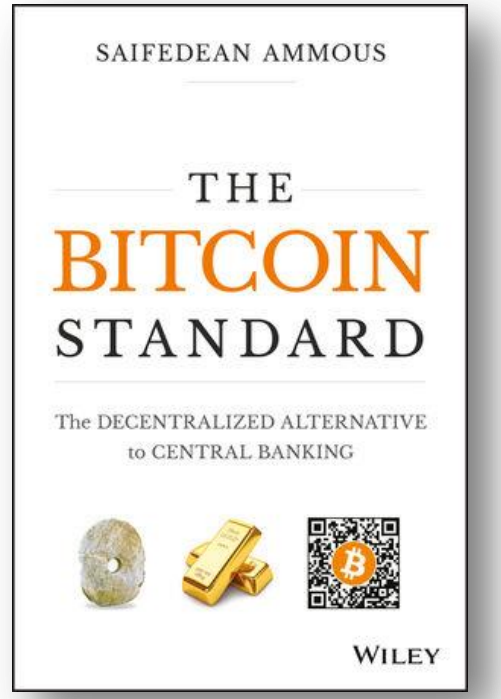
Source: https://www.juniperresearch.com/press/press-releases/blockchain-deployments-to-save-banks-more https://www.juniperresearch.com/press/press-releases/blockchain-deployments-to-save-banks-more

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






Sources: https://www.amazon.com/Truth-Machine-Blockchain-Future-Everything/dp/1250114578; https://www.amazon.de/Blockchain-Revolution-Technology-Changing-Business/dp/1101980133; https://media.wiley.com/product_data/coverImage300/61/11194738/1119473861.jpg

# 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*

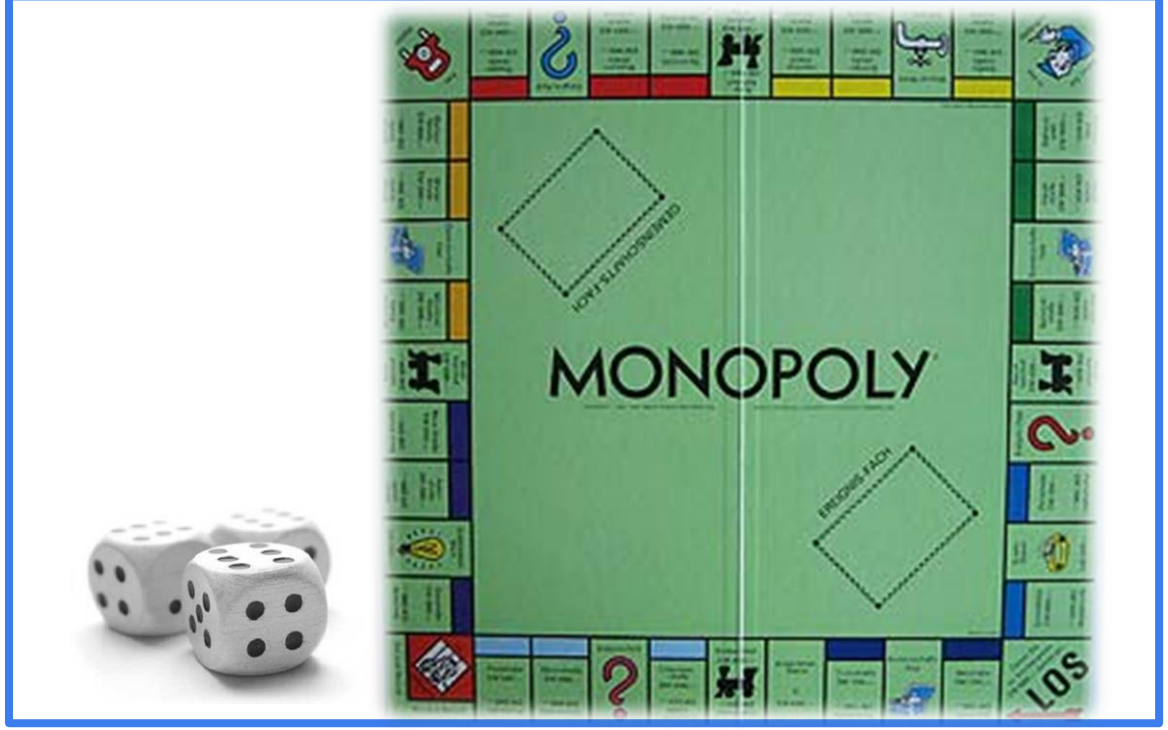
AND

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.

## Blockchain á la Bitcoin with Proof-of-Work

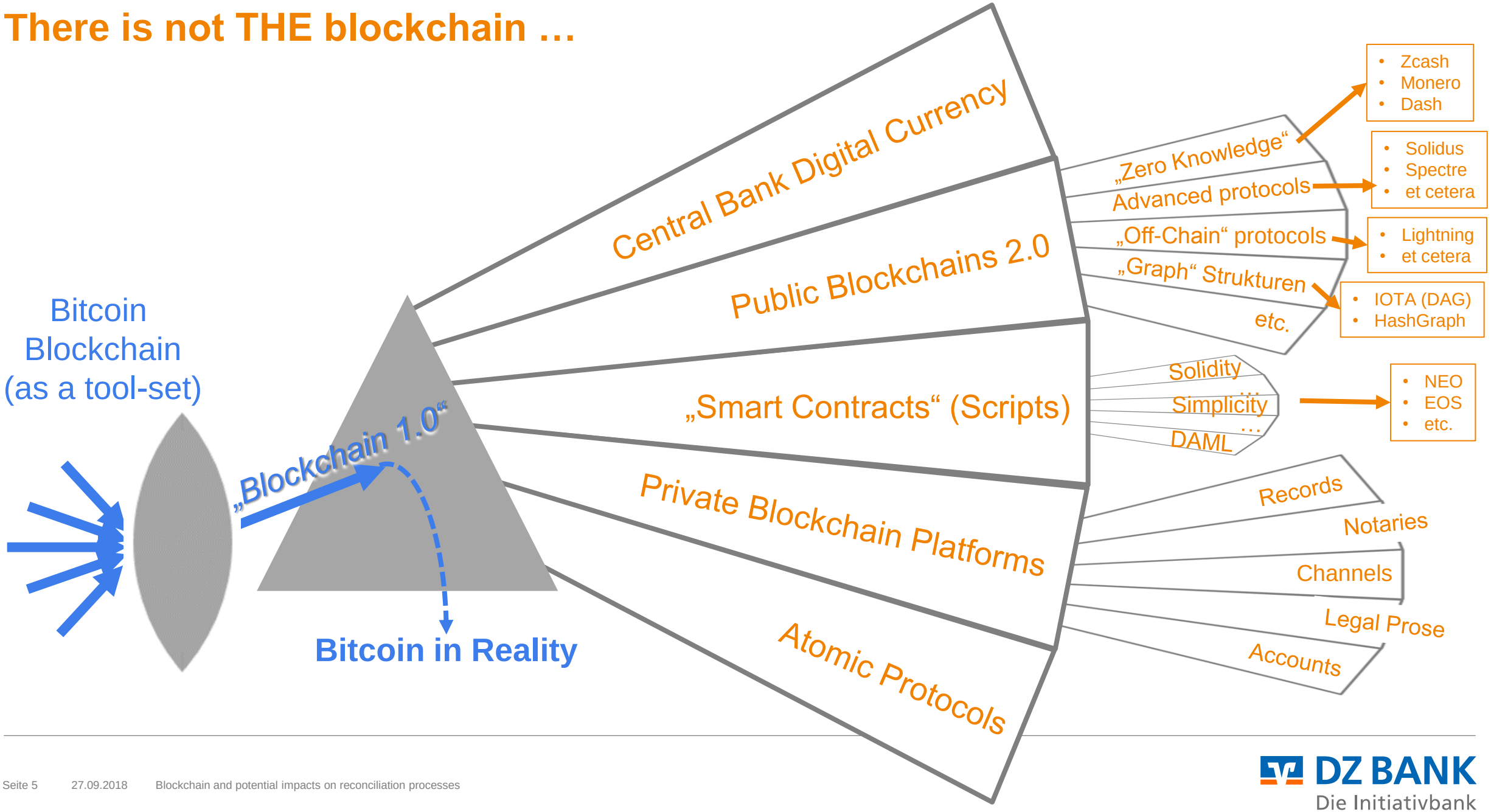



Source: Journal of the Asscktion for Computing Machinery, Vol. 32, No. 2, April 1985, pp. 374-382



DZ BANK
Die Initiativbank

# There is not THE blockchain …






DZ BANK
Die Initiativbank

# Blockchain in Reality: Efficiency, Decentralization, Finality, and Security

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

*) DAG: Directed Acyclic Graph; **) Byzantine Fault Tolerance; ***) on Bitcoin Gold and on Monacoin

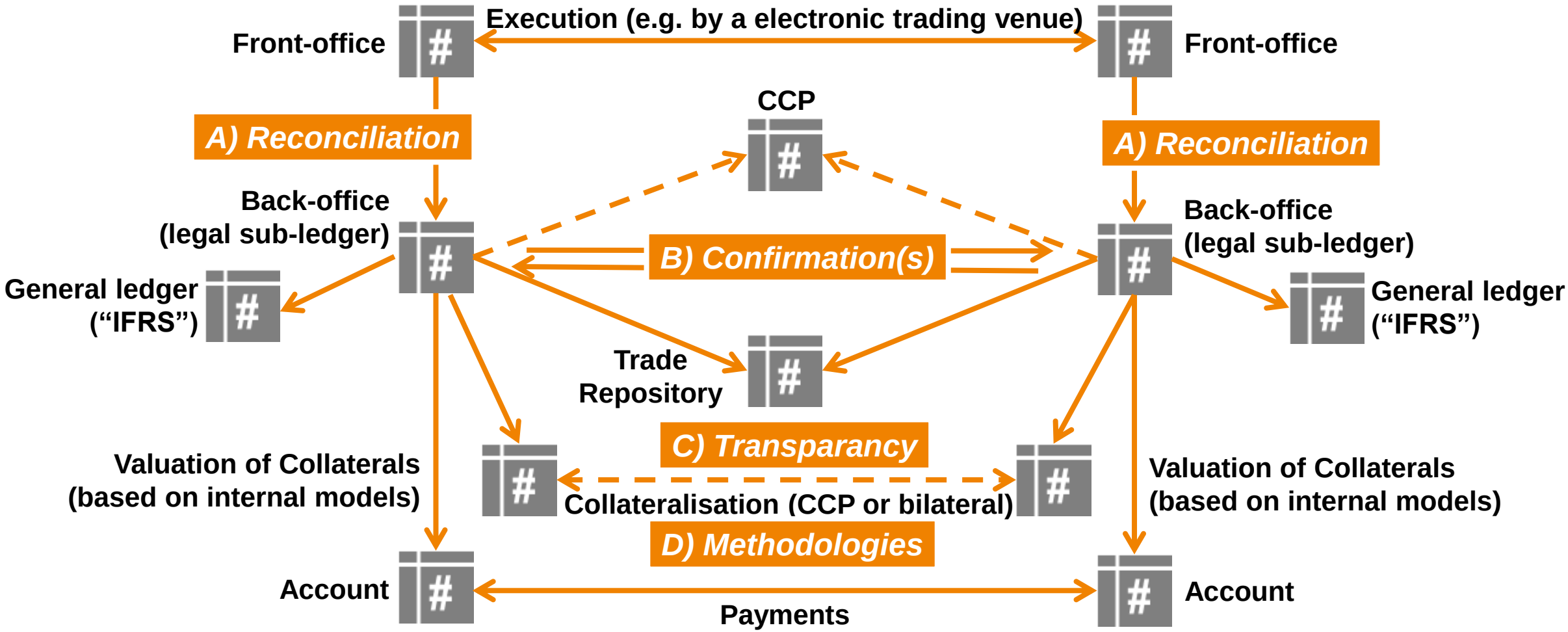
# Agenda: Practical Applications of the Tool-set “Blockchain” / DLT

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 …

Source: Siemens-Archiv

# 1. Challenges of Missing Synchonisation (illustrative and simplified)

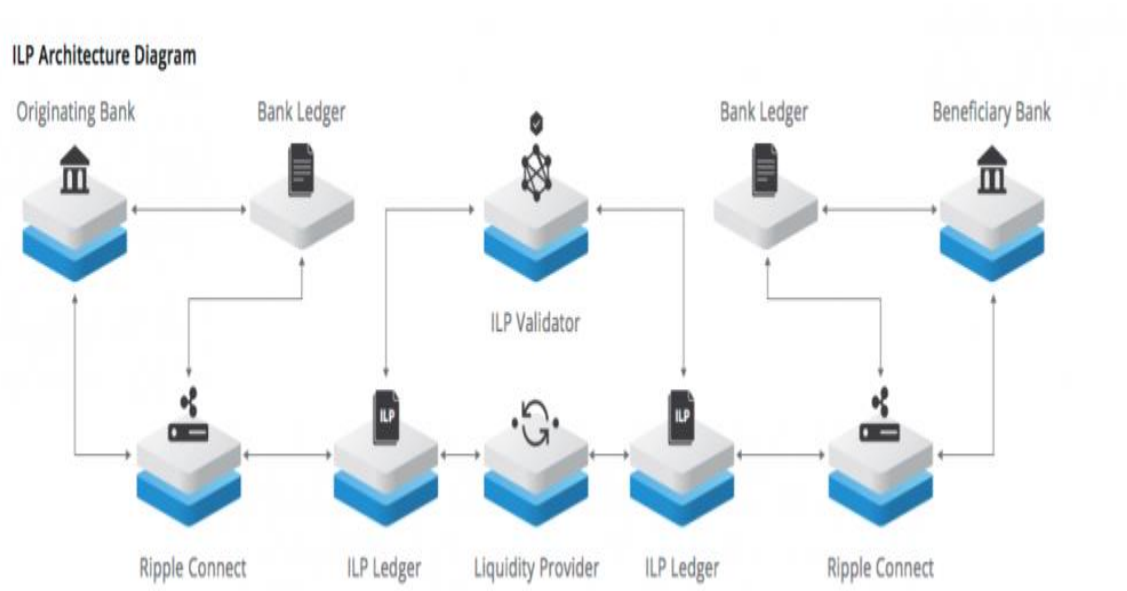




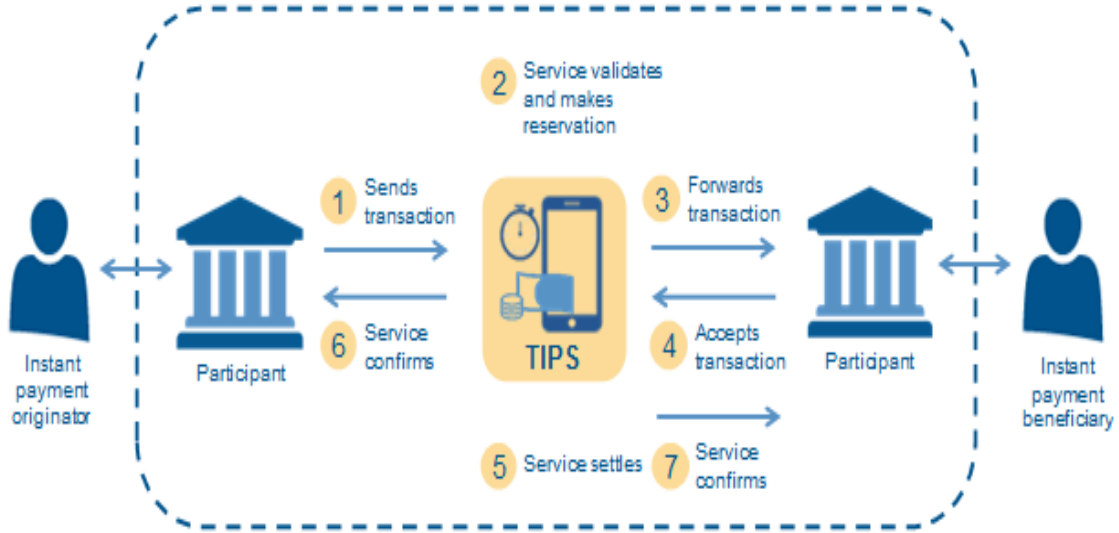

DZ BANK
Die Initiativbank

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

## Ripple InterLedger Protocol (ILP)




## SEPA Instant Payments + TIPS



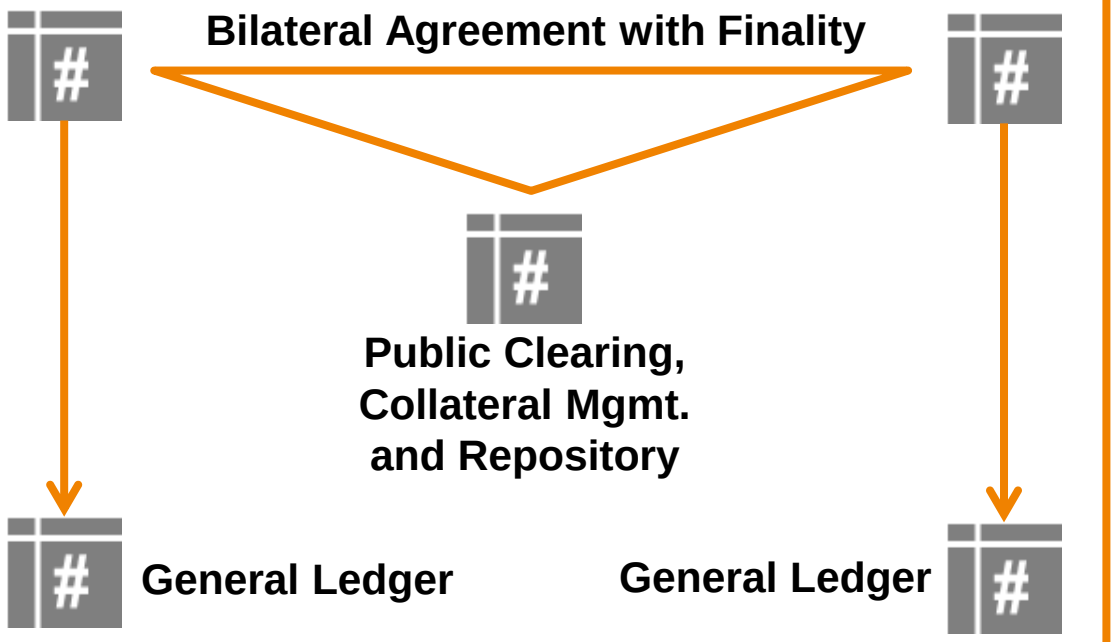

Sources: Ripple Inc.; https://www.ecb.europa.eu/paym/intro/news/articles_2017/html/201706_article_tips.en.html



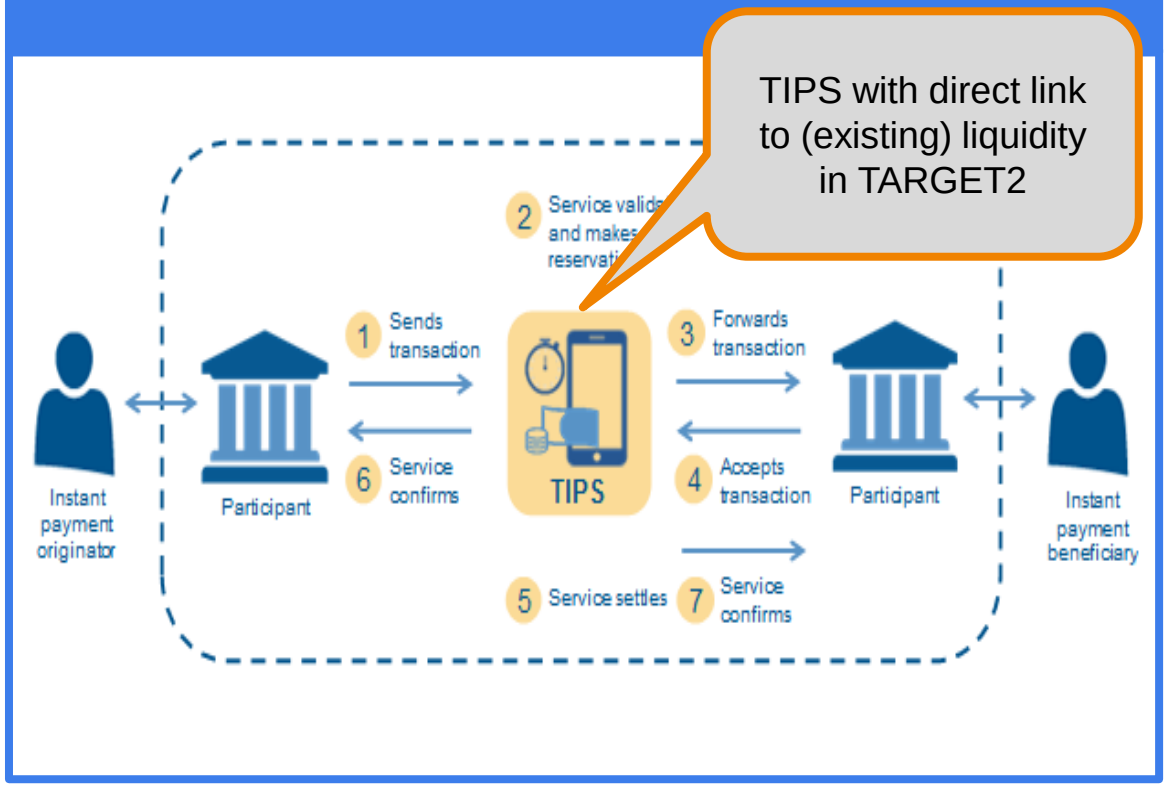
DZ BANK
Die Initiativbank

# 3. Synchonised Settlement versus DvP

## Ripple InterLedger Protocol (ILP)




## SEPA Instant Payments + TIPS

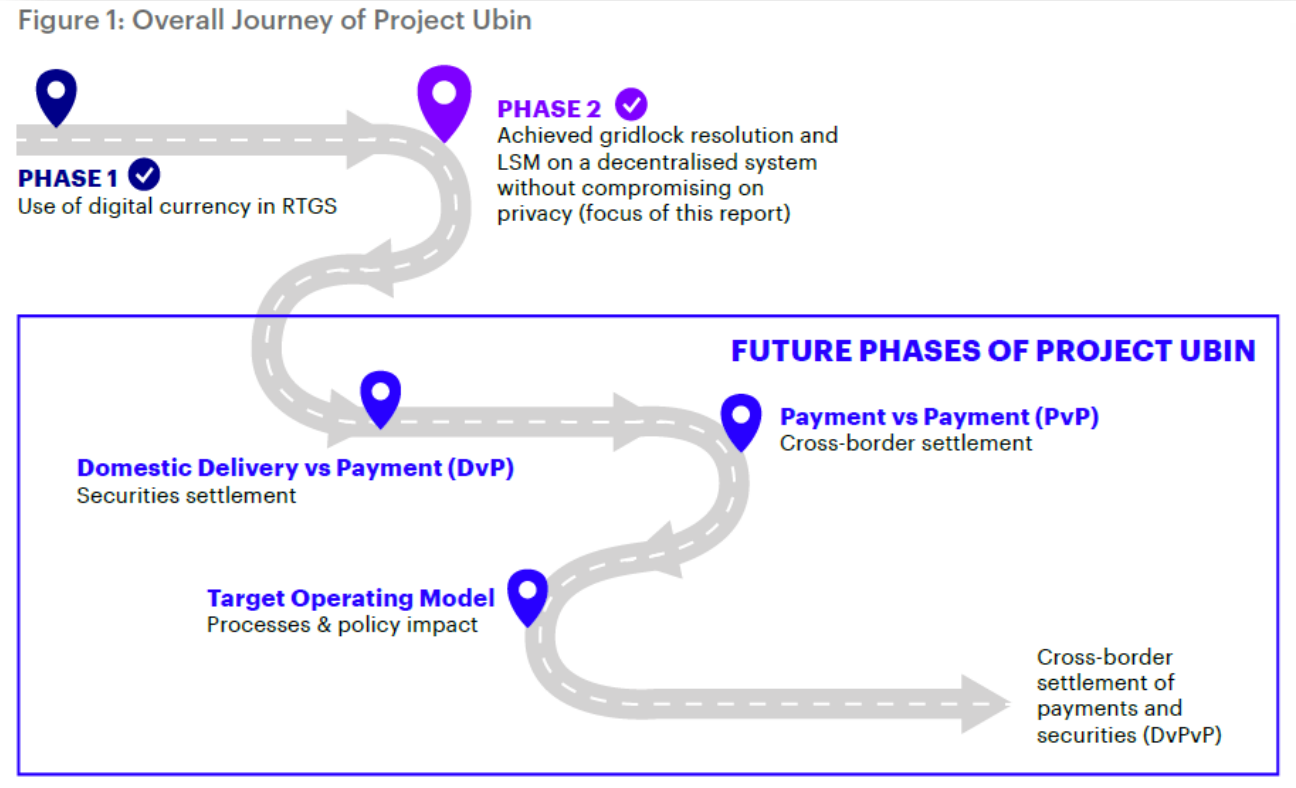



Source: https://www.ecb.europa.eu/paym/intro/news/articles_2017/html/201706_article_tips.en.html



DZ BANK
Die Initiativbank

# 3. Synchonised Settlement … @ Project Ubin 2.0




SGX

MAS
Monetary Authority of Singapore

**FOR IMMEDIATE RELEASE**

**JOINT MEDIA RELEASE**

**MAS and SGX partner Anquan, Deloitte and Nasdaq to harness blockchain technology for settlement of tokenised assets**

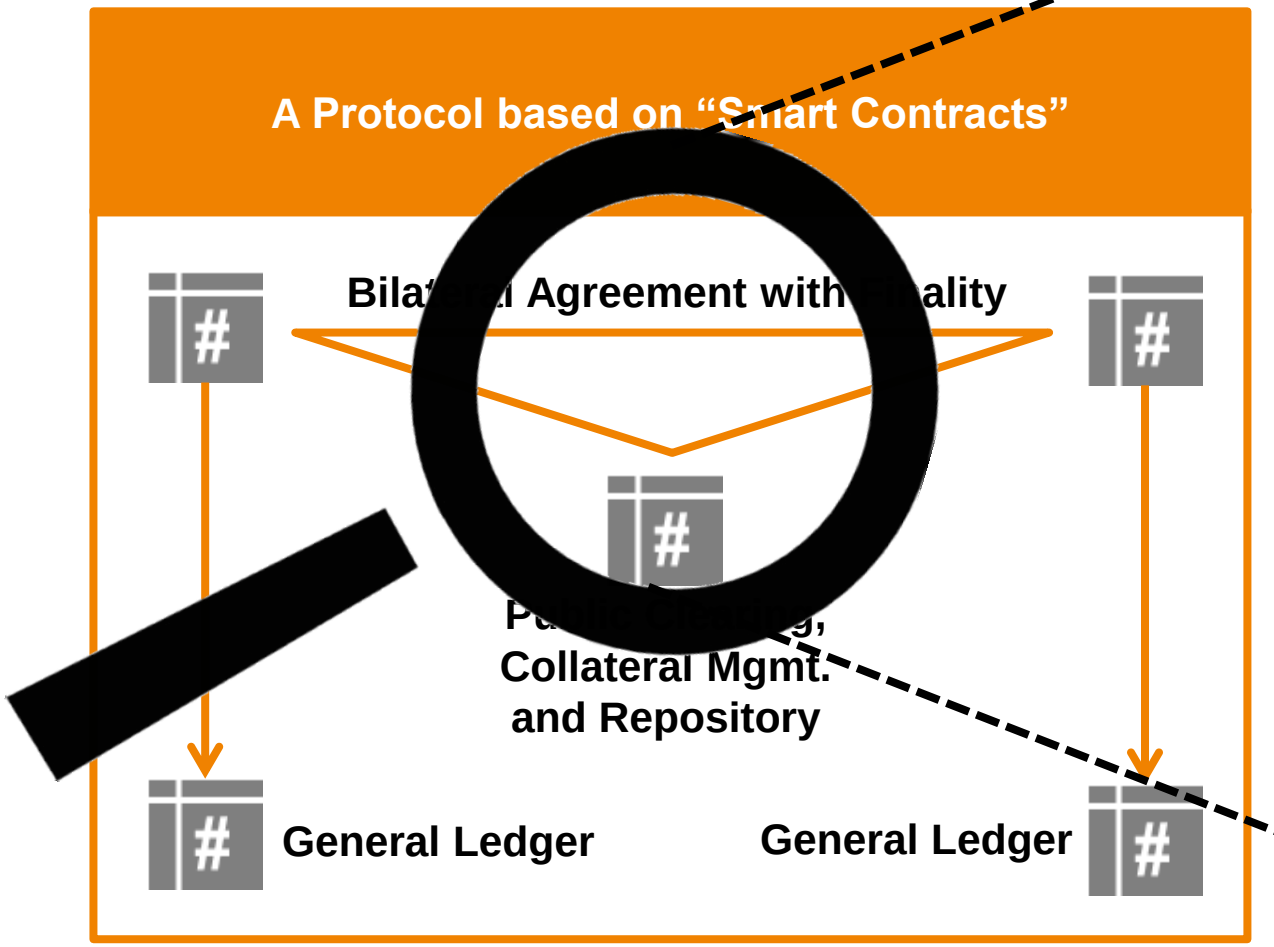
Singapore, 24 August 2018… The Monetary Authority of Singapore (MAS) and Singapore Exchange (SGX) today announced a collaboration to develop Delivery versus Payment (DvP)[1] capabilities for settlement of tokenised assets across different blockchain platforms. This will allow financial institutions and corporate investors to carry out simultaneous exchange and final settlement of tokenised digital currencies and securities assets, improving operational efficiency and reducing settlement risks.

Source: *www.mas.gov.sg*



DZ BANK
Die Initiativbank

# 4. Consensus about of Future Actions …




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

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

…

X. General clauses:
- legal text …

Z. Default:
- Definition xxx …



DZ BANK
Die Initiativbank

# 4. … but Missing Standards and Diverging Objectives …

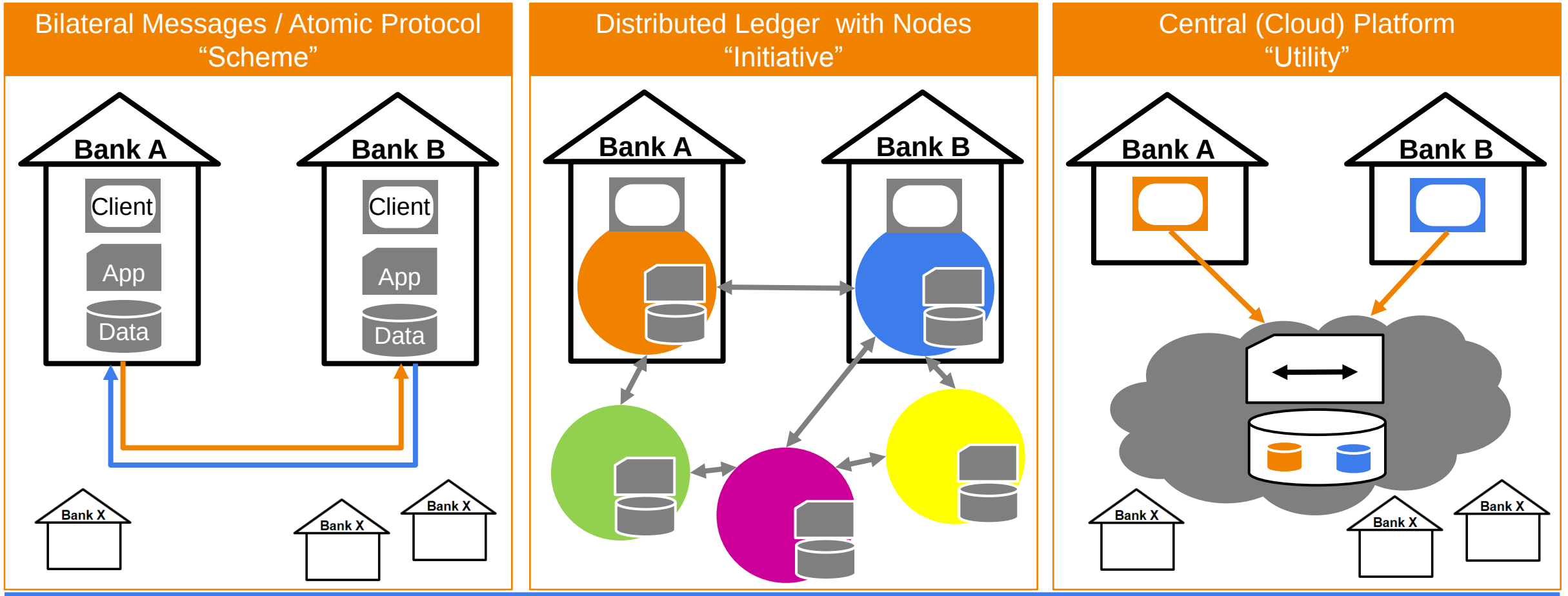
## Various Languages and Templates:

- 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?






DZ BANK
Die Initiativbank

# A Conclusion


Dec 13, 2017 • Bylined Articles

## The DLT Wave: From Hype to Progress

**By Michael C. Bodson, DTCC President & CEO**

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. …

Source: https://www.pymnts.com/cryptocurrency/2018/buffett-munger-cryptocurrencies-regulations/