DLT – An Update and Next Steps

SMPG Meeting

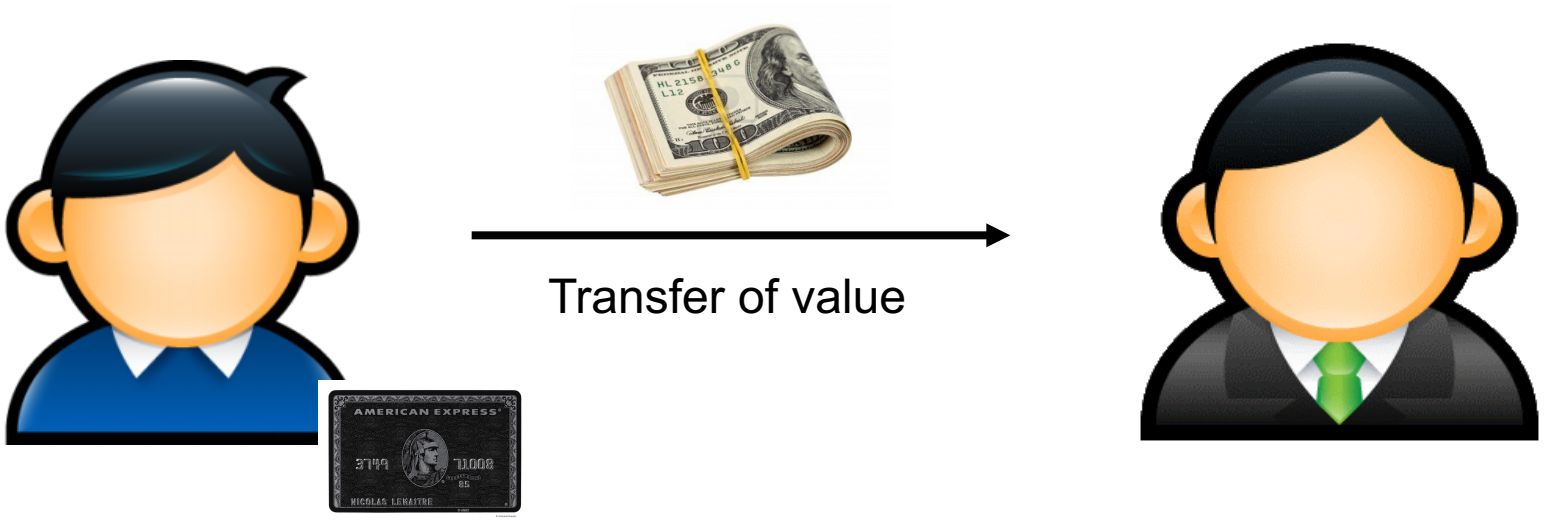
METACO

Adrien Treccani, Ph.D.

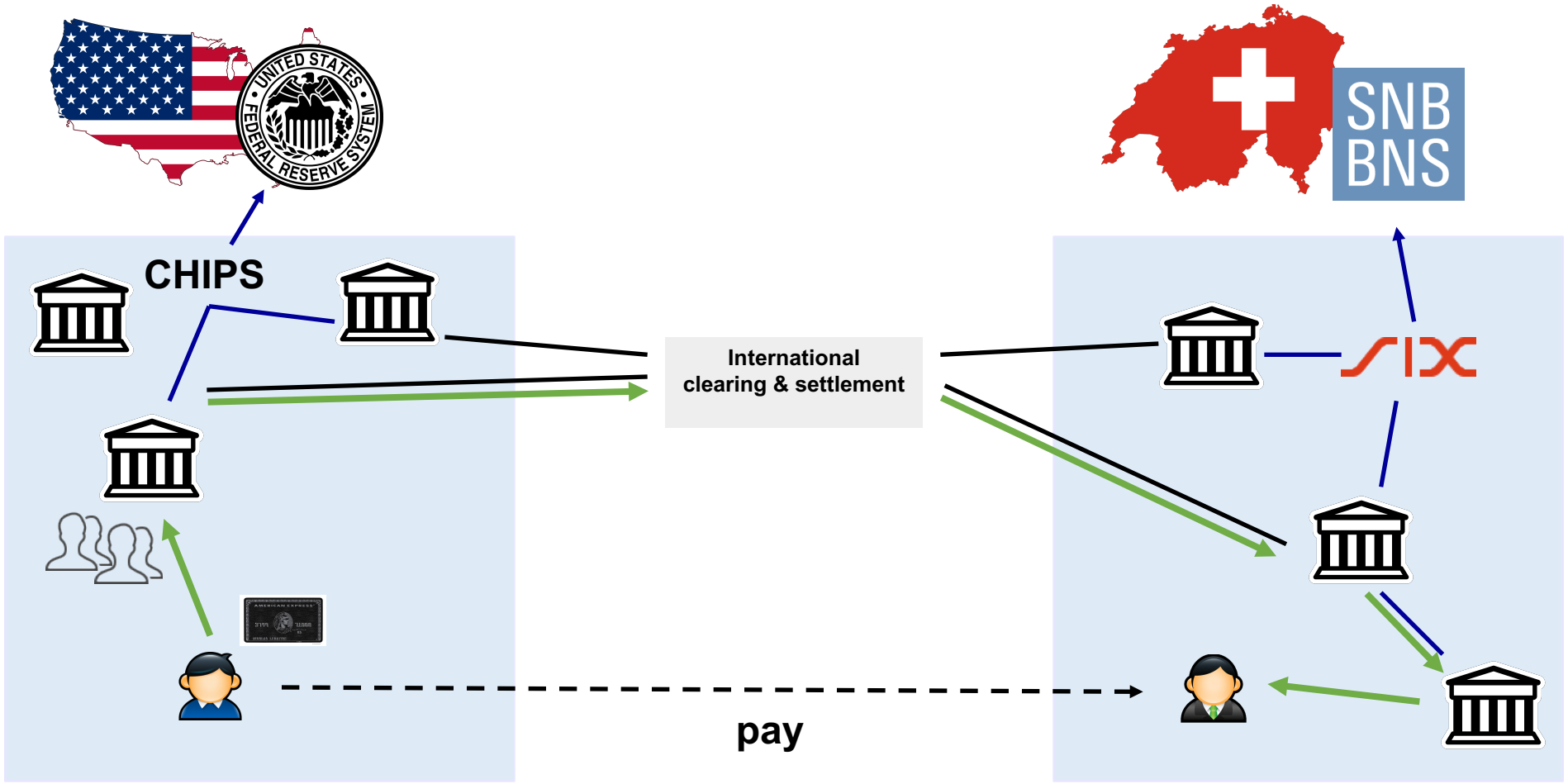
September 2016

Introduction to DLT

Finance in a nutshell



Under the hood



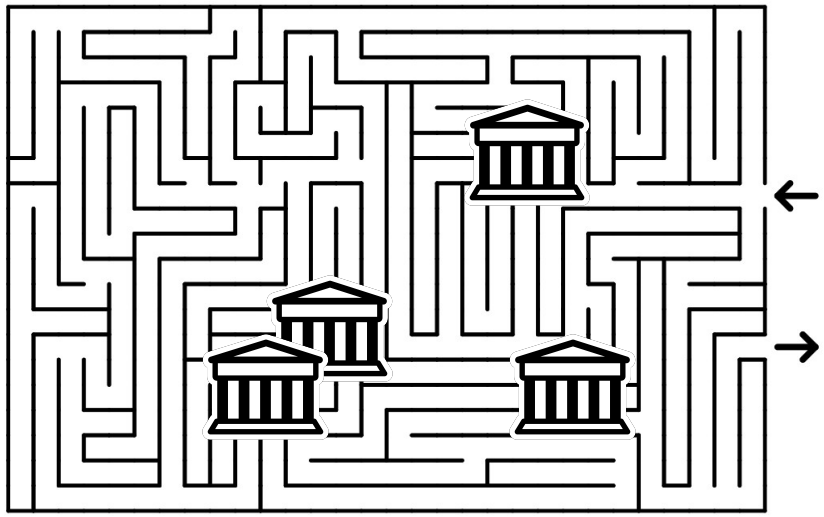
METACO

Efficiency motivation

"Blockchain could reduce banks' infrastructure costs by US$15 – 20 billion per annum by 2022." *Santander Report*

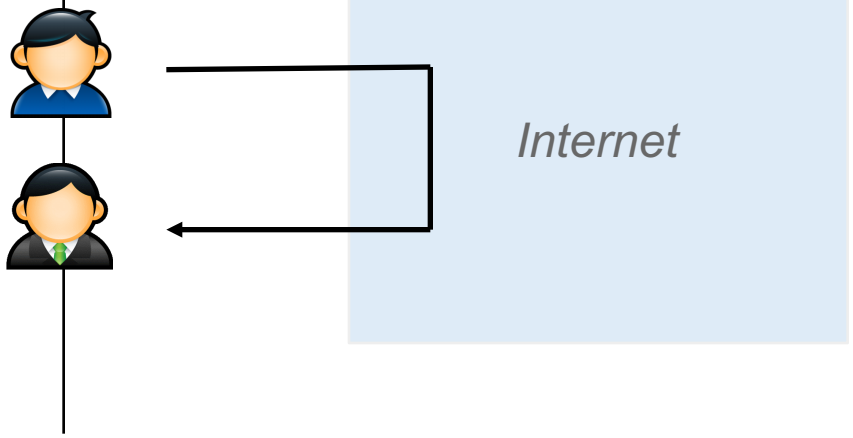
Reliance on intermediaries

Cost
Latency
Errors
Credit risk



Peer-to-peer

Inexpensive
Fast
Atomic transactions

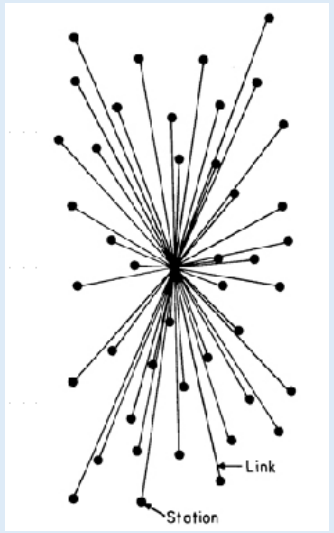


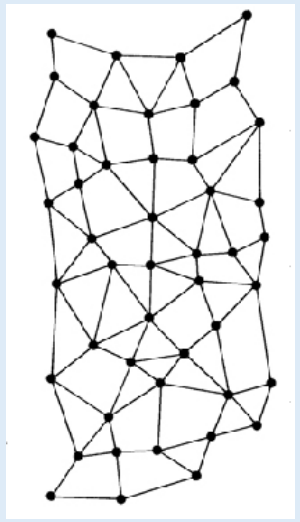
METACO

Political motivation

Centralized network

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





Distributed network

Friction-less entry
Democratic governance
Worldwide network
Algorithmic validation

METACO

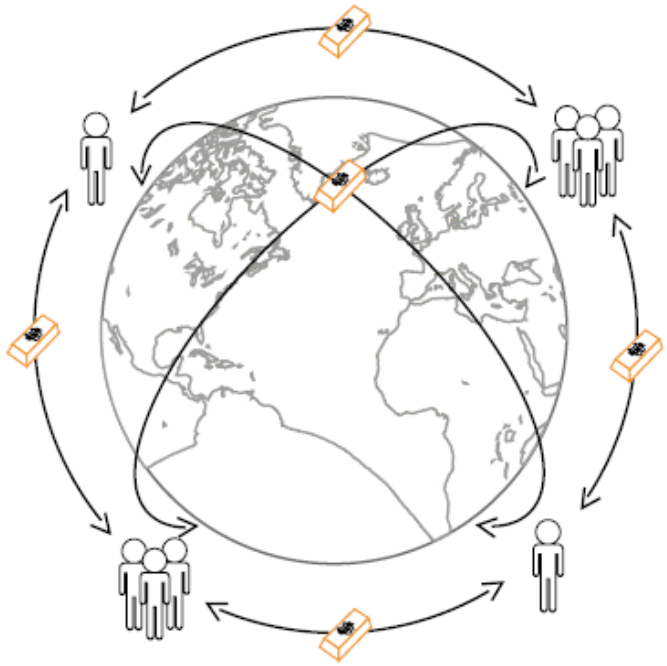
Bitcoin network

Distributed payment network

Globally available
No central authority (e.g., no bank)
Consensus-based democracy

Key numbers

- 10M users
- 2.5 tx/s
- $150M tx/day
- ~30 min settlement



Ref: *Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto (2009).*

Use case I: Bankless merchant

Use case II: Remittance

Bitcoin currency

No stabilization policy

Strict 21M cap on bitcoin supply

Deflationary monetary policy

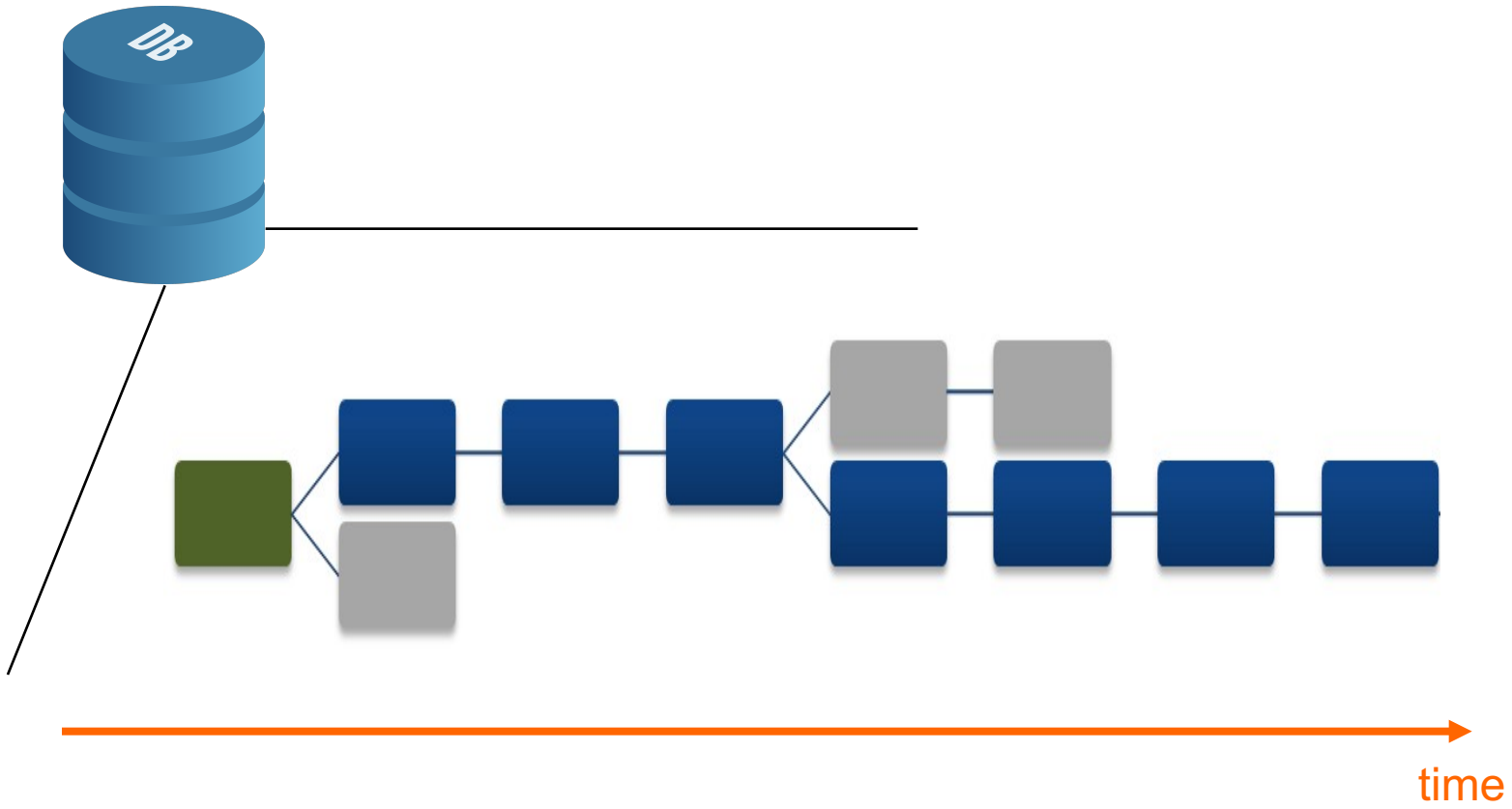
Key numbers

- $9.0B market cap
- $600 last price
- $1200 ATH price
- 200K merchants

Ref: *Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto (2009).*

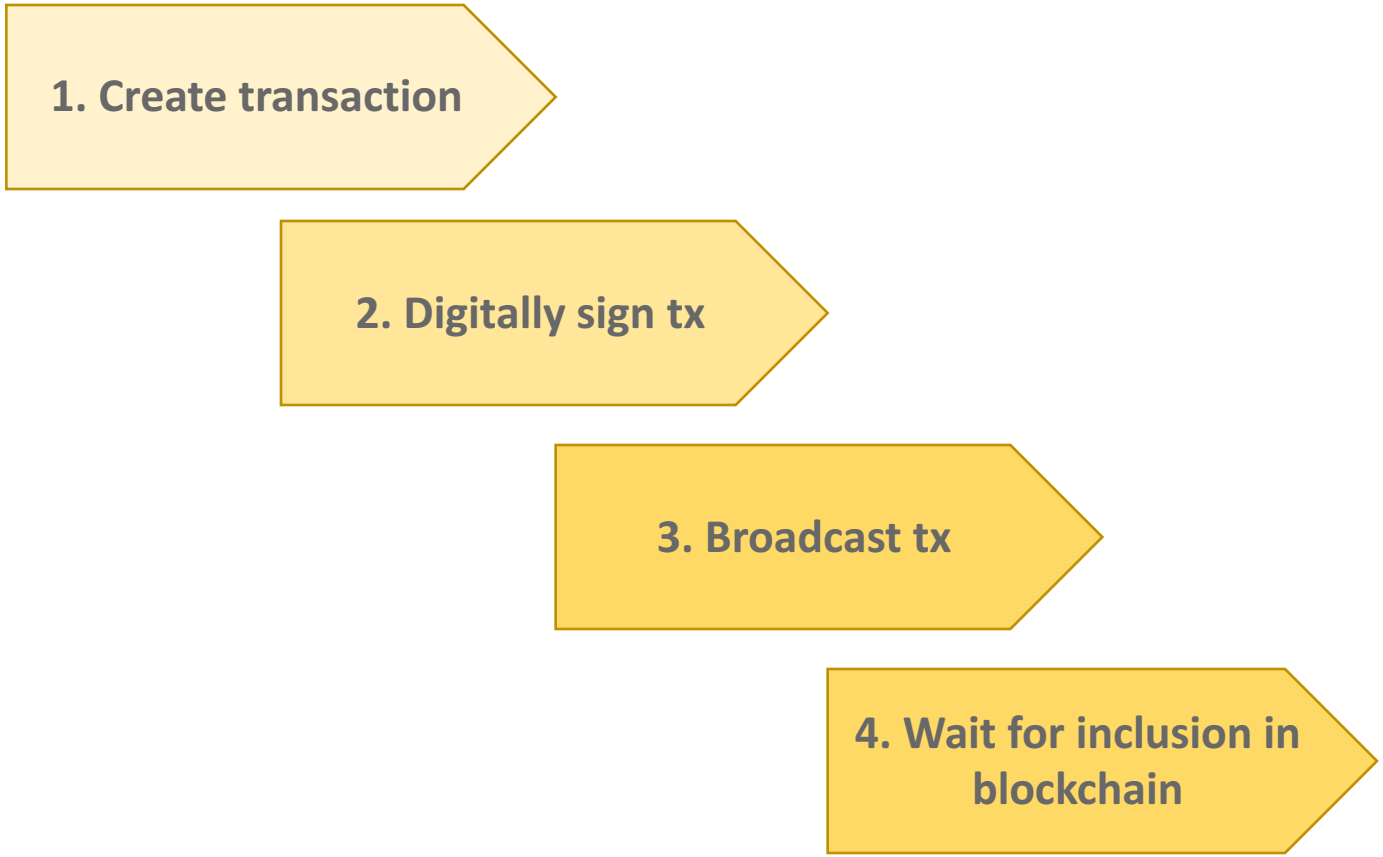
METACO

Blockchain *trust machine*



METACO

Payment processing

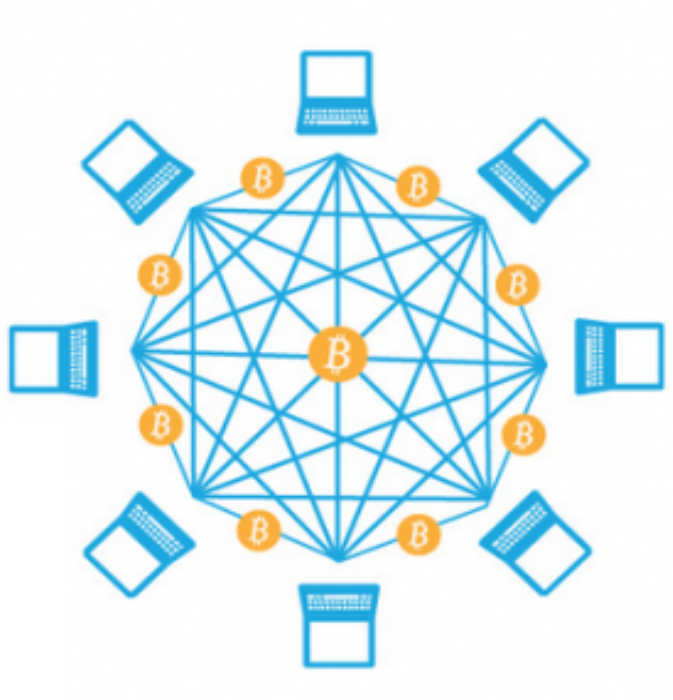


Distributed ledger maintenance

Distributed persistence

Users maintain full copy of the blockchain

- Entire history of transactions
- High redundancy
- Peer-to-peer, public network



Distributed maintenance

Blockchain is protected by cryptography

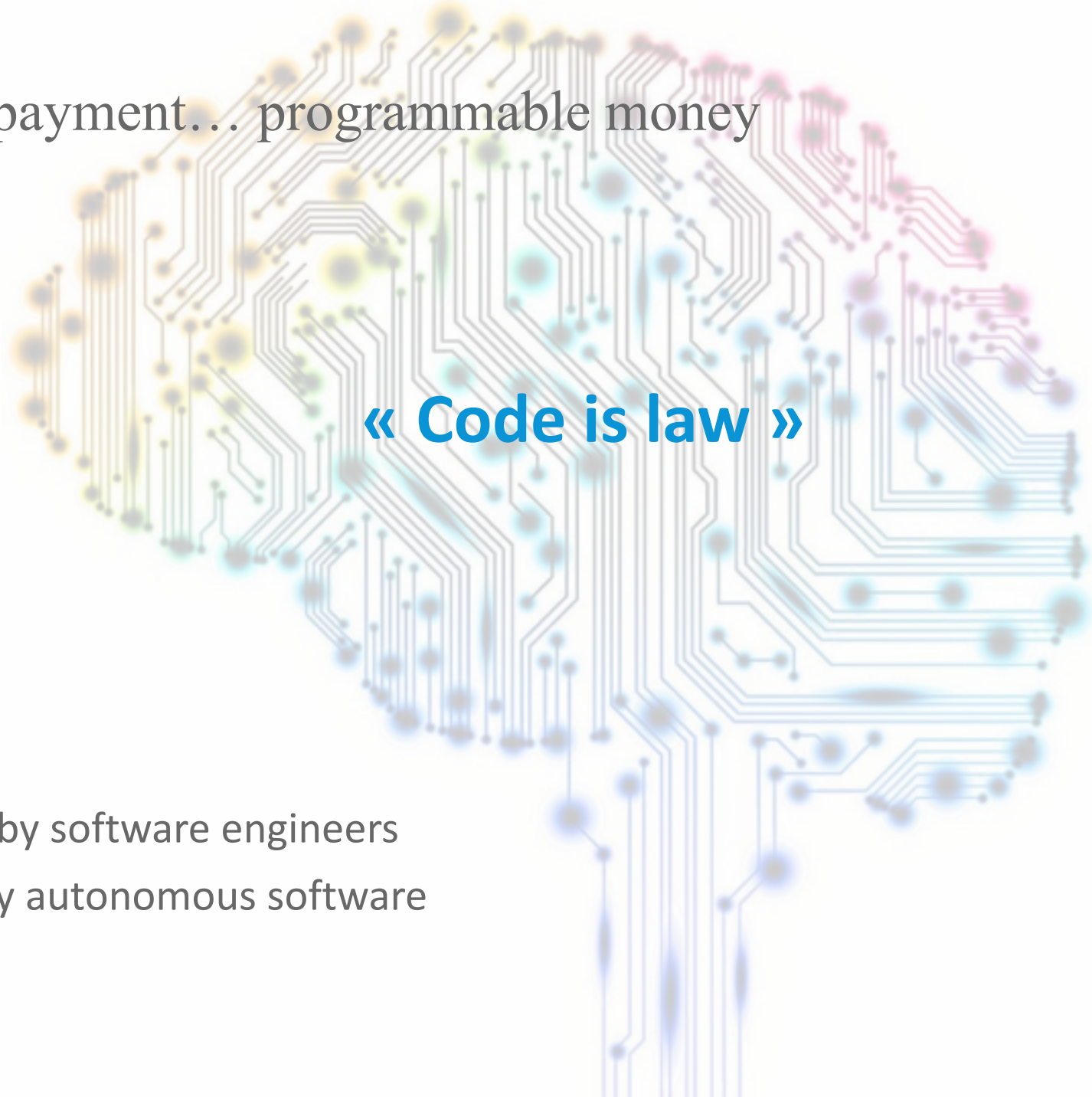
- Proof-of-work consensus (mining)
- Unrestricted, competitive mining
- 1.5 exa hash/s security

Internet of contracts

Beyond bitcoin currency

METACO

And beyond payment… programmable money



« Code is law »

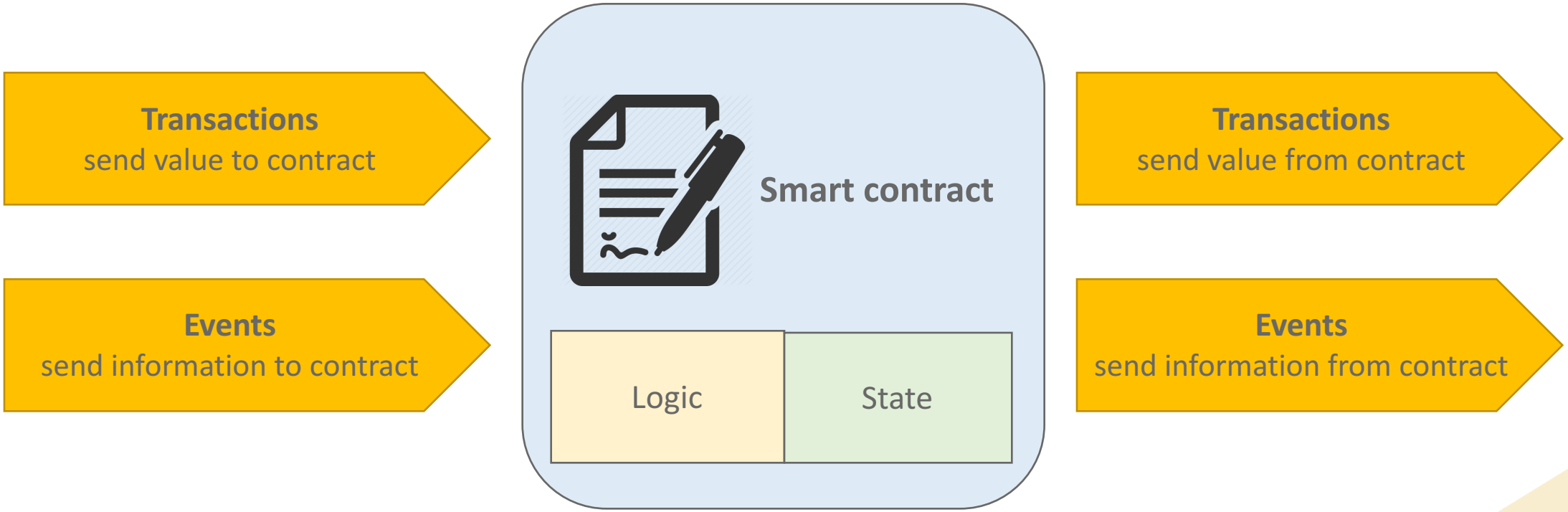
Ambition

Replace lawyers by software engineers

Replace courts by autonomous software

METACO

Smart contract



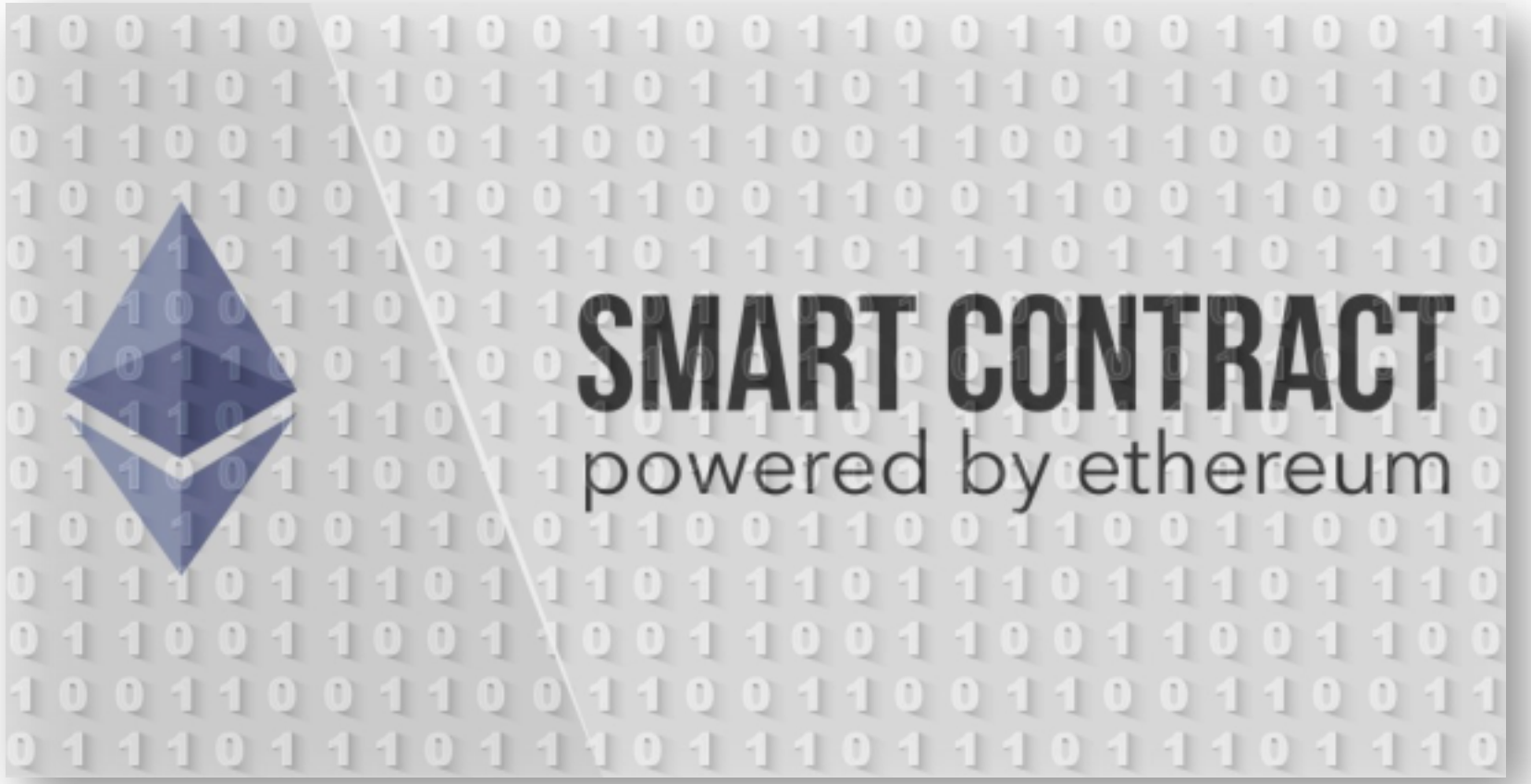
METACO

Use case III: Multi-signature account

Multi-signature

Logic	**Allow withdraw if and only if** 1. CEO orders withdraw, or 2. 2 out of 3 assistants order withdraw and volume smaller than 1M a day
State	• Balance of the contract • Authorized assistants • Amount withdrawn in last 24h

Smart contract platform



Case studies

- Peer-to-peer exchange
- Letter of credit
- The DAO

Case study: Peer-to-peer exchange

Case study: Peer-to-peer exchange

METACO

Case study: Peer-to-peer exchange

BID 10 XAU @ $1300

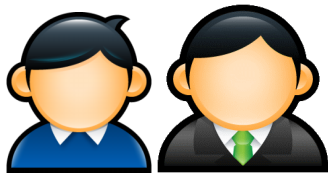
1. Place limit BID

- Locks 13’000 USD in contract
- Updates contract order book

ASK 5 XAU @ $1250

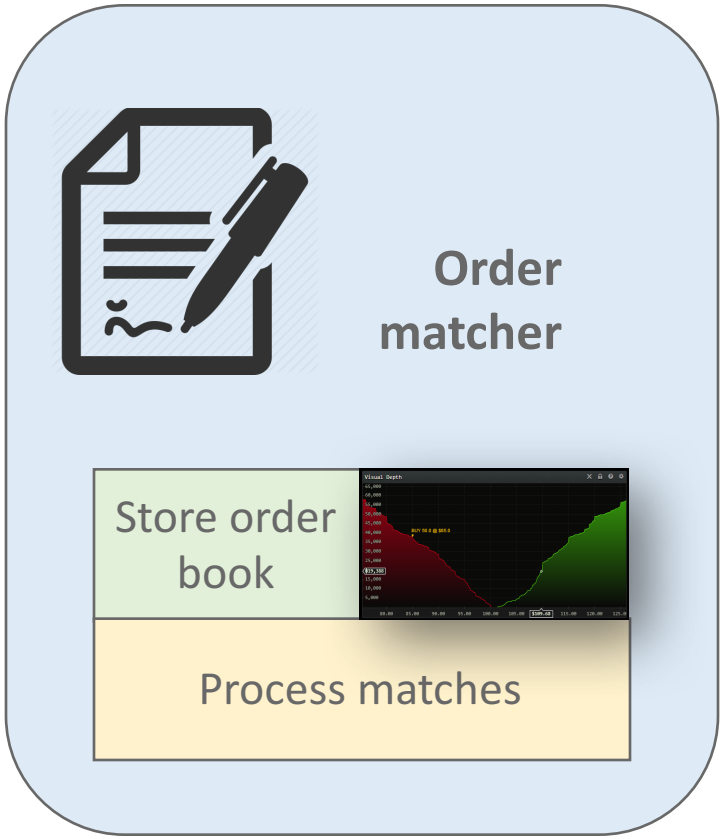
2. Place market SELL

- Locks 5 XAU in contract



3. Process order match **atomically**

- Release 5 XAU to bidder, $6500 to seller
- Updates order book



METACO

Case study: Peer-to-peer exchange

No custodian risk

Funds are locked in a smart contract

- Funds can only *exit* the contract with an order match or cancellation
- Contract follows strict algorithmic rules

No counterparty risk

Trades are atomic

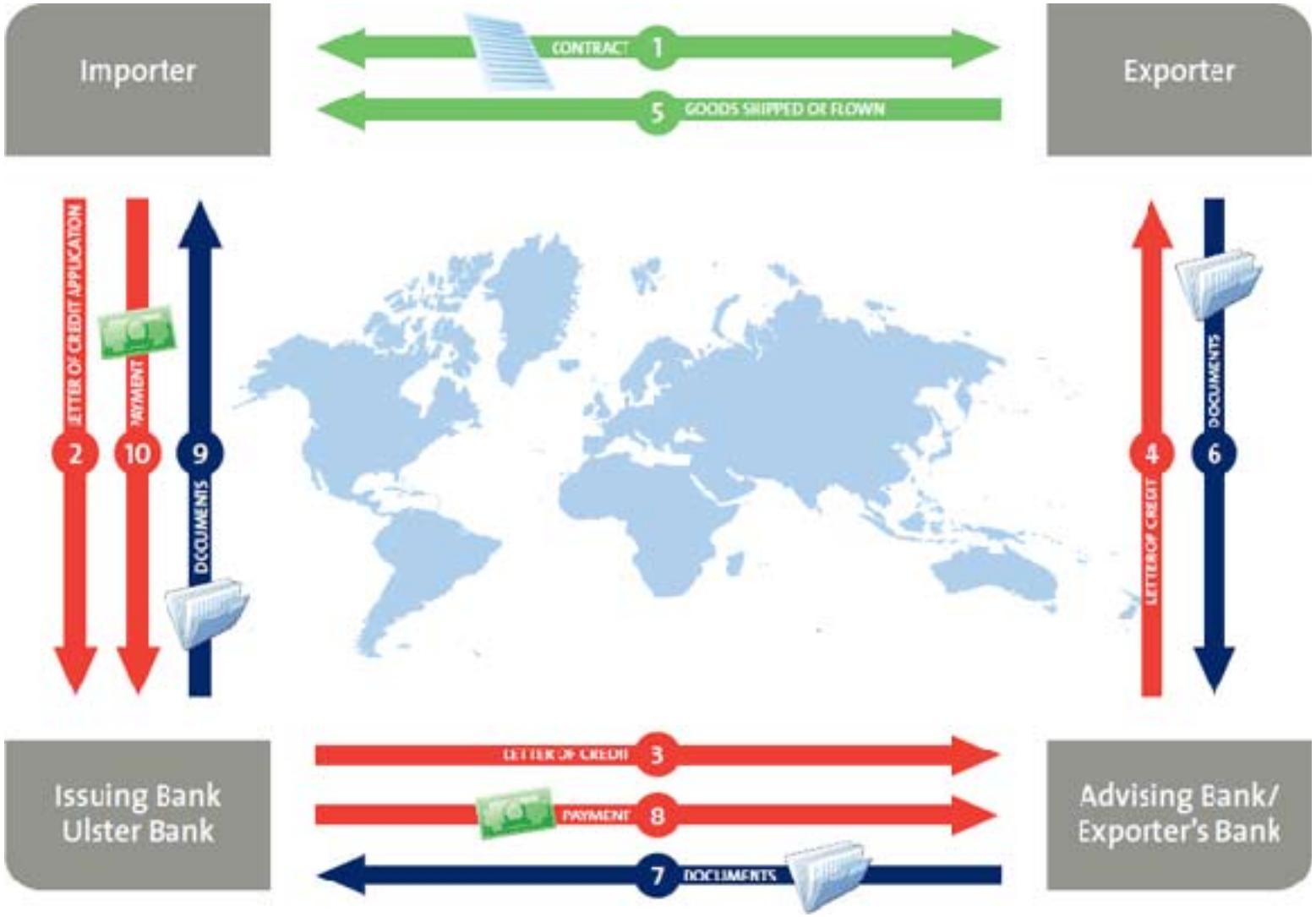
- Both legs of the trade are executed as a transaction
- Trade either succeeds or fails entirely, no partial execution

Fast settlement

Settlement time as fast as traditional transactions

- Finality of the trade takes minutes

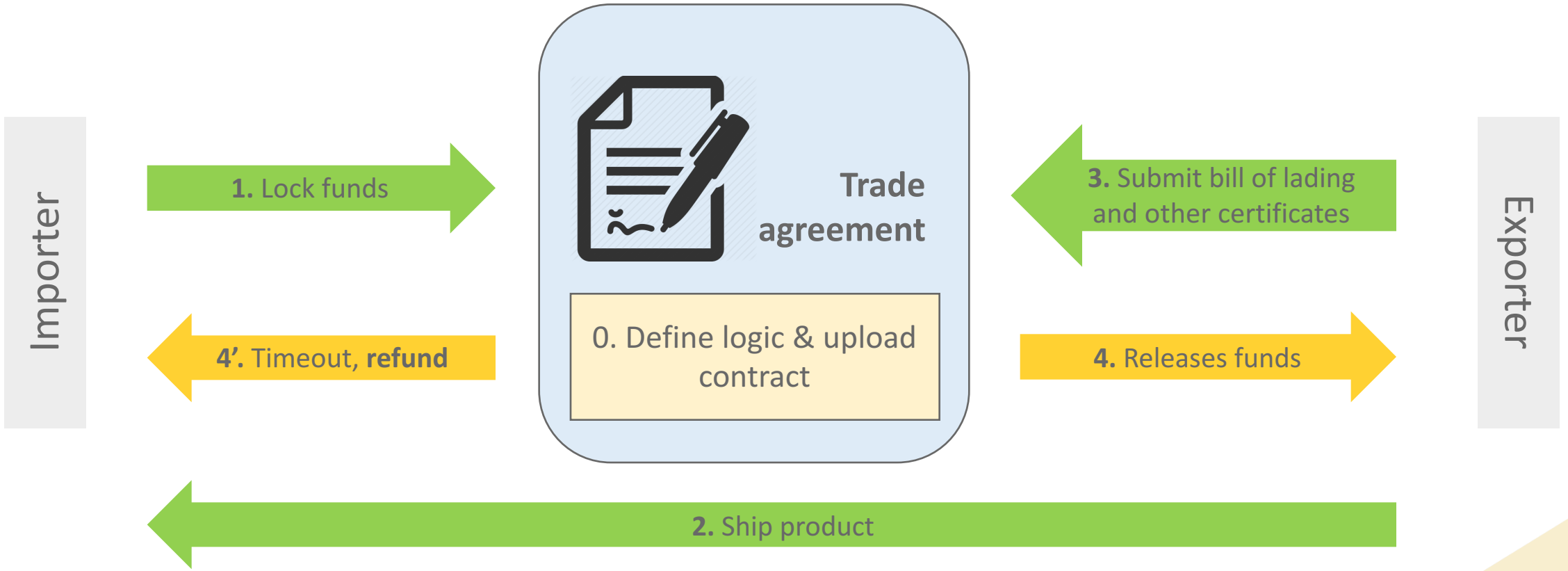
Case study: Letter of credit



Source: eon Logistics

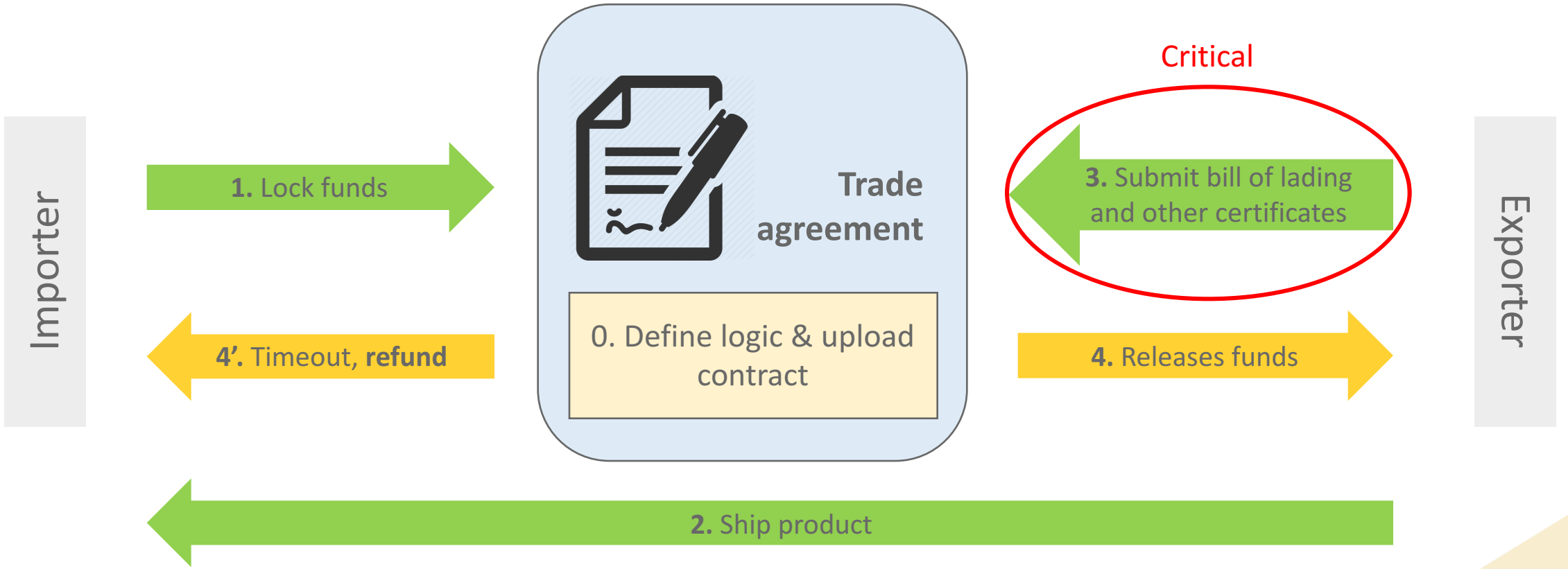
METACO

Case study: Letters of credit



Source: eon Logistics

Case study: Letters of credit



Source: eon Logistics

Case study: Letters of credit

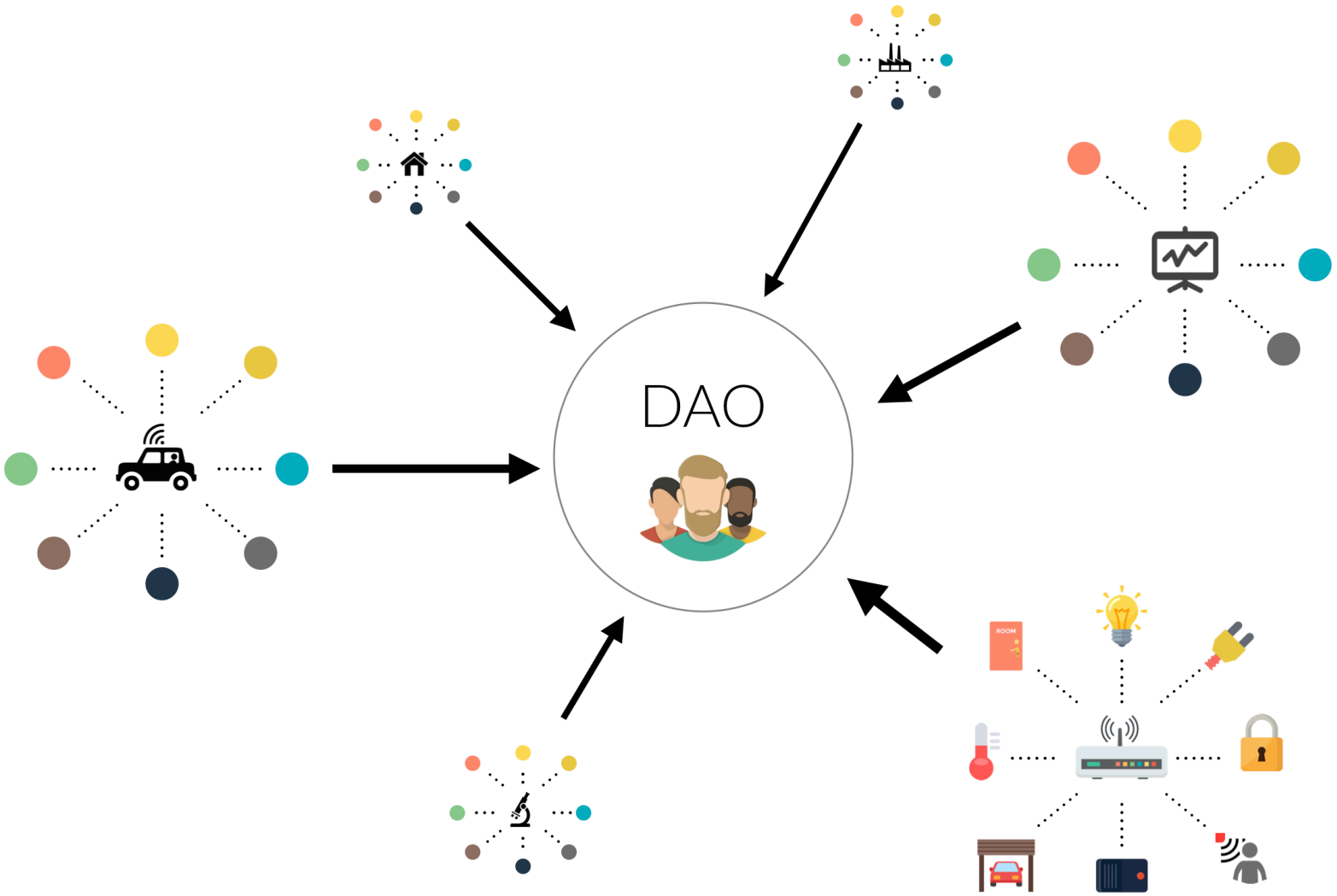
« Software cannot verify the purity of oil (yet) »

Logic	**Pre-authorize contractors to submit cryptographic proofs** • Quality check • Bill of lading • Insurance (***could be a smart contract!***)

Case study: The DAO

“Do smart contracts remove all form of risk?”

Case study: The DAO



Case study: The DAO

Case study: The DAO

METACO

Taking the right decisions

Decision criterions

1. Efficiency

- Scalability
- Latency

2. Privacy

- Too much anonymity
- Not enough anonymity

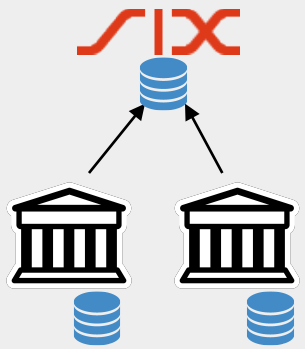
3. Control

- Supervision
- Regulations

What kind of ledger do I need? *(Do I need one?)*

Centralized

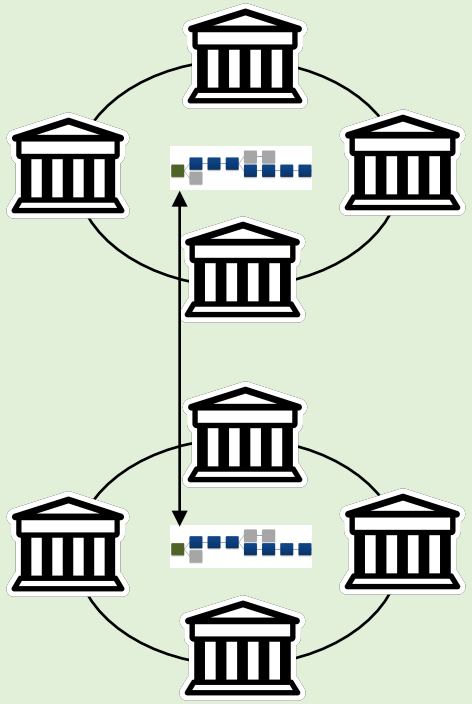
Each entity maintains
<u>own accounting</u>



Super-entity clears
inter-ledger transfers

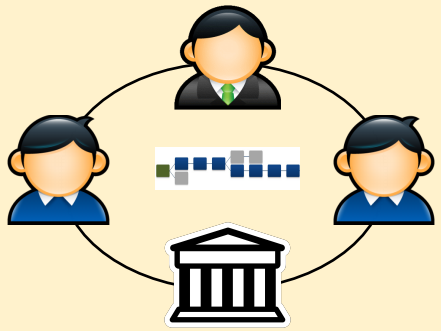
Consortium

Selected entities maintain
<u>shared blockchain</u>



Distributed

Anybody maintains
<u>entire shared blockchain</u>



bitcoin

ethereum

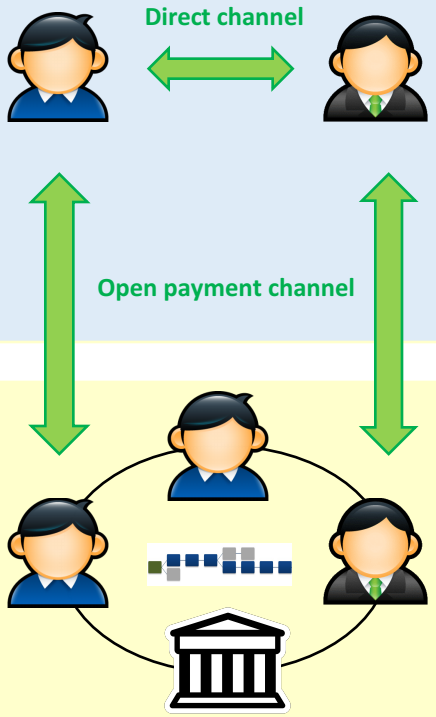
METACO

Optimization through consensus algorithm

Scaling through payment channels

Off-chain layer

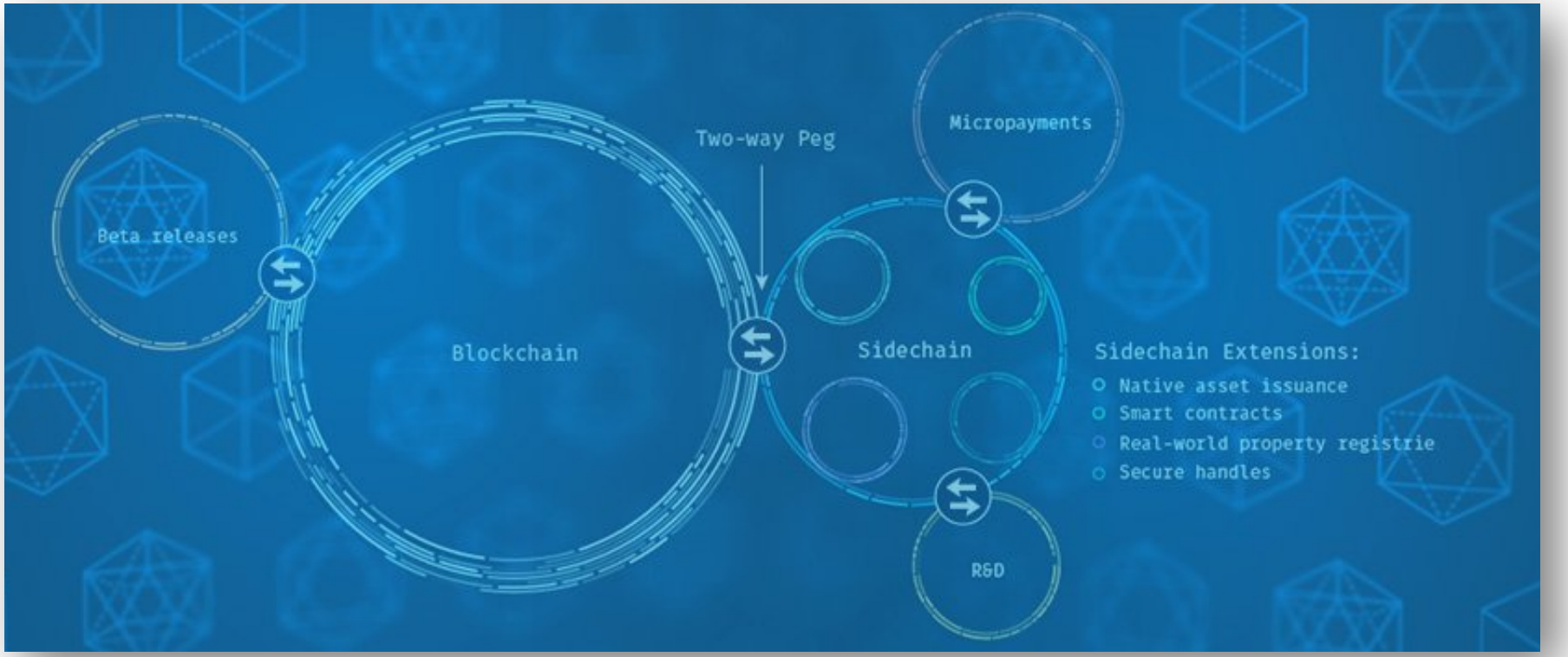
- High scalability
- Low latency
- Fully private
- Low processing cost



Distributed ledger

METACO

Specialization through sidechains



METACO

Discussion

No consensus on the consensus algorithm

- Distributed + off-chain
- Consortium + intercommunication layer
- Specialization through sidechains?

Promising applications for smart contracts

- Need digital assets first
- Software bugs issue
- Legal questions

Leverage distributed ledgers with expertise

Get in touch with us

Adrien Treccani, Ph.D.

Chief Executive Officer

treccani@metaco.com

+41 79 786 47 01