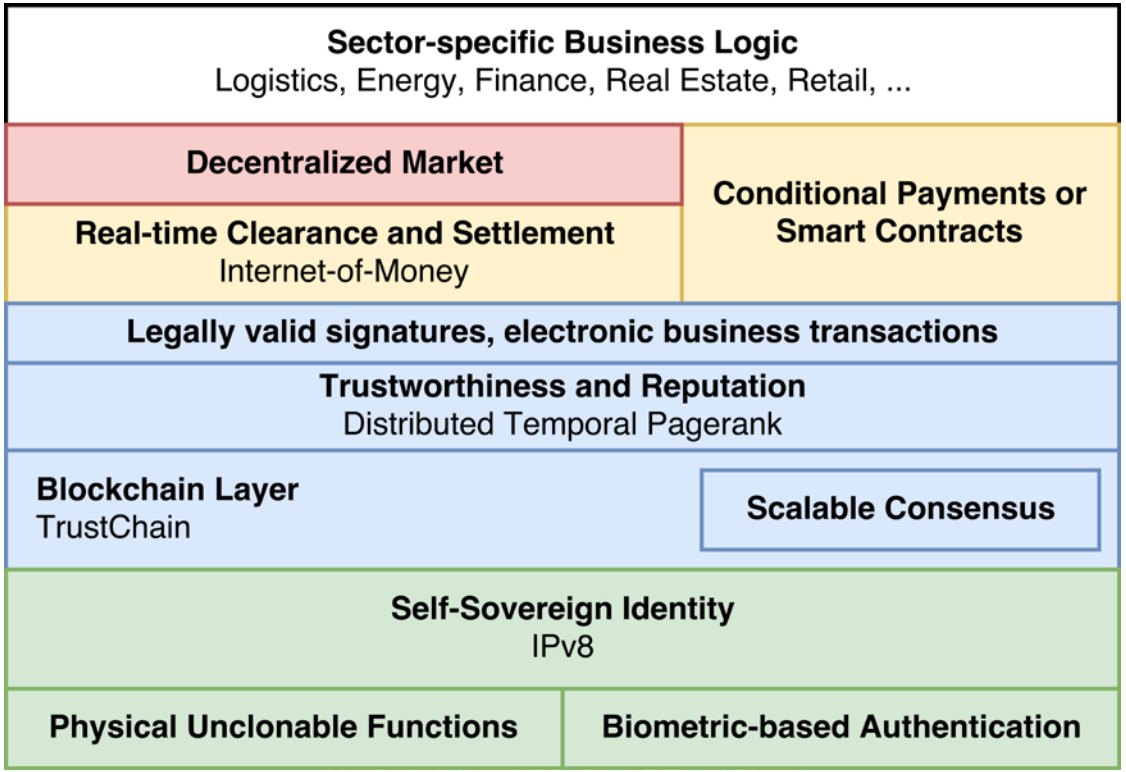
TrustChain

A scalable blockchain fabric to build trust

Martijn de Vos
Distributed Systems

TU Delft

Delft Technology Portfolio

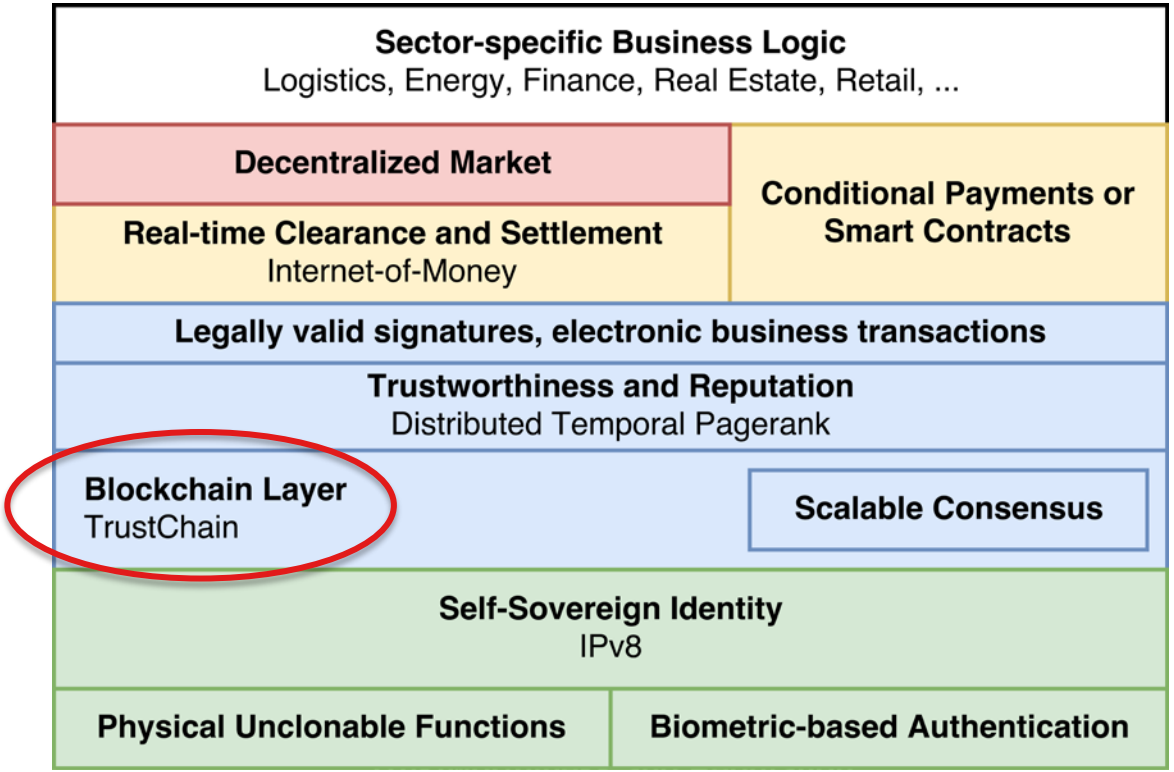


TU Delft

DELFT BLOCKCHAIN LAB

Pouwelse, Johan, et al. "Laws for Creating Trust in the Blockchain Age." *European Property Law Journal* 6.3 (2017): 321-356.

Delft Technology Portfolio



TU Delft

DELFT BLOCKCHAIN LAB

Pouwelse, Johan, et al. "Laws for Creating Trust in the Blockchain Age." *European Property Law Journal* 6.3 (2017): 321-356.

Open problems of existing Blockchain solutions

- Scalability (often constant tx/s)
  - Bitcoin Core: ~7 tx/s
  - Ongoing efforts to increase scalability (Lightning network, sharding, off-chain)
- Storage requirements
  - Bitcoin: 149GB as of December 2017

Global Consensus

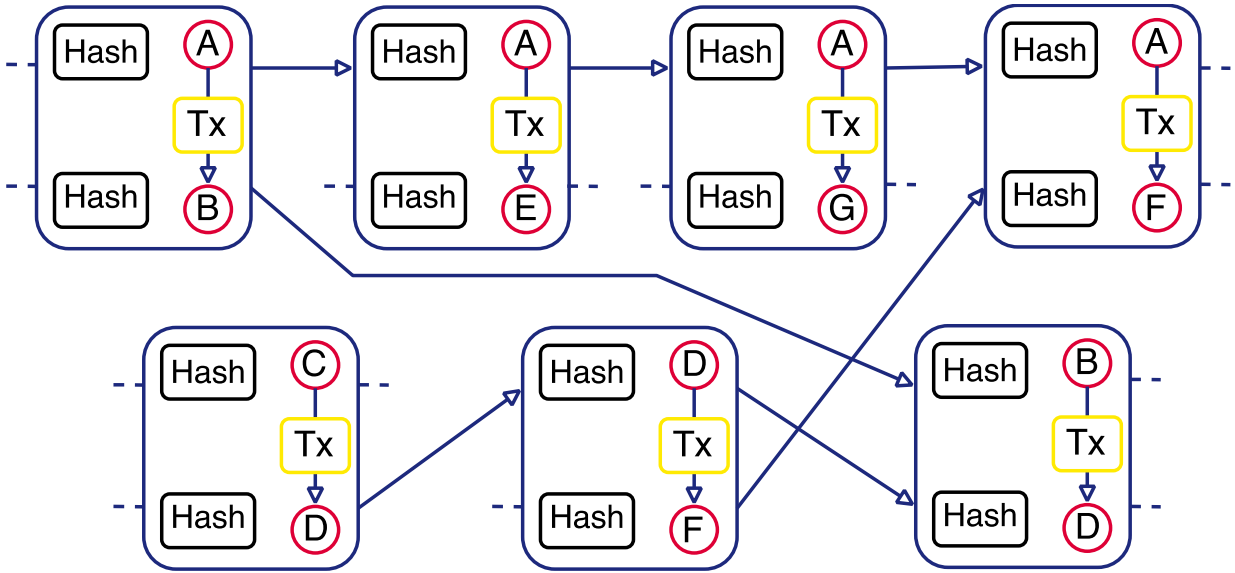
- Scalability is often limited by requirement for global consensus.
  - Proof-of-work, BFT
- Is global consensus necessary?
  - It is desired if you need scarcity
- What if we can guarantee eventual detection of fraud?
  - Like credit card companies

Transaction Ledgers

- Observation: many blockchain systems are transaction fabrics.
  - Money transfers (Bitcoin, Litecoin)
  - Contract invocations (Ethereum)
  - Attestations (Our ongoing research)

TrustChain

- A scalable blockchain fabric to build trust



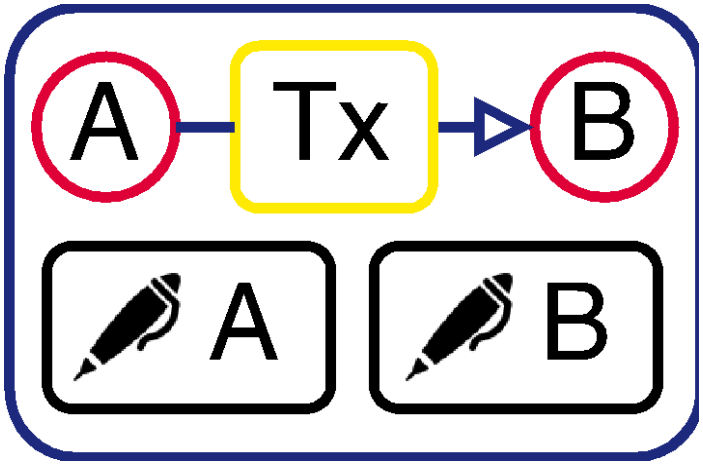
TU Delft

DELFT BLOCKCHAIN LAB

Otte, Pim, Martijn de Vos, and Johan Pouwelse. "TrustChain: A Sybil-resistant scalable blockchain." *Future Generation Computer Systems* (2017).

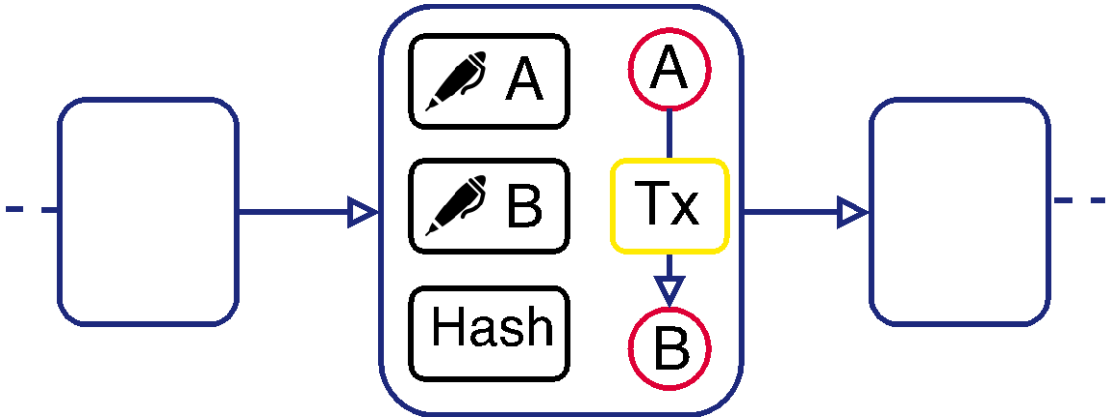
Transaction

- Consider a transaction between two users
- Both users sign the transaction
  - Using any secure signing algorithm



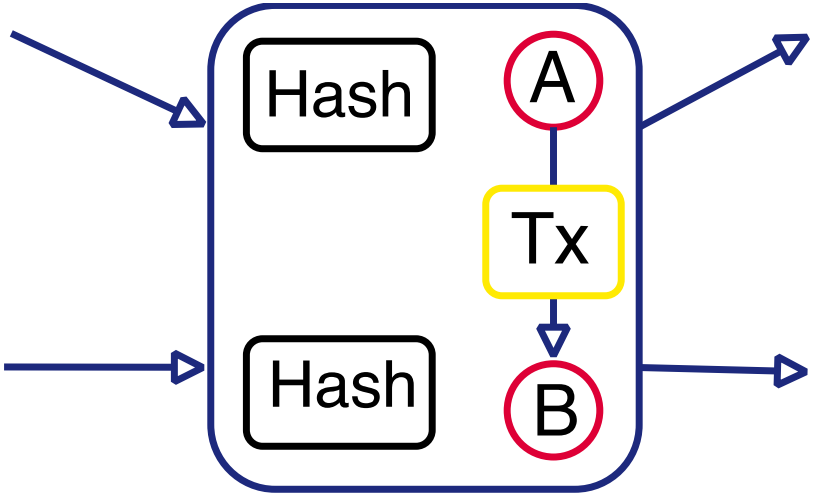
Transaction Chaining

- We can chain these transactions together
- Each users keeps track of his own transaction history

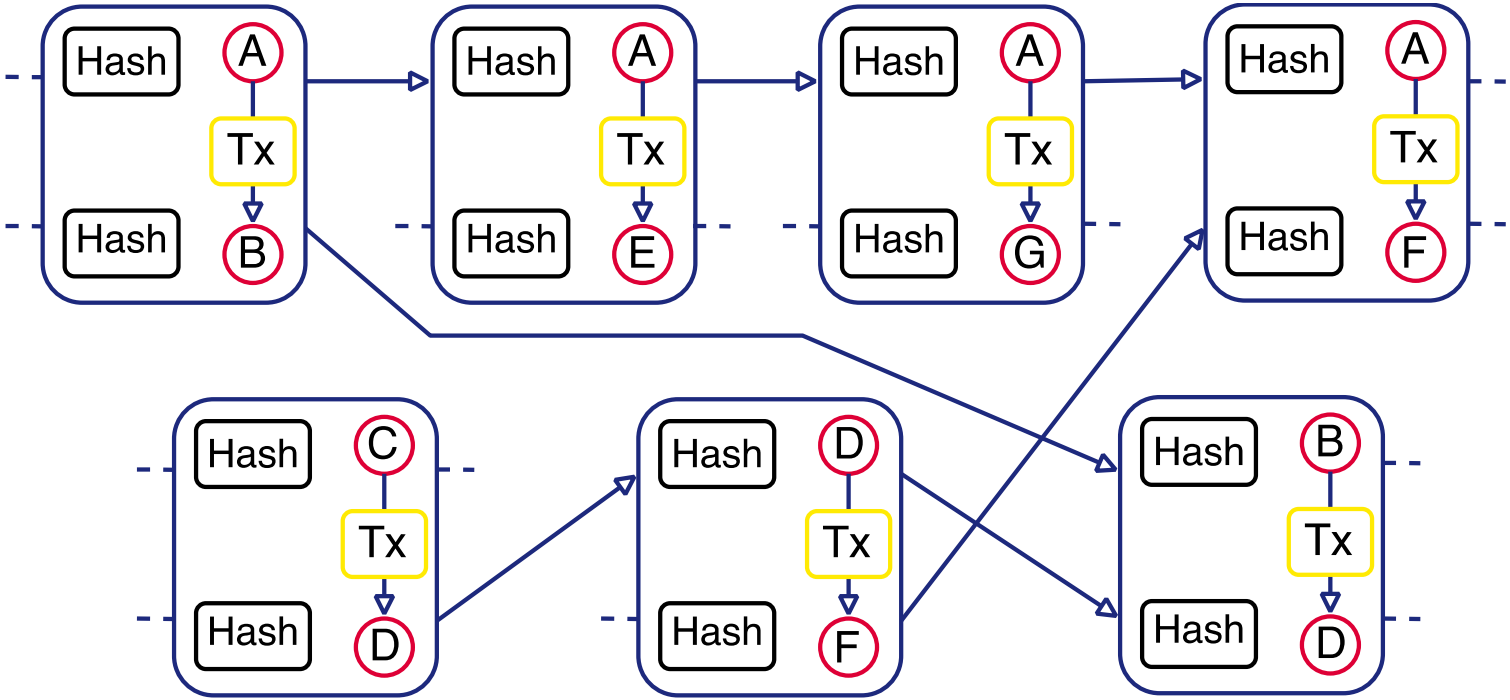


Improving Security

- We add an additional pointer to each block
  - Points towards the previous block in the chain of the transaction counterparty



Entangled Chains



TU Delft

DELFT BLOCKCHAIN LAB

Properties of TrustChain

- Entanglement
  - Makes our chain tamperproof
- Eventual detection of a double-spend
  - By gossiping blocks through the network

Advantages

- Higher transaction throughput
  - No (hard) requirement for global consensus
  - However, global consensus improves security
- Less storage required
  - At a minimum, every participant only needs to store their transactions

Research Goals

- Determine how TrustChain can help to accurately store transactions.
  - Bandwidth accounting
  - Attestations
  - Generic asset trading
- **Build trust between interacting strangers.**

TU Delft

TrustChain

A scalable blockchain fabric to build trust

Martijn de Vos
Distributed Systems

TU Delft