Spontaneous Sharding: Why Value Transfers in Blockchain Should Scale-out

Zhijie Ren, Kelong Cong, Taico V. Aerts, Bart. A. P. de Jonge, Alejandro F. Morais, and Zekeriya Erkin

Blockchain

- Blockchain is a decentralized system deployed in an unsafe environment.
- In most cases, it is in form of "distributed ledgers".
- Transaction (tx) is a message representing value transfer.
- Double-spending prevention is the key for value-transfer systems.

Consensus

- Traditionally, all tx need to be acquired by all nodes to prevent double-spending.
- Byzantine fault tolerance algorithms is used:
  - POW, POS, PBFT, etc.
- However, is will not scale-out: throughput will not increase as network grows.

Scale-out

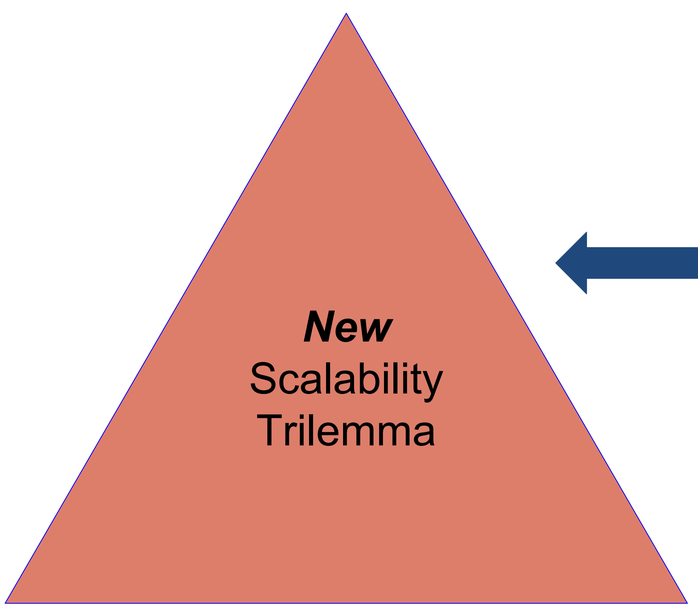
- Scale-out throughput = tx's only acquired by a part of the network.
- Techniques:
  - Off-chain
  - Directed Acyclic Graph (DAG)
  - Sharding
- However, security / decentralization is compromised

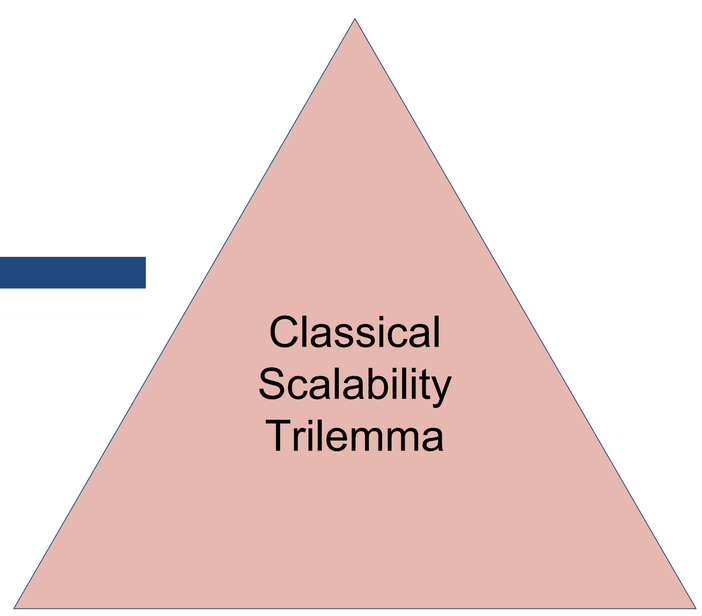
Security

Value-Transfer

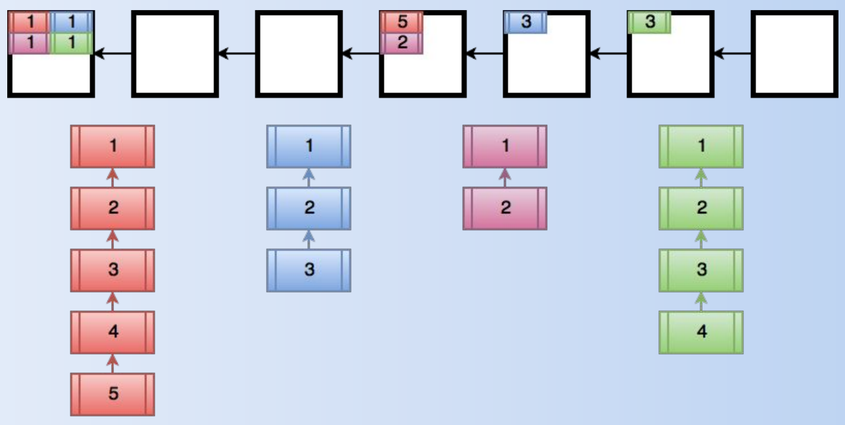
- However, classical BFT algorithms are redundant for value-transfer ledgers → they are for general data, not tx's.
- The essence of value in a tx is discarded, which are:
  - Tx is a process of value transfer.
  - Sender should prove the value is authentic to the receiver.
  - The receiver should verify it.
  - Nodes care about value, rather than tx's.

Functionality:
value-transfer, rating, content sharing, certificate revoking, etc.





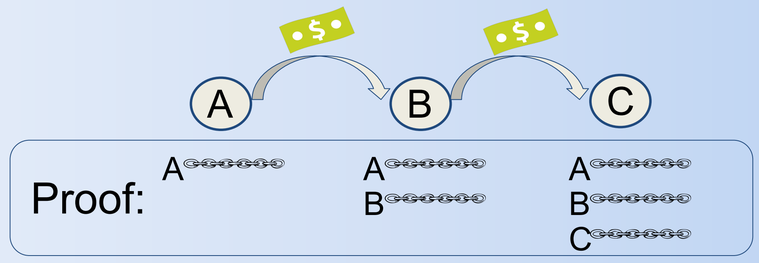
Blockchain for Value-transfer



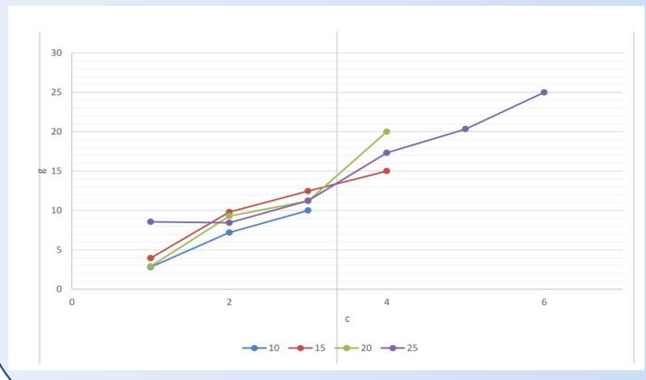
- One main chain for global consensus and individual chains for their own transactions.
- A tx is confirmed if an abstract of it or after it is on the main chain.
- A proof is associated with each piece of value.
- Proof size depends on the transaction pattern.
- Sender is obligated to provide proofs to the receiver.

Spontaneous Sharding

- For each piece of value, its proof includes the chains of all nodes that it has passed:



- Spontaneous Sharding:



- Rational nodes will try to save transmission and storage cost by cycling value in small circles.
- Result = each node only acquires some chains.
- In other words, we achieve scale-out performance with no compromise in security and decentralization.

TU Delft

Zhijie Ren
Postdoc Researcher
Cyber Security Group
Department of Intelligent Systems

Delft University of Technology
E-mail: z.ren@tudelft.nl
Telephone: +31(0)15 2783227