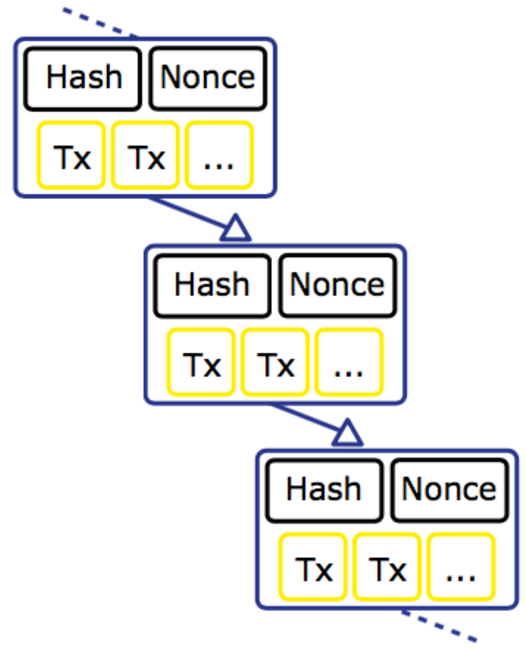
TrustChain: Building Trust with Distributed Ledgers

Martijn de Vos, Johan Pouwelse, Dick Epema
peer2peer@gmail.com

Blockchains

What is a Blockchain?

- A chained data structure to store transactions.
  - Tamper-proof
  - Distributed
  - Each record contains a hash of the previous record



Applications

- **Cryptocurrency:** Bitcoin, Ripple.
- **Distributed computing:** Ethereum.

Problems

- **Scalability:** consensus requirements limit scalability.
  - Bitcoin is limited to seven transactions per second.
- **Storage:** blockchains can become very large.
- **Double spending:** users can lie about transactions.

TrustChain

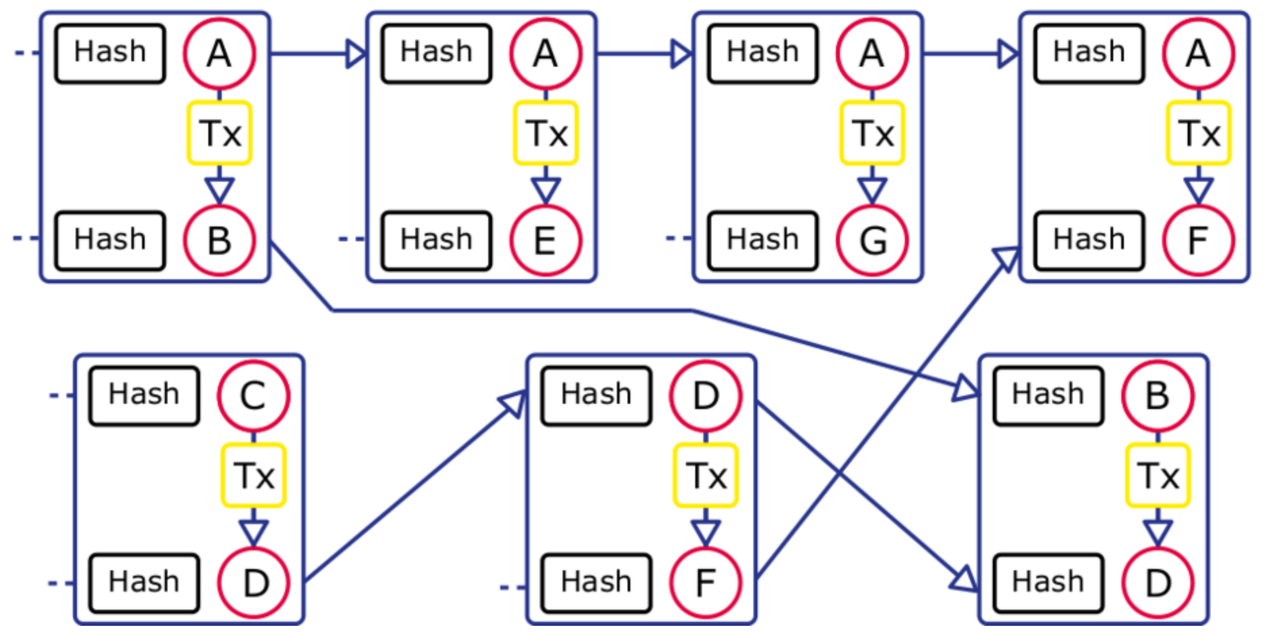
Design Specifications

- Each user maintains their own chain of records.
- When performing a transactions between two peers, their chains get intertwined or "entangled".
- Computationally efficient to verify the validity of each chain.

NetFlow

- Sybil-resistant reputation mechanism using the TrustChain graph as input for trust estimation.
- Based on max-flow computations.

TrustChain architecture with four intertwined chains



Evaluation

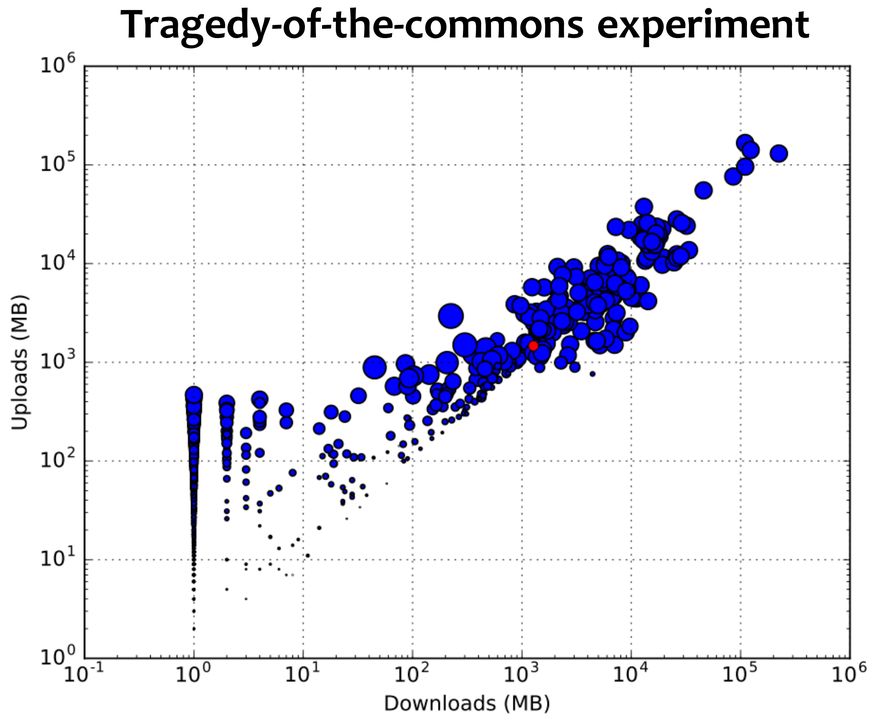
Free-rider Identification

- Implemented TrustChain and NetFlow in Tribler, our P2P file-sharing software.
- We effectively identified free-riders in our network (addressing tragedy-of-the-commons).

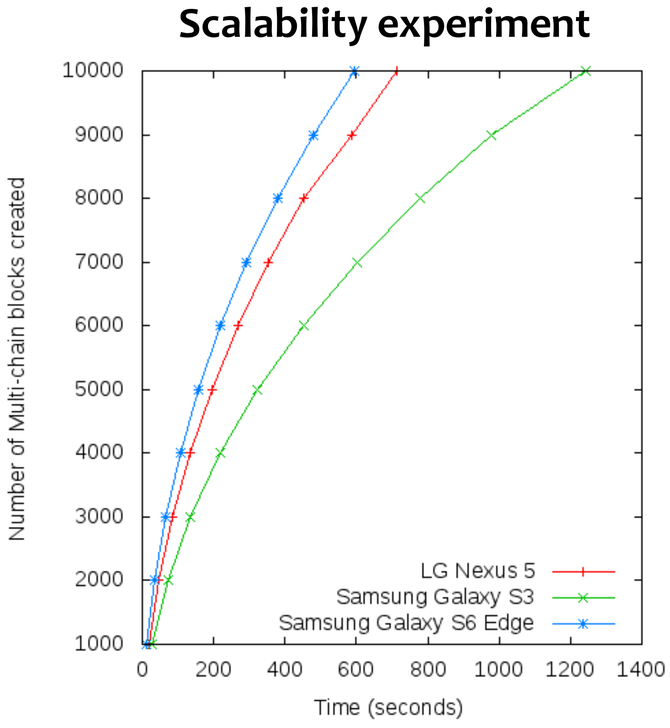
Scalability

- Tested on Android devices.
- Record creation speed is superior compared to traditional blockchain implementations.

Tragedy-of-the-commons experiment



Scalability experiment



TU Delft
Delft University of Technology

Distributed Systems Group
www.ds.ewi.tudelft.nl

Blockchain Lab
Blockchain-lab.org