

HS18

DISTRIBUTED SYSTEMS ADVANCED & BLOCKCHAIN

IOTA

T. Bocek

thomas.bocek@hsr.ch

Distributed Systems - In the News

■ 22.10.2018 Why bother with P2P when you still need to guarantee uptime?



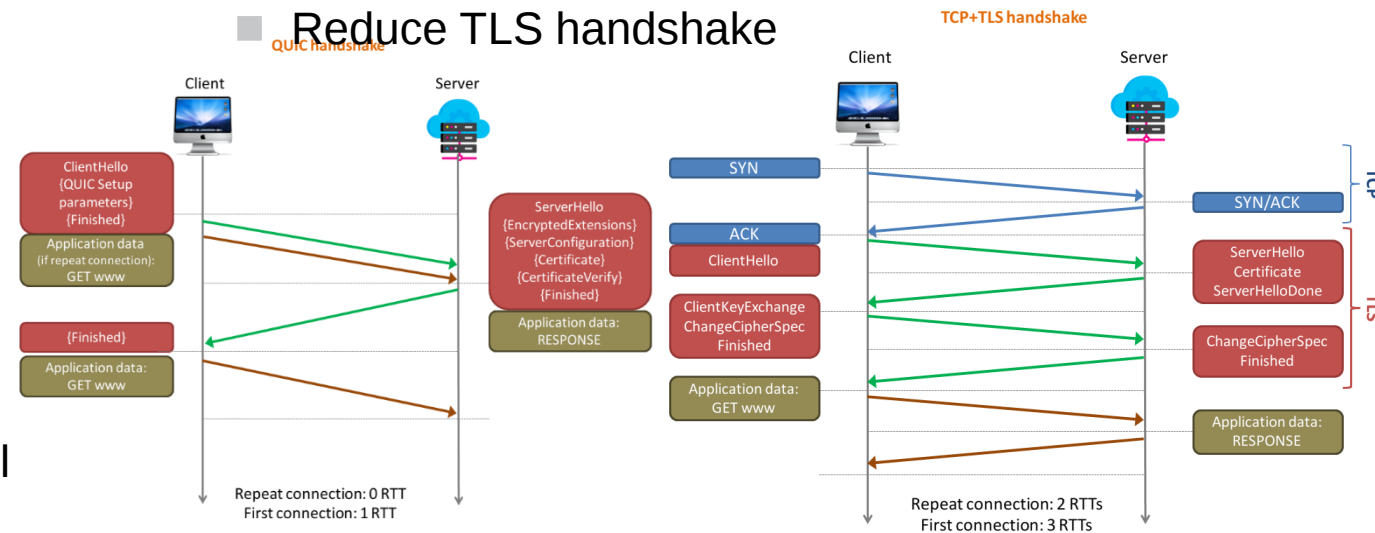
- Why bother: It's cheaper
- Why bother: It's disintermediating
- "Maybe someday a peer-to-peer protocol will guarantee uptime."

■ 29.10.2018 Problem with PRL contract

- "People are sending Ether to the contract at a rate of 1 ETH to 5000 PRL tokens (0.0002 Eth per PRL), which means that they can sell it for higher on Kucoin.." ([exit scam](#)) ([CEO](#))

■ 28.10.2018 QUIC will most likely be HTTP v3

- HTTP/3, to avoid confusion
- Reduce TLS handshake



■ What is IOTA?

- “A permissionless distributed ledger for a new economy” - for IoT
- Zero transaction fees / feeless microtransactions and data integrity for machines
 - A node can only issue a transaction after solving a cryptographic puzzle
- Quantum-proof algorithms
- “It is safe to receive any number of transactions to a given address until an outgoing transfer (a "send" transfer) is made. After that, this address should no longer be re-used!”
 - Sending IOTAs - part of the private key of that address is revealed (brute force)

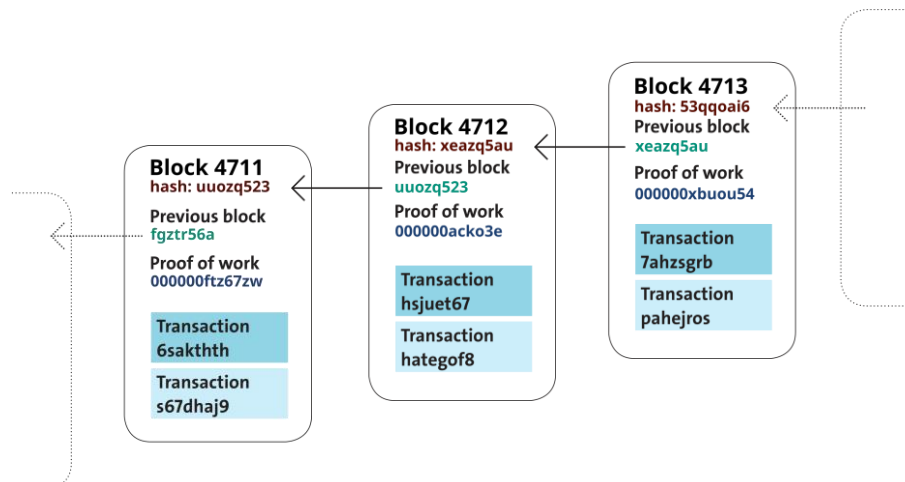
■ An Open-Source Distributed Ledger

- Uses a Decentralized Acyclic Graph (DAG) instead of a blockchain ([Tangle](#))
- Tangle: transaction must approve two previous transactions in order to be considered valid.



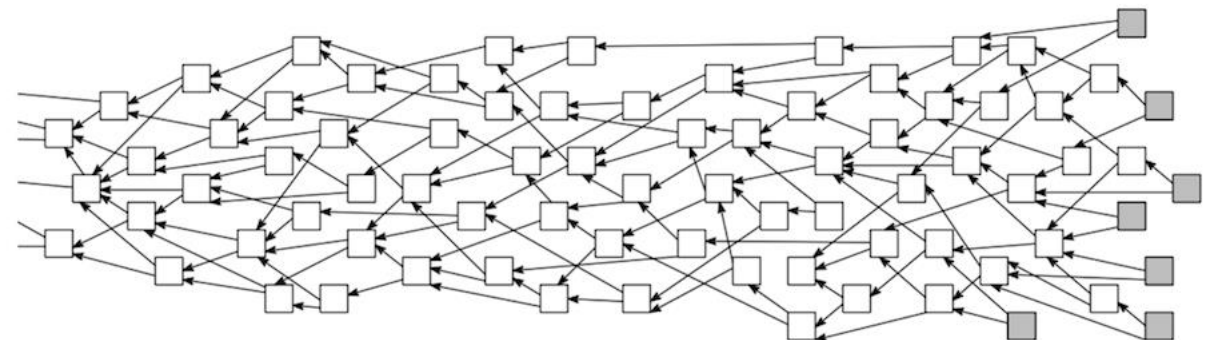
■ Blockchain

- Blocks with transactions linked to each other
- Decentralized, used in: Bitcoin, Ethereum ([uncle blocks](#)), NEO
- Transactions / sec limitations
- The older a tx in a block, the more secure



■ DAG

- Transactions linked to two previous tx
- Regular milestones (centralized?)
- More activity = more validation ([but spam attacked happened in the past](#))
- The more confidence in a tx, the more secure
 - Tip selection: weighted random walk from the genesis towards the tips
 - Run the tip selection algorithm 100 times.
 - Count how many of those 100 tips approve our transaction, and call it A.
 - The confirmation confidence of our transaction is "A percent".



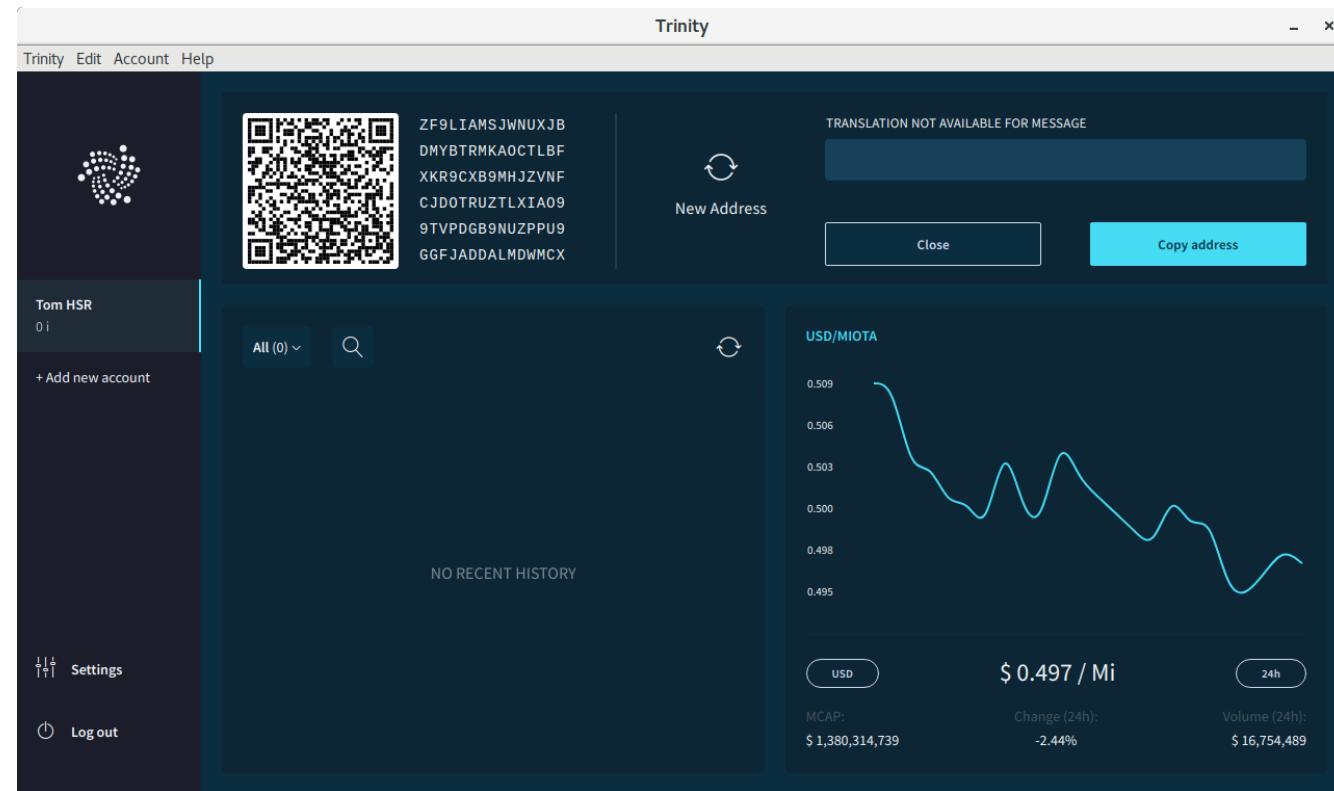
- **Milestone:** every 35 seconds the Coordinator makes a normal transaction, confirming 2 tx
- **Want to know if your tx is verified, get latest milestone and check**
- **Milestone comes from Coordinator / trusted source**
 - Pick random node – may be malicious
- **Eventually will be switched off, now active due to small network**
 - “The only role the Coordinator serves is to protect against attacks in this temporary infancy stage of the Tangle ledger,..”
- **“IOTA is currently in what should be considered a ‘transition period’ towards large scale deployment and standardization.”**

■ IOTA Snapshot

- Pruning: “This is essentially a “pruning” of the ledger - it removes all events and addresses on the ledger which do not have a positive balance.”
- “As you probably already know, we are performing global snapshots of the IOTA network on a more or less regular basis. The main motivation for global snapshots is to prune the database and allow smaller nodes to keep participating in the Mainnet.”

IOTA Wallet

- Never write your own crypto algorithms
- **Wallet:** <https://trinity.iota.org/>
 - Reference implementation in Java: <https://github.com/iotaedger/iri>
 - API in many languages: C#, Javascript, ...
 - Live demo in the challenge task presentations
- **More documentation**
 - <https://ukcryptocurrency.com/iota/introduction-what-is-iota/>
 - <https://docs.iota.org/introduction>
 - <https://blog.iota.org/the-tangle-an-illustrated-introduction-79f537b0a455>



Questions?

Prof. Dr. Thomas Bocek thomas.bocek@hsr.ch
Roman Blum roman.blum@hsr.ch