Topics I deem important (in order of importance to Tribler)

Reliable block replication mechanism
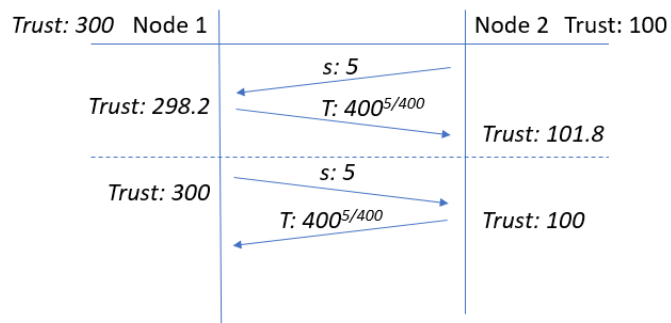
- ▪ According to Vadim a missing feature, and would be very valuable
- ▪ Was briefly brushed upon in proposal
- ▪ Main trick is to use DHT for ID and block look-up (just as Kademlia)
    - • Use previous-bock hash to determine location the block will be pushed
        - Results in at least two copies (for each party one replica)
        - Speeds up forward traversal over chains
    - • Use current block's hash to determine location
        - Results in at least one copy of block
        - Enables fast backwards traversal over chains
    - • The replication factor can be based on trust
        - Transacting with a lesser trusted or more often offline node? Replicate across more nodes.
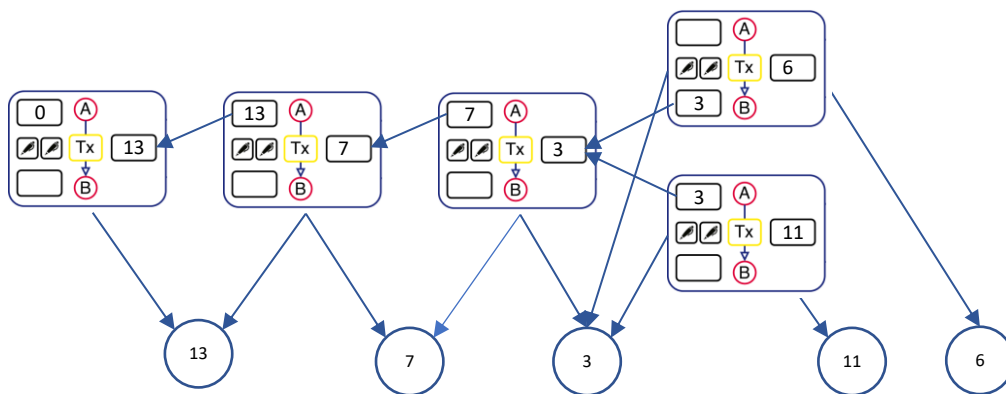
- • Next to transact can easily detect the fork by looking for the block by the hash '3' in the DHT
- • Node 3 could directly detect this
- • In case of witnesses, they could detect

Global consensus on a node's trust (with O(1) look-up)

- • Includes transitivity of trust
- • Total amount of trust within a certain cluster will never increase without net data contribution. (Does this imply sybil resistance)
- • Calculation of new trust seems to be O(1) as well:
- • Use of iterative sum (with partial sum stored in trustchain)
- • Bootstrapping could be done through allowing x% of transactions to also be done with lesser trusted nodes
- • If both 'Trust' and 'Transaction size' are stored within transaction block verification can be easily done.

Trust: 300   Node 1 | Node 2   Trust: 100

s: 5

Trust: 298.2 — T: $400^{5/400}$

Trust: 101.8

s: 5

Trust: 300

T: $400^{5/400}$ Trust: 100

Value privacy and sender-receiver anonymity.

- Implementing privacy and/or anonymity in Tribler would reduce the tracebility and would introduce plausible denial

Tribler plugin that allows for payment bandwidth tokens through the proposed platform

- Requires all of the above to be done (to a certain degree).
- Requires a trusted financial endpoint:
    - Start a payment service provider (long process, relatively expensive).
    - Use European bank account (Not very reliable, probably illegal)
    - Use PayPal (Fee's + boring, probably violates their terms and agreement)
    - Any other cryptocurrency (volatile, but easy and hard to take down