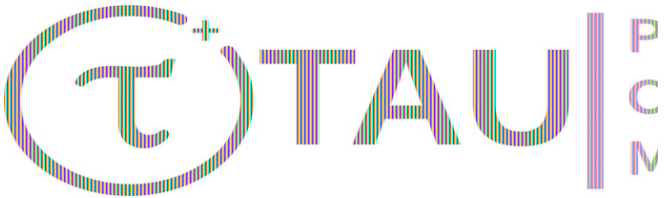

Propose a “Perishable Proof of Transaction(PPOT)” Consensus

- To enable phones with day-to-day blockchain apps without tie to servers

Token 2049
Oct 2021, London

#open-source #perishable #dht #libtorrent #server-less #permission-less #PPOT

Immutable blockchain, BTC, ETH, ADA - Community remembers full history collectively

- Benefits: good for long term assets and contracts
- Problems: ever increasing ledger size and the cap of main-chain scaling - restricts pervasive daily life applications such as order food, booking rooms and call taxi

Perishable blockchain - history beyond a time frame such as 6 months will be forgotten

- ONLY accounts with transactions in past 6 months will be valid.
- Designed to manage user's address(pubKey) and its communication; vs financial contracts.
- Demanding lower computing resource, a smart phone can operate 100 blockchains independently, so that communication speed is only limited by bandwidth
- Small community with no need of server resources can build coins system to discover value and run server-less daily applications such as delivering a pizza.
- The more communities, the higher transaction volume scales.

Perishable Proof of Transaction

- The more transactions made, that higher chances one can generate new blocks to take rewards, thanks to NXT.
- PPOT only remembers 6 months blocks history. TAU is the first team explore this idea.
- Permission-less mining and none-delegates principle from bitcoin.
- Holding shorter history flaten computing resource demand and limited size of a community, in return for parallel independent communities on phone swarms, so that communication speed is only bound to bandwidth.
- Transaction pool is converted to communication pool.
    - Each participant has a pool now, verse server nodes.

Networking

- Extended “Distributed Hash Table” from libtorrent provides nodes discovery with some changes
  - Choking design for creating incentive to share data
    - An indefinite prisoner dilemma equilibrium
    - Without choking, pure gossip(eth) protocol will cause data transmission volume explode or centered.
  - Public key as node ID to form relay coop with closer prefix peers.

- UDP with Levinstein distance to form payload integrity replacing TCP or uTP sequence based connection
  - On phone swarm, there are no stable relay nodes to establish any connection.
- Mutable data item becomes each nodes “life signal” to maintain swarm stability.

Defense attackers and some small things…

- POS secrete chain attack include history reorganization and nothing on the stake.
- NXT stake shifting attack
  - Mining power can only be burned not transferred in PePOT
  - BFT types of delegates
- DDOS attack: swarms is naturally hard to apply DDOS vector

- Concept of negative block numbers to help community rebellion.
- Transaction pool is replaced by communication pool to speed up message scaling.
- No need of TAU coins for building your own coins system, as design principle to reduce user experience infliction

- Website - https://taucoin.io
- Github - https://github.com/Tau-Coin
- Telegram - https://t.me/taucoin
- Medium - https://medium.com/@davidwu_30530
- Reddit - https://www.reddit.com/r/Tau_coin/
- White Paper - https://github.com/wuzhengy/TAU