



DAOLINAME

An Attempt to Speed UP + Scale Up Permissionless Blockchain

DaoliName DAO

January 2020

https://github.com/DaoliName/daoliname/raw/master/DTB_Chain.pdf

Content



Studies and thoughts on permissionless blockchains: What can really be more fundamental as consensus than voting for a data base writer?



What if we have internet wide available **time**

- No matter how mighty in computation power one might be, one cannot reverse, nor go ahead of, time
- Consensus in time order: Easier, fairer and speedier to reach than waiting for a “Might is Right” long chain to appear, and certainly more practical and scalable than $O(n^2)$ online discussions among permission-only Byzantine Generals

With the availability of **Decentralized Time Beacon**, permissionless blockchain with correctness, liveness, anti-denial-of-service, scalability, low latency, decentralization and anti-Sybil properties can be built

Discussion: On the virtue of standing on more fundamentals

Studies and Thoughts



Studied well-known Proof-of-Work blockchains
None of the PoW chain has avoided bothering on: “What if some powerful miner(s) created a ***secret long chain*** to revert a done deal?”

So, might is NOT right! The status-quo quality for consensus from PoW we have today:
Poor scalability and slow confirmation



PoW is however an effective anti-DDoS voting for DB writer by permissionless nodes in a potentially scalable peer network

There is something to be **more fundamental** than anti-DDoS voting:
Internet wide decentralizedly available time event; we now fortunately do have such

Decentralized Time Beacon (DTB): A permissionless blockchain's block broadcast can be used as time event service; Ignore its possibly dreadful consensus on its daily chores, even its forking branches still prove time is flowing forward; Build an overlay chain on top of it

“Handcuff” PoW Power

Input: a DTB service (we are implementing an **overlay blockchain** using Ethereum block events as DTB service)

The overlay chain still uses PoW to vote for DB writers; nodes PoW extend chain as usual, however now to hash some new elements:

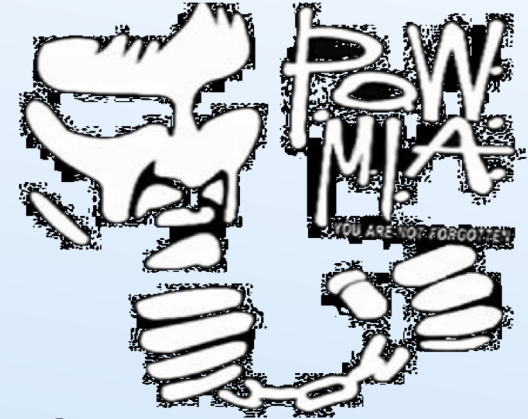
1. Current TimeBeacon, 2. Empty TX, 3. Self IDs

This is the same as mine a “KeyBlock” in Bitcoin-NG;

Upon winning to broadcast KeyBlock, the winner (in fact, its distributed contingent of nodes, see slide 7) starts to sign & broadcast real TXs blocks, as “MicroBlocks” in Bitcoin-NG, however each MicroBlock must also include a new TimeBeacon; now size of a MicroBlock becomes non-issue, so **scale** is already up

Losers go to work on voting a next KeyBlock on a new TimeBeacon, in case of KeyBlock fork, see Liveness analysis in Slide 6

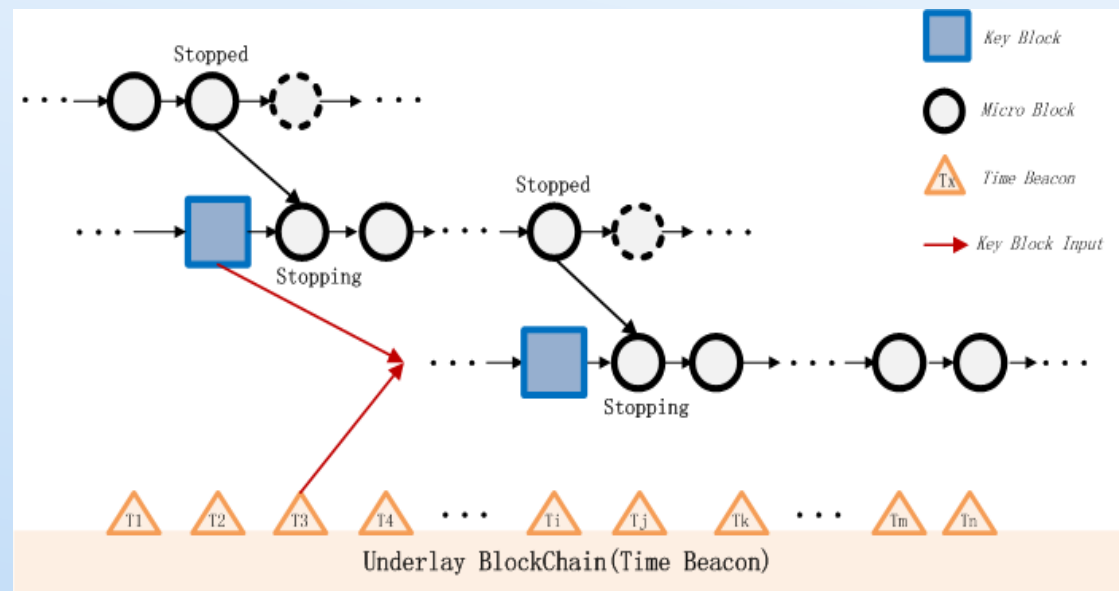
Mining a (secret?) long chain is possible only in the underlay chain, but upon opening, the underlay long chain becomes valid DTB for overlay



Correctness

The first MicroBlock of a newly won KeyBlock, which we name **Stopping MB**, in its input includes the last **correct** MicroBlock, which we name **Stopped MB**, of the previous KeyBlock; the correctness MUST mean:

1. All TXs in all MicroBlocks preceding and including the Stopped MB, of the previous KeyBlock, be correct; AND
2. The TimeBeacon in the Stopped MB be earlier than that in the Stopping MB



Thus, if and only if correct TXs, which are connected by Stopping MBs and Stopped MBs (solid circles), are appended in the ledger

Liveness and Confirmation Speed



The order of TimeBeacon (the block height of the underlay block included in the won KeyBlocks) decides overlay PoW winner

In case of TimeBeacon tie, collision-free PoW hash deterministically breaks tie

These computations can be **locally** decided by each node in the entire overlay peer network, and so voting consensus for overlay ledger writers is deterministic

Hence, there can be **no fork** for KeyBlocks in the overlay chain

Mining empty TX means a tiny small payload for KeyBlocks, and so the won KeyBlock broadcast can quickly propagate to the whole peer network for them to concede voting (Decker & Wattenhofer 2013)

Therefore, liveness for the no-forking overlay chain is even improved from that for Bitcoin, confirmation time is within one KeyBlock epoch



Anti Denial of Service

A permissionless blockchain having high throughput and quick confirmation properties inevitably invites Denial-of-Service attacks; in fact, GHOST, DAG, BitCoin-NG, all expose to DoS, e.g., Ethereum, uses very costly memory PoW difficulty with a downgraded GHOST (obscured up to 2 “uncle blocks”); some, e.g., Inclusive Blockchain, Conflux, with no discussion at all of DoS attacks



Anti-DDoS for the DaoliName DAO proposal:

- Let KeyBlock and MicroBlock nodes be distributed with different and even better dynamically changing IP addresses
- Let PoW won KeyBlock contain a plural number of public keys of distributed MicroBlock nodes
- The contingent of MicroBlock nodes of the PoW won KeyBlock node can one-by-one announce MicroBlocks, gracefully utilizing the very expensive PoW won long time interval
- Announce-then-shut-up nodes cannot be DoS-ed while enjoying the won PoW long time interval in the permissionless peer network

Anonymity + Zero-Knowledge Proof Enabled Know-Your-Customer



A bilinear pairing based signature scheme can be used to sign and verify TX's

For petty cash TXs, the user enjoys anonymity as in other permissionless blockchains

To make a KYC regulation required TX, e.g., an international payment, Alice can link her true ID, e.g., bank account info, using the pairing based non-interactive zero-knowledge proof



Any uniquely identifiable bit string, e.g., a bankcard description, an email address, etc., can play the role of a public key to verify the KYC required TX NIZK proof

A special setup TX for linking a KYC ID and an anonymous public key (wallet address) can be verified by a designated node, e.g., the user's bank, as a service; the simulatability of NIZK prevents the verifier from showing the ID-address link to any 3rd party

Standing on Fundamentals



Discussed here is tentative, however may manifest benefits standing on more fundamentals

Let TXs be DTB stamped so they are indexed in monotonic increasing order of the underlay chain's block heights

The history of blockchain's states, e.g., the UTXO set, can be chronicled into much smaller, representing shorter period of historical, TXs state sets, (think of Bitcoin's UTXO set being divided into smaller ones, each indexed in DTB monotonically increasing time epochs)



A lite node can work as a MicroBlock node, only to construct & update chronological TX state sets. To validate a TX, a lite node only needs to load in and update small sized chronological TX state sets which are indexed by the DTB stamps in the input and output coins of the TX, and look-up in the small sets is very fast since the set is DTB **sorted**

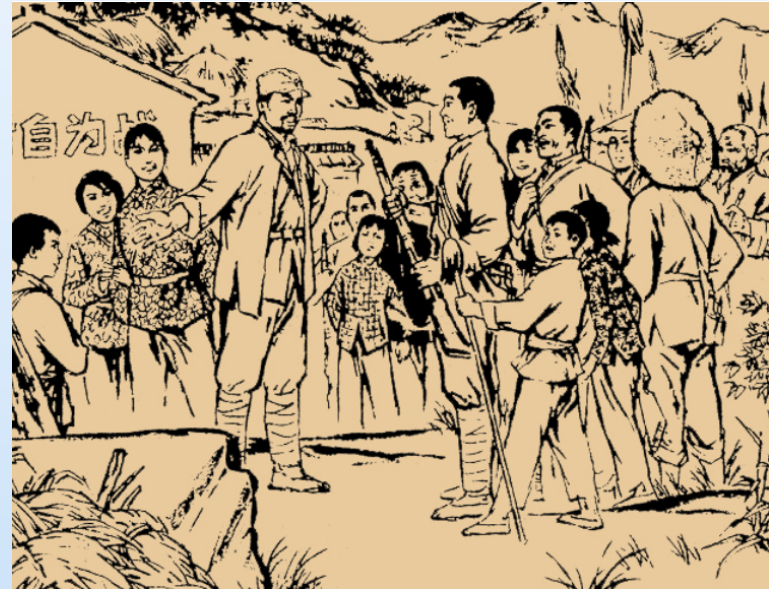
More possible innovations on exploiting DTB virtue are welcome

Decentralization

Hopefully, lite MicroBlock nodes can even be so lite as smartphones or future IoT devices, via some business or service arrangement with a KeyBlock mining full node

The more nodes to be able to participate permissionlessly in the peer network, the the more decentralized and more secure a blockchain can be

Multiple-factor availability of DTB should also render Sybil attacks on clients impractical




Critical Reviews are Suggestions Sought



DaoliName DAO wishes to work with all who reckon that permissionless blockchain is very important and in need of improvement





DA  LI NAME

Date Time: 2020-01-08 17:40:04

SHA256: 0x196fe9aa49af95104fe5c4689e763c87551c296798394d47c0c1a873ec2a2c5a

SHA512: 0x07b892495d355bb7e5480a34d9ac40f2c7ccc0c41b3914c7498b3f6a65c8f187
d2fd06b21d5064e710176834f1e09117a71a95225f74b71e140a615341418d5c