An Attempt to Speed UP + Scale Up Permissionless Blockchain

DaoliName DAO

December 2019

Studies and Thoughts

- Studied well-known Proof-of-Work based blockchains
- None of the PoW chain can avoid bothering on: "What if some powerful miner(s) PoW a ***secret long chain*** to revert a done deal?"

- So, "Might is NOT Right", ***The only and best*** status-quo consensus today: ***Slow Confirmation***
- Our view: PoW is up to anti-DDoS, and this is not too bad
- Is there anything out there to handcuff PoW power abuse?
- If some time events (aka time beacon) can be commonly heard, an ***easier consensus*** is reachable: No one can go ahead of time
- Decentralized Time Beacon (DTB): We now fortunately do have internet available DTB service! Ironically, such DTB is from PoW! Use an underlay blockchain mining output as time event!

DTB “Handcuff” PoW Power

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

Let a PoW difficulty be exponentially hard to fork (as in BitCoin); Overlay nodes PoW extend chain as usual, however hash some new elements: 1. Current TimeBeacon, 2. Empty TX, 3. Self ID; This PoW is like to mine a “KeyBlock” in BitCoin-NG; Mining empty TX minimizes network propagation time (Decker and Wattenhofer 2013)

Upon winning (& broadcast) KeyBlock, the winner starts to sign & broadcast real TXs, 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 a new KeyBlock, of course on a new TimeBeacon

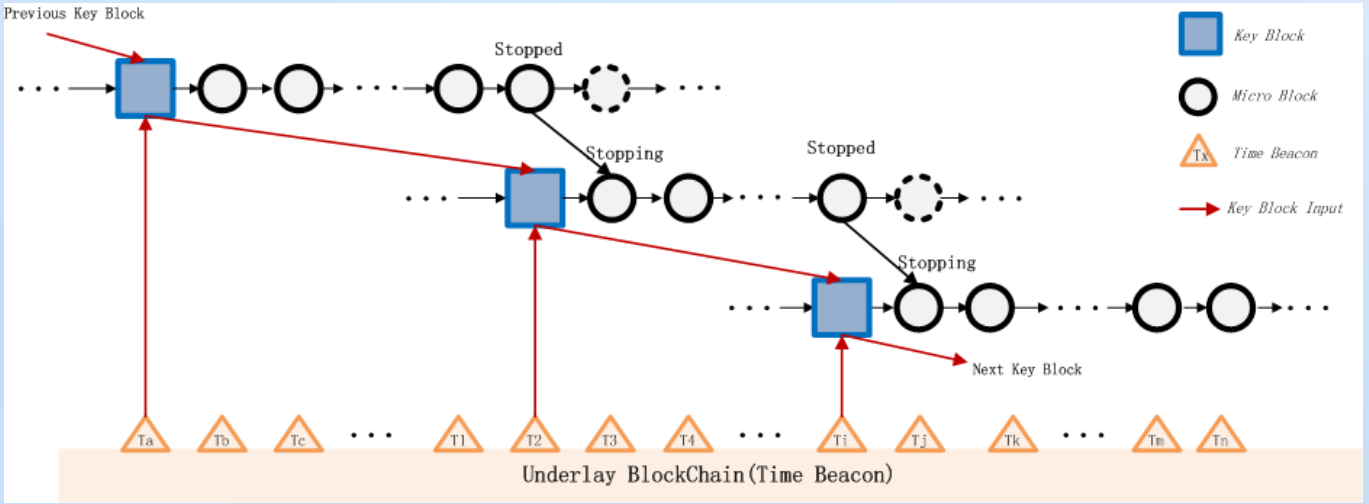
In an unlikely event of KeyBlock forking, mining difficulty (smaller hashing output) breaks tie deterministically

Can a secret long chain be mined? If not, confirmation **speed** is up!

Correctness

The first MicroBlock of a newly winning KeyBlock, which is called **Stopping MicroBlock**, in its input includes the last ***correct*** MicroBlock, which is called **Stopped MicroBlock**, of the previous KeyBlock; the correctness means:

1. All TXs in the Stopped MicroBlock, and those in all preceding MicroBlocks of the previous KeyBlock, are correct; AND
2. The TimeBeacon in Stopped MicroBlock is earlier than that in the Stopping MicroBlock



If and only if the correct TXs, which are connected between Stopped MB and Stopping MB, are appended in the blockchain

Liveness

The Chain of KeyBlocks is essentially the same as BitCoin with TimeBeacon, Empty TX, ID (= public key for verifying MicroBlocks) as block input

Therefore liveness for this new blockchain is the same as that for BitCoin

Anti Distributed Denial Service Attack

A permission blockchain aiming at high throughput and quick confirmation would naturally and likely subject to DDoS attacks

In fact, GHOST, DAG, BitCoin-NG methods all suffer from DDoS attacks, some, e.g., Ethereum, use high PoW-memory difficulty and obscured GHOST (up to 2 “uncle blocks”), some, e.g., Inclusive Blockchain, Conflux, totally avoid discussing DDoS attacks

The DaoliName DAO proposal's Anti-DDoS method:

- Let the KeyBlock and MicroBlock nodes be distributed with different and even better dynamic IP addresses
- When the KeyBlock node announces PoW success, a plural number of public keys of distributed MicroBlocks are announced, the KeyBlock node then turns to silent
- The contingent of MicroBlocks nodes then each announces MicroBlock, one-by-one and in turn of order, using un-revealed IP addresses

Anonymity + Zero-Knowledge Know-Your-Customer

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

For petty cash transactions, the user enjoys anonymity as in 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

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

Datetime: 2020-01-06 09:40:06

SHA256: 0x19dd0ca5f2afe18ba597aa39395fb8d3230454fc19cbfb3cb8c93690f32a4654

SHA512: 0x2a8f2313ff03c9b9668ae3a597b880a2591e91b6947006148765e2fe679b9f78
c1c9d99d69a82b5501ae48a139ad83caf01e143c4ddbb44dde6374a190613f09

DA名LI NAME