Metaverse: Pillars of Creation (MPC)

Key Words:

1.) Hybrid Consensus Mechanism
2.) Dual Chain Architecture
3.) Mining for tokens (MST)
4.) 51% Attack Solution
5.) Nothing-at-Stake Attack Solution
6.) Functional Smart Contracts
7.) Decentralized Social Credit System (MARS)

Abstract

Metaverse Pillars of Creation (MPC) is the next major mainnet upgrade to Metaverse since the release of SuperNova in 2018. MPC supports a three-pronged hybrid consensus mechanism composed of PoW+PoS+DPoS. This hybrid consensus algorithm will prevent any 51% attacks, PoS Nothing-at-Stake attacks, and allow for Metaverse Smart Token (MST) mining. MPC also introduces the Metaverse Avatar Reputation System (MARS), an open, decentralized social credit system based on Metaverse Digital Identity. In the initial whitepaper draft, we described a type of programmable smart assets. In MPC these will be implemented based on verifiable smart contract templates. While designing the above functions, we lay the foundation for a layer-2 architecture in Metaverse called Binary-Port-Chain. The second layer chain for standardized digital identity and functional smart contracts will help enterprises connect highly scalable services to the main Metaverse chain. We call this dual chain structure the Metaverse Binary System.

We will release MPC in two phases. In the first phase, we upgrade the consensus mechanism, activate MST mining, and set up the MARS system. In the second phase, we plan to implement programmable smart assets and the Metaverse Binary System.

Foreword

We divide Metaverse development into 4 main stages:

1. First Release (February 2017 to June 2018): issued ETP and provided the basic functionality of digital assets
2. SuperNova (June 2018 to March 2019): upgraded the capabilities of digital assets and added digital identity

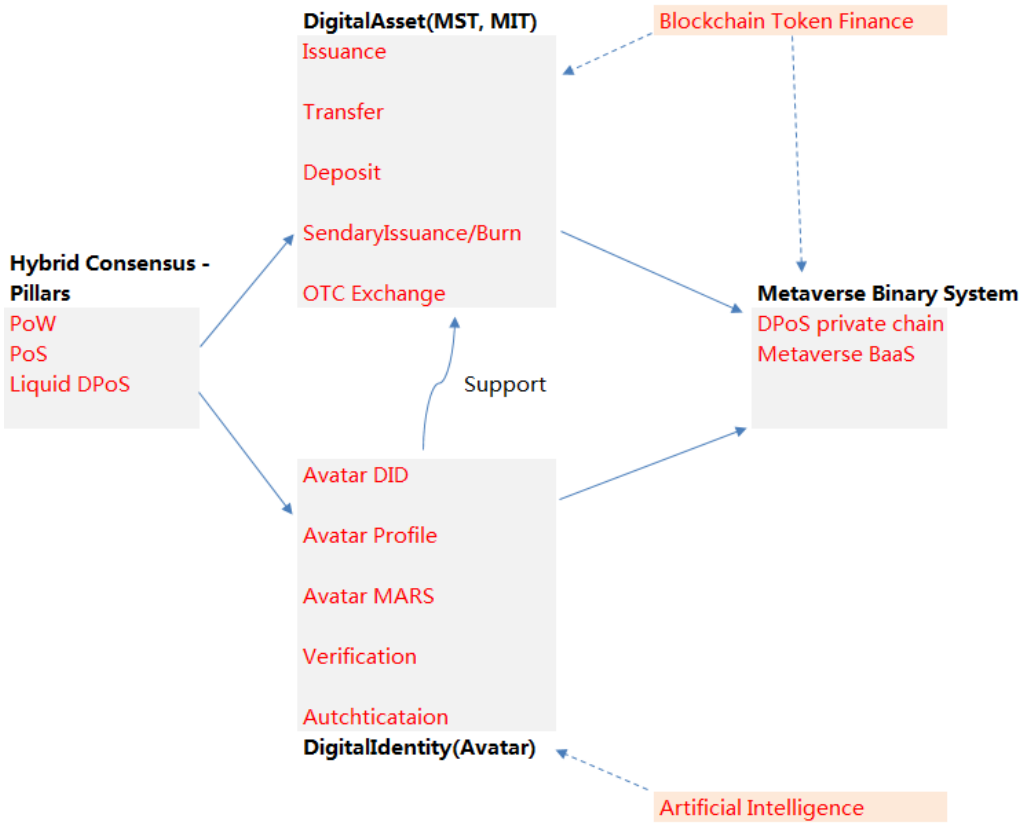
3. Pillars of Creation (March 2019 ~ 2020): dramatically increase TPS, upgrade digital identity, and add smart assets
4. Galaxy (~2020 and on): micro-inflation macroeconomic model, oriented to blockchain data, will provide digital identity and smart asset standardized service protocols for artificial intelligence.

MPC First Stage

February 14, 2019: Release 0.9.0 full node installation package
March 1, 2019: Activate the Pillars of Creation protocol at target block height 1924000

MPC Second Stage

July 2019



Metaverse Hybrid Consensus: Pillars of Creation

Overview

Pure Proof-of-Work (PoW) or Proof-of-Stake (PoS) consensus algorithms have limited transaction speed (TPS) and do not meet the scalability requirements of mainstream applications. Blockchain designs addressing scalability issues, on the other hand, are forced to make tradeoffs in terms of security vulnerabilities. As far as the current blockchain industry scaling plans are concerned, there are two main approaches:

1. Modify the consensus algorithm itself to improve TPS; or,
2. Modify the structure of the transactions to improve TPS.

Method 1 is more foundational than method 2 and should be the preferred solution. Thus, in MPC we consider a hybrid consensus mechanism to improve TPS without compromising security. Since Metaverse already operates on PoW consensus, migration to hybrid PoW–PoS consensus in MPC is relatively straightforward and fully compatible with the current PoW mining regime.

Hybrid Consensus Mechanisms

Common hybrid consensus mechanisms can be divided into two categories: PoW+PoS and PoW+BFT.

PoW+PoS can be divided into 3 cases:

1. PoW and PoS compete in parallel to generate blocks: UBTC
2. PoW packaged to generate blocks, with PoS finalizing the blocks: i.e. Decred, Casper, Espers
3. PoW and PoS jointly generate blocks, with a fixed proportion and order of block generation

PoW+BFT (or other improvements):

1. PoW generates blocks and then finalizes them by BFT
2. PoW determines Leader, Leader is responsible for writing key–block and micro–block, mainly to solve selfish–mining: represented by Bitcoin–NG, including Credo, Hcash

Metaverse Pillars of Creation (MPC)

Although the PoW algorithm is relatively simple and effective, its security is a function of hash power, raising the possibility of 51% attacks, selfish mining, and other related issues. By analyzing PoS, we know that we can choose PoW+PoS to compete for the block generation based on the foundational and fully compatible PoW consensus algorithm. Finally, the MARS system can activate DPoS on the Metaverse chain. We divide the hybrid consensus Pillars into two phases.

Pillars Phase 1

- Activation Point – block height 1924000
- Average Block Generation Time is 25.02 seconds, PoW percentage y = 90%, PoS percentage z = 10%

PoW Difficulty Adjustment

- Hash algorithm is fully compatible
- According to the theoretical and actual block time, the current PoW block time is about 33.5 seconds/block, will be **adjusted to 28 seconds/block**
- Continuous W blocks must contain one PoS block, **W = 30**

- The difficulty is adjusted to the following algorithm to make the PoW block more stable: When the computing power increases sharply, the growth rate is the same as before, and when the computing power decreases, the computing hash power drops much faster than before (beneficial to the miners)

```
bigint const interval = (bigint)(_bi.timestamp-_parent.timestamp);
bigint const adjustvalue= max<bigint>(2 - interval /10 ,-99);
target = _parent.bits + _parent.bits/2048*adjustvalue;
```

After calculation, due to the block generation, PoW miners will increase their revenue by about **7%** compared to the upgrade.

Designing PoS

- According to z=10%, adjust to **252 seconds/block**, the initial block rewards of 0.3*0.95^3, attenuate every 500,000
- When the PoW difficulty is lower than a certain value, the PoS gets a 50% return (to be determined)
- PoS mining wallet must have at least one inbound connection

```
bigint const interval = (bigint)(_bi.timestamp-_parent.timestamp);
bigint const adjustvalue= max<bigint>(18 - interval /10 ,-99);
target = _parent.bits + _parent.bits/2048*adjustvalue;
```

Pillars Phase 2

- Probable activation block – 2541142
- Average block creation time 16.35 seconds, PoW ratio y = 15/32, PoS ratio z = 1/16, DPoS ratio v = 15/32

Adjusting PoW Difficulty

- Hash algorithm is fully compatible
- According to the theoretical and actual block time, the current PoW block time is around 33.5 seconds/block, **after adjustment will be around 34.9 seconds/block**
- The difficulty is adjusted to the following algorithm, which makes the PoW blocks generate more smoothly, and the difficulty is quickly adjusted according to the type of the preceding block

```
bigint const interval = (bigint)(_bi.timestamp-_parent.timestamp);
bigint const adjustvalue= max<bigint>(2 - interval /10 ,-99);
if (prevs_header.is_pow_version() || prevs_header.is_pos_version()) {
  adjustvalue *= 2;
  target = _parent.bits + _parent.bits/2048*adjustvalue;
} else {
  target = _parent.bits + _parent.bits/2048*adjustvalue;
}
```

Designing PoS (MPC Phase 1)

- According to z=2/32, adjust to **268 seconds/block**

- When the PoW difficulty is greater than xxx or less than xxx, PoS will gain 50% (TBD)
- PoS mining wallet must have at least one inbound connection
- When PoS mining consumes any UTXO (1000ETP UTXO), the UTMO recovery period block height g(z) satisfies the following function:

$$g(z)=\frac{1}{1+e^{-z}}$$

Where z is the difficulty of mining PoS.

Designing DPoS (MPC Phase 2)

Objective:

1. Through the model design, allow the DPoS consensus to be more stable in generating blocks.
2. The MARS score is the core evaluation of the block, considering the quality of the nodes. Whether the node has a certificate, whether the staked amount is sufficient, and whether the node is actively generating blocks are three aspects for evaluation. The certificate reflects the management efficiency, normalcy, and guaranteed quality of the foundation. The stake reflects the influence of nodes on the network, and how actively blocks generate reflects whether the node has fulfilled its due obligations during the operation of the network.
3. At the beginning of each node replacement cycle, there is also a node management incentive for the development of the best nodes within the network that will take into consideration the number of nodes.

Certificate attribute:

Certificate have the following status:

- Activation state
- Inactive state

Sufficient conditions for activation: Develop at least 23 secondary nodes
Necessary conditions for inactivation: Inactivated relative to 2 million blocks
Not transferable in inactive state
Not transferable in active state
Cannot take the initiative to cancel the deactivation

Design Content:

- According to v=15/32, adjust to **34.9 seconds/block** (release curve to be determined, convex integrable function, alternative sigmoid)
- Initial block generates 23 witness certificates
- With a tier one certificate, you can set up 23~46 tier two certificates
- At least 23 nodes need to start at the tier one level to open up mining (the second tier certificate recipients must have 100,000 ETPs and be the first 100 users in the registration list), the first level certificate holder gets another 158,000 ETP (if mining then will be released, if not mining then will not be released)
- Ordinary investment investors can choose certificate holders, rent their stake to the certificate holder, and get the proceeds from it

- The possibility of DPoS witnesses being elected is entirely determined by their MARS value

MARS Value = F (NodeCert, NodeStake, NodeBlockMiss)

NodeCert: the certificate explained above
NodeStake: the stake holding the ETP
NodeBlockMiss: Missed statistical value of the blocks

1.) Overview of the number of nodes, rights and obligations

Table 1

Node Type	Number	Rights	Obligations
Tier 1 Node	23	1.) Hold a Level 1 certificate (valid for two months) 2.) Generate up to 46 secondary certificates 3.) Increase the MARS value after activating the level 1 certificate, valid for 2 million blocks 4.) Get block rewards based on the block creation situation	1.) After obtaining the first level certificate, develop at least 23 secondary nodes to participate in the consensus and activate the validity of the certificate. 2.) Actively participate in the block creation, maintain the MARS value, avoid freezing that will lead to the revocation of the certificate
Tier 2 Node	At most 1058	1.) Hold a Level 2 certificate and increase the MARS value, valid for 2 million blocks 2.) Get block rewards based on the block creation situation	1.) Actively participate in the block creation and maintain the MARS value

2.) MARS Design
MARS is affected by three factors: certificate, stake, and block miss rate:

$$MARS(Node) = Cert(NodeCert) + Stake(NodeStake) + BlockMissRate(NodeBlockMiss)$$

(1) Hold a valid level one or level two certificate, and the cert score is 30 points.

$$Cert(NodeCert) = \begin{cases} 30, & NodeCert = true, \\ 0, & NodeCert = false. \end{cases}$$

(2) Stake number score: For example, 100,000 ETP corresponds to 30.9 points, and the formula is as follows:

$$Stake(NodeStake) = \log(NodeStake) \times 6.18$$

(3) BlockMissRate score: Definition – the node EpochNum is selected as the candidate block node of epoch, the 23 representative nodes will take turns to create 230 blocks, meaning each node will take turns generating 10 blocks. If it is the turn of Node to generate the block, and Node misses the block for network reasons, then

BlockCount<10. At the end of the current epoch, the BlockMissRate score of the EpochNum block of the Node is calculated. The formula is as follows:

$$BlockMissRate(NodeBlockMiss) = 30 + NodeBlockMiss \times \begin{cases} 0, & NodeBlockMiss < -0.2 \\ 15, & 0 > NodeBlockMiss \geq -0.2 \\ 5, & NodeBlockMiss \geq 0 \end{cases}$$

Among them, NodeBlockMiss is the block error rate of the Node from the first time it has become a candidate. The recursive calculation formula is as follows, and defines NodeBlockMiss(0, BlockCount)=0:

$$NodeBlockMiss = NodeBlockMiss(EpochNum, BlockCount) = \frac{NodeBlockMiss(EpochNum-1, BlockCount') \times (EpochNum-1) + BlockCount}{EpochNum},$$
$$EpochNum \in N+$$

3.) MARS related incentives, as well as node development incentives (**draft**)

The following are projections and are not final figures. These are subject to change as we garner feedback from the community before MPC Phase II.

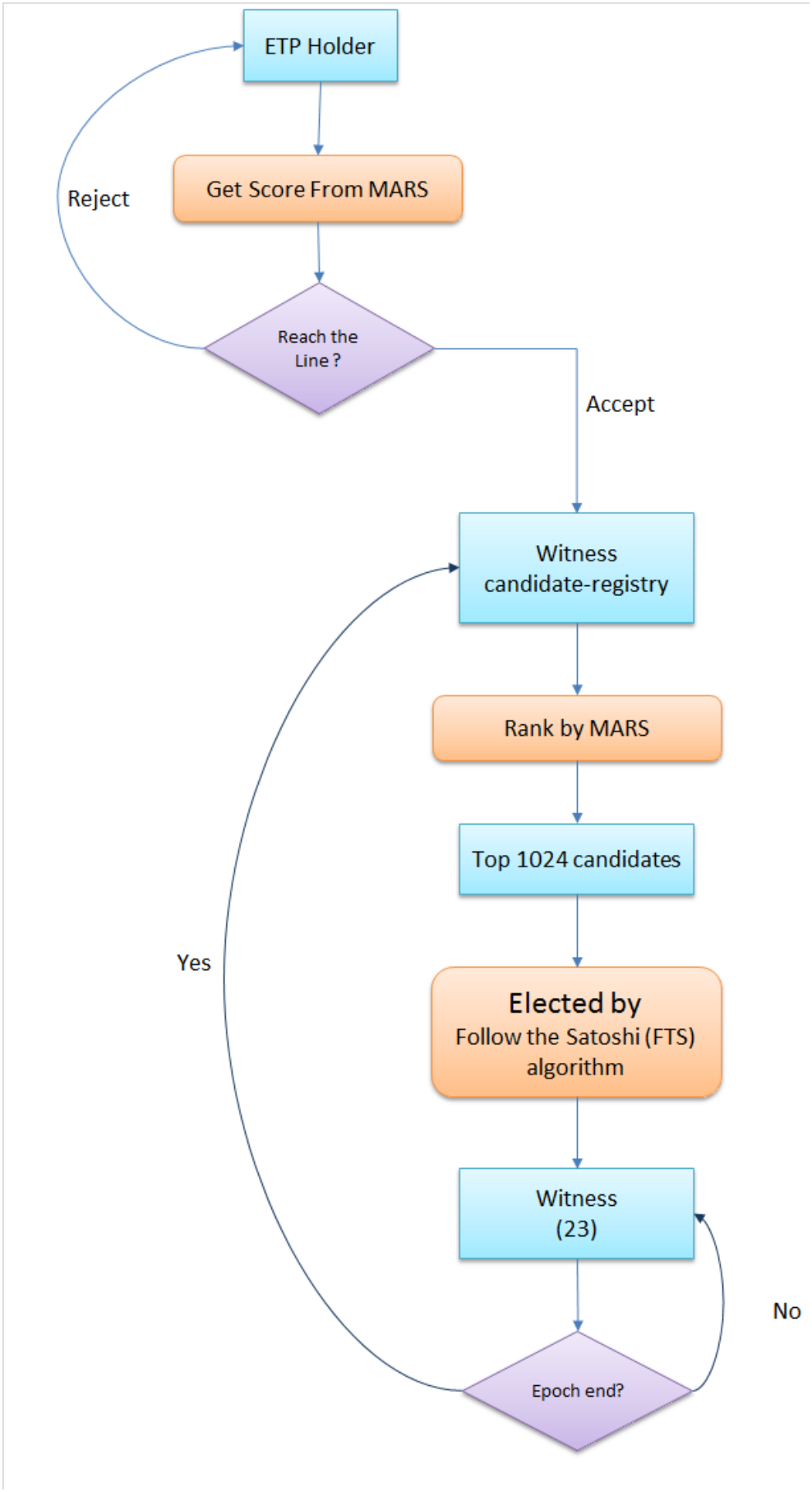
Table 2

Node Type	Action	Incentive
Tier 1 Node	Earn a level 1 certificate issued by the Foundation	Earn **18,000 ETP**, released in 12 months Increase MARS scores, making it easier to generate blocks
	Develop 23 level 2 nodes in two months, activate the certificate	Earn **158,000 ETP**, released in 12 months Increase MARS scores, making it easier to generate blocks
	Block Creation	0.5 ETP： block reward Secondary level 2 node number*0.01 ETP: Node management reward x ETP: current block's transaction fee MARS value is stable and easier to generate blocks
	Level 1 certificate is revoked	Decrease MARS scores, more difficult to generate blocks Remaining locked ETP that is forfeited to be returned to the Foundation
	Level 1 certifcate expires	Decrease MARS scores, more difficult to generate blocks

	Level 2 node development fails	Level 1 certificate to be revoked, reducing the MARS score, making it harder to generate blocks
	MARS score is low for an extended period of time	Freeze the Level 1 and secondary Level 2 certificates Stop issuing the locked ETP until the node contacts the foundation After 3rd freeze, will revoke Level 1 and Level 2 certificates
Tier 2 Node	Obtain the secondary level 2 certificate issued by the tier 1 node and the Foundation	Earn **6,000** locked ETP, released in 6 months Increase MARS scores, easier to generate blocks
	Block Creation	0.5 ETP: Block rewards x ETP: current block's transaction fee MARS value is stable and easier to generate blocks
	Level 2 certificate is revoked	Decrease MARS score, harder to generate blocks Remaining locked ETP that is forfeited to be returned to the Foundation
	Level 2 certificate expires	Decrease MARS score, harder to generate blocks

4.) Algorithm Basic Flow

Basic Flow:



Witness–MARS combines the Satoshi Nakamoto's random number algorithm, and the MARS score as a weight affects the probability of selection. If 1024 is insufficient, it will be selected according to the actual person. If more than 1024, then according to the MARS ranking selected pre 1024, the MARS influence factor is degraded to PoS only when it is staked.

Competitive PoW–PoS hybrid block production

First, due to similar block structure and consistent block generation logic, we consider the simultaneous activation of PoW and PoS consensus. The difference between the two is that PoS has more coinstake structure than PoW, thus we only need to simultaneously validate PoS blocks and PoW blocks in the verification part of the consensus.

Figure: Flowchart of **Blackcoin's** PoS mechanism process:

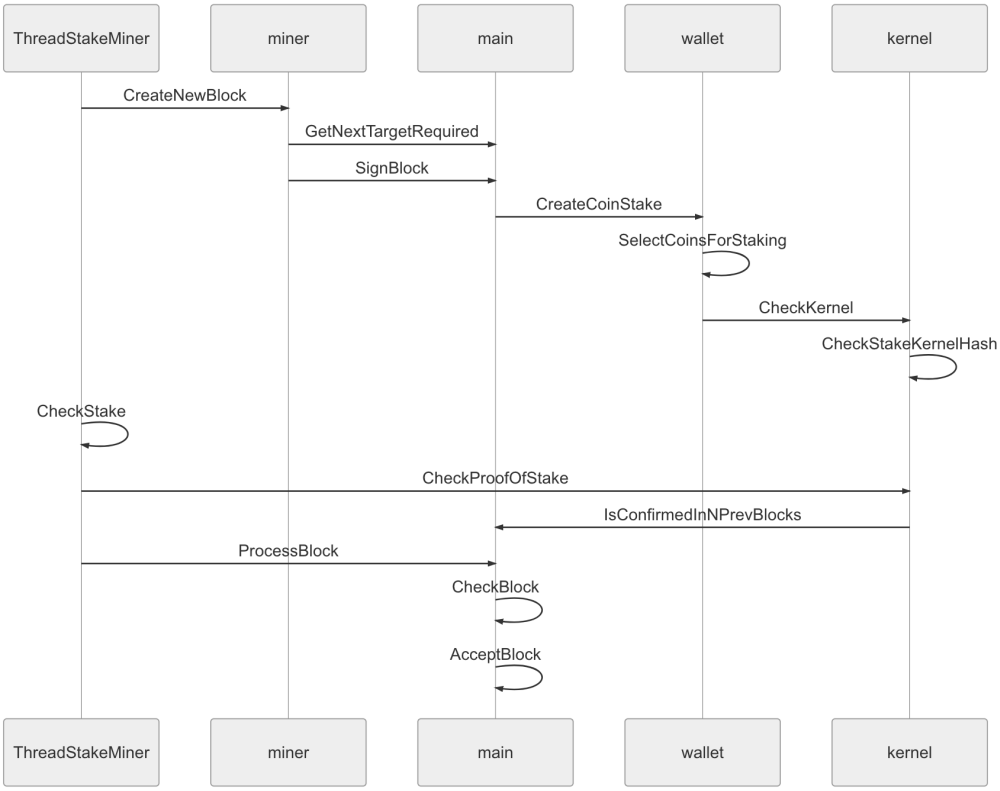
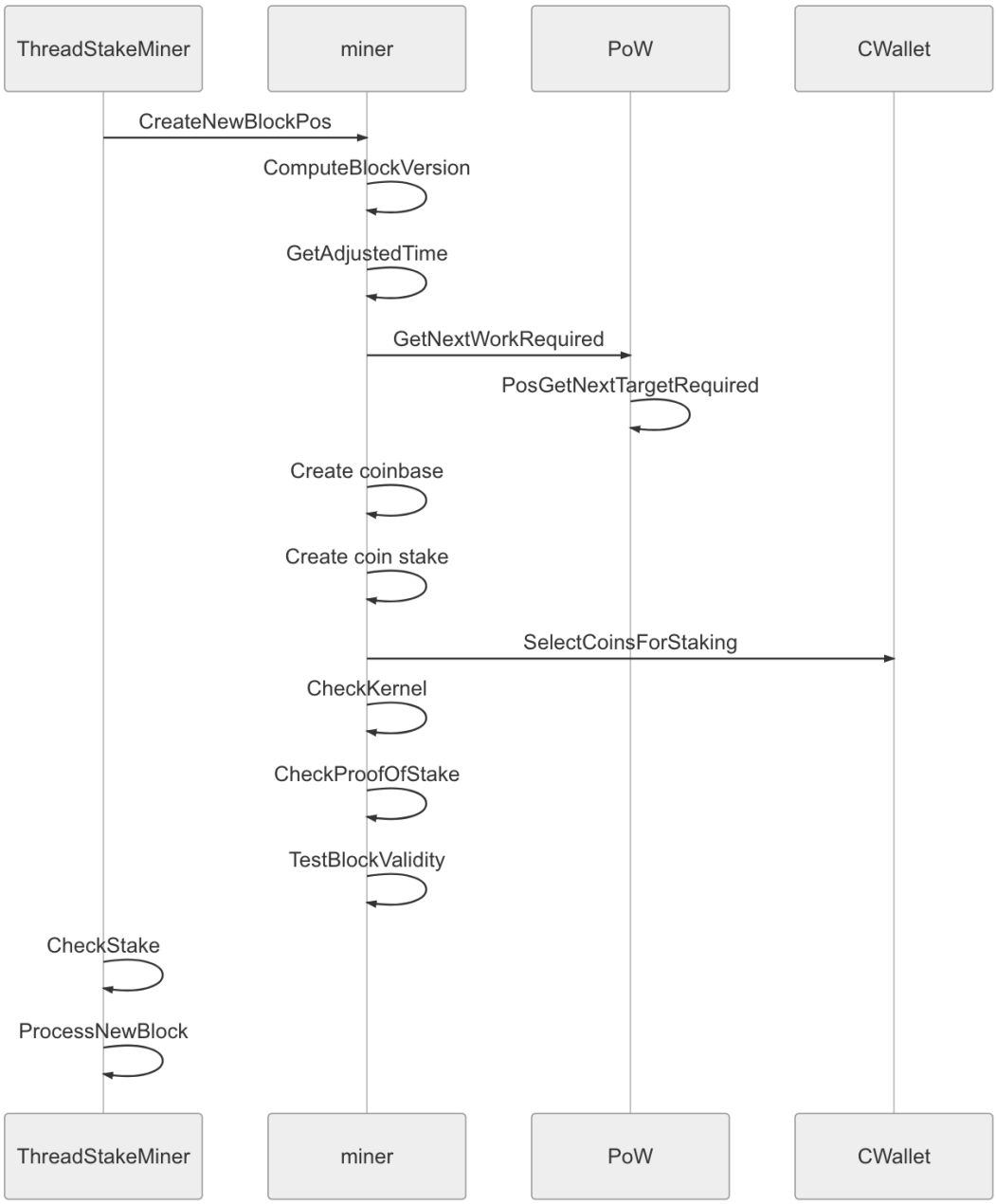
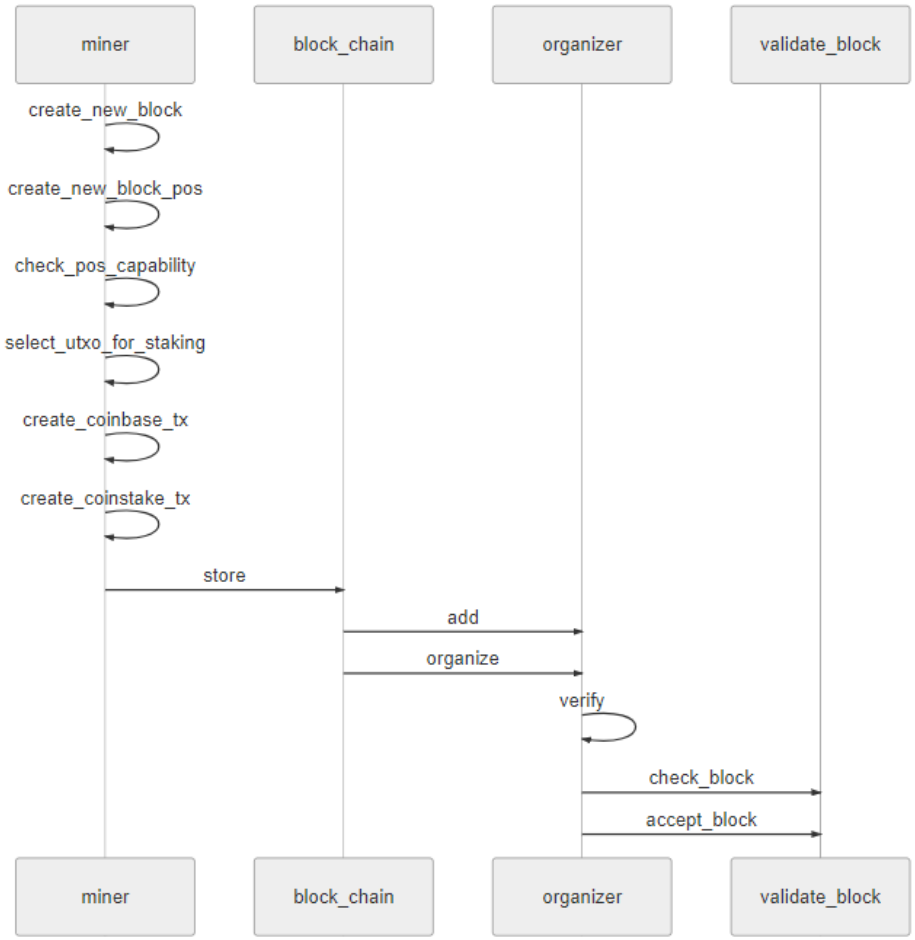


Figure: Flowchart of UBTC's PoS mechanism：



These two mechanisms give us a design roadmap for hybrid PoW+PoS consensus:



By modifying the Metaverse code according to the above flowchart, we create a PoS block in **miner::create_new_block**, set that block's version as **block_version_pos**, and at the same time add a **coinstake** transaction in that block's transactions. As noted previously, a coinstake transaction has the following specified transaction formats:

- inputs, the first entry represents mining stake UTXO;
- outputs, the first entry is empty;
- outputs, the second entry is the corresponding UTXO output of the first input entry;

At the same time, in order to prevent identity forging and block tampering, the PoS block header also contains the signature **blocksig** of the entire block with the witness's private key.

In order to activate PoS we must fulfill the following conditions:

1. lock a certain amount of ETP;
2. Hold a certain amount of ETP that can be used for mining; a UTXO must meet a certain level of maturity before it can be used for mining;

In order to collect small UTXO and split large UTXO for mining, each coinstake transaction includes a small_collect and large_split function.

PoS also has a MARS score requirement to fulfill before mining.

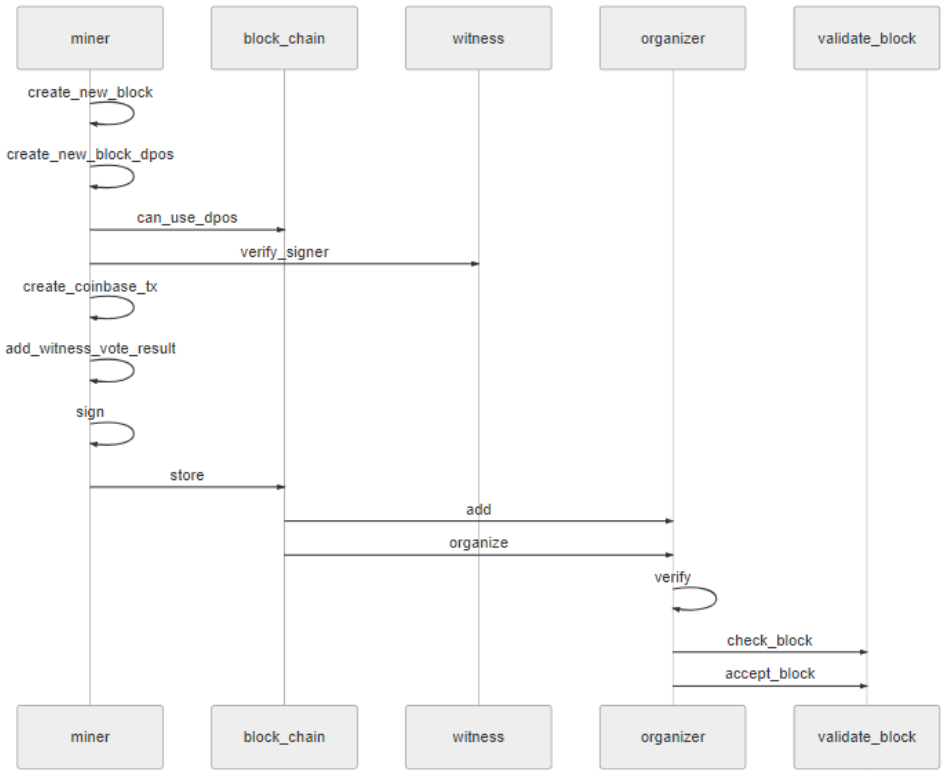
DPoS follower-block production

Metaverse hybrid consensus also supports DPoS follower-block production, that is, after a PoW or PoS block is produced it can be followed by a DPoS block. First, a DPOS consensus table of witness candidates is generated and registered as a Merkel hash on the block header recording which credentials are valid and which are invalid. Then, witnesses are randomly selected according from the DPoS registry, weighted by MARS score.

The DPoS process is as follows:

1. DPoS miners are registered as witness candidates;
2. Witness candidates stake a certain amount of ETP;
3. The first block in each epoch randomly selects a group of witnesses based on the proportion of candidates' stake;
4. Within an epoch, the elected witnesses produce a block;
5. To avoid situations with offline witnesses, witnesses with far-below average block production in each epoch are prohobited from participating in the next round of elections.

DPoS Block production:



As shown in the chart above, a new DPoS block is created in miner::create_new_block, that block's version is set in block_version_dpos, and the witness's public key is added to the block header.

At the same time, in order to prevent identity forgery and block tampering, the PoS block header also contains the signature blocksig of the entire block with the witness's private key.

DPoS activation requires meeting the following two conditions:

1. Initiate a transaction to register as a witness candidate;
2. Lock a certain amount of ETP as stake.

Advantages of Metaverse Hybrid Consensus

PoS Analysis

A discussion of MPC design advantages begins win an analysis of current PoS variations, such as **Pure PoS1.0/PoS2.0/PoS3.0, Dynamic PoS, Liquid PoS, Lease PoS, and Forging PoS**. All PoS implementations are based on the following logic:

> On the PoS protocol, blocks are separated into two distinct types: PoW blocks and PoS blocks. The PoS in the new type of blocks is a special transaction called coinstake (named after PoW special transaction coinbase). In the coinstake transaction, the block owner pays himself thereby consuming his coin (or coin age), while gaining the privilege of generating a block for the network and minting for PoS. The first input of coinstake is called kernel and is required to meet a specific hash target protocol, thus making the generation of PoS blocks a stochastic process similar to PoW blocks. However, a significant difference is that the hashing operation is done over a limited search space (more specifically one hash per unspent wallet–output per second) instead of an unlimited search space as in PoW. Thus, no significant consumption of energy is involved (King & Nadal, 2012).

In other words, PoS itself contains PoW, and in the Pure PoS algorithm, the PoS part is strengthened and the PoW part is weakened. We analyzed PPCoin, NovaCoin, YaCoin, and BlackCoin, and found that the PoW+PoS hybrid mode was adopted early on.

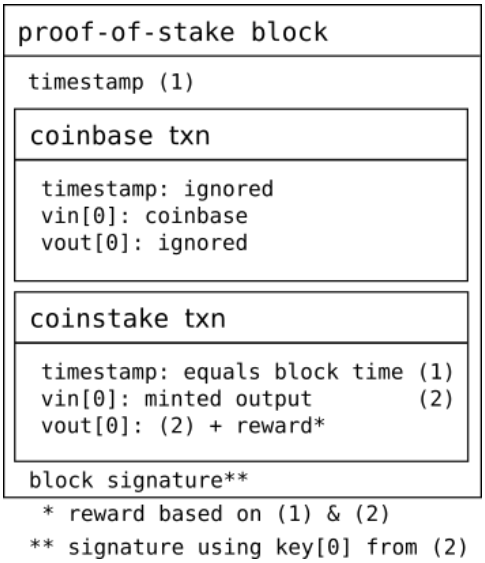
To generate blocks on the PoS algorithm, the following conditions must be met:

hash(stake_modifier, current_time, UTXO) < coin(UTXO) * difficulty

1. Users at every second (current_time) traverse all of their UTXO, substituting into the above formula to see if it can satisfy the inequality condition. If it is satisfied, record the corresponding UTXO in the block and release the block. (see Point 4)
2. Stake_modifier is the value after hashing some of the fields in the previous block. This is added to prevent users from knowing in advance when they have the right to mine.
3. Difficulty will be dynamically adjusted according to the recent block output time to ensure a stable block generation time interval.
4. Since we only need to complete the hash calculation equal to the number of UTXOs per second, the required computing power is lower.
5. From the inequality equation, we can see that the more UTXOs are held, the greater the amount of tokens in UTXO (coin(UTXO)), the longer UTXO holds (age (UTXO) or the age of the coin), and the easier the inequality is to solve, the easier it is to mine.
6. Generate block reward settings for coin(UTXO) * age(UTXO). That is, the larger the UTXO amount and the longer the holding time, the higher the reward.
7. In order to record eligible UTXO into blocks and be compatible with the original PoW mode, Peercoin designed the logic of coinstake: Keep the original first transaction as coinbase, but the required input quantity must be equal to 1, and the input

”prev.out” field must be set to a null value, and the output quantity must be greater than or equal to 1. If the second transaction needs to be coinstake, this requires the input quantity to be greater than or equal to 1, and the first input is UTXO that meets the condition, the output quantity is greater than or equal to 2, and the first output must be blanked, and the second output is block reward.

The structure of a PoS block is as follows:



In some versions of PoS design, the following formula is used:

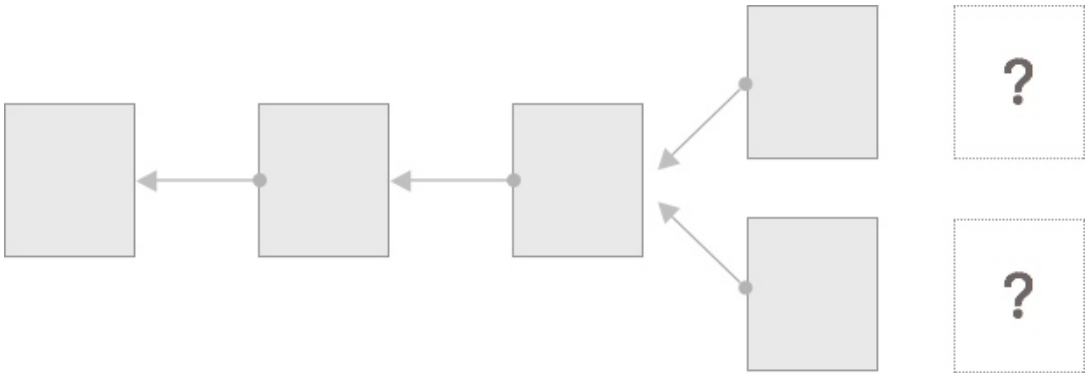
hash(stake_modifier, current_time, UTXO) < coin(UTXO) * age(UTXO) * difficulty

Due to the introduction of time factor, there is the possibility of a Coin Age Accumulation Attack. That is, the node is shut down, and when the age (UTXO) is large enough, the node mining is started, thereby saving power, which causes the problems that the number of online nodes is too small and the system is fragile. Of course, it is fine to set an age limit, but doing so also loses the meaning of age as a moderator. In summary, the hybrid consensus Pillars will not consider the scheme of coin age.

Potential Attacks

Nothing-at-Stake Attack

In the PoW mechanism, when the ledger is forked, the PoW is a computationally sensitive algorithm. The miner must choose a direction to mine to maintain the chain with the most difficulty. Due to the PoS mechanism being not sensitive, PoS miners tend to mine in multiple directions in an effort to maximize their profits. Over time, the chain tends to diverge rather than converge, so when most miners are mining together on multiple forked chains, it is easy to have a double spend attack, so the ledger of this chain is basically unusable.



Long Range Attack

In PoS, the speed at which each block is generated is much faster than PoW. Therefore, a few unscrupulous nodes will think about rewriting the entire blockchain consensus ledger. In the PoW consensus mechanism, this is the classic 51% problem: If a node controls more than 51% of the hash power, this node will have the ability to reverse tamper the ledger for up to 6 blocks. This kind of inversion abruptly increases the number of reverse blocks, so even if you have more than 51% of the computing power, it is very difficult to tamper with more than 6 blocks in reverse. However, in PoS, there is no constraint on physical computing power, then the reverse tampering with the ledger can achieve any block height. From this perspective, PoS is not as safe as PoW.

Bribe Attack

The bribe attack process is as follows:

1. The attacker buys a good or service.
2. Merchants wait for the network to confirm the deal.
3. At this point, the attacker begins to claim for the first time in the network and **rewards the current longest chain that does not contain this transaction.**
4. When the main chain is long enough, **the attacker begins to give out more rewards to miners who mine the chain that contains the transaction.**
5. The attacker gives up the reward after six confirmations are reached.
6. When the goods arrive, the attacker gives up the chain he selected originally.

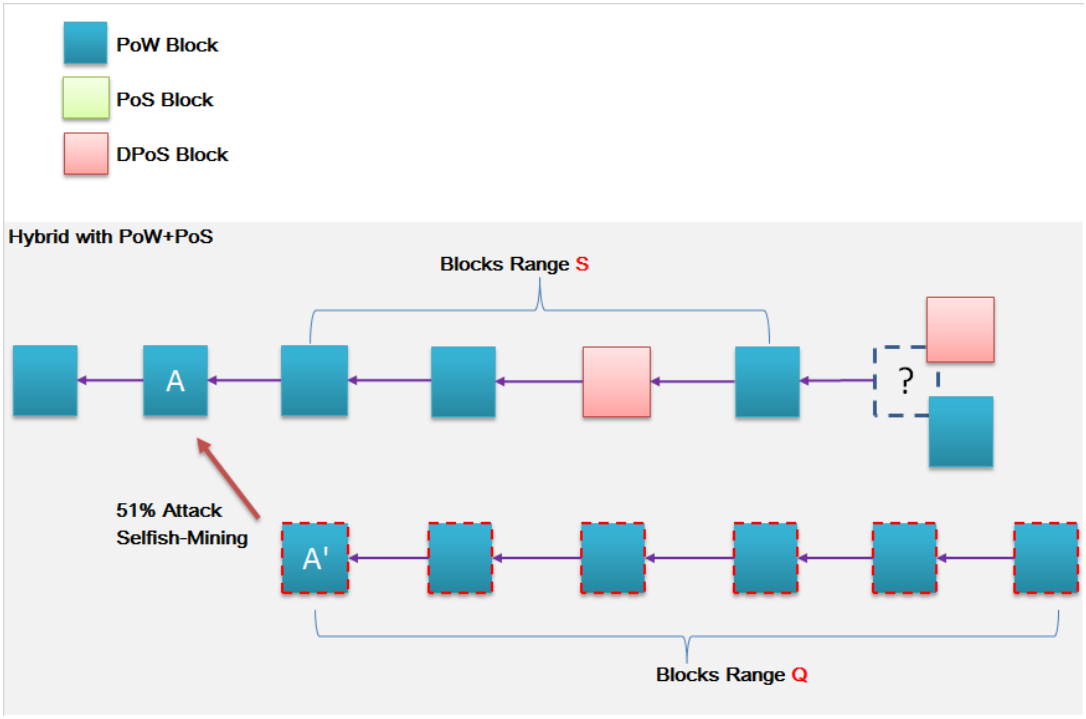
Therefore, as long as the cost of the bribery attack is less than the cost of the goods or services, the attack is successful. In contrast, bribery attacks in the PoW mechanism require the bribery of most miners, so the cost is extremely high and difficult to realize.

Although pure PoS has many problems, PoS has better flexibility than PoW, so we will consider solving these problems in the Metaverse hybrid consensus Pillars.

MPC Attack Resistance

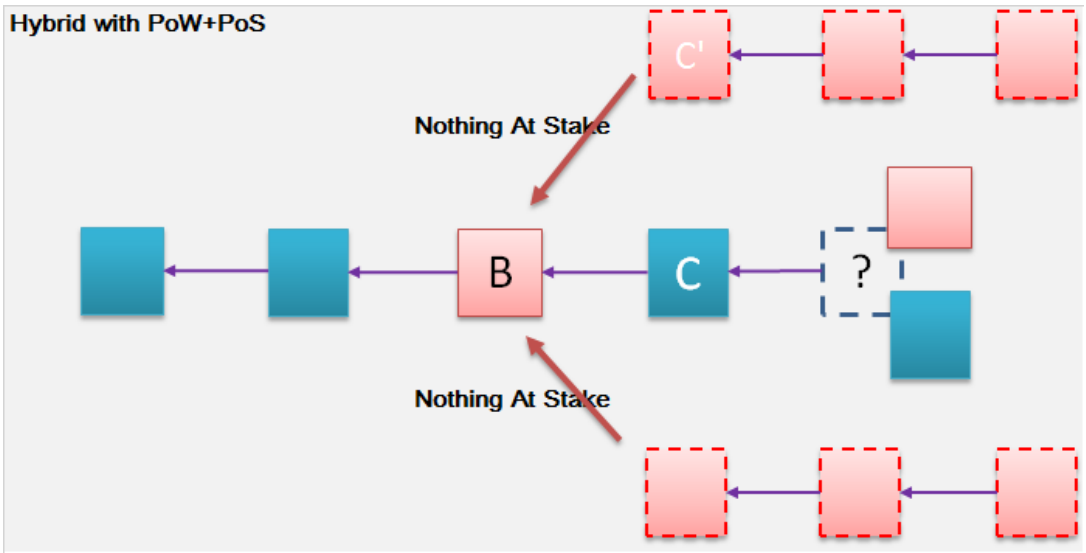
51% Attack Resistance

Consider a typical 51% attack, as shown in the following figure:

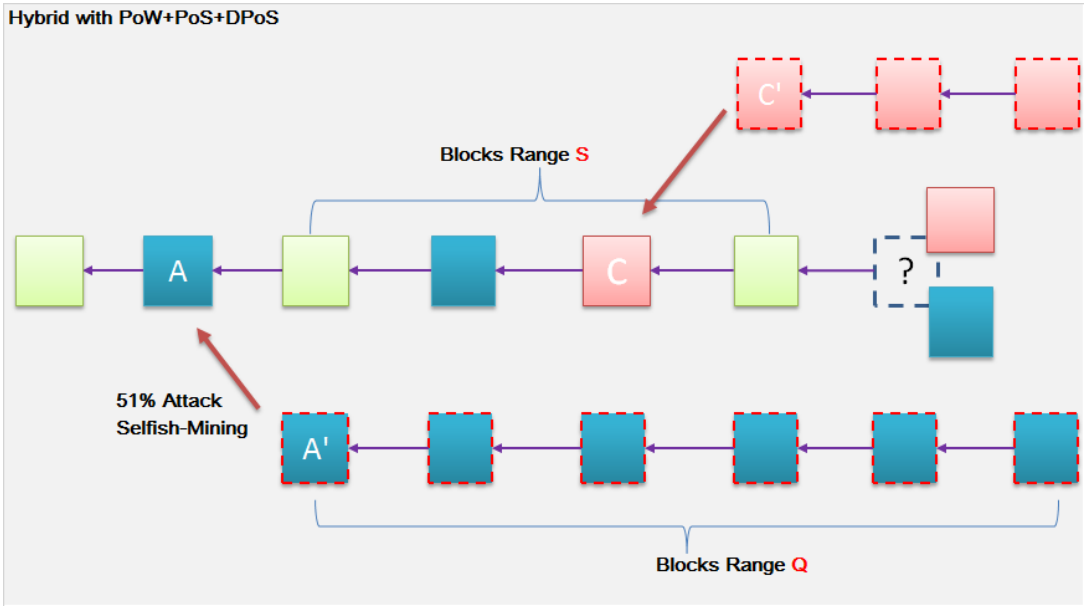


When an adversary initiates a 51% attack or engages in selfish mining, a branch chain of length Q is accumulated at attack point A. When Q is greater than S, the attacker must satisfy the following when releasing the Q chain:

When Q is greater than or equal to W=30, the attacker's Q chain is not accepted;
When Q is less than or equal to W=30, the attacker's Q chain is still in a state where the security confirmation number is not reached;



When a PoS miner initiates a Nothing-at-Stake attack at block B, it is determined by the subsequent PoW block C. The PoS miner cannot maintain a longer fork chain.



Entering the three–way hybrid consensus stage, the DPoS block follows the PoW block. The DPoS block prevents attacks on A' and C'; on the other hand, if DPoS tries to attack it will be rejected by PoW and PoS blocks.

Sybil Attack Resistance

While no consensus algorithm can currently resist a Sybil attack, the Avatar MARS score makes such an attack significantly more costly, thereby establishing a cryptoeconomic incentive structure that reduces the probability of Sybil attacks to near–zero.

Confusion Attack Resistance

1. A malicious actor could tamper with the PoW block version, causing consensus failure due to a PoW block falsely modified to have a PoS block structure. A valid PoS block must meet these conditions:
   a. block version is block_version_pos;
   b. the block's first entry must be a coinbase tx;
   c. the block's second entry must be a coinstake tx;
   d. first coinstake tx input entry must represent the miner's stake UTXO;
   e. first coinstake tx output entry must be empty;
   f. second coinstake tx output corresponds to first input entry UTXO;
   g. the witness's private key pair corresponds to the blocksig contained in the block header;

A PoS block can only be valid when the above conditions are met, preventing a PoS–PoW confusion attack.

2. A malicous actor could tamper with the PoS block version, causing consensus failure due to a PoS block falsely modified to have PoW block structure. A valid PoW block must meet these conditions:
   a. block version is block_version_pow;
   b. the block's first entry must be a coinbase tx;
   c. there are no coinstake transactions in the block;

A PoW block can only be valid when the above conditions are met, preventing a PoW–PoS confusion attack.

3. Timestamp attack
   The timestamp of a qualified block must meet the following conditions:
   a. The timestamp cannot be earlier than the previous block's timestamp;
   b. The timestamp must be no later than the time of validation plus a narrow time–window;

The Metaverse time–window is adjusted to 38 seconds. Since PoW and PoS timestamp validations are different, thus it is impossible to cause consensus failure by timestamp confusion attack. With an average block time of 25 seconds, an attacker could at most produce 2 attacking blocks; any more, and the difficulty increases, slowing block production and preventing a timestamp attack.

P2P Network Carrying Capacity

The theoretical limit for the P2P network to process all blocks is about 10 seconds. Currently Metaverse block times are not suitable for optimization to around 15 seconds without further improvement of the P2P network and without uncle blocks.

Support for Lightning Network（@MPC Phase1）

The first stage of MPC will support Lightning Network, a second–layer network which depends on the underlying blockchain for security. By using real Bitcoin–like transactions and using its native smart–contract scripting language, it is possible to create a secure network of participants with high throughput without significantly compromising security. Since Metaverse transaction structure is similar to the Bitcoin network, it is relatively simple to develop our own LN implementation.

Adjustment of Original ETP Locking Reward（@MPC Phase1）

In MIP–2 we assessed that the original ETP locking reward is unreasonable as it may cause total circulating supply to reach the maximum limit of 100 million ETP after 7–14 years. Given the similarity between the original locking reward and PoS staking reward functions, we will convert all ETP locking rewards into PoS and DPoS rewards. ETP previously generated by locking will remain permanently. Due to faster block time, currently locked ETP deposits will be released ahead of schedule.

Upgrade of Digital Asset Protocol

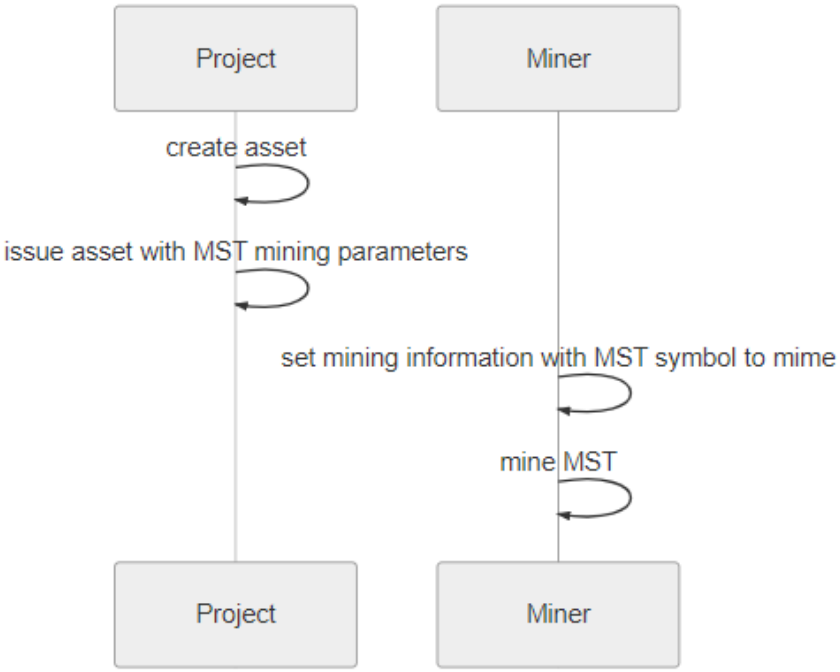
MST Mining（@MPC Phase 1）

In order for MST to share the asset distribution functionality of Metaverse consensus algorithm, MPC Phase 1 supports PoW mining and PoS minting for MST assets. In the second phase of MPC, PoW, PoS, and DPoS mining and minting will be supported.

All Metaverse asset structures are UTXO-based, and we have made output extensions for the coinbase as follows:

```
{
    "hash" : "bf4ca43a2c23c8d5b06",
    "inputs" :
    [
        {
            "previous_output" :
            {
                "hash" : "0000000000000000000",
                "index" : 4294967295
            },
            "script" : "[ b71f0f ]",
            "sequence" : 0
        }
    ],
    "outputs" :
    [
        {
            "address" : "Miner's Address'",
            "attachment" : // nomarl coinbase
            {
                "type" : "etp"
            },
            "index" : 0,
            "value" : 94338400
        },
        {
            "address" : "Miner's Address",
            "attachment" : // new MST output for coinbase
            {
                "quantity" : 300000000,
                "symbol" : "TEST001.MINING",
                "type" : "asset-transfer"
            },
            "index" : 1,
            "value" : 0
        }
    ],
}
```

MST Mining Flowchart：



Specific steps are as follows:

1. MST asset is designated mineable when created;
2. MST asset is registered on mainnet and mining reward parameters are set;
3. Miner designates which MST asset to mine;
4. Miner begins mining as usual; MST mining rewards will start to be included in their coinbase rewards.

Asset Pricing Replacement Swap（@MPC Phase 2）

Refer to MIP-15

Digital Identity Protocol Upgrade

Open MARS Standard（@MPC Phase1）

Refers to MIP-16
MPC Phase 2 will implement DPoS algorithm referencing MARS scores

Compatibility with OIDC Unified Login Portal（@MPC Phase 2）

Avatars inherit OIDC when a Metaverse wallet is opened, providing decentralized identity services and allowing the extension of Avatars to traditional internet applications.

Metaverse Standard Identity Service（@Galaxy）

Precision airdrop service
Personal Achievement Certificate service
Public blockchain data mining (AI-friendly)

Metaverse Binary System – Galaxy

There is a continual challenge facing blockchain applications, finding the balance between TPS and decentralization. When the TPS is upgraded, this hurts decentralization, so we consider the double-chain architecture. The current Metaverse infrastructure acts as a foundation that has decentralization capability. The second chain provides high TPS transmission capacity and can be synchronized with the DPoS on the main chain. The problem with the second chain is how to adapt to the existing system.

The Microeconomy of the Main Chain

To be written...

Binary Port

There are many architectural patterns, and we only discuss single-point applications, layered architecture patterns, event-driven architectural patterns, and micro-service architecture patterns. We will discuss where MBaaS should be in these architectural patterns.

The Relationship Between MBaaS and Wallet

First of all, MBaaS is a collection of services. The representation in the system is a type of service process, which is usually generated by the wallet program.
Currently we can operate two modes:
1.) **Wallet-segregated mode:** Separate functions from the wallet program into a multi-process mode, with each process providing a lightweight MBaaS;
2.) **Wallet program unified mode:** The wallet program provides MBaaS, but can form a master-slave relationship and make an internal distributed network instead of connecting to the public network. The unified model puts higher demands on the optimization and stability of the wallet.

Separation mode

Metaverse provides at least the following basic module separation:

- P2P Network
- Transaction verification and resolution
- Private key management
- Persistent block storage

The light wallet is the first case of the separation mode, from the full node wallet.

Unified Mode

The wallet program at least provides internal high-speed synchronization, and the internal nodes change from final consistency to strong consistency, which requires that internal nodes can achieve strong consistency when the blockchain forks.

Separation mode and unified mode are not absolute, and there may be a mixture in the actual application. We will now discuss the architectural model.

Monolith Applications

Single-point applications are divided into client-side single-point applications and server-side single-point applications. An example of the server-side single-point application is WordPress. If we want WordPress to support MST, the quickest way is to build the Metaverse wallet on the the WordPress backend, and then modify the backend code to call the MST related API. The final interface will display the MST token. This situation is suitable for a unified mode and rapid deployment. Single-point applications are more commonly used in the Microkernel Architecture mode. For example, the Metaverse Avatar is embedded in the Eclipse IDE, which requires the Metaverse light wallet to be plugged into Eclipse as a plugin. This situation is suitable for segregated mode, such as a light wallet.

Layered Architecture

Layered architecture is suitable for both segregated and unified modes depending on the scope of the layer structure. Segregated mode is clearly more suitable for large-scale layers such as a Service-oriented architecture (SOA). In segregated mode, MBaaS can be placed on the business layer as a standard compenent as the wallet API only needs to be compatible with other modules on the same layer. Structural blockchain storage may be required for a persistent data layer, otherwise the wallet itself can directly replace the block storage function. In unified mode, MBaaS is suited for small-scale applications where it can directly refer to the server node.

Event-driven Architecture

Event-driven architecture is suitable for segregated models. This model focuses on the distribution and processing of events. Looking at the logic of blockchain, we can see that the blockchain is based on transactions and a transaction itself is an event.

In Mediator mode, the ability to resolve transactions is needed to parse and redistribute transaction types and data. For account status model, it must also read account status; in Broker mode, each Processor can parse and determine the transaction without involving changes made by the Broker.

The above process is input as an event, and when transaction output is required, we can think of the wallet as a processor and only deal with the business related to the blockchain, but here we may encounter the problem that the processor evolves into a central processor. Because the ultimate goal of any core business flow is payment, the wallet processor will become a collection of authentication, signature, and broadcast transactions, and will encounter significant performance bottlenecks.

Therefore, the network module and transaction verification module in segregated mode can be horizontally extended. To accomplish this Metaverse should provide a complete SDK to support event distribution and processing.

Microservice Architecture

Microservice architecture is suitable for both unified and segregated models. In a unified model the wallet becomes a microservice component as long as the wallet functions are sufficiently cohesive. For example, a wallet can perform payment in component A and perform transaction validation in component B. This requires the wallet functions to adhere to the microservices architecture and to provide a robust query-verify API. On the other hand, the architectural concept of microservices fits very well with segregated models, thus it is not difficult to standardize Metaverse microservice components.

Smart Contracts（@Galaxy)

Standard Template Library of Smart Property
Standard Template Library of Avatar
Functional Language for Smart Contract
Code Template Upgrade System Manager

References

- 《PoW, PoS, & Hybrid protocols: A Matter of Complexity?》https://arxiv.org/pdf/1805.08674.pdf
- 《2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely》https://eprint.iacr.org/2016/716.pdf
- https://github.com/mvs-org/mips/blob/master/mips/mip-2.md
- https://github.com/Nevacoin/nevacoin
- https://github.com/dashpay/dash/issues/2268
- https://github.com/mvs-org/mips/blob/master/mips/mip-16.md
- http://newmetaverse.org/white-paper/Metaverse-whitepaper-v3.0-EN.pdf