1 Background

An important indicator of bitcoin mining is power-consumption ratio, higher power-consumption ratio, higher income. This document introduces multi midstate mode, A scheme to Improve the power-consumption ratio of Mining:

Solution: change the value of the block version.

The feasibility of the scheme is based on: In the bitcoin protocol, the bitcoin network (bitcoind nodes) allows at least two version(or even higher version of block). Some bits of the version fields can be redefined to identify the midstate.

This document is based on bitmain chip protocol, but the principle of scheme is the same throughout.

2 Scheme principle analysis

2.1.1 The basic principle of bitcoin mining

Necessary parameter:

- Block version: version
- Hash value of the previous block : prev_hash
- The value of the hash tree for the transaction to be packaged: merkle_hash
- Update time: ntime
- Current difficulty: nbits

The length of each parameter is as follows:

Version (4 bytes)	Prev_hash (32 bytes)	Merkle_hash (32 bytes)	Ntime (4 bytes)	Nbits (4 bytes)	Nonce (4 bytes)

2.1.2 Mining operation formula

The mining process is to find a suitable nonce value, makes the following formula was established:

SHA256(SHA256(version + prev_hash + merkle_hash + ntime + nbits + nonce)) < TARGET

- The range of nonce values is 0~2^32
- TARGET can be calculated according to the current

  difficulty=current difficulty/(2^32)。
- Because of the discrete random characteristics of hash algorithm, to find such a nonce value meets the formula, traversal search is the only way.

2.1.3 operation process

- Generate midstate :

version + prev_hash + high 28 bytes of merkle_hash : make an hash

to generate midstate。

- Generate work :

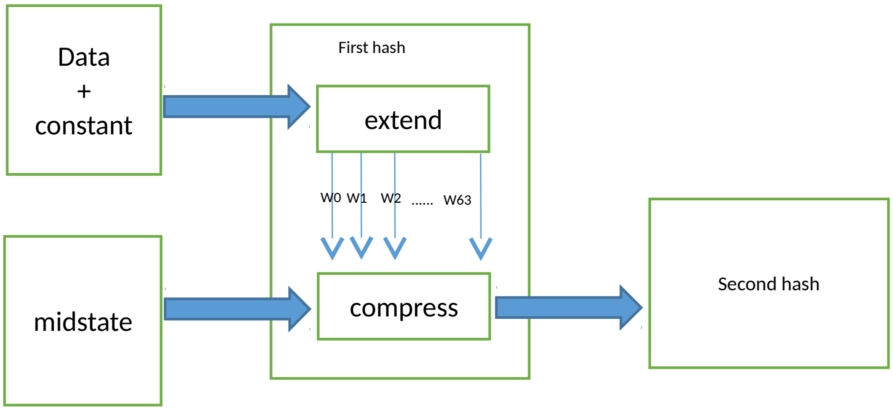
Low 4 bytes Merkle_hash + ntime + nbits = data2。

Midstate + 20 bytes 0x0 + data2 = work。

2.2Principle of multi midstate

2.2.1 Mining process

The operation process of bitcoin mining chip as below:



The design ideas are as follows :

1) In N cycles, date2 remains unchanged. In those cycles, the extended circuit can be closed. N=The number of midstate.
2) By changing version to generate N midstate.
3) Each midstate can make an operation with data2.
As you can see, in 1) turning off the extended circuit periodically can save the power consumption.

2.2.2 parameter analysis

We know that prev_hash can not be arbitrarily changed, the hash Merkle_hash is divided for two parts are used in the midstate and data2 in the, to find a midstate correspond to the same data2, the only way is changing the version. in the bitcoin protocol, the bitcoin network (bitcoind nodes) allows at least two version(or even higher version of block), So proposed this scheme.

Because more than one midstate shared the same data2, so in the theory when the number of midstate is N, the expansion of the circuit part of the power consumption will be 1/N.

3 Adaptation of pool

3.1Reason

Change version to generate mulit midstate is completely done by miner. So Pool need to know the version of nonce which submitted by multi midstate miner. Then pool can be based on the version information to restore the complete, correct block data and broadcast out

3.2API definition

Pool customization requirements:

1. Added multi midstate mode query instruction:

In the authentication stage miner will be sent to the pool: {"id": id, "method": "mining.multi_midstate", "params": midstate_num } if

pool supported multi-midstate mode reply : {"id": id, "method": "mining.midstate_change", "params": ["0x00000004", "0x04000004","0x08000004","0x0C000004"]}, Doesn't relay or replay error means doesn't support this mode.

2. Pool side only send the current version of the job, miner

change the version itself.

3. Submit protocol need to add version information : {"params": ["worker_name", "job_id", "nonce2", "ntime", "nonce", "version"], "id": 6, "method": "mining.submit"}.

4 Recommendations to bitcoin community

According to the development of bitcoin, the 4 byte (32bits) width of the version field is completely redundant. , This multi midstate scheme can be used as a kind of open universal technology scheme, can improve the efficiency of the whole network.

This scheme will submit multiple versions of block to the network , In order to avoid the forks risk , we wish to make the following proposals. :

1. Select N bits from version as midstate mask , Use only in check, not as a real version number. suggest N=2。
2. Definition version mask : 0x0C000000（N=2）, Used for block block version number extraction。（Note: in the Classic version,

version has used some bits as other uses)

3. Base on stratum protocol add or change the following instructions :

- Multi midstate query instruction : {"id": id, "method":

"mining.multi_midstate", "params": midstate_num } miner volunteer to submit the number of midstate.

- Multi midstate query instruction response : {"id": id,

"method": "mining.midstate_change", "params": ["0x00000004", "0x04000004","0x08000004","0x0C000004"]} Pool decides which version to use in the end.

- Multi midstate submit nonce instruction : {"params":

["worker_name", "job_id", "nonce2", "ntime", "nonce", "version"], "id": id, "method": "mining.submit"}