BHD Mining Pool Whitepaper

Version	Author	Date	Note
0.8	z	9/29/2018	Create document
0.9	z	6/10/2018	Wallet Api Instruction
0.9.1	z	2/11/2018	Api Instruction Update

Table of Contents

Summary

BHD launched officially on August 3, 2018 at 16:00, up to now (2018.9.29), the total hash rate reached 136.63P.

The continuous increase in hard disk hash power (capacity) represents the participants (miners)' approval. In order to better service miners and optimize the BHD ecosystem, mining pools can provide services collectively, share risks, or provide value-added services.

For these reasons, the BHD Foundation has published a whitepaper to provide references for those interested in developing the BHD mining pool.

Definitions of Terms

BHD

Bitcoin HD， Short for bitcoin Hard Disk,

Official Website: www.btchd.org。

Mining Pool

Collectively gather hash power (answers) submitted by miners, generate blocks to the public chain on behalf of the miners.

Miners

Hard disk holders who submit hash power to the mining pool or SOLO wallet.

SOLO Mining

Submit answers to their own wallets, then wallets generate blocks

Mining Software

Scan for answers in the hard disk and submit to the mining pool or own wallets.

Collaborative Mining

According hash power estimation, every T needs 3 BHD as mining condition. The main net calculates the miner hard disk capacity every time another 2016 blocks are generated, by combining all the blocks generated by this miner before.

Dual-Mining

The miners submit answers to the mining pool and their own wallets at the same time.

Mining Pool Requirements

1. **Stability**

   Online 24/7.

2. **Security**

   Wallet is safe at all time
   DDOS attacks, clients submit answers to bombard.

3. **High Concurrency**

1000+ miners can be online at the same time
3000+ answers submitted by miners can be processed in 5 minutes
Response to answer submitted in less than <= 100 milliseconds

4. Equitable distribution of profit

Value of the Mining Pool

1. Stable Wallet

With the increase of number of transactions and data on the chain, miners do not need to install wallets for each of them while mining.
Occupies less hard disk space.

2. Unified Monitoring

Miner status can be monitored real-time to see if the line has dropped.

3. Stability

Professional team provides professional service to enable a more stable mining pool operation.

4. Risk Diversion, Evenly Distributed Return

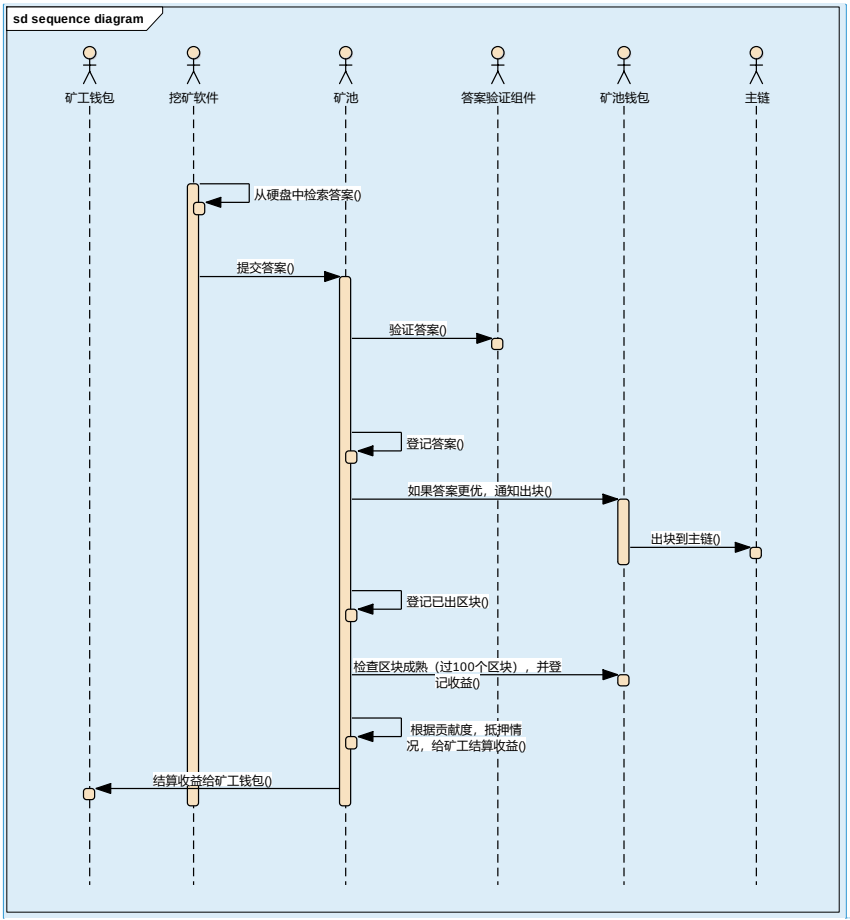
The miners with less hash power can enjoy a return daily.

5. Value-Added Services

For example, the Collaborative Mining service.

Mining Process

批注 [KW1]:



Graph 5-1 Mining Process

批注 [KW2]: 矿工钱包 – Miner wallet
挖矿软件 – Mining software
矿池 – Mining pool
答案验证组件 – Answer verification component
矿池钱包 – Pool Wallet
主链 — Main Net
从硬盘中检索答案() - Scan for answer in the hard disk ()
提交答案() – Submit answer ()
验证答案() – Verify answer ()
登记答案() – Register answer ()
如果答案更优，通知出块() – If the answer is optimal, notify to generate block
出块到主链() – Generate block to the main net
登记已出区块() – Register generated blocks ()
检查区块成熟（过 100 个区块），并登记收益() – Check block maturity (after 100 blocks) and register return ()
根据贡献度，抵押情况，给矿工结算收益 () – Compute miners' return according to contribution and whether pledge condition is met ()
结算收益给矿工钱包() – settle and send returns to miners' wallets ()

Responsibilities of the Mining Pool：

1, Receives answers submitted by miners；

2, Miners verify answers；

It is recommended to use independent verification components, which require higher CPU requirements, or GPU.
Needs to support horizontal expansion.

3, Generates block, checks maturity;

4, Define rules of return,

5, Calculates and distributes returns to miners ;

6, Register miner status ;

7, Dual-Mining penalty inspection.

Responsibilities of the miners :

1, Submit answers ;

2, Submit BHD for collaborative mining ;

3, Receive dividend ;

4, Understand contribution and distribution ;

Responsibility of the Answer Verification Component :

1, Verify answers ;

Responsibilities of the Mining Pool Wallet :

1, Generates blocks,

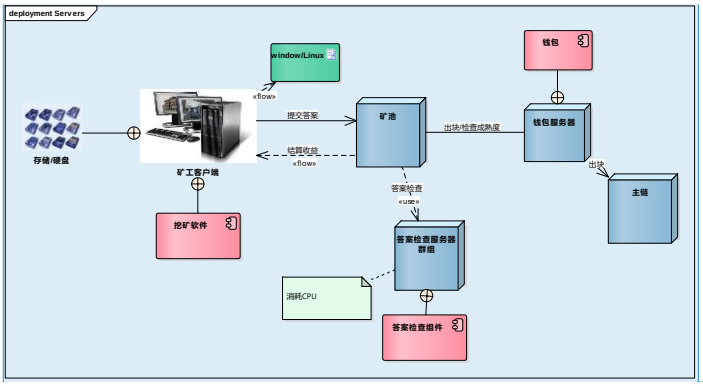
2, Receive and distribute returns ;

3, Collaborative mining ;

To ensure security of the Mining Pool Wallet, it is recommended to use two separate tallets:

1. Wallet for collaborative mining/block generation;
2. Wallet for return distribution.

Mining Pool Deployment



Graph 6-1 Mining pool Deployment

批注 [KW3]: 存储/硬盘 – Storage/Hard Disk
矿工客户端 – Miner Client
挖矿软件 – Mining Software
提交答案 – Submit Answers
结算收益 – Settle Returns
矿池 – Mining Pool
答案检查 – Verify Answers
答案检查服务器群组 – Answer Verification Server Group
消耗 – Consume
答案检查组件 – Answer Verification Components
钱包 – Wallets
出块/检查成熟度 – Generates Block/Check Maturity
钱包服务器 – Wallet Server
主链 – Main Net

Commonly Asked Questions

Q：Is the network-requirement high？

A：You only need to submit answers, so ordinary home broadband is sufficient.

Q：What are the requirements for the CPU's hash power?

A: The Mining Pool has a relatively high requirements for the CPU's hash power as every answer submitted needs to be verified.

Q：Can you please explain the principle of block generation?

A：5 minutes per block. BHD forks based on BTC, block generation mechanism is the same as POW.
Wallet computes Deadline according to answers submitted by miners. When Deadline is reached, wallet packages the transactions and broadcast to the whole net. Once other nodes receive the blocks, they start block verification, and if blocks are successfully verified, the nodes accept the new block.

Q：How to tell miner capacity accurately?

A：Main net checks the most recent 2016 blocks, checks plotterid corresponding block generation history, then calculates the plotterid capacity based on the difficulty level

given current block height.

The wallet provides RPC interfaces of plotter capacity, getplotterminginfo。

Q：How to avoid cheating?

A：Normally we want to avoid miners dual-mine, as in miners solo and submit answers to the pool at the same time.
What the pool has to do is just to check if the answer submitted by the miner has also generated blocks on the main net.

Wallet API Instruction

getMiningInfo

get method

to get information about the next mine
{
  ""requestProcessingTime"": 0, //new add
  ""height"": ""472016"" //string
  ""baseTarget"": ""18325193796""
  ""generationSignature"":
“43f51d240a5ce52bb9a6e0cef104e8c2a8ed46e3964f14a144ca6d450590d481""
}"

submitNonce

post method

Parameters：
nonce：
accountId（plotid):
height: by default send 0。
address
nonce=$nonce&accountId=$accountId&height=0&address=xxxx

If you want to understand more about the api and architecture, a good reference would be the ‘Bitcoin Core Apis’ article.

References

1. BHD Whitepaper 1.0
2. Bitcoin Whitepaper: A Peer-to-Peer Electronic Cash System
3. Bitcoin Core Api

   https://bitcoin.org/en/developer-reference#bitcoin-core-apis
4. Genaro Yellow Paper。
5. Mining software

   Mining software requires reading codes。