BHD 矿池白皮书

版本	作者	日期	说明
0.8	z	9/29/2018	创建文档
0.9	z	6/10/2018	更新钱包 api 说明。
0.9.1	z	2/11/2018	更新 api 说明

目录

概述

BHD 2018 年 8 月 3 号 16:00 公网上线，截至今日（2018.9.29）主网算力达到 136.63P。

硬盘算力（容量）的不断上升，代表了参与者(矿工)对 BHD 的认可，为了给矿工提供更好的服务，并优化 BHD 生态，矿池可以集中服务，分摊风险，或者提供增值服务。

基于以上原因，BHD 基金会发布本白皮书，为有意开发矿池的伙伴提供参考。

名词解释

BHD：Bitcoind HD， 比特硬盘简称，官网 www.btchd.org。

矿池：集中收集矿工提交的算力（答案），代表矿工出块到公链。

矿工：持有硬盘，并提交算力给矿池，或者 SOLO 钱包。

SOLO 挖矿：答案提交给自有钱包，自有钱包出块。

挖矿软件：从硬盘中检索答案，并提交给矿池或者自有钱包。

抵押：按照评估算力的，每 T 需要抵押 3 个 BHD。

主链是按照最近 2016 个块， plotterID 出块，合并计算硬盘容量。

双挖：矿工同时提交答案给矿池和自有钱包。

矿池要求

1. 稳定性

   7*24 小时在线。

2. 安全性

   钱包安全。

   DDOS 攻击安全。客户提交答案进行轰炸。

3. 高并发

   同时在线矿工 1000+；

   5 分钟内处理矿工提交答案 3000+；

   提交答案响应速度 <=100 毫秒。

4. 收益分配合理。

矿池价值

1. 稳定的钱包。

   随着交易增加，链上数据增大，矿池挖矿，矿机不需要每个都安装钱包。

   减少硬盘占用。

2. 统一监控

   可以实时监控矿机状态，是否掉线。

3. 稳定

   专业化服务团队，矿池运行更稳定。

4. 分散风险，均匀收益。

对算力比较小的矿工来说，每天都有收益。

5. 增值服务

如抵押服务。

挖矿流程

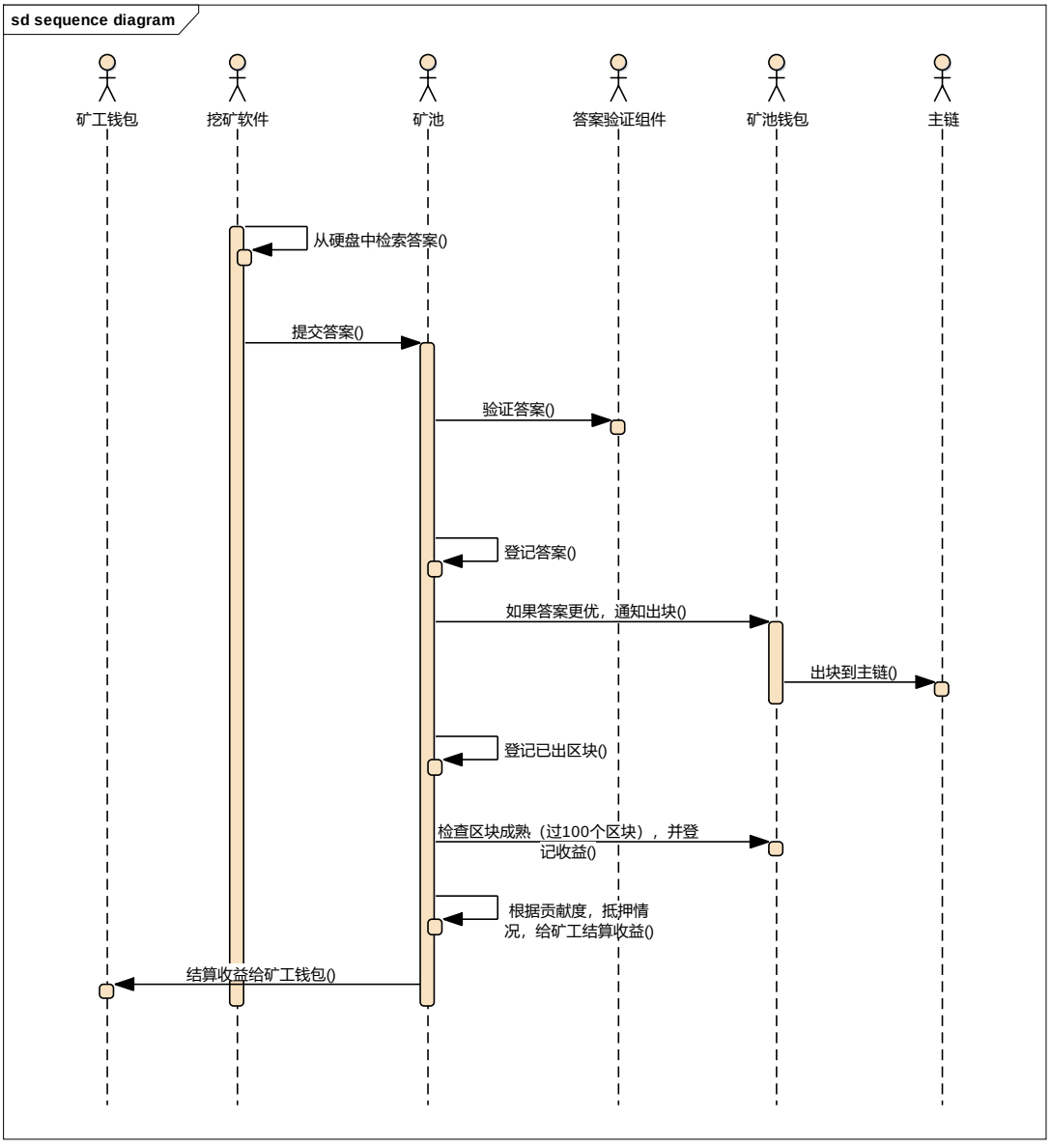

图 5-1 挖矿流程

矿池职责：

1，　接收矿工提交答案；

2，　矿工验证答案；

建议采用独立的验证组件，对 CPU 要求比较高，或者采用 GPU。

需要支持水平扩展。

3，　出块，检查成熟度；

4，　定义收益规则，

5，　计算收益，并分配；

6，　登记矿机状态；

7，　双挖惩罚检查。

矿工职责：

1，　提交答案；

2，　提交抵押；

3，　接收分红；

4，　知悉贡献及分配；

答案验证组件职责：

1，　验证答案；

矿池钱包职责：

1，　出块，

2，　接收，分配收益；

3，　抵押；

矿池钱包注意安全。

建议分成两个钱包:

1, 抵押/出块钱包;

2, 收益分配钱包。

矿池部署图

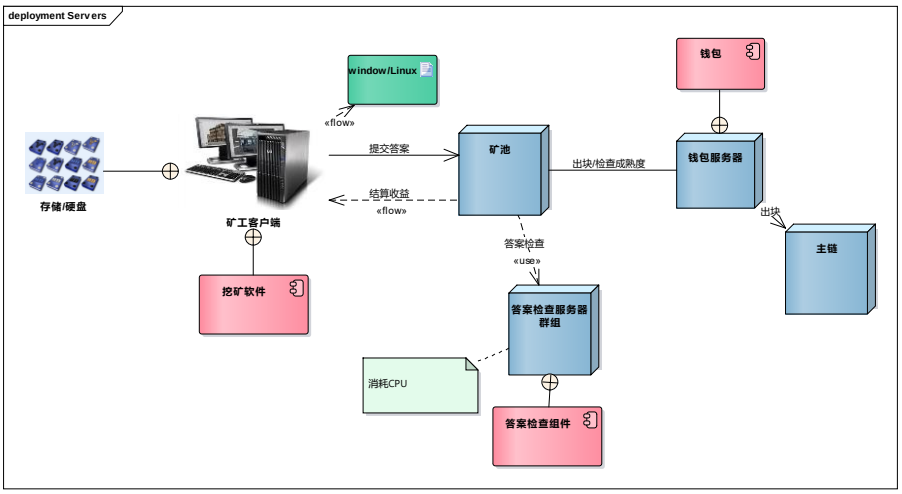

图 6-1 矿池部署图

常见问题

问: 对网络要求高不高?

答: 只是正常提交答案, 对网络要求不高, 正常家庭宽带即可。

问: CPU 计算要求?

矿池对 CPU 的计算能力要求比较高。每个答案提交上来后, 都要做验证, 所以, 对 CPU 计算能力要求比较高。

问: 出块原理

答: 每 5 分钟出块。BHD 基于 BTC 进行分叉, 出块机制跟 POW 一样。

钱包根据矿工提交答案, 计算出 DeadLine, 当 Deadline 达到后, 对交易进行打

包，并 broadcast 到全网。其他节点收到区块后，进行验证，通过验证，则接受新区块。

问：如何准确判断矿机容量？

答：主链检查最新 2016 个区块，检查 plotterid 对应的出块记录，并根据区块所在高度的难度，计算该 plotterid 的容量。

钱包提供了 plotter 容量的 RPC 接口，getplotterminginfo。

问：如何防作弊？

答：防作弊主要是防止矿工双挖，即同时 solo，和给矿池提交答案。

矿池需要在主链上检索该矿工提交给矿池的答案，是否也在主链上出过块即可。

钱包 API 说明

getMiningInfo

get 方法。
获得下一个要挖的矿的信息

```
{
   ""requestProcessingTime"": 0,          //new add
   ""height"": ""472016""                                  //string
   ""baseTarget"": ""18325193796""
   ""generationSignature"":
“43f51d240a5ce52bb9a6e0cef104e8c2a8ed46e3964f14a144ca6d450590d481""
}"
```

submitNonce

post 方法。

参数：
nonce：
accountId（即 plotid):

height: 默认传 0。
address
nonce=$nonce&accountId=$accountId&height=0&address=xxxx

关于如何理解 api 及体系结构，可以学习 Bitcoin Core Api 说明。

参考资料

1. bhd 白皮书 1.0
2. 比特币白皮书：一种点对点的电子现金系统。
3. 比特币 Core Api

   https://bitcoin.org/en/developer-reference#bitcoin-core-apis
4. Genaro 黄皮书。
5. 挖矿软件

   挖矿软件需要阅读代码。