版本发布说明文档

概述

本次版本更新，主要修改/新增如下功能：

1. 调整算力惩罚措施；
2. 修改难度调整算法；
3. 增加POW挖矿搜索空间；
4. BUG修复。

算力惩罚措施

目前主网版本，对于选中但没有上报基础算力的矿工主节点，只会将其加入“算力黑名单”且不分配“选中周期”的矿工参与奖励。

本次版本会对加入“算力黑名单”的矿工节点增大惩罚，措施如下：禁止“算力黑名单”节点1个轮询周期的参选矿工主节点的资格。也就是说，“算力黑名单”节点，在接下来的轮询周期内，不会被选中。

难度调整算法

在目前主网版本运行中，我们发现存在如下缺陷：

1. 由于“验证者Leader更换”引起的计算难度值偏低；
2. “快速建立阶段”和“跟踪阶段”衔接不当导致难度值稳定速度慢；

由于“验证者Leader更换”引起的难度计算偏低

在一个挖矿周期内（3 个区块时间），如果出现“验证者 Leader 更换”（验证者节点采用轮流出块机 制，一个区块的出块验证者节点称为该区块的验证者 Leader 节点，在规定时间内该节点没有出块，那 么更换该区块的出块者）时，这个挖矿周期的时间会增加，相应的计算下一个区块的难度时，难度会降低；但是这个增加的时间不是由于矿工算力不足引起的，无法反映真实的算力（实际上，当一个验证者节点故障时，会频繁出现该现象，导致难度调整无法生效，难度值很低，矿工算力无法发挥）。

出现这种情况时，我们无法准确知道矿工实际的挖矿时间，在计算难度时，我们采取了折

中处理，使用“期望的出块时间”代替实际的出块时间。

“快速建立阶段”和“跟踪阶段”衔接不当导致难度值稳定速度慢

目前主网难度调整算法分为两个阶段：

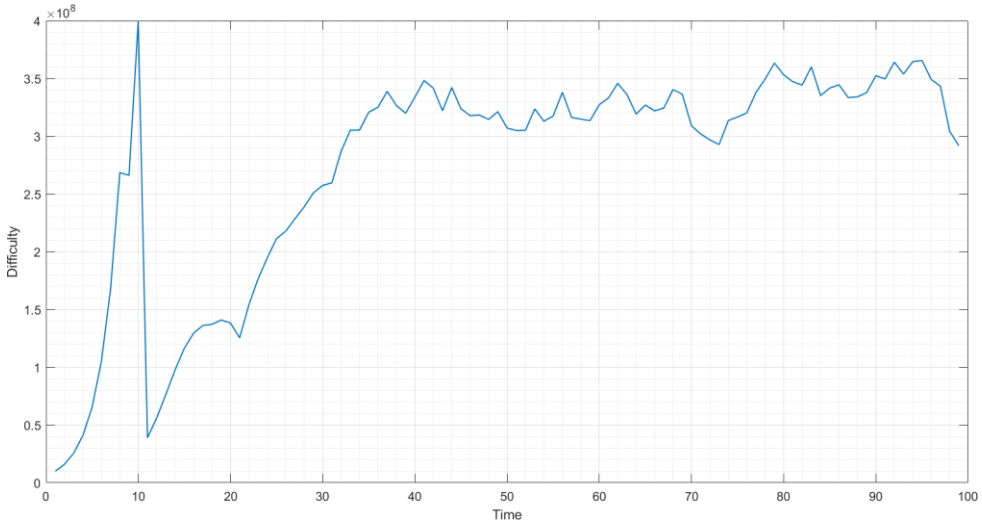
1. 快速建立阶段。前N个挖矿周期采用快速建立算法，指数级别调整难度值，尽快使难度估计值接近真实算力；
2. 跟踪阶段。在快速建立阶段后，采用“指数加权移动平均”的方法，跟踪全网算力变化。

目前主网版本在“指数加权移动平均”计算时，起始阶段会采用“快速建立阶段”的区块信息（难度值和时间），这信息并不能准确反映算力情况；由于“快速建立阶段”最后一个区块信息相对准确，本次版本，在“指数加权移动平均”计算时，使用“快速建立阶段”最后一个区块的信息代替该阶段所有区块信息参与难度计算。

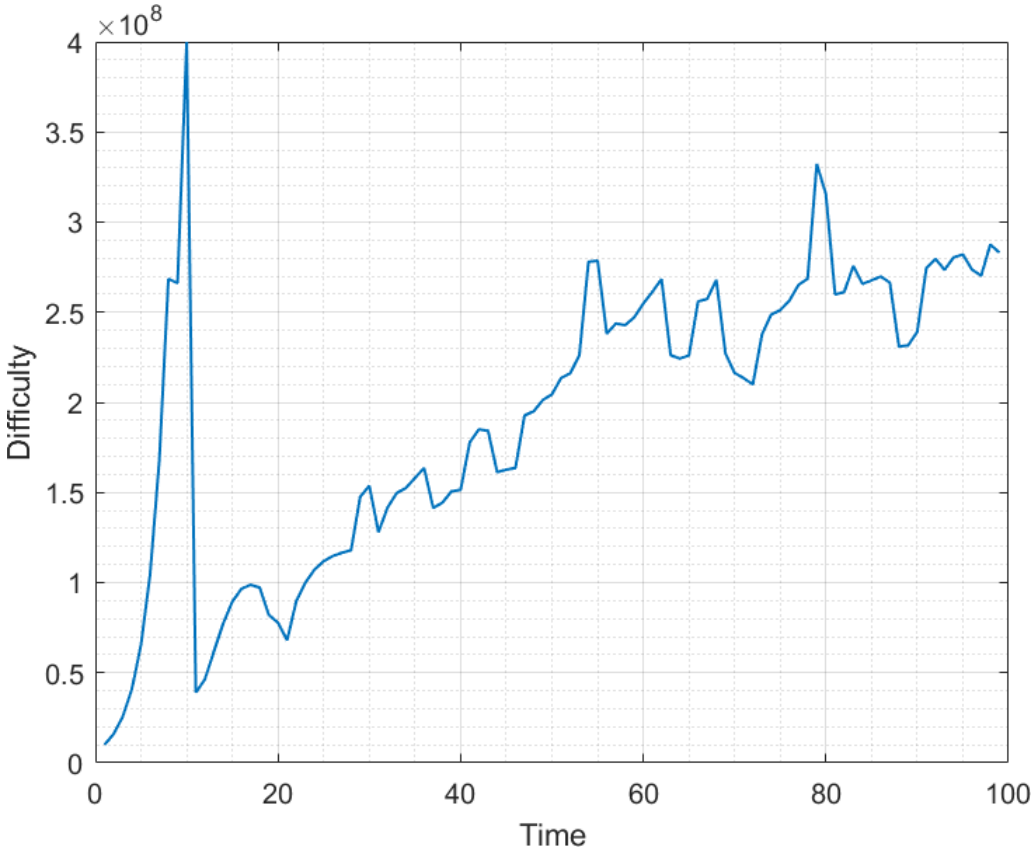
算法修正效果对比

相同的初始难度以及算力的情况下，我们从无“验证者Leader切换”和有“验证者Leader切换”进行仿真，对比版本修改效果。 下面是四张难度值随时间调整的过程图。

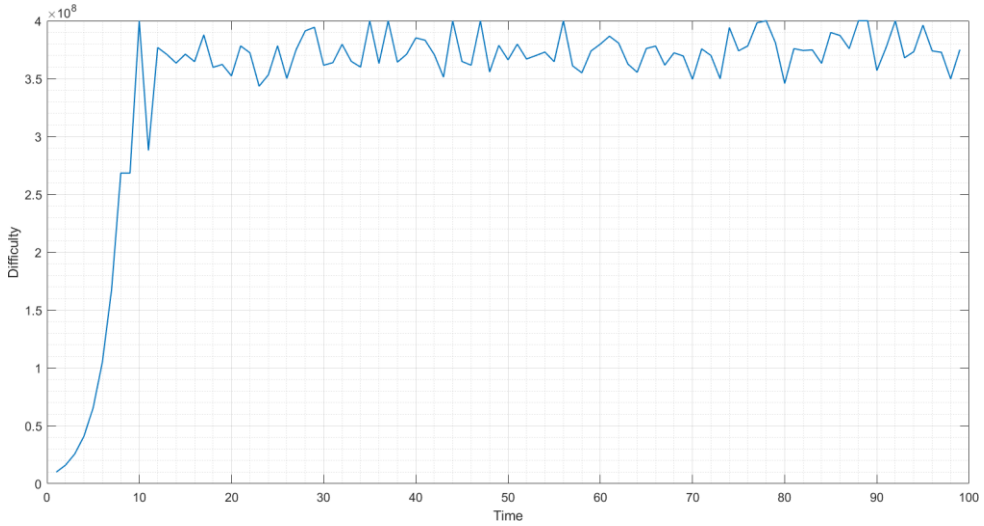
1. 图 1 为目前主网版本，且没有“验证者 Leader 更换”时的难度值调整图；



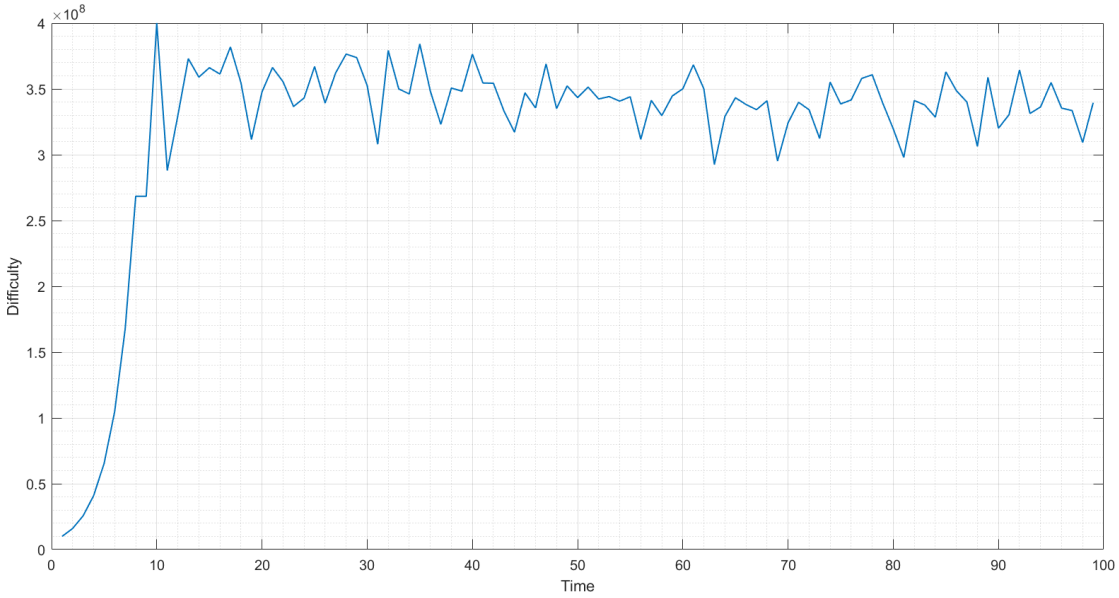
2. 图 2 为目前主网版本，且有“验证者 Leader 更换”时的难度值调整图；



3. 图 3 为本次版本，且没有“验证者 Leader 更换”时的难度值调整图；



4. 图 4 为本次版本，且有“验证者 Leader 更换”时的难度值调整图；



从图 1 看，目前主网版本在快速建立后，又存在一个下降过程和一个缓慢的上升过程，到难
度值稳定经历较长时间；从图 3 看，在快速建立后，难度值很快保持稳定。本次版本对于“快速建立阶段”和“跟踪阶段”衔接存在的缺陷，修复是有效的。

对图 1 和图 2 进行对比，可以看到，图 2（存在“验证者 Leader 切换现象”）难度值上升比较慢，且最终难度值相对图 1 偏低；对图 3 和图 4 进行对比，可以看到，图 4（存在“验证者 Leader 切换现象”， 且参数和图 2 参数一致）难度值上升的速度没有明显变化，虽然最终难度值略有降低，但偏差很小。本次版本对由于“验证者 Leader 更换”引起的难度计算问题的修复是有效的。

参数调整

根据目前主网运行情况，修改难度调整算法配置参数

参数类型	目前主网版本配置	本次版本配置
目标出块时间（秒）	11	12

参数类型	目前主网版本配置	本次版本配置
选举初始难度	1000万	2000万
最小难度	200万	1500万
X11最大难度	4亿	无限制
SM3最大难度	4亿	4亿

POW挖矿搜索空间增加

目前主网 POW 挖矿的搜索空间为 4 字节，在难度非常高时，存在遍历完所有的搜索空间都无法获取合适目标值的可能性。本次版本新增 12 字节的搜索空间，内容存放在区块头 mixDigest 字段的前 12 字节。

BUG修复

本次版本更新，主要修复如下BUG：

1. 修复“验证者缓存矿工挖矿结果深度不够”的BUG；
2. 修复“CPU挖矿时，nonce不能为0”的BUG；
3. 修复“P2P模块，某些代码对map访问未加锁”的BUG；

修复“验证者缓存矿工挖矿结果深度不够”的BUG

目前主网验证者只能接受比本地高度大 1 的挖矿结果；当 POW 挖矿难度较小时，可能出现挖矿结果提前 2 个区块到达，有概率导致算力高的矿工挖矿结果没有被采纳。本次版本修复该缺陷。

修复“CPU挖矿时，nonce不能为0”的BUG

目前主网版本在CPU挖矿中，代码限制nonce不能为0。本次版本修复该缺陷。

修复“P2P模块，某些代码对map访问未加锁”的BUG

目前主网版本，P2P模块，某些代码对map访问时未加“锁”，在连接节点较多时，会存在程序崩溃的可能性。本次版本修复该缺陷。

注意事项

1. 矿工需要妥善的维护节点，如果选中后没有上报基础算力，除本次选举没有收益外，下一个选举轮次，节点将丧失选举资格；

2. 经过实验室进行对比，40核心的CPU在算力上远远落后于矿机，没有出块的机会。矿工要保证收益率，需要购买矿机进行挖矿；或者抵押成验证者（或加入联合抵押），获取验证者奖励。