随着君士坦丁堡分叉的临近，以太坊上许多悬而未决的项目开始接连跟进。最终目的是踏上POS这条“康庄大道”。

今日记者获悉，coindesk报道称，以太坊开源开发社区成员暂时同意实施一种新算法，将阻止专门的挖矿硬件或ASIC，他们将对提议的代码进行进一步测试。

如果用户网络接受，那么被称为“ProgPow”的代码更改将阻塞ASIC（Bitmain等主要矿业公司所生产的ASIC），取而代之的是，新软件将允许通用或GPU硬件在平台上竞争奖励。

惹人厌的ASIC

从中本聪用多核CPU开采出创世区块开始，到个人GPU挖矿的诞生，再到FPGA、ASIC的更新迭代，由PoW衍生出来的矿工行业，为了竞争，一直在不断寻求更高效的挖矿捷径，而以太坊身为PoW大户，也难逃此劫。

众所周知，以太坊采用的是Ethash算法。这一算法在很长一段时间内都没有被ASIC矿机攻破，而GPU由于可以大规模地向很多个人提供，这些人本身并没有涉及到加密货币，没有财务动机，具备明显的去中心化特性，所以，在以太坊上，这些年GP

U挖矿一直是主流。

但是，2018年4月比特大陆宣布即将开启首批ETHhash ASIC预售的消息，打破了这一局面。

以太坊ASIC矿机算力明显优于GPU矿机，这样一来，算力很可能集中在少数持有大量ASIC矿机的矿工手上，使以太坊面临中心化问题。所以，纵然ASIC是挖矿业紧跟潮流的产物，以太坊社区对这台机器显然并不感冒。

此前，V神就公开坚称，要尽自己所能阻止ASIC的到来，以保护以太坊的安全和去中心化。

然而，社区的意见并不代表矿工的意志，这个拥有超强逐利性的群体只会向钱看，而且，如果由于支持GPU而拒绝高性能挖矿，这也是以太坊不愿意看到的。

在这种两难抉择的困境下，ProgPow共识机制孕育而生。

ProgPow

从名字就能看出来，ProgPow是PoW的延伸，其基本原理与PoW相同，都是工作量证明，即算力大小决定收益多少。

记者了解到，这个被称为“ProgPOW”的算法，至少在2017年就已经开发出来了。在GitHub上有详细的描述：

“ProgPOW是一种用于缩小专用ASICs可用效率差距的工作证明算法。它利用了几乎所有的商品硬件（GPUs），并对以太坊网络中使用的最常用硬件进行了预调。”

换言之，虽然一些算法为高度专业化，昂贵的采矿设备提供了比更常见的优势，但ProgPOW试图通过减少进入的财务障碍来平衡竞争环境。许多其他区块链考虑并实现了ASIC算法，包括Zcash（最终被拒绝）和Monero（已实施），作为减少矿业池集中化的一种方法。

此前，GPU供应商以及这次代码更改的主要开发者Kristy-Leigh Minehan在接受采访时就表示：该代码的设计目的是最大化GPU硬件的特性，使用80%的整体显卡性能来计算算法，而不是传统的加密货币挖矿的10%到20%。

也因为如此，Minehan表示，如果一个硬件设计师试图建立一个ProgPoW ASIC—

—也就是一个专门的芯片，它的唯一功能就是计算ProgPoW——它最终会变成GPU硬件。

保证过渡安全性

以太坊最终的归宿是POS，而POS不需要矿工。所以，从POW到POS的过程，注定是矿工从兴起到衰亡的过程。

但是，算力战的出现已经让人们见识到了矿工可不好惹。如何能在不引起矿工联合抵制的情况下完成向POS的转化，是以太坊需要思考的问题。

在以太坊白皮书中，有这样一个名词：Difficulty Bomb（难度炸弹）。

难度炸弹指的是计算难度时，除了根据出块时间和上一个区块难度进行调整外，加上了一个每十万个区块呈指数型增长的难度因子。

刚开始附加的难度并不引人注意，但是，随着区块高度的增加，呈指数增长的难度因子比重将会显著提高，使得出块难度大大增加，矿工将难以挖出新的区块。这种对矿工温水煮青蛙式的过程，就是V神最初的构想。

不过，理想很丰满，现实很骨感。虽然有难度炸弹护航，但是，可以预想到，要在保持以太坊运行稳定的情况下，其推进过程必然是艰辛重重，而且POS机制中有很多问题需要解决。时至今日，人们可以看到，POS的开发时间比以太坊原先计划要长得多。

众所周知，此次君士坦丁堡分叉的来临，除了对以太坊自身优化之外，还有两项举措：引入POW+POS混合共识机制，和矿工开采奖励从3ETH降低到2ETH。

引入POW+POS混合共识机制，为的是让POW向PoS的过渡更加流畅。但是，对矿工来说，挖矿的收益会大幅度地降低。

对此，有业内人士担忧称，挖矿奖励的减少，可能会把矿业的力量集中在少数几个可以获得廉价电力，以及有资源买到ASIC矿机的矿池手里。

所以，ProgPow的推进迫在眉睫。

近日，在以太坊开发者电话会议上，ProgPow成为了讨论的焦点。

以太坊安全主管Martin Holst Swende表示，他更喜欢这种转换，因为它将有助于

确保以太坊最终向股权证明过渡的安全性。这是一种新的系统。

“我们今天知道ethash有缺陷，目前正被瞄准。所以，这就是为什么我想尽快转换，给我们时间去证明利害关系。” Martin Holst Swende进一步表示。

Ethuunm基金会通讯官Hudson Jameson也表示，“听起来，我们已经达成共识，我们正在试探性地进行ProgPow，这意味着我们将继续进行，除非在测试或类似性质的事情中发现重大问题。我们将继续推进ProgPow。”

这意味着，除非开发人员在变更中遇到意外的问题，否则ProgPow将在未来2到4个月内作为独立的系统范围升级或硬分叉的一部分发布。

目前，ProgPow的时间安排仍不清楚，但是，开发者同意在1月18日的下一次开发者电话会议上提出升级时间问题。无疑，接下来发生的事情很重要。