近期在各大社区关于是否抗 ASIC 的讨论不绝于耳，各方都有自己的观点，不过很多人其实是完全不知道大家在说啥的，今天我就来简单的讲解一下几个基础概念帮助大家理解。

ASIC 概念与起源

ASIC 即 Application-Specific Integrated Circuit 专用特殊集成电路，一般用来是指根据定用户要求和特定电子系统的需要而设计、制造的集成电路芯片。ASIC 矿机挖矿始于阿瓦隆，发扬光大于比特大陆自主研发的针对比特币的矿机，通过该类矿机，可以让挖矿更加有效率性，以 S9
系列矿机最为出名。比特大陆也是当下市场份额最大的矿机制造商。ASIC
矿机挖矿不是挖煤，而是挖特定的数字货币，比如比特币 ASIC
矿机只能挖比特币。挖矿的本质也是解决交易出块中的数学难题，从而获得区块 Block 出块的奖励。

ASIC 起源来自 1981 年 3 月 Sinclair 公司推出的一款电脑 ZX81，采用 Z80
处理器，也被公认为业内最早的 ASIC 原型。第一台比特币 ASIC 矿机是南瓜张于 2012 年 9 月发布的阿瓦隆 Avalon，由烤猫团队网上融资制作，该团队其余成员后收编组成了当今的比特大陆。

矿机方法与矿机种类

当前挖矿方法与矿机主要有 4 大类：ASIC, FPGA, GPU, CPU 挖矿。

ASIC已经讲过，Application-Specific Integrated Circuit，特定挖矿的矿机。

FPGA- Field Programmable Gate Array 属于一种可编程的半定制芯片，灵活性，可编程性是其很大的特点，通过软件升级就能够实现硬件功能的重新自定义。但灵活性高也意味着效率相对 ASIC 就低了些，可用于 Scrypt 计算与 GPU
类的矿币。

GPU- Graphics Processing Unit 即，我们平时说的显卡，主要用于 Equihash 算法为主的加密货币挖矿，Equihash 是图形类算法，所以这个显卡它也算是专业对口，速度也快了很多，烧显卡操作也从大型网游过渡到了挖矿新纪元。

CPU
挖矿，这个应该是最亲民易懂的了，毕竟每天玩电脑的我们时时刻刻都在燃烧着 CPU 的「卡路里」，靠 CPU 的计算能力直接去解题挖矿，数字货币早期还是比较容易的，那时候全网算力也不过 100 多

GH/s，但现在的难度系数大很多，但如果是超级 super CPU,
还不如花这钱买点别的矿机去 POW 了。

ProgPoW 概念与抗 ASIC 逻辑

ProgPoW （Programmatic Proof of Work 的缩写），本质也是 POW
挖矿机制，希望通过优化 GPU
矿机的挖矿算法来推动挖矿产业的去中心化程度。改变了以太坊的 Ethash
算法，从而降低了 ASIC 的计算能力优势，前面我们讲到与 GPU
显卡挖矿不同，ASIC 是高度专门化的机器，特定于它们所开发的挖矿算法。

但以太坊的社区还是比较反对 ProgPoW 这种提案的，原因也在于 ASIC 其实在
ETH 也没有那么集中，而以太坊算法本来就比较抗 ASIC
类了，更应该担心的是集中优化 GPU
的显卡挖矿集中化，因为就算哪怕是成本较低的 GPU
挖矿，绝大多数算力同样也是掌握在矿场和矿池手里。并且 ProgPoW
有意增加特定 GPU 矿机的优化，这对于其他 GPU
来说也是一个风险。虽然很多爱好者也可以通过自身的高级显卡参与，门槛相对于
ASIC 比较低一些，但实际更多爱好者通过矿池参加也比较容易在当下参与 POW
类的挖矿。

而矿池这种大众规模中心化的概率相对没那么夸张，矿场的中心化也更多集中在电费便宜的地方。一般理解到这种程度就够了，具体算法内在的代码性能细节差别这里不做过多陈述。

到底要不要抗 ASIC

Future 认为 ASIC 唯一被 Diss 的地方也就是它卓越的挖矿性能了，由于挖矿性能的好处导致大规模购置后的算力集中担忧，以及作恶担忧。目前比特币完全支持 ASIC 矿机，并不存在大中心化的问题。

我个人认为，ASIC 如果被抗没了，新的优越性能的 GPU 完全也有可能成为新的 ASIC，依旧该集中的还是会相对算力集中。不过话说回来，开矿厂，办矿池，粉丝自己买矿机挖矿最终目的当下还是为了获得奖励而赚钱，如果我掌握了超大比例的算力，我正常维护系统就能赚很多钱，我何必作恶呢？至于去中心化，我倒是觉得矿池可以推出拼团够矿机系列，或者拼团云算力系列，让更多热爱的人不必要一下子花那么多钱买矿机，但是可以合伙平均分币。

今日的 ASIC 明日也会让更优秀的 ASIC

芯片代替，这无意间也推动了芯片行业的发展，所以高性能的 ASIC 芯片不一定被替代就是好事情。去集中化完全可以通过更多经济可行的方式来实现。GRIN 也将推出自己的矿机，口碑不错的社区 RVN 也在不断推出抗 ASIC 的新算法，同时支持一定抗 ASIC 但不那么排斥的 ASIC 的 X16R 算法也被矿工支持推出 RVNClassic。

隐私性较高的门罗币 XMR 也在 18 年 4 月开始调整 PoW 算法（CryptoNight-R），希望可以限制网络中的 ASIC 矿机，但也有团队完全认可 ASIC 从而形成了分叉链 Monero-Classic(XMC)，探索新的发展。Blockstream 的数学家 Andrew Poelstra 也说，通过修改算法的确可以让短期让 ASIC 矿机失效，但这种抵抗最终会被证明是徒劳无效的。这也证明了 ASIC 和完全抗 ASIC 孰优孰劣依旧是一个验证阶段，我认为能让生态健康发展就是一个好事情，相对的集中化并没有什么太大的问题。

我们国家抗击疫情的效率多么优秀，众志成城，世界称赞，反而看其他有的民主国家，还在哈利路亚。区块链世界亦是如此，集中和分散永远是如同阴阳一样相对交替而循环往复的事情，哪个做的好哪个才是当下最适合的。最后用博弈论的纳什均衡收尾，其实这就是博弈论的问题，我个人认为的均衡点就在蓝色部分，而黄色，绿色部分则是相应个体的最优解，弱无法最优解则蓝色部分最可能发生。