今年3月，比特大陆发表了一种基于新款 ASIC 的矿机蚂蚁矿机
X3，主要是针对门罗币（XMR）以及依赖 CryptoNight 算法的加密货币，门罗币随即发出反制声明，将改变核心算法以对抗ASIC算力的入侵。

BITMAIN @BITMAINtech 15 Mar

We are pleased to announce the all-new Antminer X3, to mine cryptocurrencies based on the CryptoNight hashing algorithm. Two batches: shipping in June (goo.gl/fK9boQ) and shipping in May (goo.gl/rjBtji)
To prevent hoarding and to enable.... (1/2)
pic.twitter.com/PBKdXrwg9b

BITMAIN
@BITMAINtech

...to enable more users in different time zones to order, we have set a limit of one miner per user and will release both these batches with an equal stock thrice today: 3PM, 6PM and 9PM (15 March, GMT+8). Order while the batches last! (2/2)
pic.twitter.com/ezp181HuWB

3:09 PM - Mar 15, 2018

77 130 people are talking about this

另外，以太坊一直以来也是苦恼于 ASIC 利用各种手法对其算法的挑战，且因为ASIC算力集中度高，违反其去中心化思想，亦在北京时间4月5日宣布对其算法进行改版，推出仅仅是改动5个函数的 EthashV2，但也足以让目前的 ASIC 挖矿设备失去效用。比特大陆也推出了反反制方法，一场争夺加密货币主导权的血战似乎正要展开。

ASIC挖矿争议重重

比特大陆等挖矿专用ASIC设计公司因为加密货币的热潮而兴起，由于在挖矿的效率大幅超越了传统GPU以及CPU，因此极受挖币矿工的欢迎，营收不断暴涨，也连带让台积电等晶圆代工厂商营收进补。

ASIC挖矿本身虽然已经发展了一段时间，其效率也受到广大的矿工认可，甚至也有说法指出其将会取代GPU等其他挖矿形式，但ASIC挖矿在过去一直存在相当大的争议。

2017 年比特大陆利用比特币(BitCoin)算法的漏洞，开发了一款 ASIC Boost 程序，让自家矿池的挖矿速度比竞争者快上 20%，这种做法引发不小争议。但在争议事件后没多久，比特大陆的芯片被发现一个称为 Antbleed 的漏洞，有人怀疑比特大陆根本就是蓄意留存这个漏洞，就能恣意阻止矿工挖矿。当然，比特大陆坚称其维护币圈价值，不会使用这些台面下的手段来增加产品或营运上的优势。

而为了避免企图以不良算力污染这些以区块链为技术基础的加密货币，区块链加密货币开发者也积极采取各种措施来抵抗ASIC。比如说门罗币(XMR)与以太坊(ETH)近来宣布要针对核心算法进行调整，让ASIC挖出来的货币不被区块链承认。

若比特大陆这类挖矿芯片开发商要支持新的算法，就必须开发针对新算法调整的新款ASIC芯片，或者是在未来的芯片设计上增加更大的弹性，容许微码的调整或存储，前者将大大降低挖矿芯片的市场吸引力，毕竟没有人想要买只能挖个半年的矿机，后者则是大大增加挖矿芯片的设计与制造成本，甚至提高到与GPU类似的程度。

但是，改变算法并无法完全阻挡ASIC的侵略，只能拖慢速度，或期待ASIC厂商因成本增加或顾客不买单而知难而退。另外，挖币的庞大利益却很难与加密货币原本的崇高理念完全切合，也因此，支持不同挖矿算力来源的矿工也可能会通过”分叉”(fork)的作法来确保加密货币会朝己方偏好的形式存续下去，比如说BitCoin与BitCoinCash的分叉，以太坊也曾闹过ETC、ETH分家。若ASIC矿商在掌握足够的算力的情况下，是可以通过分叉来占原本加密货币的便宜，从而建立起属于自己分叉的区块链，事实上，比特大陆已经开始这么做了。

然而，这样的区块链恐怕就会违背原本加密货币所强调的去中心化理念。

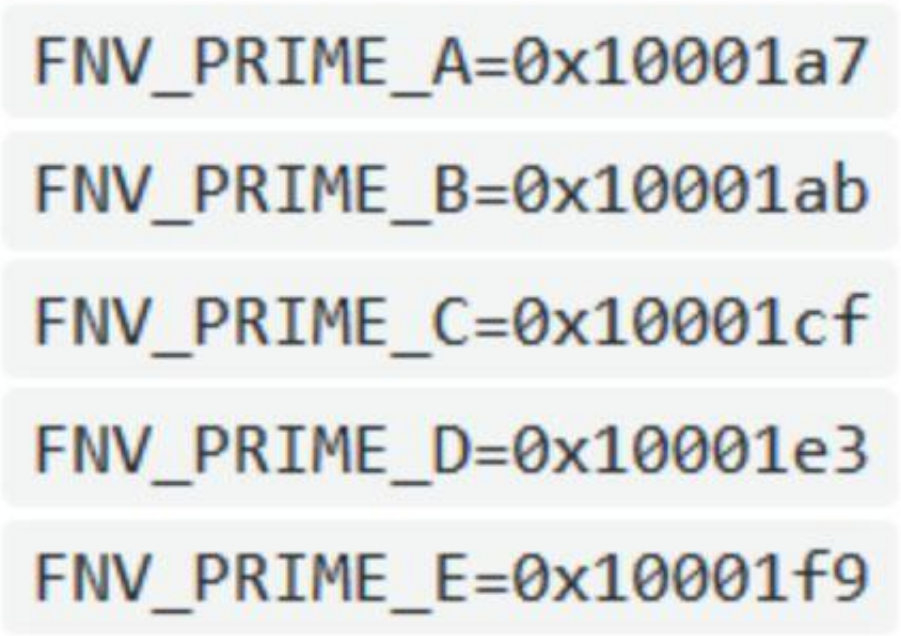
门罗币与以太坊主动出击

其实，主要加密货币的开发者对于 ASIC 挖矿一直以来都是抱以不信任的态度，但并非因为挖矿计算架构，而是担心挖矿方案的供应商过于集中，容易导致原本加密货币强调的去中心化形同空谈，且挖矿方案商比特大陆曾发生后门与使用漏洞的事件，加上其极为强势的态度，更加深这些开发者与仍坚持去中心化理念的矿工们对ASIC的不信任。

自从比特大陆宣布针对采用 CryptoNight 算法的加密货币推出蚂蚁矿机方案后，门罗币就抢先在该产品上市前宣布要修改核心算法抵制，开发人员宣称未来可能一年会进行两次的算法升级，将整个门罗币区块链完全推移到新算法的基础上，淘汰以旧有算法为基础的挖矿形式，形成软分叉(Soft Fork)。

由于门罗币极度强调隐私与去中心化的理念，事实上，它也是目前公认隐私性最高的加密货币之一，门罗币开发者极为坚持自身的价值，因此希望通过算法升级避免不良ASIC算力入侵。

以太坊最近通过修改算法的提案，同样也是要针对比特大陆的新挖矿产品。以太坊预计将把挖矿算法更新为EthashV2，EthashV2和Ethash将使用相同的规格，但是会把hashimoto中用到的5个fnv函数改掉。



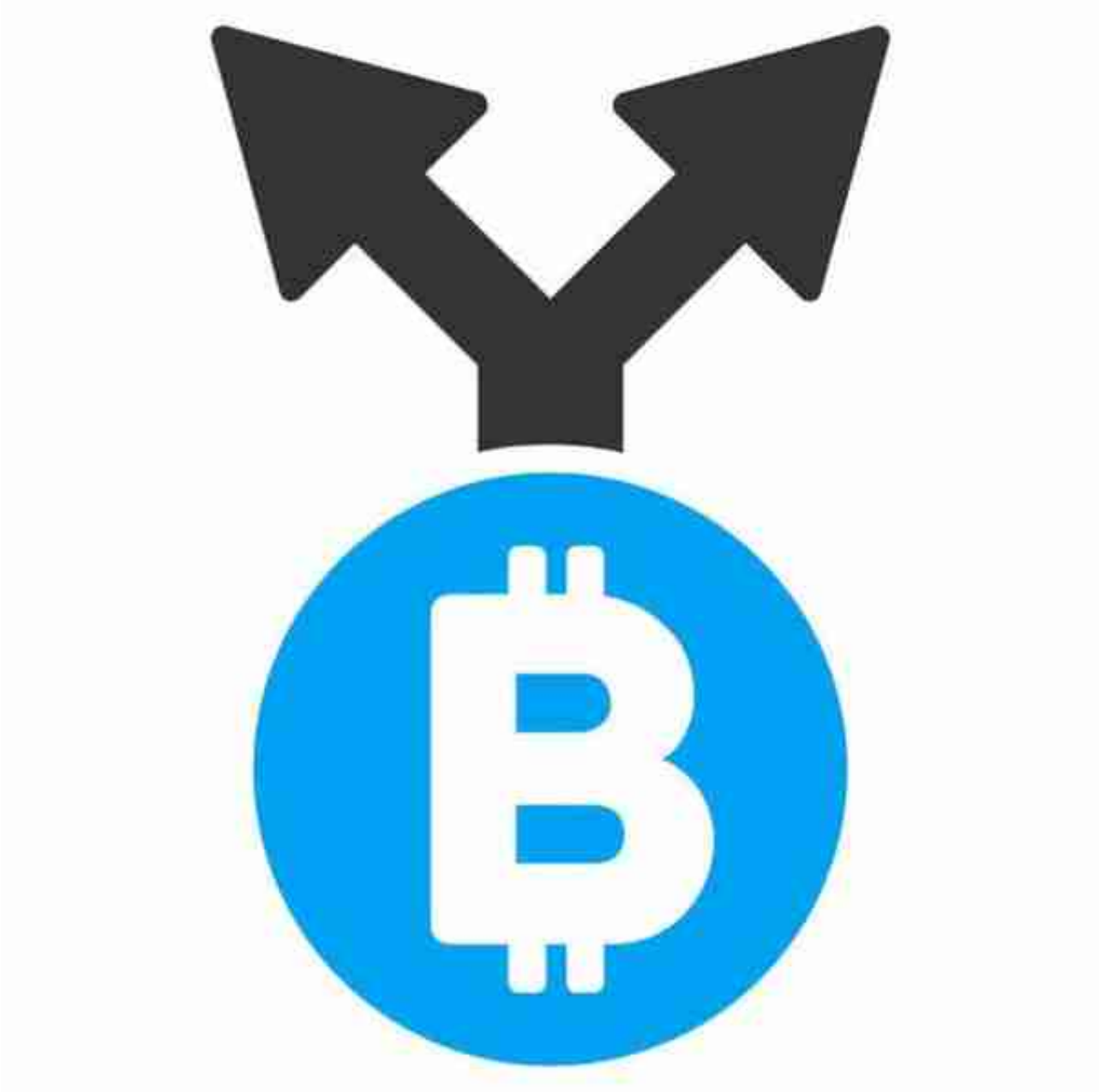
图｜新版EthashV2算法修改的fnv函数，虽然仅修改5个，但足以让ASIC挖矿无效化

在更改算法函数之后，ETH也会更新挖矿程序，既有的GPU挖矿不受影响，维持区块链正常运行。

改变算法，真的有用吗？

对矿工而言，改或不改算法的选择就会成为分叉，也就是说，在区块链上，算力为王，只要算力足够，就能够把既有的区块链节点洗成新结构，只有采用新算法的区块才能通过节点认证，未来才有办法进行交易和纪录，这就是所谓的软分叉：新的算法借此会彻底取代旧有算法。

但如果对抗的势力足够强大，那么就有可能形成两个算法并存的状况，这就是所谓的硬分叉，过去以太坊就曾经发生过这种状况，The DAO在2016年黑客通过split DAO函式递回传送模式上的漏洞曾经窃取了360万个以太币。



以太坊社群通过以硬分叉的方式追回这笔窃款：方法是让整个区块链状态回溯到被黑客入侵前，让原本被偷走的钱再度回到使用者的钱包。并从那一个区块另外岔出一条新的、独立的以太坊分叉链，也就是ETH(以太坊分叉链)，让被窃之后的交易在新的区块链上通通不算数。而被窃走的那一大笔钱如果在整条区块链人去楼空之后，也就毫无价值了。

多数以太坊使用者支持这种作法，导致大量的矿工离开原始的ETC(以太坊原链)，改投靠 ETH。不过还是有一些矿工选择留在 ETC，这些人坚持区块链不论因为何种因素都不应该更动，即便是被黑客偷走也是一样。然而，因为算力落差大，ETC的价值远不如新的ETH。

改变算法对ASIC这种更新周期长，且因为成本考量，把算法写死在芯片逻辑中，无法通过常见微码或固件更新来支持新算法的挖矿架构杀伤力相当大，当然，挖矿IC设计商可以大幅缩短IC世代更新的时间，也或者可以通过变更IC本身的设计，让微码的更新变成可能来因应算法的改变。可不论何种作法，成本大幅增加都是可预见的结果，尤其是前者，每次的世代交替恐怕会制造庞大电子垃圾，冲击环境，浪费资源。

但如果新加入的算力足够庞大，尤其是像比特大陆这种单一来源，并具备庞大算力的供应商，那么是有可能反客为主，把原本去中心化的区块链变成中心化的结构，挖矿、交易认证一把抓，这么一来，加密货币就会变成特定商人口袋里面的筹码，原本的设计精神也将荡然无存。而这也是门罗币和以太坊所极力避免的状况。

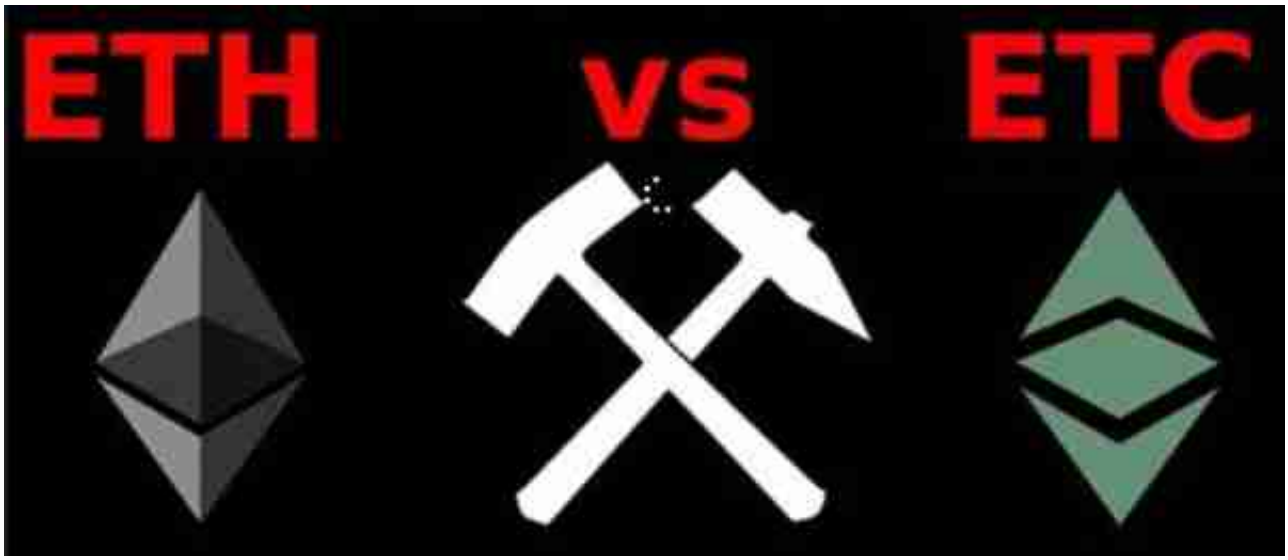
比特大陆的反击能否奏效？

矿机最主要就是要有矿可挖，而且挖出来的矿要有价值，二者任一若无法成立，那么矿机业务也会瞬间变成泡影。

乍看之下，比特大陆的蚂蚁矿机推出前就已经走上绝路，而比特大陆也绝不可能在短短几个月内重新投片生产符合新算法的挖矿架构，那么，蚂蚁矿机这个产品已经可以宣布死刑了吗？

以过去比特大陆的销售模式来看，其在产品正式推出之前就已经上线挖矿，而且不

少客户都已经下单预定新的矿机，如果几个月后这些矿机就无法再产生具有价值的区块，那的对既有客户，以及比特大陆未来的产品布局都将是极大的伤害。



因此，比特大陆决定仿照 ETC 和 ETH 这样的关系，以旧算法另外建立硬分叉，也就是在门罗币或者是以太坊的官方分叉演进之外，使用自己的算力建立另一个分叉，这个分叉基本上就是以蚂蚁矿机建立的算力为主，借此，比特大陆可以说服客户，其基于现有架构的矿机仍能产生价值。

而另一方面，比特大陆也强硬的规定，售出的矿机不论何种情况都不接受退款退货的要求，这也等同逼迫那些已经购买矿机的客户必须支持比特大陆版的分叉，成为其分叉区块算力的一部份，即便其分叉与加密货币的原始创立精神已经完全背离。

当然，目前绝大多数门罗币或以太坊的挖矿行为都还是以GPU进行，蚂蚁矿机出货有限，因此在有限的算力之下，其分支的加密货币的价值势必远远不如原开发者的分叉，但不论如何，只要价值不是零，那么还有机会通过蚂蚁矿机生态的扩大来强化算力，借以增加其货币价值。

只是，一个完全由个别厂商、单一架构来掌握整个区块链的加密货币是否能够说服整体市场，恐怕并不是那么乐观。

台积电是否会被砍单反而受害？

原本台积电南京厂喜迎挖矿大单，但遭此变故，比特大陆有可能会抽单，或变更订单总量，而台积电是否会因此受到影响，将十分值得观察。

当然，以比特大陆目前资金雄厚的实力，还是有可能维持原本的产能规划，但通过自行挖矿，或者是降低矿机报价来扩大市占，并增加自有分叉的市场吸引力，毕竟，若比特大陆在这个事件上认输，未来恐怕就很难再说服挖矿客户持续采用风险较高的ASIC方案。

若这笔订单以最好的推测，维持住了，往后呢？

如果抵制ASIC变成加密货币的共识，而且新创的货币分叉因为”中心化”而不被认可，往后比特大陆的挖矿芯片代工订单恐怕也就不是那么可靠，则对于包括台积电在内的晶圆制造商而言，像洪水财一样的挖矿芯片生意，往后的变量与风险也随之升高。

加密货币与区块链的困局

去中心化一直以来都是加密货币与区块链的核心思维，但随着挖矿的矿工数量增加，国家控管转严，且个别厂商又不断尝试将黑手伸进其中，之间的庞大利益纠葛与政治冲突让加密货币的发展蒙上一层阴影，开发者能否维持初心，以或者是继任的开发者能否延续前人的中心思想，其实也是有很大的疑问。

目前加密货币的发展方向乍看之下仍能以相对民主的方式决定，但这样的模式也可能被希望以掌控算力或其他资源的企业组织所污染，最终下决定的是台面上的人物

？还是背后的势力？

在区块链快速发展的过程中，有许多过去并没有被妥善考虑的问题状况正在持续显现，这对于所有区块链技术开发者与应用者，都会是必须严肃面对的课题。毕竟相较于其他技术，对于区块链真正可能为这个世界带来的改变，甚至是可能引发的问题，我们其实仍然所知有限。