AETH

一种基于混合证明算法的区块链系统

前言

2008 年比特币利用区块链技术实现安全的去中心化支付后，使得区块链技术进入大众视野。而后几年，Ethereum 用区块链实现了智能合约以及提出 DAC 和 DAO 的理论概念，区块链再次进入高速发展阶段，区块链帮助我们进入了 Token 经济时代。上述都预示着区块链作为一种可信化的基础服务设施，能有效释放信任成本，改善社会生产关系，创造全新的去中心化经济模式，能为多种行业和应用场景提供健壮的技术支撑。

基于 Satoshi Nakamato 的愿景，Bitcoin 的 PoW（工作量证明）是最广为人知且最安全的区块链，其共识安全性在久经考验后获得不俗的表现，但由于算力竞争导致挖矿难度不断上升，为维护整个生态稳定性和安全性不得不消耗大量电力和计算资源参与共识，破坏地球生态，浪费大量自然资源。

同时由于 ASIC 矿机的诞生，大量 PoW 矿机的生产技术和生产材料被个别中心化企业所垄断，矿机的购买和矿机维护不同程度上被中心化机构控制。PoW 矿工面临 ASIC 矿机残值率低，维护难度高，这样的情况，事实上提升了小矿工参与挖矿的学习成本和投资风险，对于矿工的分散性影响尤其负面。

现如今，Ethereum，DASH，XMR，Ripple 和 EOS 等公链的崛起，逐步的实现了更多比 Bitcoin Blockchain 更据优势的区块链数字资产交易和管理的功能，例如智能合约，环签名和零知识证明等，同时也用不同方式提升了区块链的性能。但他们或多或少都因为历史原因采用了 PoW 的算法，或如同 Ripple 和 EOS 等公链，则为了提示分布式处理性能，选择牺牲去中心化走到了区块链修正主义的道路上。

在本文中，我们将描述一个全新的区块链系统，它将使用一种基于容量证明和带条件的权益证明作为共识算法。它比 PoW 依赖更少的物理资源，同时在不牺牲区块链去中心化特性的前提下，满足共识安全性的要求，同时支持智能合约，跨链技术和匿名交易等新兴的区块链功能，应对各种使用场景的区块链技术平台。

目录

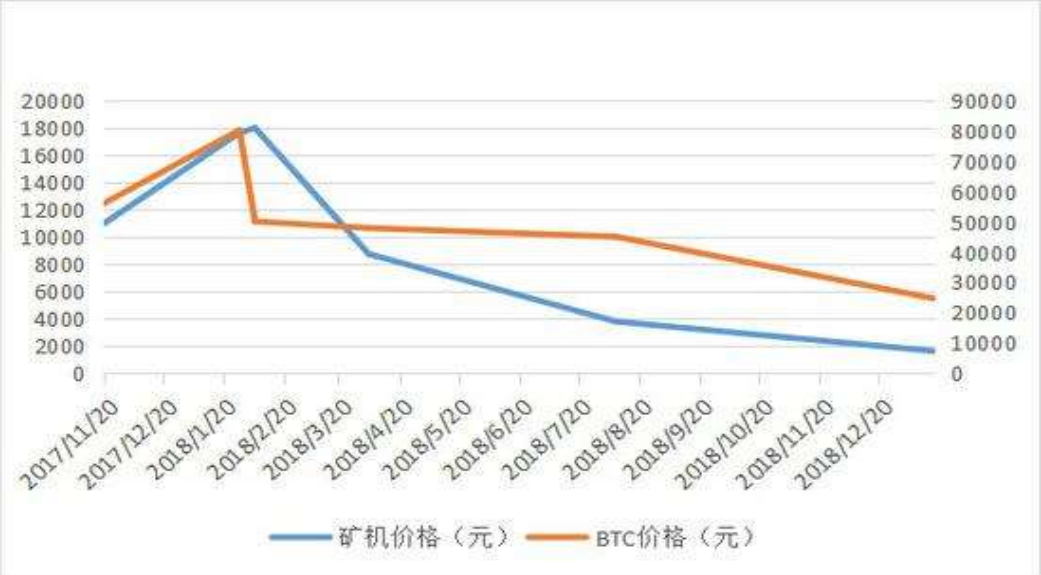
1.技术背景

1.1 Bitcoin 和 PoW 的困境

回顾区块链历史，各种新兴公链层出不穷，各种共识算法都在努力成为下一代技术，而经典的 Bitcoin 却止步不前，过去多年来，在技术上毫无革新，经典的 PoW 共识已经沦为各大 ASIC 矿机厂商争权夺利的玩物。

据统计比特大陆生产的 ASIC 矿机所占有比特币网络算力已超过 60% ,仅比特大陆一家矿池所拥有的算力超过全网 20%。在比特币价格高峰期，普通人购买一台比特币矿机的难度已经超乎想象，矿机被寡头高度垄断随意涨价，矿场越来越趋向中心化导致的大户垄断和政府政策压力，超过 159 个国家的巨大电力消耗以及矿机噪音热量的挖矿环境限制，整个挖矿行业被精英阶层所统治。

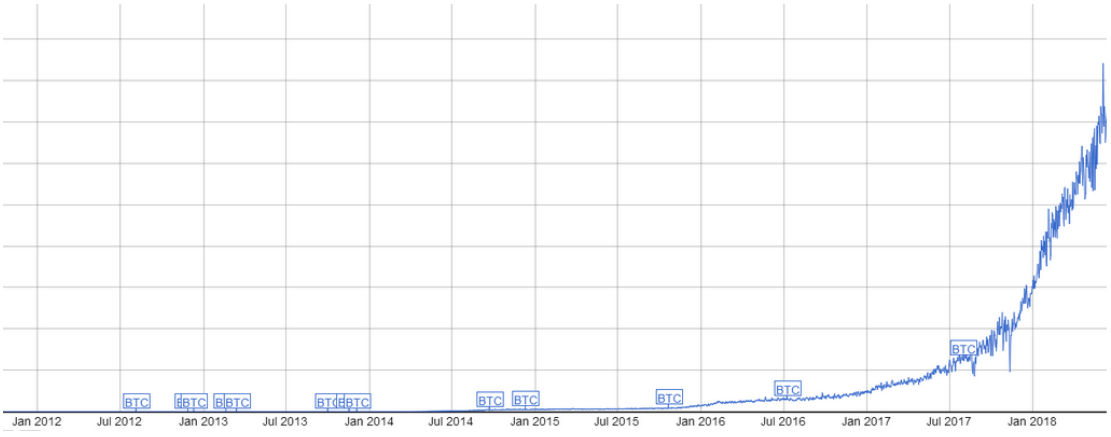
甚至这些矿霸们还在数字货币市场火热的时候 ,为了利益随意分叉创新含量很低的山寨币，通过分裂社区和炒作价格来为自己牟利。



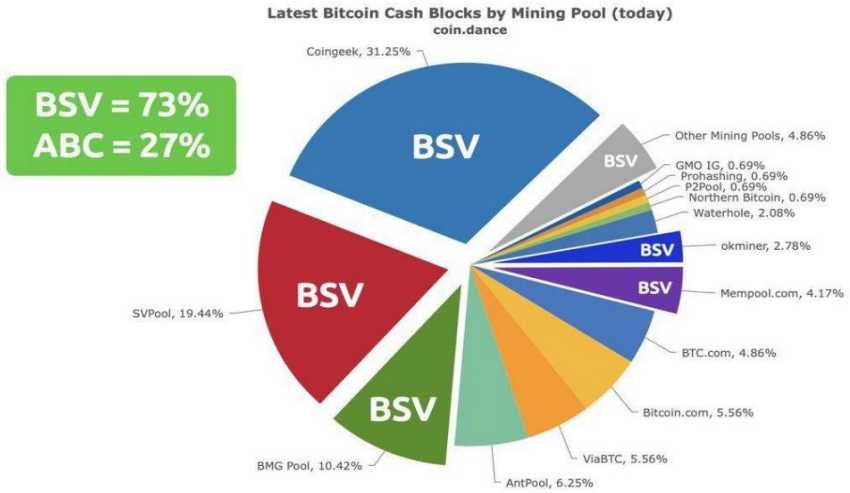
我们不得不承认 PoW 矿机的生产和销售已经被巨头所垄断，普通人已经难以真正参与去中心化生态。这样的现状与中本聪曾经的理想国相去甚远，促使社区开始新的思考，真正符合愿景的去中心化数字货币的未来到底何去何从？

1.2 算力支撑过度与性能低效

目前全网算力已经达到了近 100 EHash/s，全球所有超算全部开机计算 HASH 的算力，都无法达到目前 Bitcoin 全网的计算能力。这意味着目前的算力已经远远超出为了保障全网共识安全正常所需的水平，而由于 Bitcoin 价格上升，该数值还在不断增加，这在未来将陷入资源浪费的死循环。下图是 Bitcoin 全球算力的增长曲线。



其次，由于 Bitcoin Core 开发团队的不作为，导致在不断耗费资源的情况下，Bitcoin 性能在过去近 10 年没有得到实质的提升，常年维持在极低的水平（25TPS），这也激发了社区内部的矛盾，例如 BCH 和 BSV 等多种 BTC 分叉币的诞生，这些新的 PoW 区块链诞生又进一步加剧了算力资源的恶行循环。下图是 Bitcoin 社区分叉币种的 PoW 算力占比。



1.3 挖矿成本过高导致的问题

由于 PoW 算力竞争所导致的电力成本过高，挖矿设备残值率低，使得矿工们为了支付电费必须尽快抛售自己手中的存量资产，特别是在价格下降过程中，矿工们会加速这一行为，这就加剧了矿工投资风险，使得 PoW 挖矿投资逐步集中在少数资产储备较大，抗风险能力较强的大矿工手里，从而影响算力的去中心化和资产的分散性。

1.4 PoS 的流动性风险

目前采用 PoW 和 PoS 混合共识的公有链 Ethereum，是笔者比较欣赏的公有链之一。但 Ethereum 即将切换到单一 PoS 共识，这将导致在单一的 PoS 共识下矿工们的挖矿成本将会接近于零，使得矿工在某些时候，可能会长期不因为成本而出售挖矿资产，这就导致市场可能会出现流动性问题，可能价格会长期虚高或者造成较低的市场成交量。所以单一的 PoS 共识也不是笔者所支持的。

2.技术目标

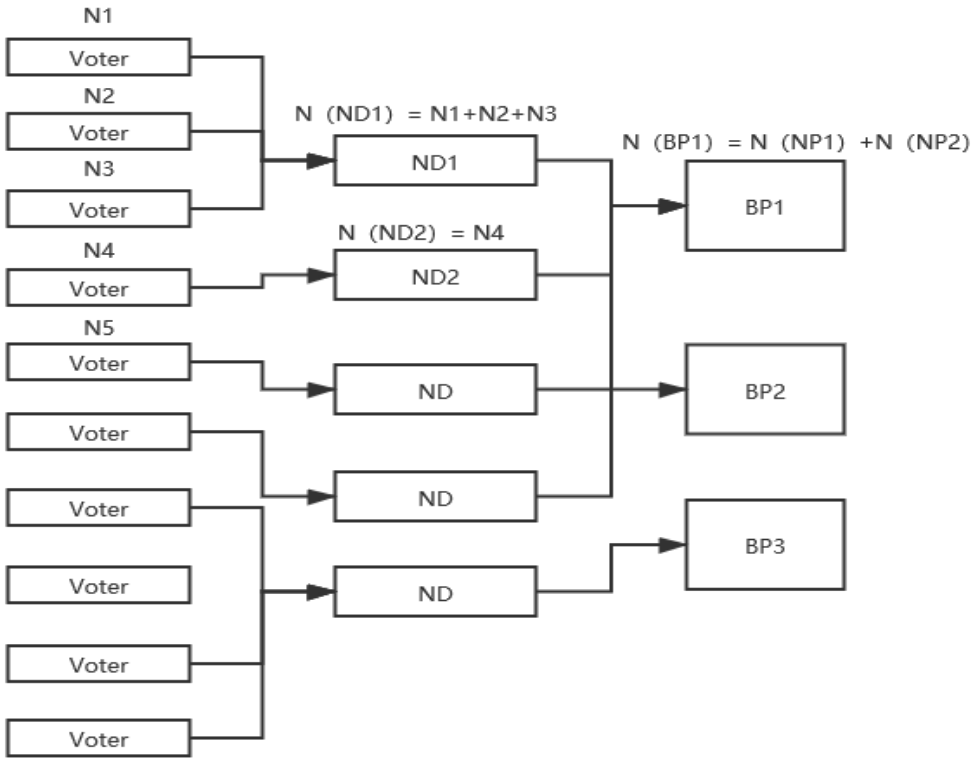
2.1 容量证明

该系统将采用安全的 Proof of Capacity（PoC）容量证明共识机制。该共识是一种 PoW 的空间换时间转换算法，所以它和 PoW 具备相同的安全性。它将计算结果事先算好，有序的存入存储介质，挖矿过程中去通过二分法去介质中搜索最小的目标值，若你的存储空间越大，则能存储更多的计算结果，那么当共识难度越大的时候，则发现最小目标值的可能性就越高，否则越低。在该算法下，矿工需要通过扫描存储介质进行挖矿。

2.2 有条件的权益证明

与此同时，该系统将会采用另外一种带条件的权益证明（CPoS）和 PoC 间隔出块，该 CPoS 共识采用币龄作为证明条件，设币权为 N，承诺抵押周期为 C，已累计抵押周期为 P，则某个产块节点的币龄的计算公式为该三个值的乘积：$CA = N * C * PT$。每一轮的 CPoS 出块竞争中，由币龄最高者胜出，该出块节点（BP）需要在共识时间内履行出块职责，否则将会受到抵押总量 10%的惩罚。出块后已累计抵押周期 P 归零，从新一轮重新开始计算。

该共识中的 BP 节点的币权 N 由其他普通节点（ND）用该节点的币权指向后累加，ND 节点的币权由普通持币者（Voter）进行锁仓指向后累加，该指向逻辑如下图。



当 BP 节点出块后 ,挖矿奖励的 30%归 BP 节点所有 ,20%归 ND 节点所有，剩余 50%按照 Voter 节点的锁定量在该 BP 节点总锁定量中的占比进行分配。

2.3 混合共识模式

上述两种共识模式将在该系统中间隔出块，奇数高度的块由 PoC 共识产出，偶数高度的块由 CPoS 共识产出，PoC 和 CPoS 矿工将会平等的获得挖矿奖励。在该模式中，PoC 矿工产出的资产，可以用于 CPoS 的挖矿竞争当中。没有算力的普通持币者，也可以用自己持有的资产进行锁仓抵押享受收益。而 BP 需要拓展 ND 节点，获得币权指向进行挖矿竞争，ND 节点则需要去拓展持币者为自己锁定和指向获得收益。

2.4 经济模型

为什么该系统采用 PoC 和 CPoS 的混合模型，一方面由于单一的 PoC 模式在早期流动性较差的阶段，存在一定的挖矿产生的通胀泡沫，所以采用 CPoS 可以有效的通过资产锁定来消除泡沫，另一方面，笔者和社区核心开发者认为，其他采用 PoC 的区块链项目所采用的 CPoC 模式，存在不同程度的公平性问题，以及分散性问题，以 BHD 为例，BHD 采用的抵押模式，导致了持有币的大矿工，拥有更多的抵押筹码，导致强者愈强，弱者愈弱，币将会集中在少数大矿工手里，而 BHD 采用的巨块奖励算法，更是加剧了这一情况。

而该系统采用的 CPoS 则不会存在该问题，散户可以通过类似票选的币权锁定指向，联合 ND 节点和持币量较大的个体进行抗衡，从而保障分散性。

3.发行和挖矿

3.1 发行模式

初始块奖励	240 AETH/block
出块时间	5 分钟
减产周期	每年出块奖励递减 15%
基金会持有	2000 万枚
总量	约 1.88192 亿枚
矿工占比	约 90%

3.2 PoC 产块流程

3.2.1 P 盘（Plot）

AETH 的矿工首先需要 P 盘，P 盘需要一个 PID（Plotter ID），该 ID 对应的是钱包地址，证明该 ID 是该钱包地址产出的。通过 Sha256 改进算法不断计算 HASH，然后将产生 Plot 文件完成 P 盘工作。硬盘容量越高，产生的 Plot 文件越多，Hash 越多，更容易爆块。

3.2.2 产块（Generator）

因为写入的 HASH 正在存储介质中分布是有序的，所以整个挖矿过程是一

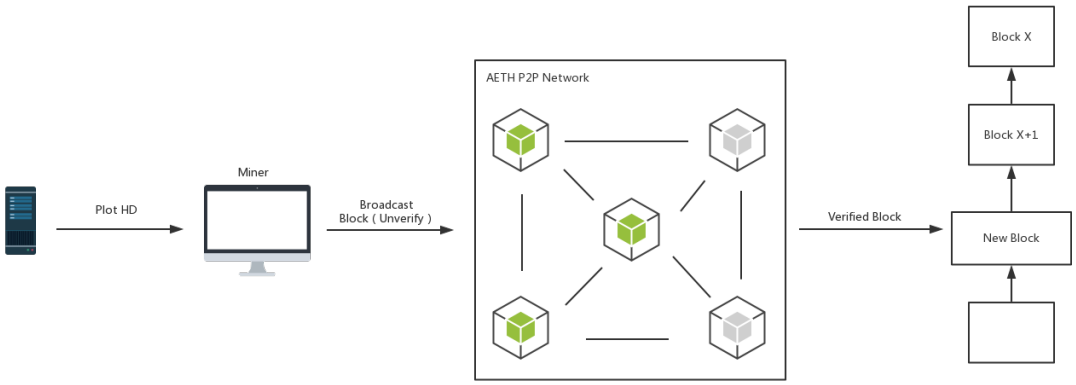
个通过二分查找 Plot 文件中 HASH 的过程，加速该过程需要足够快的硬盘读写速度，所以我们建议尽量使用 SSD 作为 Plot 文件的存储介质，确保挖矿速度最优化，同时需要额外很少量的 CPU 计算资源。

3.2.3 打包交易和广播（Forging）

AETH 的钱包将通过 P2P 网络获得正处于等待（Pending）状态的交易，将这些交易收集在内存当中，当计算出正确的目标 HASH（Target Hash）后，将这些交易按照时间和手续费综合权重打包进入区块当中。

3.2.4 达成共识和难度调整（Verify）

打包完成区块后，通过 AETH 的 P2P 网络，将区块广播给其他节点，其他节点将对区块做一系列检查，包括验证目标 HASH 的有效性、时间戳、区块格式、大小和所包含交易，完成验证后的区块将获得共识。后续的矿工会跟随该块进行挖矿。在这个过程中，也会根据实际产块时间和共识时间对比，若不符，则会调整挖矿难度，确保共识时间不会因为算力大小受到影响。整个过程如下图所示。



3.3 CPoS 产块流程

3.3.1 成为 BP 节点（Registe）

普通节点想要参与出块竞争，需要发起一笔特殊的交易，在区块链上注册成为一个 BP 节点，成为 BP 节点后，需要保持节点在线，并处于网络质量和计算性能稳定的环境下，当币龄在当前一轮出块中达到最大值时，执行出块责任。

3.3.2 关于 ND 节点（About ND）

若你没有打算成为 BP 节点承担出块责任，你也可以成为 ND 节点，仅进行币权投票来分享挖矿收益。成为 ND 节点同样需要在区块链上发起一笔特殊交易注册成为 ND 节点，注册成为 ND 节点后，你将可以让其他持币者锁定资产指向你来增加你的币权值。然后你再将你的币权指向到 BP 节点获得收益。

3.3.3 持币者锁定和指向

若你是持币者，想让自己短期内没有交易需求的资产进行稳定增值，那么你

可以通过钱包发起一笔特殊的交易，将自己的资产锁定并指向到一个 ND 节点上。当 ND 节点所指向的 BP 节点出块后，你就可以获得收益。但锁定期间，你所锁定的资产，将禁止交易，这类似于银行的定期存单。

3.4 分叉的处理

在 PoC 算力或 CPoS 出块过程中，可能会产生分叉的情况，一般由于攻击或者网络同步延时导致，在这种情况下，我们将认可 PoC 难度累加值加上 CPoS 中出块币龄累加值最大的那条链为唯一结果，来保障分叉的安全性。

对于链上交易和合约调用，我们建议使用 10 次区块高度确认来确保交易的安全性，防止双花攻击。

4.社区和治理

4.1 社区运营

该系统是一个由社区驱动的全球性开源软件项目，全球爱好者、开发者、文档维护者、社区活动组织者、代币持有者等组成了全球性社区，社区生态是项目的根基，也是项目的生命力所在,打造全球社区是最重要的工作之一。

相信通过分享和学习可以帮助那些渴望不断提高自己的开发者。社区将以建设纯粹高质的技术交流平台，提供完善的开发文档和成熟的开发工具，组织多样

化的开发大赛，扶持优秀应用，奖励项目贡献者等方式，促进生态的发展。未来，会启动区块链人才培养计划，注入新的活力和思想沉淀技术，不断为生态系统培养技术开发力量。

除了发展和完善开源社区，将完成更多应用场景的植入，实现网络和共识等模块的自我进化，大规模启动和推进更多应用接入，形成对接各行业应用的标准技术方案体系；在全球各地，本地社区以用户组的形式存在，每个用户组都有负责人、运营团队，他们都是社区的支持者，以志愿者的方式投入社区工作。用户组负责组织、维护和发展本地社区。主要工作包括：推广数字货币、区块链理念，研讨技术，参与项目开发，文档撰写和翻译，组织本地社区聚会，协助组织官方全球性活动。

4.2 基金会

该系统将在新加坡成立基金会，基金会将预留一部分链上资产作为启动资金。基金会将通过启动资金和社会募集捐助为社区服务者（包括开发者、推广者、运营和管理者等）给予奖励，以保障社区的健康和稳定发展。同时也将提供一部分资金鼓励应用开发者使用、学习和传播该项目，为该项目撰写学习资料等。

5.免责声明

一、本白皮书仅作为一份概念性文件，用于描述 AETH 项目，并不构成招股说明书、要约文件、证券要约、投资招标或出售任何产品和资产的要约。基金会和 AETH 团队无法保证白皮书信息的准确性和完整性，您应该在参与本白皮书中所述任何活动之前咨询自己的法律，财务，税务或其他专业顾问。

二、所有 AETH 项目的支持者，应当仔细阅读白皮书和官方网站的相关说明，全面理解区块链技术，明确了解项目的风险，参与者也应该明白获取 AETH 本质上为捐赠行为，不可退款，不能取消，且无法获得赔偿。

三、AETH 仅作为 AETH 系统的使用 Token,并不代表分红、增值、股权、证券及其衍生品的收益许诺，项目方不提供任何回售渠道，持有人获取后有权自主决定使用。本白皮书有多种语言版本，如存在任何分歧，以中文版为准。

四、AETH 团队将不遗余力实现白皮书中提出的目标，并积极探索项目更长远的发展空间，然而由于外部环境和内部资源的不确定性，我们将保留对白皮书描述内容进行调整的权利，白皮书内容的所有变更我们并无主动告知义务，请参与者通过相关渠道及时了解更新，区块链技术仍然是一项非常早期的技术，AETH 团队不能完全确保所有技术的顺利落地。

五、所有的技术类项目都具有被黑客攻击或代码漏洞造成用户损失的可能，我们不承担由于程序所出现的任何损失。AETH 目前通过智能合约发布，由于智

能合约同样是一个比较早期的技术，AETH 团队不保证 AETH 的合约完全没有安全问题，我们不承担智能合约安全问题造成的任何 AETH 的损失。