B4-Flash Memory

白皮书

第一版 2019 年
官网：UPbfm.com

目录

1、 项目背景.....1

1.1、半导体对当今社会的的重要性.....1

1.2、全球半导体市场的规模.....1

1.3、半导体储存的机会.....1

1.4、未来半导体储存技术所需的性能.....1

1.5、B4-Flash 介绍.....2

2、 BFM 概述.....2

2.1、加密货币.....3

2.2、寻求替代者.....4

3、 BFM 需要解决的四大问题.....5

3.1、垄断问题.....5

3.2、算力集中化问题.....7

3.3、能源消耗问题.....8

3.4、现有 POC 货币设计激励层问题.....11

3.5、BFM 为何现在出现.....12

4、 BFM 技术解决路线.....12

4.1、CPOC.....12

4.2、BFM 架构及共识算法.....13

4.3、BFM 技术特性.....23

5、 应用场景拓展.....25

6、 治理架构.....27

6.1、治理架构和机制.....27

6.2、链上治理—BFM Chain 理事会和信任节点.....27

6.3、链下治理—BFM Chain 基金会.....29

7、 经济模型.....35

7.1、BFM 经济模型和价值场景介绍.....35
7.2、治理价值.....35
7.3、应用价值.....36
7.4、协同价值.....36
7.5、BFM 分发机制.....37
8、 创始人简介.....38
9、 结论.....39

1、项目背景

1.1、半导体对当今社会的的重要性

众所周知，半导体芯片一直都是我国科技发展的“芯病”，国家已经把半导体行业的发展提高到了国家级战略的高度，把集成电路产业列为“十三五”期间重要的新型战略性产业等。同时也用各种政策引导各路资本来大力扶持该行业的发展，二级市场中的科创板设立就是一大体现，同时也加大该行业人才等的培养。

随着大数据、云计算、物联网等产业的发展，半导体芯片在整个产业链中扮演角色的重要性不言而喻，各行各业几乎都会与半导体芯片相关，尤其是高端制造、人工智能、大数据处理等等，未来社会的发展更加离不开半导体行业的支持，可以说“芯片强则产业强，芯片兴则经济兴”。

1.2、全球半导体市场的规模

当今社会已经离不开万物互联、人工智能、数字化等带给我们的便利，为这一切的基础都是基于半导体芯片实现。半导体之于产业，其作用相当于人的大脑，如果失去芯片，那即使是再好的电子设备也会顷刻瘫痪。目前半导体产业已经发展到全球每年接近 3 万亿人民币的产业规模，但这个半导体产业作为核心基础支持的“事物”和“服务”的总规模要大的多，将超过 100 万亿的体量。

1.3、半导体储存的机会

存储芯片作为半导体元器件中不可或缺的组成部分，有着非常广泛的应用，在内存、消费电子、智能终端等领域均有运用。随着大数据、云计算、物联网等发展，其在整个产业链中扮演的角色将更加重要。

半导体储存行业占整个半导体行业的三分之一。其中一半是用于临时储存计算机处理数据的易失性存储器，另一半用于程序或数据储存的非易失性存储器，即使电源关闭也能存储数据。随着数字计算机社会的发展，其影响力在该行业的比重会不断扩大。

1.4、未来半导体储存技术所需的性能

1.4.1、快速处理

为了处理大量数据，总是需要加速任何数据处理。存储器的快速操作变得更加重要。加

快存储程序和数据的存储读取以及重写速度至关重要。

1.4.2、高可靠性

随着互联设备链接的扩展，人类生活环境中以及智能手机为中心的内存性能将发生变化。它需要在包括汽车、工业设备等恶劣的操作环境中工作，此时需要该半导体高可靠性。

1.4.3、高温操作

所有设备的高级计算机不仅需要高温下的数据存储，还需要在高温环境中操作。现在需要更广泛地在诸如 125℃的高温环境中操作（之前仅需要用于特殊设备）。

1.4.4、增加程序存储器容量

通过将所有设备连接到 Internet,中央数据处理设备和终端设备变得复杂并且高速运行。用于终端设备的操作程序的储存器变大，且需要高速重写。

1.5、B4-Flash 介绍

B4-Flash 是中岛盛一先生（创始人，后文有详细介绍）独家开发的半导体非易失性存储器，相较于传统 NOR 和 NAND, 其优势在于：（1）唯一可以同时高速重写和读取闪存；（2）可以在所有半导体存储器技术的最高温度下保存最长数据；（3）可轻松实现 125℃内存的高温运行，是将物理结构创新为闪存的结果；（4）B4-Flash 超出了传统的 NOR Flash 的小型限制，可以同时高速重写程序数据。

2、BFM 概述

B4 Flash Memory(简称 BFM)是基于 Conditioned Proof Of Capacity(以下简称：CPOC）的新型加密货币。其主要的特点是使用 B4 闪存芯片作为共识的参与者，减少温度对矿机芯片的损耗，提高芯片的重写、读取的速度，提供最高的可靠性存储等，从而降低加密货币对电力资源的消耗，降低参与门槛，让其生产方式更趋向去中心化方式，并更加安全可信，让人人都能参与到加密货币的开采，通过数学算法以及分布式开采产生信用和价值。本文将从本加密货币系统塑造出的信用体系和技术特征分别对其进行阐述。

2.1、加密货币

提到加密货币，Bitcoin(比特币，以下简称 BTC)是最广为人知的，在其之外，整个加密货币产业已经开始尝试一些新的技术方案来提高支付速度，扩大支付范围，很多改进型加密货币应运而生，比如 Dai-Wei 的 B-Money 和 Ripple。

Ripple，我们已经看到，其已被少部分不同国家银行之间用于结算，由于其在生产方式上过于中心化，并未得到大面积的应用。相较于更去中心化的加密货币(如 BTC)，项目中心化的运作更易受到其他应用型公司的青睐。在这个体系内自然也不会有加密货币矿工的出现，毕竟大多数的步骤和矿工无关，因其发行方主要以公司性质的身份参与整体项目。

B-Money 由于其设计中需要大量的网络同步操作，使得其很容易产生网络阻塞，而当时的网络速度并没有那么快，信息在传输的的途中经常卡顿而出现问题，或者全体网络都在等待一个比较慢的包，最终因得不到回复信息而导致传输失败，使其在使用上不尽人意。

BTC 通过自己 nakamoto 型共识，也就是现在大家熟知的异步 proofofwork(以下简称 POW），走到了舞台前。在初期，看好这个项目的人并不多，源于其共识并没有通过同步转账结果来保证转账的结果不会出错，而是使用很有趣的方式——最长链。也就是说，这个分布式系统中节点更认可哪个包，那个包中的交易就是正确的结果，那么怎么出现这个包呢，当然是通过这个系统中的节点来共 同验证，只给定一个超时打包的时间，这个包在这段时间中只要有更多的节点参与认可，那么它就是对的。在这个逻辑中，会存在一种情况，那就是系统中的节点可以集体做坏事，让正确的交易没有被打包，这样网络的传输就是无效的，这也是这个方式中有趣的地方，因为它既对又不对。对，是因为它避免了网络中很大量的通讯，异步更加适合交易的步骤；不对，是因为在极端情况下，即 系统中坏人占多数时，系统就变成无效系统，这也是在后期大家经常提到的 51%双花攻击。金融系统最不能做的就是回滚和双花，这也是一开始 BTC 没有被大规模接受的原因。

随着时间的推移，拥有了很多由于利益而进入到系统的参与者，系统层面由于出块（也就是上文提到的打包）难度的存在，将坏人进入的成本大大提高，系统也随之变得更加稳定，毕竟做好人比做坏人得到的收益要高多了。这时候人们开始认可这个新型的加密货币，其从一个不稳定的金融系统，通过多年的难度增加，让双花和回滚变得非常困难，系统逐渐趋于稳定。也因此产生了 BTC 的原教义者：加密货币爱好者。这时就有很多新型的加密货币以分叉的方式被制造出来，又因为其算力的独占的问题被 51%双花攻击，其主要原因就是在低难度下，这个系统是一个不安全的；而高难度安全系统则需要非常大能源的消耗。

我们可以通过观察发现 BTC 的一些技术特征： 首先 BTC 从来都不是技术激进派，反而是挑选了相当成熟的现有技术去完成安全可信的点对点现金系统，越是被验证过、越是简洁、成熟的技术，越是安全、可信，例如 nakamoto 共识中用到的 SHA256 这个算法，是由 NSA（美国安全局）设计，其安全可信性是被有效验证过的，说明初期设计之时可能根本没有考虑到现在的 ASI（Application-Speci?cIntegratedCircuit，专用集成电路，以下简称 ASIC）和电力垄断问题，只是为了极致的可信而设计，为了极致的安全可信，甚至牺牲了互联网原有的高效交易并发量。

2.2、寻求替代者

在资源被大量用来出块，成本逐渐提高的时候，加密货币爱好者开始致力于寻找更低功耗的替代者，主要分为两类：更低成本获得收益的替代者和更通用可堆叠组件的替代者，这就是 ASIC 挖矿以及抗 ASIC 算法开发的大航海时代。其中 ETH，Monero 的初衷都是以抗 ASIC 为目的，他们希望出块的计算方式能够抵抗 ASIC 芯片，并且维持比较低的出块成本，让它变成一个不受控于 ASIC 芯片进行挖矿的加密货币，不过在加密货币发行之后，市值一旦达到 ASIC 芯片投入的范畴，ASIC 的开发商依然 会想办法将这些通过计算方式去挖矿的加密算法设计成为矿机。另外一个著名的加密货币 LTC 也是其中的代表，使用 Scrypt 算法的 LTC，以对抗 ASIC 为技术亮点，不过很快 ASIC 设备生产商就优化了他的算法，将其做成了矿机，形成了设备以及算力的垄断，带来了巨大的能源消耗。电力的依赖和矿场的门槛让挖矿成为少数人的游戏。

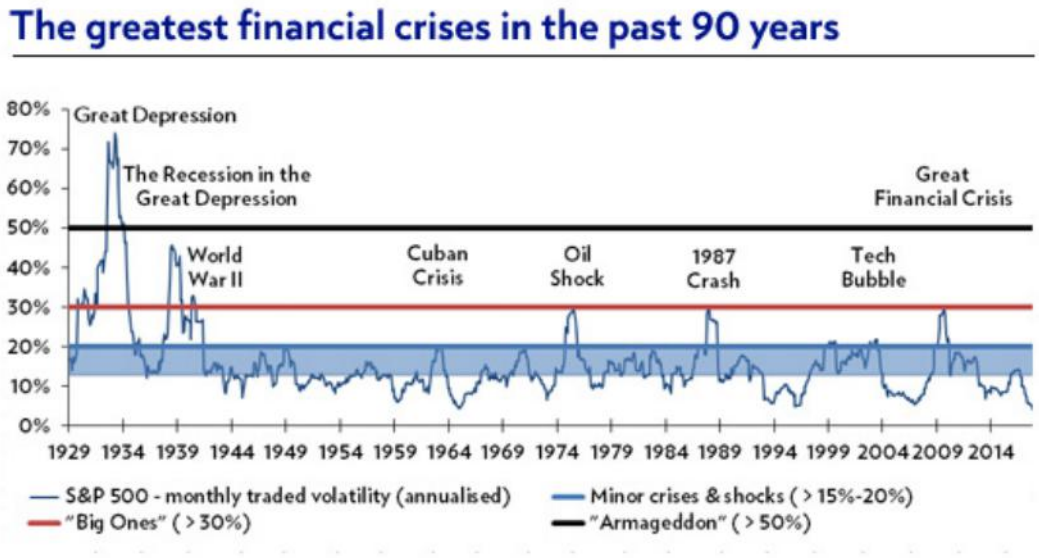
而 BFM 则是一个集大成者，其即能达到更低的能源消耗，又能方便矿工自制通用组件参与其中，同时维持相对高的难度来保证系统的稳定性。BFM 使用的 CPOC 共识，是非常去中心化的一个共识算法，相对于 POW 引起的算力证明大航海时代，CPOC 将会开拓一个基于 B4 闪存芯片证明的新大航海时代。CPOC 使用 B4 闪存芯片来作为共识的主要载体，让更多的普通人可以通过自己的电脑参与到算力的组建中，能够回归到中本聪设计 POW 的部分初衷，让每个人都能参与到去中心化的革新之路。BFM 与此同时继承了 BTC 的传统，因为 BTC 在设计之初便是一个服务于多数参与者的系统，即每一个参与的者都可以是一个思考、支持、甚至是颠覆系统的角色。CPOC 继承了这种开放性、包容性，伴随着更加亲民的高性能 B4 储存芯片共识，可进一步将加密货币推向向大众视野，让更多的人参与到 BFM 经济系统的建设。

3、BFM 需要解决的四大问题

POW 型共识的设备垄断、算力集中化、能源消耗以及现有 POC 的激励层问题并行成为现在行业内四大问题。BFM 从设计之初，就是针对现有行业的四大问题进行解决。下面我们一一进行阐述。

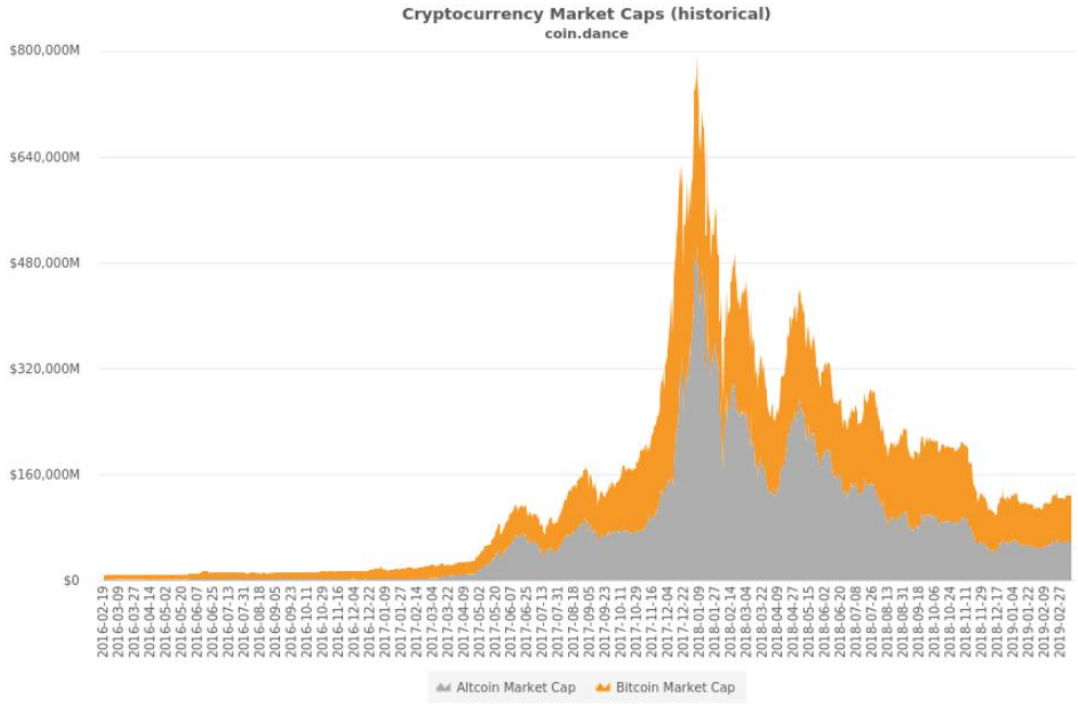
3.1、垄断问题

BTC 从诞生之初，就是想要解决金融机构的垄断问题和信任危机。从 08 年的金融危机之后，中本聪 就认为金融系统的垄断性会一次又一次的重蹈金融危机覆辙（如下图），去中心化是解决这种问题 的最好方法之一。



Source: Bloomberg Finance L.P., Julius Baer

那么多年之后，BTC 现状又是如何呢？



上图是整个由 BTC 引领的加密货币市场的价值曲线，是不是比较像金融危机周期中的一次波动？这不得不引起我们思考，BTC 在算力垄断的现在，是否依然那么的去中心化？

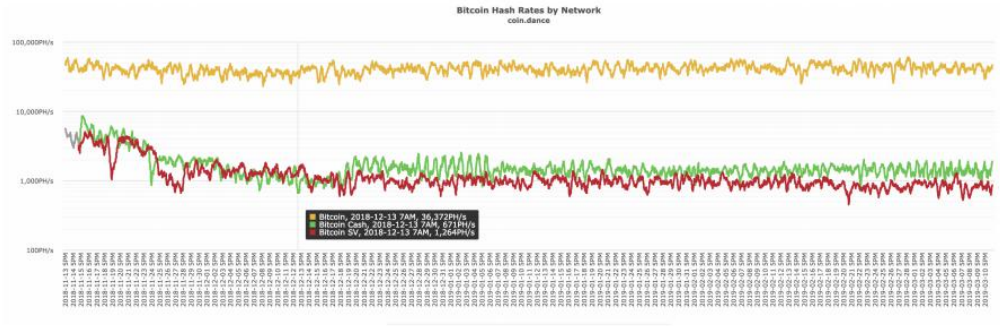
BTCCore 的技术部分由核心开发者掌控，代码更新速度缓慢，可谓是代码中心化；BTC 的算力巨大，普通人无法参与到共识，只能进行交易，可谓是算力中心化；BTC 的出块时间比较慢，10 分钟左右，个位数的 TPS 难以达到现有网络使用的正常体验；另外 BTCCore 钱包在?年间并未做出任何优化，也没有 BTCCore 的手机版，完全没有根据现有使用者的体验进行更改升级，可谓是体验中心化；更甚者，想要部署闪电网络，让更多中心化的公司参与到闪电网络节点中，让整个 BTC 系统越来越中心化，使用体验远远没有中心化支付系统(如 VISA)好。

既然人们愿意相信 BTC，就必须要接受新生事物对它发起的颠覆性挑战，同时去思考如何贯彻去中心化好让每一个人都能参与到这场革新之中。BFM 就此应运而生，BFM 的设计之初就选择了更经济的去中心化方式，可以将信用成本再次降低，从 POW 的不间断计算方式更改为更低成本的存储+检索中。我们相信中心化的加强会重蹈一次又一次的危机，我们的目的就是在 BFM 上实现完全的去中心化，从根本上杜绝潜在危机的诞生。

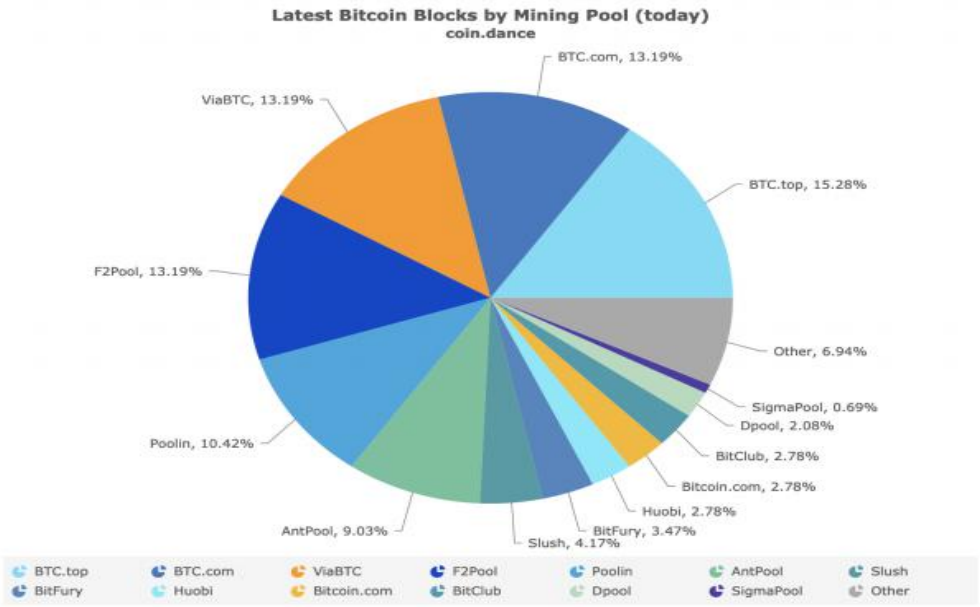
3.2、算力集中化问题

我们提到，BTC 能够作为成功加密货币的主要原因是其算力维持在一个相对高的范围，在 2017 年 BTC 总算力为 4400P，每天比特币产量为 1800 个，平均下来每 P 挖到的 BTC 是 0.4 个，现在问题来了，这些矿机制造商可以通过调节矿机的价格来影响 BTC 的价格。也即是随着加密货币参与者对 BTC 收益的预 期提高，每一个人都愿意用更高算力的机器来生产加密货币，也就是通过打包得到奖励。比特币挖矿前四位的机构占有大约 53%的挖矿份额；在以太币的系统中，集中度更高，排名前三的挖矿机构占有 61%的挖矿份额。此外，全球 56%的比特币挖矿软件和 28%的以太币挖矿软件集中在数据中心，显示出比特币的经营更加公司化。

下图可以看到现在 BTC 的算力已经在 30,000P-40,000P 左右，那么相对于 2017 年上升了 10 倍，也就是参与者的难度加大了 10 倍。



从下图而我们可以看到,算力已经开始公司化，可以看到熟悉的 F2Pool，AntPool，Slush。

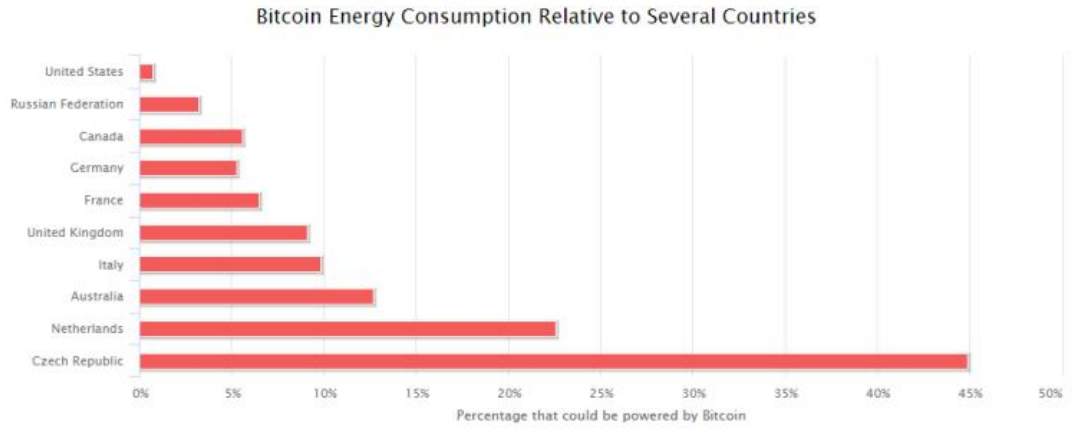


在算力的一步一步攀升中，矿机制造商通过制造更高算力的机器来提高整个生产难度，并通过增加难度来增加自己矿机的配置，让普通的加密货币参与者望而却步。

BFM 是通过对 B4 闪存芯片的优势，减少温度对矿机芯片的损耗，提高芯片的重写、读取的速度，提供最高的可靠性存储等从而降低加密货币对电力资源的消耗，加快运算速度，降低参与门槛，让其生产方式更趋向去中心化方式，并更加安全可信，让人人都能参与到加密货币的开采，通过数学算法以及分布式开采产生信用和价值。

3.3、能源消耗问题

当然，算力集中化也带来了能源消耗的问题，在上一个环节中提到了，对于特定哈希碰撞的大量计算，那么这个计算需要消耗多少资源呢？ 举一个例子，按照现有 BTC 网络的能源消耗，大约和意大利 10%的电力需求相仿。都说条条大路通罗 马，BTC 给大家带来罗马的同时，也带来了相当于罗马、米兰和威尼斯总计 600 万人口的用电量。

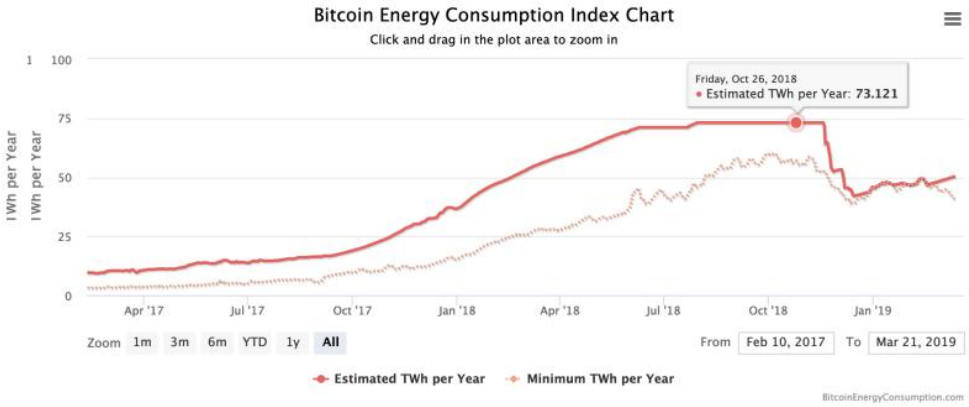


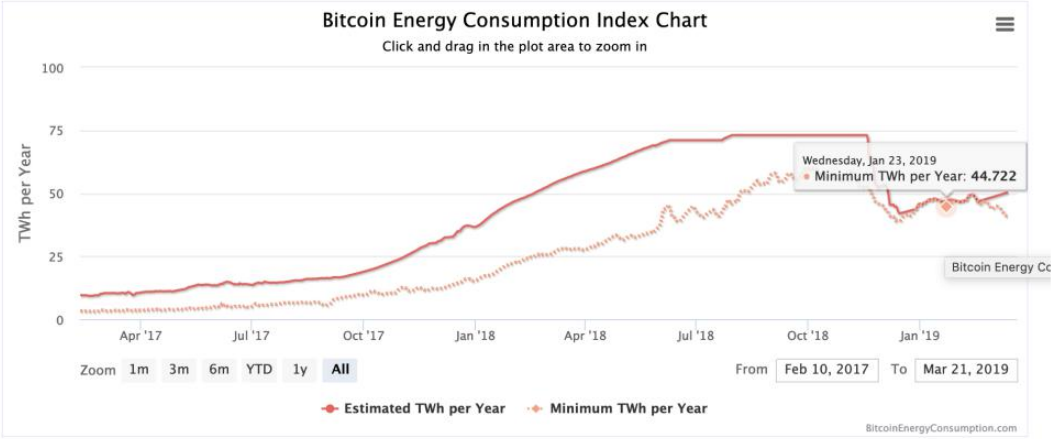
目前大多数矿工都在中国大陆境内（如 BitMain），那么我就举一个中国的例子，现在 BTC 的算力在 45EHash/s 上下，那么在 1P 的算力，消耗 0.1 人民币一度电的情况下，需要花费大约 140000 度电，也就是平均 14000 元人民币。那么按照中国的高铁每千米行走耗电 2 度多的情况下，时速 350 公里的高铁 每小时耗电 9600 多度，按照上海到北京 5 小时高铁计算，需要使用将近 48000 度电，也就是现在产出 1 个 BTC 的能源消耗足够高铁绕着中国的北京上海跑一圈半。

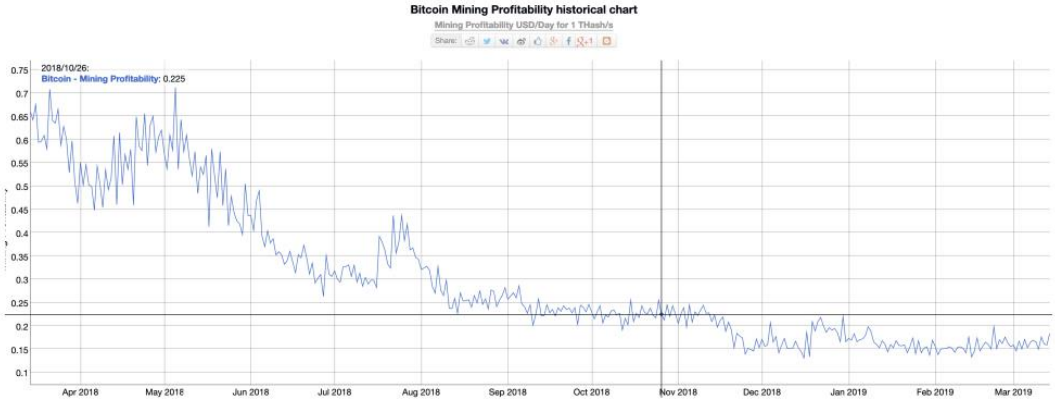
在这种巨大的能源消耗差别下，BFM 利用芯片和算法的优势节省下的能源可以更多的为其他实体进行使用，而不是重复的浪费性消耗。这种弱能源消耗的共识体系可以让更多的人参与进来，不再是少数人的游戏。

能源消耗巨大带来的另一个问题就更为严重了：POW 算力通过能源消耗体现，由于能源在任何国家都由国家政府掌控，随着 POW 算力的逐渐扩大，过度的能源消耗会引发一系列社会性问题，最终很可能政府会出面干预导致 POW 的全网算力波动，安全性也将大打折扣。

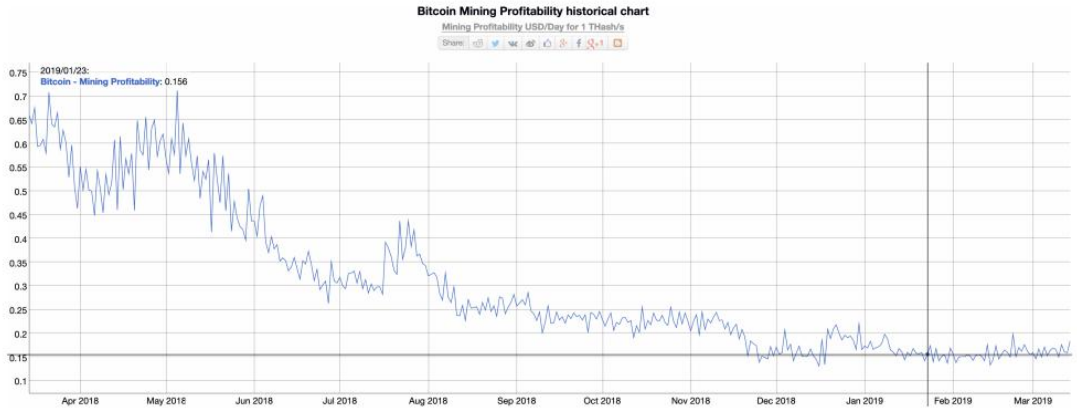
从下图的表中可以看到，BTC 电力消耗在 2018 年 10 月份为 73121 度，在 2019 年 1 月份直接降到了 44722 度。这个通过能源减少带来的算力降低会影响到整个出块的难度以及矿机的收益，对于 BTC 尚且如此，对于使用 POW 的小币种，带来的则是分叉的风险，而分叉又是致命的威胁，威胁到整个共识的正确性与安全性。







(chartfromhttps://digiconomist.net/bitcoin-energy-consumption)



（https://bitinfocharts.com/comparison/bitcoin-mining_pro?tability.html）

也就是说，如果矿场聚集在一个国家政府，那么政府可以通过调控相关能源资源的方式影响系统中的难度及收益，会因为一次潜在大规模的电力资源下降引发算力下降，更有甚者可以分叉一个 POW 为共识的代币。BFM 的低功耗在这个侧面也给予了解决方法，通过减少对能源的依赖，发展一个更适应长期生存的生产方式。POC 的意义也是将 ASIC 的高能源消耗替代为低消耗的闪存芯片查找，通过高性能的闪存芯片作为一个整体来提供保证高安全特性的随机数，从而保证底层的安全性。

3.4、现有 POC 货币设计激励层问题

之前有没有人考虑过使用芯片来作为货币共识体系的载体呢？答案是有的。2014 年诞生的 Burst 是首个 POC 共识体系货币。Burst 很快将 POC 共识算法推广下来，并且拥有了不少的拥护者，但也与此同时暴露了一些原有 POC 共识算法的问题。BFM 总结了 Burst 的失败教训，经过了技术部分的一系列改动，于 2018 年 8 月份问世。

Burst 在设计之初并没有适当的激励方式，大部分的货币被早期加入的矿工以非常低的成本挖到，随着团队的宣传推广，后期进入 Burst 的参与者缺乏足够的货币层回报，极大降低了参与者的热情，以至于 POC 加密货币慢慢走出了人们的视野。BFM 在设计激励的时候使用了双重激励的方式，可以通过条件或者非条件的方式进行挖矿，以此调节运营团队费用和矿工收益。即矿工在其条件出块的时候，矿工可以获得全部收益；让矿工条件撤出的时候，出块的奖励大部分分配到运营团队。BFM 采用条件的方式来保证链的持续发展以及新的矿工引进，以这样的方式来维护长期的社区正向发展。

3.5、BFM 为何现在出现

为了解决以上四个问题，BFM 应运而生。

随着加密货币爱好者愈发增多，其去中心化的目标离我们更进了一步。每一个参与者都希望自己能 够参与并且从中收益，这一合情合理的需求在 POW 领域愈发变得艰难。随着 BTC 的能源消耗越来越大，矿机厂商越来越中心化，甚至产生了戏剧化的分叉，而基于 POC 的加密货币比在 2019 年变得更为加密货币爱好者需要。再加上其特殊的共识算法保证了在上线可以迅速完成对算力的积累及难度的控制，在保证系统安全性、健全性的同时，对交易者及共识支持者进行奖励。在这几个方向上，BFM 都是优于现有的加密货币的，共识的迭代也提供了高于 Burst 所提供的安全性，技术维度和信用维度完全超越其他加密货币。

相较于高能源开销的 POW 算法，我们更相信低功耗也能赋予算法以足够的信用来保证未来每一个人都可以使用上加密货币。

4、BFM 技术解决路线

BFM 以 POC 共识算法为基础，通过设计长期激励的经济模型保证整个加密货币的良性发展，同时也对 现有 POC 进行优化做出了一些改进，将其升级为 CPOC（Conditioned-Proof of Capacity）共识。

4.1、CPOC

BFM 的共识算法在 Burst POC2 (Proof of Capacity) 的基础上进行了升级，称之为：CPOC(Conditioned-Proof of Capacity),即”条件化容量证明”，也就是有条件的容量证明。

以解决以下问题：

(1)防止经济模型攻击

POW 共识算法下的矿工因成本所迫抛售货币，将会导致整个矿业经济的萎缩，CPOC 的挖矿经济模型使矿工成为生态利益的共同体、并用币作为新型生产资料代替了原本的电力消耗资源，使 BFM 整个生态不停的自动扩张。

(2)POW 维持成本高

基于 POW 共识的链，维持其安全需要消耗大量的电力，在市场处于低迷周期时电力是 POW 成本构成的根本，远超硬件本身所带来的资源消耗，矿工不得不卖币付电费，矿工无法

建立利益一致性和认同感，矿工消耗的电力系统的价值也未能沉淀于其货币系统中，这部分的价值无时不刻都在从 POW 体系中抽离出去。

(3)无经济动力持续推动发展

没有经济动力驱动，关键技术无法更新。从而得不到长期有效的发展和迭代，团队后续版本甚至会产生无法区分主链的分叉情况。

(4)矿机垄断

POW 共识算法，必然导致矿机的军备竞赛，为了获得更高的算力，必然会研发更高性能的专用矿机，普通人无法参与挖矿。而 POC 共识算法，叠加 B4 闪存芯片的性能优势，减少了温度对矿机芯片的损耗，提高芯片的重写、读取的速度，提供最高的可靠性存储等从而降低加密货币对电力资源的消耗，加快运算速度，降低参与门槛，让每个人都能参与价值的攫取。

在传统商业供应链中供应商一般不会成为用户的直接竞争对手，但在 POW 中的 ASIC 厂商本身就是其最大的矿工，也就是说 ASIC 厂商既是矿工的直接竞争对手也是矿工的供货商，当你的商业工具源头来自于你的竞争对手的时候，你所拥有的利润就是被对方套利的风险部分，矿工完全沦为了 ASIC 厂商方的套利工具。

(5)电力资源垄断

电力垄断导致 POW 内生经济系统不再扩张，矿工挖矿成本已高于挖矿收益，收支不平衡，而对于 CPOC 挖矿而言，硬盘耗电低，矿工的收益将会更加可计算，还可以利用民用计算机硬件的线性保值率保证矿工可以在相对安全保本的情况下对冲二级市场的价格波动风险。

4.2、BFM 架构及共识算法

BFM 钱包源自 BTC，共识源自 BurstCoin。

BTC(Bitcoin)始于 2009 年 1 月，经过 10 年的迭代，其钱包稳定性及交易链稳定性已得到广泛的认可， 在其 QT 钱包基础上进行 POC 共识的部署将会非常安全可信。

BurstCoin 始于 2014 年 8 月，经过 4 年的迭代，于 2018 年升级到 POC2，技术相对成熟、完善。

把这两者结合，取长补短，BFM 成为目前 POC 共识算法下最可信赖的公链。

通过采用成熟的 POC2 共识算法，BFM 瞬间获得一个稳定，可信赖的共识算法，社群具备对 BFM 公链的信心。通过兼容 BurstCoin Plot 文件，矿工仅仅需要增加微小的投入，便可以获得 BFM 和 BurstCoin 两份收益。

BFM 钱包继承了 BTC 优良的 P2P 网络架构，及 UTXO 体系，成熟、稳定。

继承自 BTC 钱包，可以保持对 BTC 社区最新进展的跟踪：如闪电网络，脚本升级等。

保持跟 BTC 的相同的接口规范，钱包，交易所对接获得了极大便利。

CPOC：Conditioned Proof Of Capacity，即有条件的容量证明。

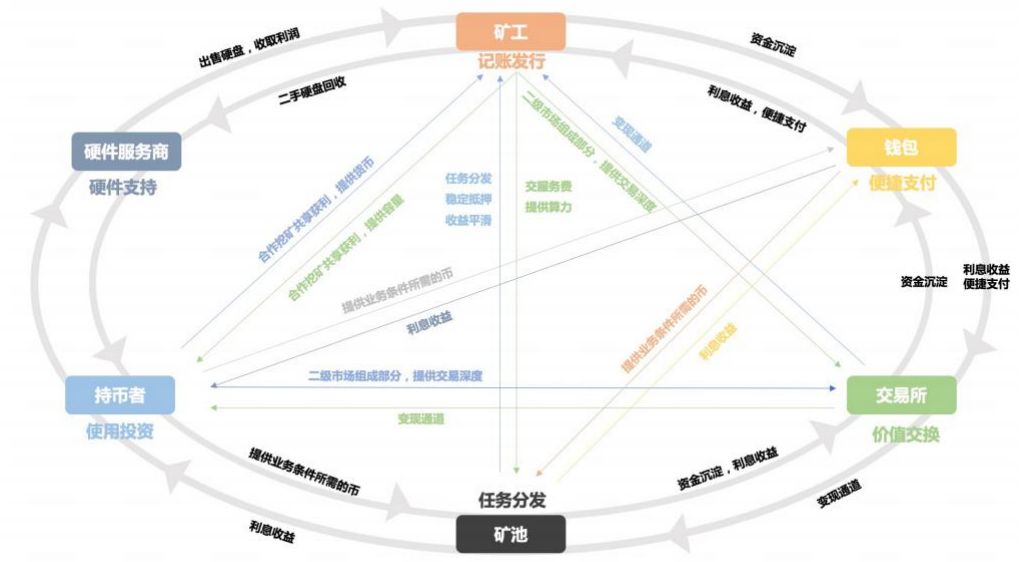
参与挖矿有条件，需要条件 3 BFM/T。通过条件属性，有助于整个社群的稳定，可持续发展。

POC：Proof Of Capacity，即容量证明。

CPOC 经济模型博弈

角色：矿池、矿工、持币者、钱包、交易所、硬件服务商。

CPOC 生态中的商业博弈，产生内在经济循环和外部资源的进入会使之扩张发展，BFM 价格上涨，会使矿工增加；矿工预先看好 BFM 网络加入也会助推 BFM 价格上涨，反之亦然。



POW 的成本制存在 4 个特性：1、作恶成本； 2、铸币成本 ；3、获取的容易度 ；4、挖矿设备价值本身的沉淀，但最终 POW 也会成为低毛利率行业，短暂的暴利是因为其规模不够大，二级市场的波动和挖矿设备的增加曲线不对称导致。POC 中由于硬件相对线性保值，电力消耗小，对于 POC 未来的共生生态矿工免费获得币的权重过于高，不用付出任何风险即可获得几乎免费的其他附产小币种，CPOC 在这个系统中让矿工低成本的付出风险成为其他币种的持币股东，防止矿工的恶意作恶。同时 CPOC 系统高度看重发行权和记账打包权的无门槛释放，这决定了这个系统的公平性。

4.2.1、矿工挖矿流程

（1）、P 盘(Plot)

Miner（矿工）在本地硬盘 Plot 文件，用含有自己公钥的哈希值，综合 Shabal 算法填充硬盘。我们将 plot 文件（p 盘）认为是软件制造“poc 矿机”的过程，将垄断矿机厂商的权力释放给每个普通的人。硬盘容量越大，填充的 Hash 值越多，爆块的概率越高。Hash 算法采用 Shabal256，具有抗 ASIC 特性。

（2）、转账(Transaction)

钱包组成的 P2P 网络（基于 BTC）；钱包之间进行转账操作。

（3）、打包(Forging)

Miner 通过钱包，侦听 P2P 网络，每当收到一个块，就开始下一块的打包过程。

钱包组织一个 Block,把 block 的哈希值发给 Miner，Miner 寻找最匹配的 Nonce。

钱包收到 Nonce 后，把 Nonce 转成 Deadline（时间），然后等待这个时间结束后，把块广播出去。

（4）、验证(Verify)

收到 Block 之后，进行验证。

4.2.2、Plotting-创建 Plot 文件

算法和缩略词

Shabal：Shabal 是 BFM 中使用的加密/散列函数的名称。 与许多其他类似 SHA256 相比，Shabal 是一个相当沉重和缓慢的加密。 因此，使它成为 BFM 等容量证明的良好加密方案。因为我们存储预先计算的哈希值，同时它仍然足够快以进行较小的实时验证。 BFM 使用的是 Shabal 的 256bit 版本，也称为 Shabal256。

Hash / Digest：散列或摘要是 Shabal256 加密的 32Byte（256 位）长字符串。

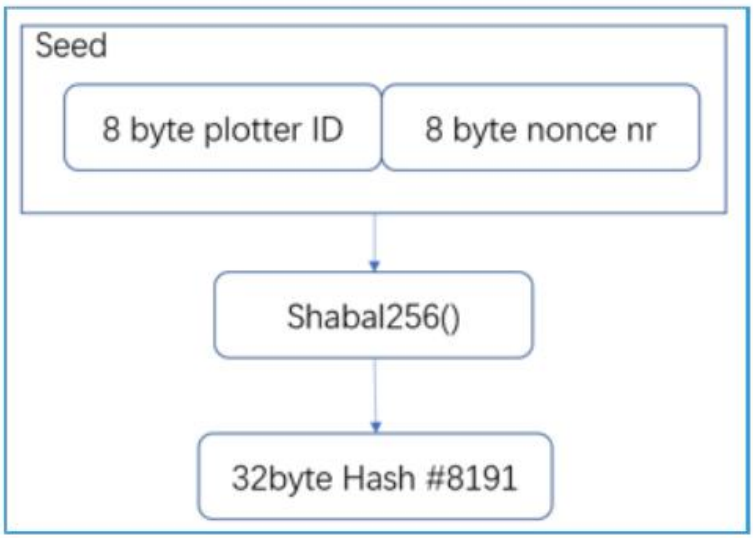
Nonce：生成 Plot 文件时，会生成一些名为 nonces 的字节。 每个随机数包含 256 千字节的数据，矿工可以使用这些数据来计算截止日期。 每个 nonce 都有自己的个别编号。 该数字的范围可以在 0- 18446744073709551615 之间。 在创建 nonce 时，该数字也用作种子。因此，每个 nonce 都有自己独特的数据集。 一个绘图文件可以包含许多 nonce。

Scoop：每个 nonce 被排序到 4096 个不同的数据位置。 这些地方被称为 scoop number。每个 scoop 包含 64 字节的数据，其中包含 2 个哈希值。 这些哈希中的每一个都使用最终哈希进行 xored(异或)（我们在生成 nonce 章节时得到最终哈希）。

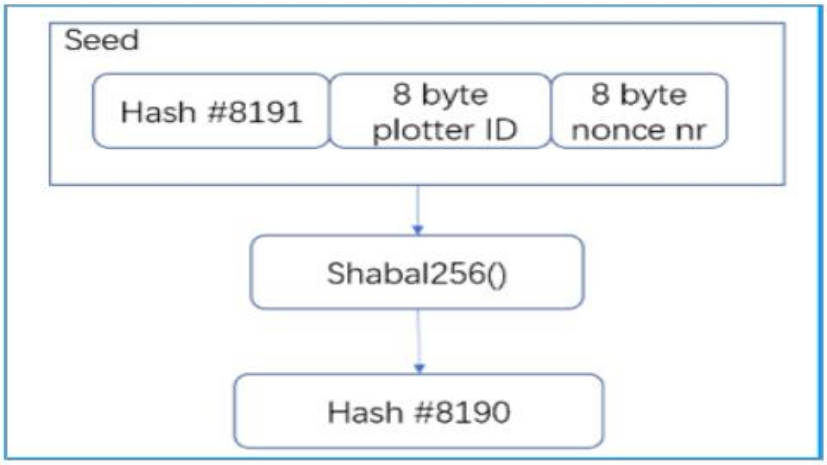
Plotter ID：创建 Plotter 文件时，它将绑定到特定的 BFM 帐户。 创建随机数时将使用 Plotter ID。 因此，即使他们使用相同的 nonce 数字，所有矿工都有不同的 Plotter 文件。

4.2.3、生成 nonce

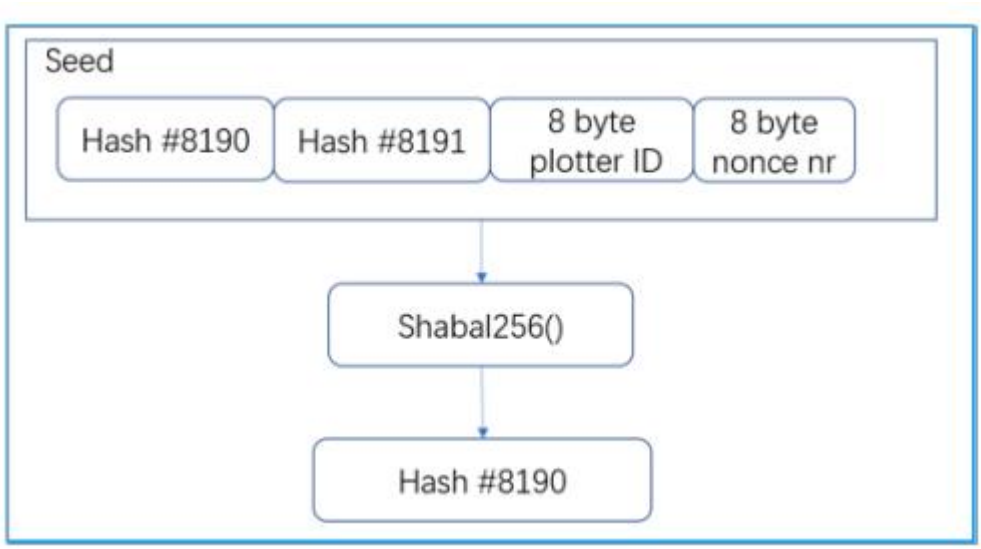
创建 nonce 的第一步是制作第一个种子。 种子长 16bytes，包含 Plotter ID 和 nonce number。 完成后我们用 Shabal256 函数生成第一个哈希值。



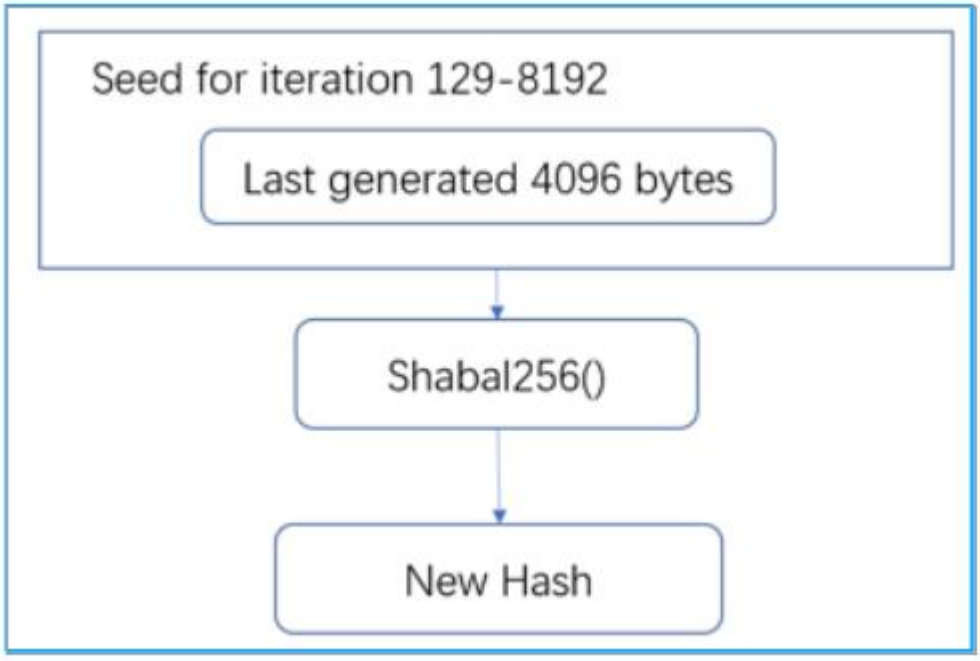
创建首个哈希。 作为 nonce 中的最后一个哈希：＃8191。 把哈希＃8191 附加到起始种子。 作为下一轮 shabal256 计算的种子。



创建了两个哈希： 哈希＃8191 和＃8190。 将 Hash #8190 附加到最后一个种子上，作为新种子。

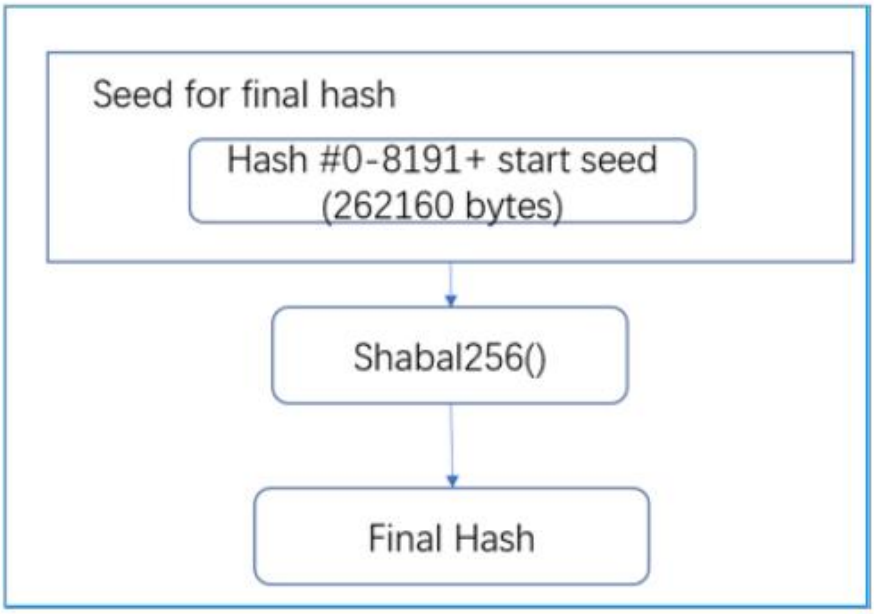


创建新哈希。 对于全部 8192 个哈希，继续将哈希附加到，生成新新种子。迭代 128 次之后，种子长度超过 4096 字节。 剩余的迭代，只读取最后 4096 个字节。

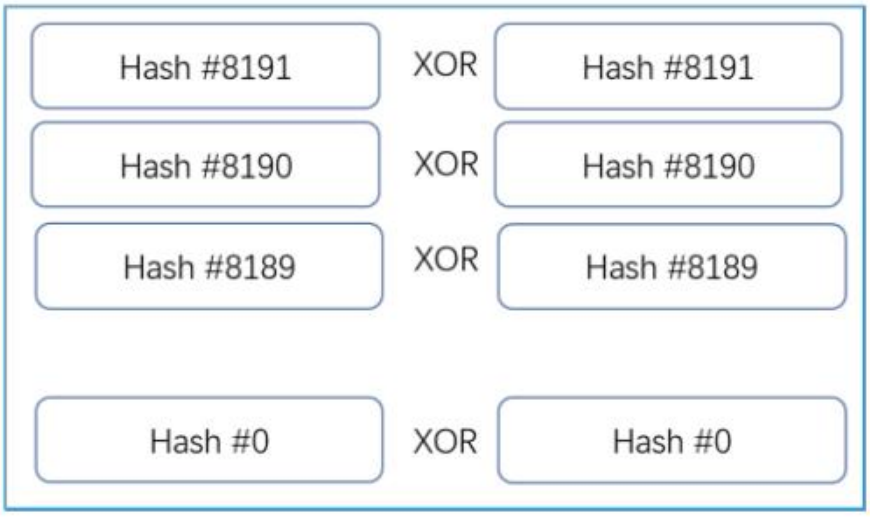


生成终极哈希(Final Hash).

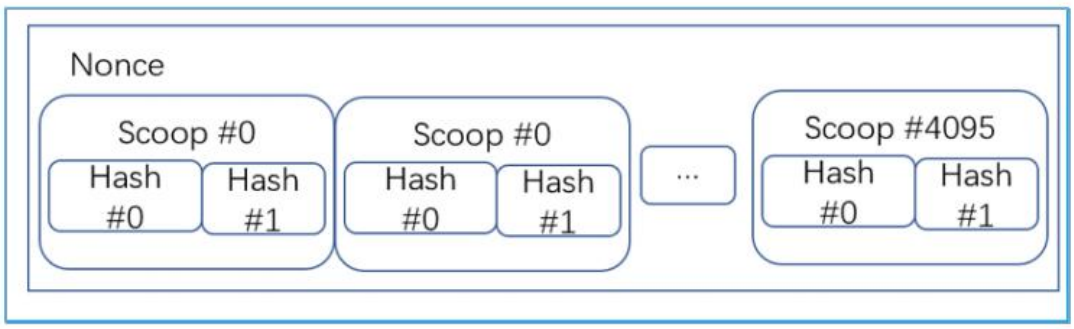
用生成的 8192 个哈希，创建终极哈希。 全部 8192 个哈希值和前 16 个字节作为种子，Shabal256 函数后，生成终极哈希。



终极哈希单独 xor 所有其他哈希。



重复创建 nonce，并把它存到 plot 文件中。



4.2.4、POC 格式

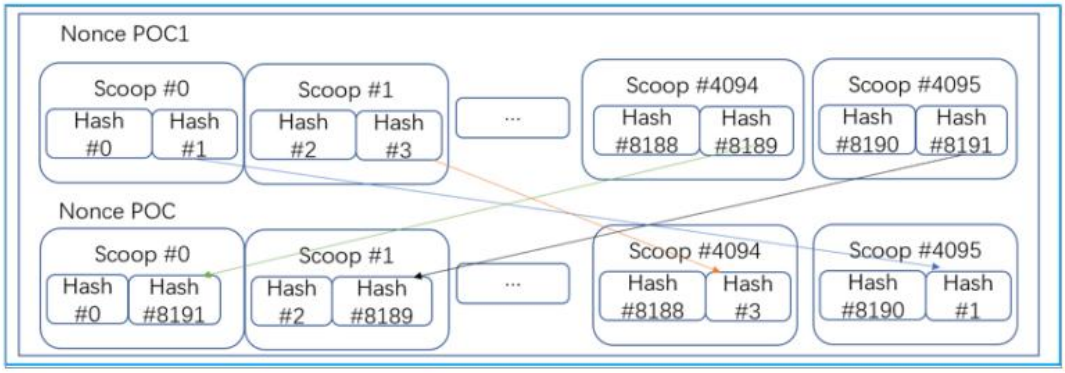
POC nonce 与 Burst POC1 构造方式相同，只是在流程结束稍作调整，混一下数据。

数据混洗流程：

1.将 nonce 分成两半，范围 1：0-2047，范围 2： 2048-4095 的范围。

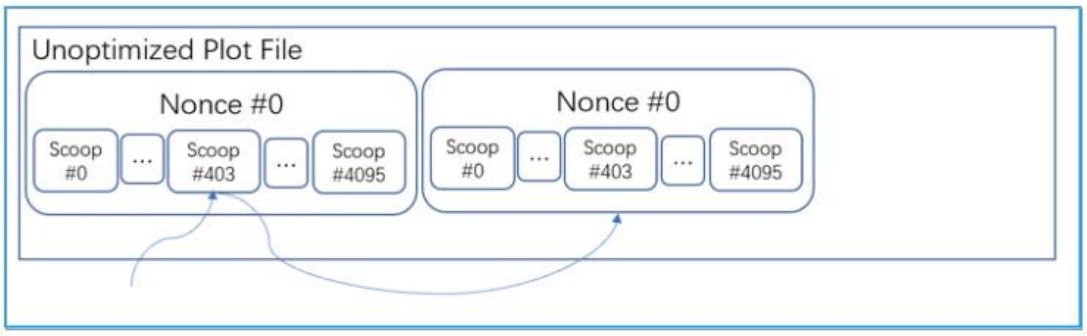
2. 0-2047 称为低 scoop 范围，2048-4095 称为高 scoop 范围。

3.从低 scoop 中取出第二个散列，并将与高 scoop 范围中的镜像 scoop 中的第二个散列交换。 镜像 scoop 是这样计算的： MirrorScoop = 4095 - CurrentScoop



4.2.5、Plot 结构

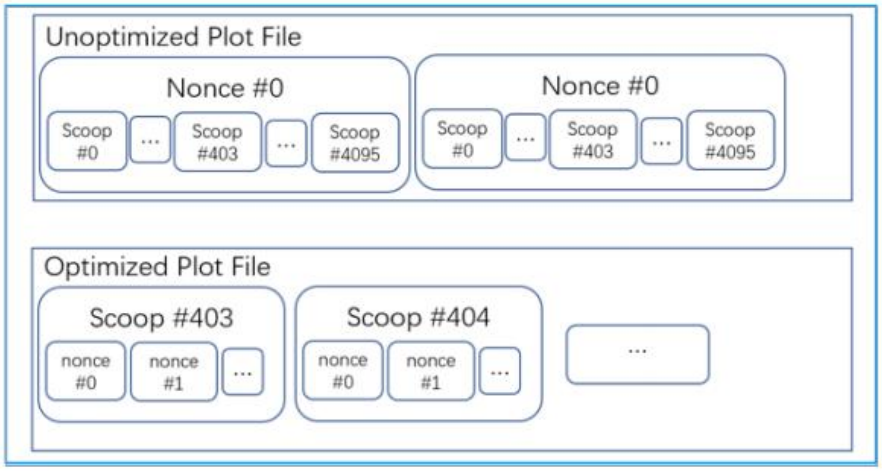
Mining 时，从一个或多个 plot 文件中读取 nonce。 矿工软件打开一个 plot 文件并寻找 scoop 位置来检索 scoop 数据。 如果 plot 文件未经优化，则 scoop 将位于多个位置。 下面示例矿工读取＃403scoop。



矿工花费大量时间在存储上寻找位置，才能读取 scoop，非常低效。

为了提升效率，可以优化 plot，或创建 plot 的时候，做好优化。

优化方案：重新排序 plot 文件中的数据， 把相同 scoop#的数据放在一起。



将 plot 文件分成 4096 个部分，根据 scoop 数量分割所有的 nonce 数据。

当矿工现在想要读取 Scoop 4096 时，它只寻求一次并按顺序读取所有数据，因此比较高效，符合机械硬盘慢寻址特性。

4.2.6、Mining 和锻造区块

算法和缩略词

Shabal / Sha256

Shabal,Sha256 是本文中使用的加密哈希函数。Shabal 是 BFM 使用的主要方法。Shabal 是一个相当沉重和缓慢的加密哈希函数，与 SHA256 等许多其他函数相关。 因此，它得以成为像 BFM 这样的容量证明货币的加密算法。这是因为我们存储了预先计算的哈希值，并且它仍然足够快以进行较小的实时验证。BFM 使用的是 Shabal 的 256bit 版本,也称 Shabal256。

Deadline

当您挖掘并处理 Plot 文件时，最终会产生称为 deadline 的数值。 这些值表示在允许锻造区块之前，自上一个块被锻造以来必须经过的秒数。 如果没有其他人在这段时间内锻造一个区块，你可以锻造一个区块并获得区块奖励。

Block reward

如果你幸运地铸造了一个区块，你将获得 BFM 作为奖励。 这被称为块奖励。 每 420000 个区块，区块奖励减少 50%。 初始奖励是每个区块 25 个 BFM，其中 1.25 归属基金会，在足额条件的情况下，矿工会得到 23.75 个 BFM。

Base target

Base Target 是根据最后 288 个块计算得出的。 该值调整了矿工的难度。 基准目标越低，矿工越难找到数值小的 deadline。 它的调整方式是一量让 BFM 每个区块平均间隔时间为 5 分钟。

Network Diffificulty

Network Diffificulty(网络难度)，或简称 NetDiff，是一个值，可以看作对 BFM 存储空间的评估，单位为 Byte。 这个值随块而变， 以 base target 为基准。

Block Height

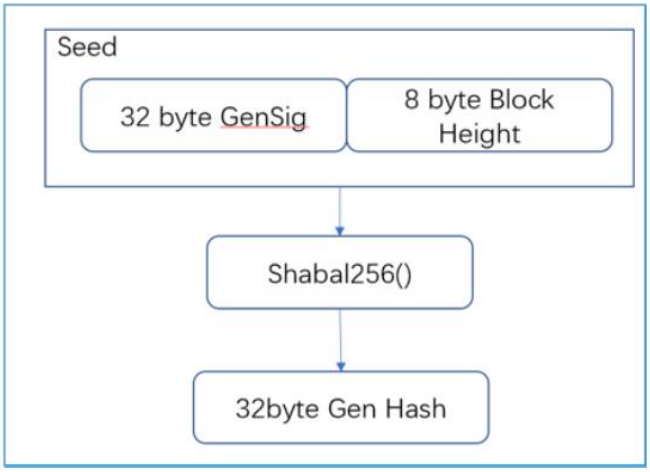
每个被锻造的块都有一个单独的数字。每个被锻造的新块都会在前一个块的编号上+1；此编号称为块高度，用于标识唯一的区块。

Generation Signature

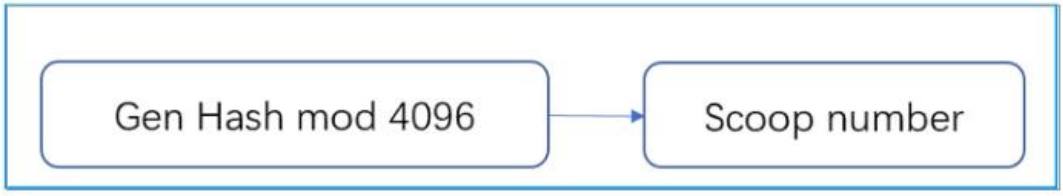
生成签名是基于先前的块 merkle 根和区块高度，然后矿工使用该值来锻造新块。 生成签名长度为 32 字节。

4.2.7、挖矿过程

矿工从钱包获取挖矿信息，此信息包含新的 generation signature，base target 和下一个块高度。 在钱包发送此信息之前，通过将上一个 generation signature 和 plot id 创建生成签名，并通过 shabal256 运行此方法以获取新哈希。 矿工将采用新的 32 字节生成签名和 8 字节块高度，并将它们作为 Shabal256 的种子放在一起。 生成 Generation hash 的哈希值。



矿工对哈希进行小规模数学计算，通过散列对 4096 取模，找出 scoop number。



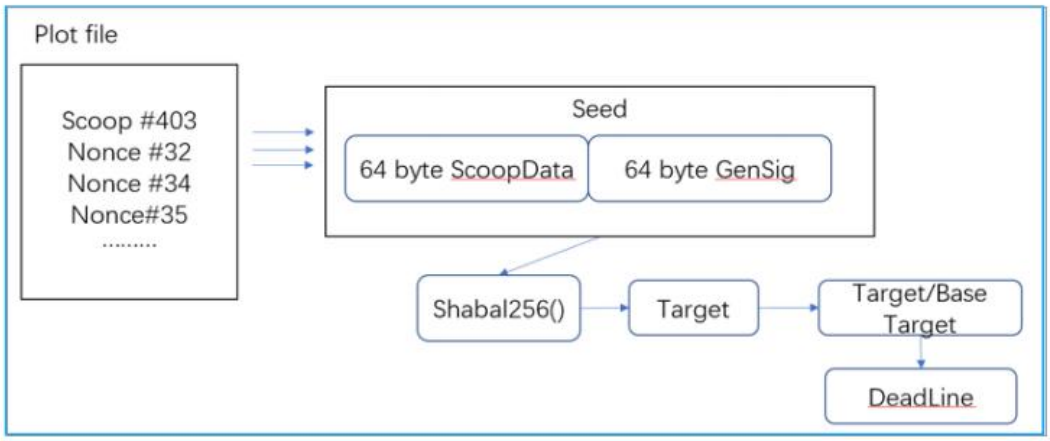
下一步读取 plot 文件，从所有的 nonce 中，获得 scoop,处理这些 scoop.

方案： shabal256(scoop.hash,generation signature)，生成目标哈希，称为 target。

Target 除以 base target，得到的前 8 个字节是值就是 deadline。

Target = shabal256(scoop.data,generation signature)

Deadline = target / base target;



为防止对钱包进行“nonce spamming”，矿工通常会检查当前 deadline 是否低于目前为止发现的最低 deadline。 可以设置一个最大值，因为任何人都无法使用大得离谱的 deadline,检查之后,矿工把信息提交给钱包。 此信息包含绑定到 plot 文件的 Plotter ID,以及包含用于生成 deadline 的 scoop 数据的 nonce。

4.2.8、区块锻造过程

处理 Deadline

钱包收到矿工提交的信息，创建对应的 nonce，以便找到并验证的 deadline。

然后，钱包现在将检查 deadline 对应时间的流逝，直到 deadline 对应的时间（秒）用光。

如果在 deadline 之前在网络上收到其他钱包的有效区块，则钱包将丢弃提交的 Mining 信息。

如果矿工提交新信息,钱包将创建 nonce,并检查 deadline 值是否低于之前的 deadline。

如果新 deadline 较小，钱包将使用该 deadline。

Deadline 有效时，钱包现在开始锻造一个新的区块。

锻造

首先，钱包获取从用户或网络收到的所有未经确认的交易。

钱包将尝试包含一可能多的交易，直到达到 8M 的上限，或者直到处理完所有交易。

钱包对交易进行合法性检查。 例如，如果交易具有有效签名，如果它具有正确的时间戳等。

钱包还将总结所有添加的交易金额和费用。

BFM VS BTC

参数	BTC	BFM
供应量	2100 万	5000 万
出块时间	10 分钟	5 分钟
区块大小	1M	8M
减半周期	4 年减半	4 年减半
初始出块奖励	50	25

BFM 继承自 BTC，相对 BTC：

BFM 增加区块到 8M/Block，区块变大，单个区块可以包含更多交易，提升转账速度；

出块时间调整为 5 分钟，出块时间减半，提升转账速度；

初始出块奖励调整为 25BFM/block，4 年减半；初始出块奖励减半，可以让社区有更多得时间，聚集；

社区资源，矿工群体可以分享更多收益，同时维持 5000 万货币供应总量。

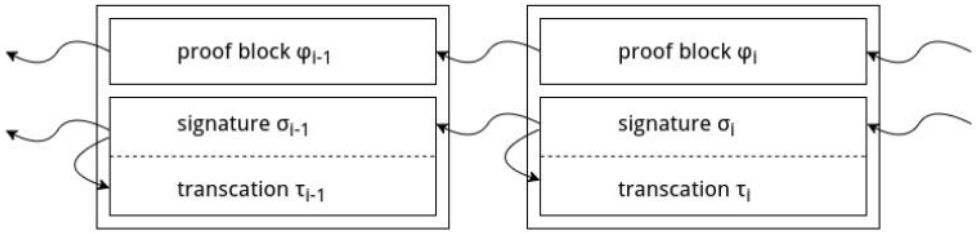
4.3、BFM 技术特性

1. POC2 共识算法；
2. 出块时间 5 分钟，交易速度更快；
3. 8M 区块大小，提升网络效率；
4. 全网容量达到 3000P 计划加入零知识证明；

5. 使用硬盘挖矿，抗 ASIC，无需专业设备即可挖矿；

6. 绿色环保，低能耗，低噪音；

4.3.1、区块链



- 块包括 proof sub block, signature sub block and transaction sub block。
- 箭头表示该子块包含矿工对箭头指向子块的签名。
- 我们的 challenge 由 Δ 块之前的 proof 子块的 hash 生成。

4.3.2、Possible attacks 可能的攻击及防范设计 Block grinding

矿工可以在创建块的时候，尝试不同的交易组合，使得创建的块对自己有一定偏向性。我们的区块结构中 proof 子块的独立性可以防止这个攻击。

Challenge Grinding

• 矿工在挖矿的过程中，可以将自己的空间分成 m 份，然后对区块链上的连续 $t = 2$ Δ 块进行重构，如果区块链的 Quality 定义如下:

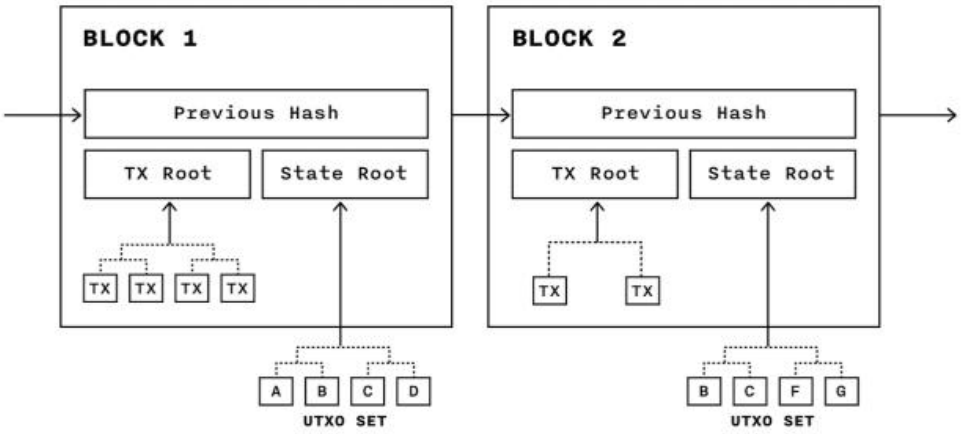
• 那么可以通过尝试第 i 块的 proof，使得 i + Δ 的 Quality 最大。在以上基于线性求和的 Quality 下，按照上述的攻击方法，将会导致攻击者可以获得 m 倍的机会取得更大 Quality 2 24

• 通过重新定义区块链的 Quality 的，来降低这种攻击的获得收益倍数，将 Quality 的计算由线性叠加改变为乘积的方式，定义如下：

• 在该定义下，攻击者获取的概率提升将会降低为 $log(m)$。同时，让连续的 Δ 块的 challenge 由同一个块来决定，将会进一步降低该攻击的影响。

4.3.3、Transaction 交易

BFM 交易结构同 bitcoin 一样，即一条 UTXO 到 UTXO 的链。这种 transaction 的设计方式也是经过了多年通用可用，也是用这种有效的办法来实现其基础的属性。



5、应用场景拓展

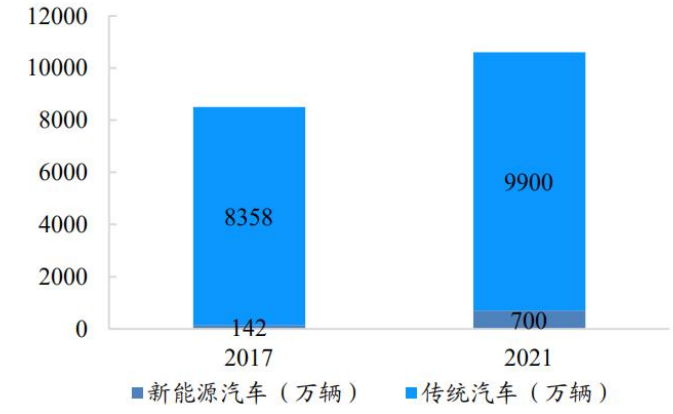
基于 B4 闪存芯片的优质性能（高速、高可靠型数据程序存储，耐高温等），除了在加密货币开采能提供超大价值外，在很多其他领域，例如新能源汽车、高铁控制、通信基站、工业机器设备、智能电网等，都能带来难以估量的巨大价值。以下就以新能源汽车为例，拓展 B4 芯片的应用价值。

近年来，新能源汽车放量和汽车电子成本占比上升，汽车行业对芯片需求量增大，尤其是纯电动轿车和混合动力轿车这类新能源汽车，需要电源管理类芯片控制电流和电压。汽车电池管理系统（BMS）是 一套保护汽车锂电池安全的系统，通过传感器对汽车电池实时监控，控制最大输出功率，保证电池安全。根据 Strategy Analytics 的测算，传统汽车电子成本为每辆 350 美元，其中电源管理芯片的成本为 118 美元，新能源汽车的电子成本为 704 美元， 其中 Power IC 的成本为 387 美元。2018 年，中国新能源汽车销量为 104.86 万辆，同比增长 79.31%，新能源汽车保有量达到万辆，占全球市场的 50%以上。我国是全球最大的新能源汽车市场，国家对新能源汽车给予补贴优惠政策，预计在未来我 国新能源汽车会维持高速增长，新能源汽车市场对芯片需求巨大。

根据 IHS 和 PwC 的数据，2017 年全球新能源汽 车产量为 142 万辆，传统汽车产量为 8358 万辆。

市场增长动力：新能源汽车产量增加，汽车半导体中芯片成本上升，带动芯片市场增长。2021 年全球汽车出货量将达到 1.06 亿辆，其中新能源汽车产量为 700 万辆，传统汽车产量为 9900 万辆。

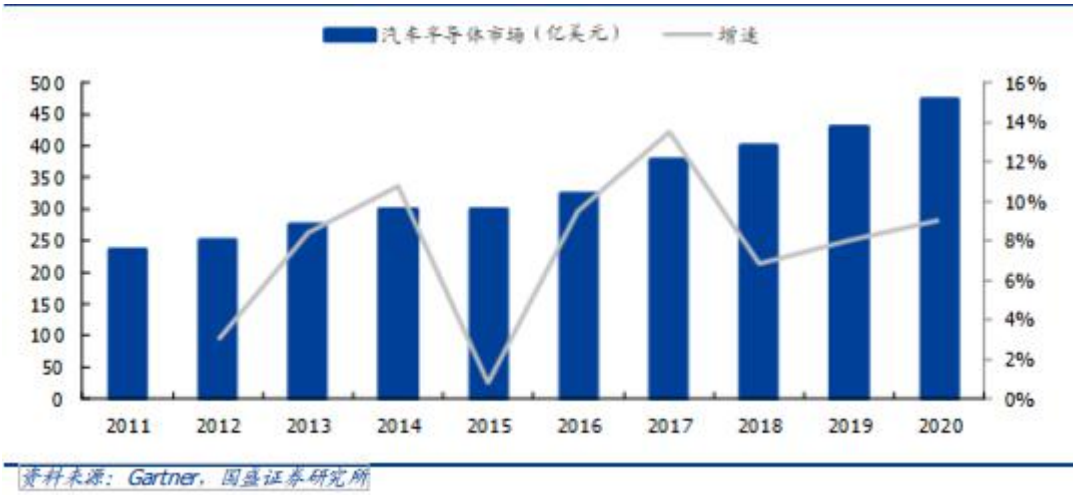
新能源汽车产量持续增加



资料来源：： IHS 预测、PwC 预测、新时代证券研究所

汽车电子化使用更多芯片，预计 2020 年汽车半导体全球市场 434 亿美元。我们分析了新能源汽车由于使用电能驱动，导致结构相比于传统燃料汽车有了很大的改变，三大结构：电机、电池、电控对半导体的需求大幅提升，尤其是对功率半导体器件。根据 Gartner 预测，2017 年全球汽车半导体市场为 377 亿美元，预计到了 2020 年市场将达到 434 亿美元，年复合增长率 CAGR 为 7.8%。

全球汽车半导体市场及增速



资料来源：Gartner，国盛证券研究所

而 B4 半导体芯片高速读取、擦写，耐高温、高安全性、高信赖性（高温动作 125℃、长时间使用 20 年）就是天然契合该新能源汽车的市场。所以随着新能源汽车的需求不断增大，对 B4 芯片的需求也不断增加。

6、治理架构

6.1、治理架构和机制

“治理”是公链的核心命题，一个去中心化治理的公链才会有最长久的生命力。BFM Chain 通过链 上与链下治理的结合将人与代码同时引入到公链的复杂治理体系中去，从而在实现治理的去中心化的同时保证治理的有效性。每一位 BFM Chain 资产持有者都有参与去中心化治理的权利。公链生态中的运营和发展方向，都会由全体 BFM 持有者以协商投票的方式来决定。

BFM Chain 的链上治理结构由理事会(Committee)和信任节点(TrustNode)构成。链上理事会由 11 名成员组成，可以提议修改 BFM Chain 的动态全局参数。信任节点由 21 名节点成员组成，负责 BFM Chain 网络的交易记账、交易验证、区块打包和确认等工作。

6.2、链上治理—BFM Chain 理事会和信任节点

BFM Chain 的链上治理是通过 BFM Chain 理事会和信任节点实现的。BFM 持币人可通过信任节点去方便、快捷地行使 BFM Chain 的治理权。BFM Chain 的生态内有 21 个信任节点，为 BFM Chain 提供网络、存储和计算等基础设施。BFM Chain 鼓励每一个信任节点构建自身的社区，使得每一个信任节点的社区都能在相互竞争中共同发展，壮大 BFM Chain 生态。信任节点按得票数的前 11 名当选为 BFM Chain 理事会成员，它是 BFM Chain 社区的核心链上治理组织。

6.2.1、BFM Chain 理事会和信任节点

在 BFM Chain 的治理生态中有如下三个角色：

1）持币者：持有任意数量 BFM 的个体或机构。

2）信任节点 ：由全体 BFM 持币者投票选举出的个体或机构，每 1 小时统计一次投票，共有 21 个信任节点。节点竞选投票中，得票数排名前 21 的成为信任节点。 信任节点负责 BFM Chain 网络的交易验证、交易记账、区块打包和确认等工作，成功打包区块将获得对应的奖励。信任节点接受 BFM Chain 社区的监督。

3）BFM Chain 理事会 ：信任节点按得票数的前 11 名当选为 BFM Chain 理事会成员。

BFM Chain 理事会是 BFM Chain 社区的核心链上治理组织，主要职责是设定合理的公链全局参数，以此促进 BFM Chain 长期的健康发展。其中包括：

1）修改区块链的动态参数，比如区块大小、区块间隔等；

2）信任节点出块奖励、信任节点数量和活跃理事会成员数量等；

3）转账、发行资产及各类交易手续费；

4）智能合约的创建和调用费率等。

6.2.2、信任节点竞选规则

每一位 BFM 持币者都可成为信任节点的竞选者。竞选者需要向系统抵押 1 万 BFM(具体金额由理事会投票决定)，退出竞选时可在 30 天后 (系统动态参数，可由理事会投票调整) 取回。若节点作恶，其抵押的 BFM 可由理事会投票处理。为了保障节点竞选的高效进行，BFM Chain 针对信任节点候选人制定了一系列的标准和规则。由 BFM Chain 基金会的生态建设委员会 (BFM Chain-ECO) 根据标准和规则对候选节点进行审核。信任节点候选人必须符合以下基本条件：

1）具有合法设立的组织主体，且拥有官网及公共自媒体平台账号；

2）具有可供社区成员测试的节点；

3）拥有可运行节点的服务器和节点运维技术；

4）创建信任节点，需要抵押一定数量的 BFM，若取回抵押的 BFM，则视为退出竞选；

5）已制定未来三年的预算支持，技术方案，硬件扩容以及社区支持计划；

6）拥有一定规模的社区用户。

6.2.3、节点收益

信任节点的收益主要来自出块奖励，由理事会投票决定出块奖励金额。在每一次区块打包完成之后，信任节点将获得相应的出块奖励。出块奖励池子由转账手续费以及基金会捐赠节点奖励两部分构成。为激励信任节点在 BFM Chain 生态中做出的积极贡献，BFM Chain 基金会将捐赠 400 万枚 BFM 注入系统资金池作为节点出块奖励，奖励分 8 年发放，每年释放 50 万枚。

6.2.4、信任节点投票产生方式

每一个 BFM 视为一票，可为多个候选节点投票。参与信任节点投票的 BFM 将被质押在自己的钱包，如果资产转出，则视为撤票。累计票数排名前 20 名节点自动当选为信任节点，第 21 个节点从剩余的备选节点中随机产生。 投票途径主要有 3 种：

1）BFM 投票

在 BFM 钱包中的 BFM，可通过 BFM 的投票通道进行信任节点的投票。

2）手机钱包和 PC 钱包投票

在 BFM Chain 手机钱包和 PC 钱包中的 BFM 可进行信任节点的投票。

3）交易所投票

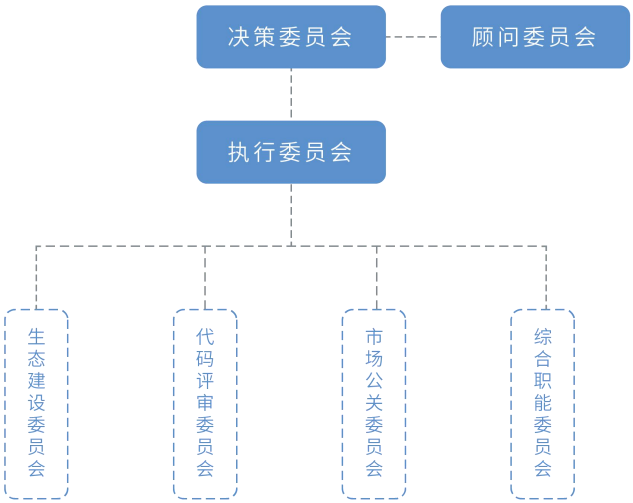
如果用户的 BFM 在交易所钱包里，且该交易所支持 BFM Chain 的信任节点投票，便可以采用此方式进行投票。

6.3、链下治理—BFM Chain 基金会

6.3.1、BFM Chain 基金会的设立

BFM Chain 基金会，全称为 BFM Chain foundation LTD.，旨在通过科学、合理、有效的治理机制推动并维系基金会及 BFM Chain 生态的建设和健康发展，为 BFM 持币者提供合适的保护和平等权利，构建 BFM 持币者、社区、节点、dApps 开发者等不同角色之间的高效沟通渠道。 BFM Chain 基金会每年将向社区披露 BFM Chain 的开发情况、运营情况、BFM 的使用情况等，并将引入第三方审计机构，监督项目的财务运作，审计报告将在年度信息披露中公告。

6.3.2、BFM Chain 基金会的组织架构



6.3.3、决策委员会

1、简介

决策委员会是 BFM Chain 基金会的决策机构。

2、人员组成

决策委员会由 11 名成员组成，包含主要发起人、开发者代表、投资者代表及社区代表，设主席、副主席、执行总裁各一人，从决策委员会成员中选举产生，其他代表名额不固定。

3、人员介绍

决策委员会成员由选举产生，存在人员名单不确定性，具体名单请以官网公布的为准。

4、议事规则

决策委员会至少每年召开一次会议，由决策委员会主席负责召集并主持，于会议召开 30 日前通

知全体成员，决策委员会会议需由 1/2 以上的成员出席方可举行。决策委员会会议中，一般事项的

决议须经出席成员 2/3 以上表决通过，特殊事项还须经决策委员会主席投赞成票方为有效。任何需

决策委员会决议的事项，如决策委员会成员以书面形式一致表示同意的，可以不召开决策委员会会议，

直接作出决定，并由全体成员在决定文件上签名。

5、主要职权

决策委员会主要行使下列职权：

(1) 制定、修改基金会治理机制；

(2) 选举、罢免主席或副主席；

(3) 根据主席的提名选举执行总裁、副总裁和其他执行委员会成员；

(4) 决定基金会的经营计划和投资方案；

(5) 年度收支预算、决算及资金分配方案审定；

(6) 通过授予荣誉职务（ 包括聘请名誉主席和顾问 ），增减顾问委员会成员；

(7) 决定设立办事机构、分支机构、代表机构；

(8) 听取、审议主席所做的工作报告，检查执行总裁的工作；

(9) 决定基金会的分立、合并或终止；

(10) 决定其他重大事项。

其中，有关第 (1)、(4)、(5)、(9) 项的决议属于特殊事项。

6、任职资格

决策委员会成员需具备下列条件：

(1) 有加入基金会的较强意愿，认同基金会的宗旨；

(2) 在基金会的业务领域或社区内，具有一定影响力；

(3) 对基金会的发展壮大，有所帮助或有所贡献者；

(4) 无任何违法犯罪记录。

7、人员的产生和罢免

(1) 第一届决策委员会成员由主要发起人、开发者代表、投资者代表分别提名并共同协商确定；

(2) 决策委员会换届改选时，由决策委员会提前 60 日发布公告公布成员资格条件及改选规则等事项，面向全体 BFM 持有人征集候选人，最终由 BFM 持有人进行投票，选举产生新一届决策委员会成员；

(3) 决策委员会成员需在任职期间接受授信调查，并公开薪酬情况；

(4) 任何成员因违反基金会制度、损害基金会声誉或给基金会事业造成损失等，经决策委员会审议后终止任职；

(5) 任何成员因违法、违纪受到处理，职务即时终止；任何成员因涉嫌犯罪被起诉或接受调查，决策委员会合理地认为该成员继续担任职务可能影响基金会声誉或形象的，经

决策委员会审议后终止任职；

(6) 任何成员自动请辞，死亡或因疾病、意外事故等丧失工作能力的，经决策委员会审议后终止任职。

8、任期

决策委员会成员每届任期为 2 年，任期届满，连选可以连任。

9、主席、副主席主要职权

决策委员会主席主要行使下列职权：

(1) 召集和主持决策委员会会议并组织实施；

(2) 提议召开临时决策委员会会议；

(3) 代表基金会签署重要文件，检查决策委员会决议的落实情况；

(4) 对重大突发事件进行紧急决策；

(5) 提名执行总裁、副总裁和其他执行委员会成员的候选人，各项职务应至少提名 2 位候选人供决策委员会选定。

副主席在主席领导下开展工作，经主席书面授权可代主席行使相关职权。

6.3.4、顾问委员会

1、简介

顾问委员会是 BFM Chain 基金会的专家顾问团，由决策委员会挑选业务相关专业领域内较具有影响力的人员组成，包括但不限于技术专家、资深投资人、资深律师等，为基金会运营管理事务提供咨询与指导。

2、人员组成

不超过 7 名，由决策委员会选定。

3、人员介绍

顾问委员会存在人员名单不确定性，具体名单请以 UPbfm.com 官网公布的为准。

4、主要职权

顾问委员会主要行使下列职权：

(1) 为基金会运营管理事务提供咨询与指导；

(2) 受决策委员会邀请可列席决策委员会会议，但不具备投票权。

5、任职资格

顾问委员会人员需具备下列条件：

(1) 在基金会的业务相关专业领域内，具有一定影响力；

(2) 无任何违法犯罪记录。

6、人员的产生和罢免

(1) 由决策委员会挑选并授予荣誉职务，包括聘请名誉主席、顾问等；

(2) 因违反基金会制度、损害基金会声誉或给基金会事业造成损失等，经决策委员会审议后终止任职；

(3) 因违法、违纪受到处理，职务即时终止；因涉嫌犯罪被起诉或接受调查，决策委员会合理地认为该人员继续担任职务可能影响基金会声誉或形象的，经决策委员会审议后终止任职；

(4) 自动请辞，死亡或因疾病、意外事故等丧失工作能力的，经决策委员会审议后终止任职。

6.3.5. 执行委员会

1、简介

执行委员会是 BFM Chain 基金会的执行机构，负责基金会日常运营管理事务的具体执行，设执行总裁一人，其他执行委员会成员在执行总裁领导下开展工作，指导并管理下属专门委员会工作。

2、人员组成

执行总裁、副总裁、秘书及各专门委员会负责人

3、人员介绍

执行委员会存在人员名单不确定性，具体名单请以 UPbfm.com 官网公布的为准。

4、主要职权

执行委员会主要行使下列职权：

(1) 执行决策委员会的各项决议；

(2) 指导下属专门委员会开展工作；

(3) 决定下属专门委员会人员的聘用与解聘，包括决定其报酬事项；

应对基金会紧急事件，拟定应对方案供决策委员会主席决策。

5、人员的产生和罢免

(1) 由决策委员会主席提名，经决策委员会审议后选定；

(2) 因违反基金会制度、损害基金会声誉或给基金会事业造成损失等，经决策委员会审议后终止任职；

(3) 因违法、违纪受到处理，职务即时终止；因涉嫌犯罪被起诉或接受调查，决策委员会合理地认为该人员继续担任职务可能影响基金会声誉或形象的，经决策委员会审议后终止任职；

(4) 自动请辞，死亡或因疾病、意外事故等丧失工作能力的，经决策委员会审议后终止任职。

6、任期

每届任期为 2 年，任期届满，连选可以连任。

7、执行总裁主要职权

执行总裁主要行使下列职权：

(1) 主持开展基金会日常工作，组织实施年度运营计划，并向决策委员会汇报工作情况 ；

(2) 拟订基金会的内部管理规章制度，报决策委员会审批；

(3) 协调各下属专门委员会、分支机构开展工作。

6.3.6. 下属专门委员会

1、生态建设委员会

生态建设委员会负责 BFM Chain 生态建设相关事宜，包括对 BFM Chain 上开发者项目的投资、孵化，为构建 BFM Chain 生态筛选合作伙伴，进行尽职调查并负责后续合作对接工作。

2、代码评审委员会

代码评审委员会负责 BFM Chain 底层技术构建、API 服务开发、开发者代码评审、代码合并与 Github 发布等工作。同时，代码评审委员会人员通过定期分享会、不定期交流会等形式保持技术团 队紧跟行业趋势，积极研究最新区块链技术。

3、市场公关委员会

市场公关委员会负责基金会形象的建立与维护及社区的运营与推广，以及危机公关等工作。

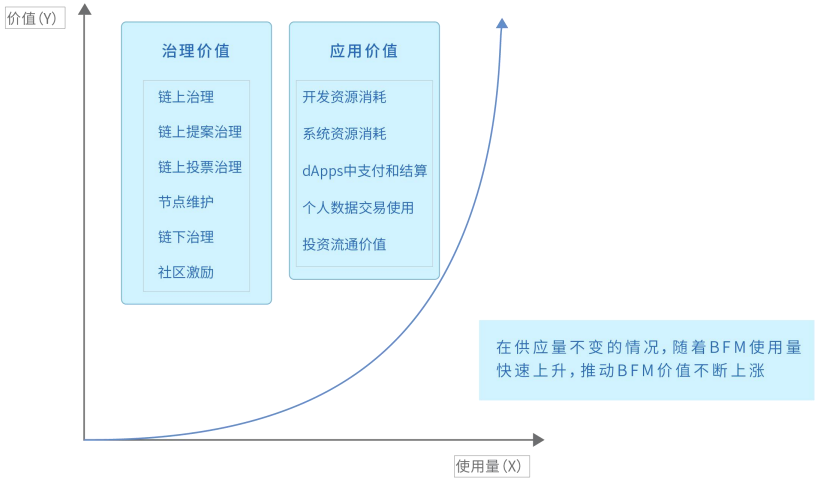
4、综合职能委员会

综合职能委员会负责基金会日常资金使用的审核与管理、基金会内部人事管理、行政事务管理 。

7、经济模型

7.1、BFM 经济模型和价值场景介绍

BFM 是 BFM Chain 的核心资产，中文名为信任币，总量 5000 万。BFM 类似于 Ethereum 主链的 ETH 以太币，EOS 主链的 EOS。BFM 作为 BFM Chain 非常重要的治理和应用核心资产，具体的经济模型和价值场景图如下：



7.2、治理价值

BFM 在 BFM Chain 的链上治理都发挥着重要的作用，用于促进更大范围参加有效的治理。

在链上治理中，BFM 主要扮演者表达介质与激励机制的角色；在链下治理中，BFM 主要用于激励更多的社群用户参与 BFM Chain 的治理

在链上治理中，BFM 主要有以下几点用途：

1) 链上提案治理：理事会成员发起提案需要消耗 BFM，提案的通过与执行也需要理事会支付相应的 BFM；

2) 链上投票治理：在选举信任节点与治理委员会时，用户持有的 BFM 作为唯一选票使用；

3) 信任节点维护：创建与修改信任节点都需要消耗 BFM。

在链下治理中，BFM 主要用于激励开发者以及社区用户参与治理。BFM Chain 基金会对开发者以及社区用户积极参与 BFM Chain 治理、推动 BFM Chain 发展的行为会给予一定的 BFM 奖励。

7.3、应用价值

B4 芯片以其高性能（高速读取、擦写、耐高温、高可靠性等）在芯片储存领域占有至关重要的地位，为新能源汽车、工业机器、智能电网、通信基站、人工智能等带来了新的成长空间，其科技价值和市场价值巨大。

而 BFM 是基于 Conditioned Proof Of Capacity(以下简称：CPOC）的新型加密货币。其主要的特点是使用 B4 闪存芯片作为共识， 在数据经济中有着广泛的应用价值，为区块链在数据经济的落地与大规模商业应用提供了重要价值介质。 BFM 的应用价值主要有以下几个方面：BFM Chain 开发资源的使用、BFM Chain 上各类系统资源的消耗、dApp 中的支付与结算、个人数据交易使用、投资价值流通等。

7.4、协同价值

未来三年内企业处于一个快速的投资发展期，主要着力于 B4 芯片的市场开发和技术再创新，巩固市场地位。

预估第四年净利润为 26500000 美元，之后因市场的不断拓展，利润将会呈爆发性增长。

为了与广大投资者共同发展，一起维护 BFM 的市场价值和社会价值，将 B4 芯片打造成未来的“芯世界”。

所以作出以下方案：

（1）三年后，如果企业利润达到或者超越预期，将会把三分之二利润用于持币者分红，以回馈广大投资者和维护者，三分之一留存企业继续投资发展。

（2）如果企业未达到预期的利润，将会根据社区广大投资的的投资表决进行一定的回购，以保障广大投资者的利益。

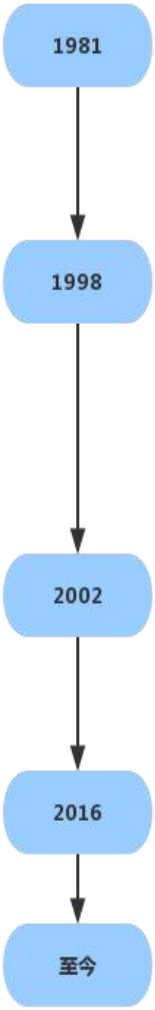
7.5、BFM 分发机制

供应总量	5000 万枚
开发团队	10%：500 万枚。方式：预挖，主网上线前以 ERC20 代币流通
推广团队	5%：250 万枚。方法：随挖矿的每块产出
矿工	85%：4250 万枚。方式：挖矿
出块时间	5 分钟
初始块大小	25BFM/Block, 8MB 区块大小
减半周期	4 年，首次减半时间约为 420000 区块高度
初始 TPS	70 笔交易/秒
条件化容量证明	每 T 持有 3000 个 BFM 作为条件。 说明：IT 硬盘是根据爆块率对全网占比进行评估，不是绝对值

在挖矿初期的前 1 个月，矿工挖矿完全免条件；从第二个月开始，矿工实行条件挖矿，如果矿工不满足条件挖矿，只能获得 30%的收益，70%的币将会纳入基金会用于系统开发、市场推广和运营；如果矿工满足条件挖矿，将会获得 95%收益，5%纳入基金会用于市场推广。CPOC 条件挖矿的发行方式会让矿工、矿池和基金会等参与方的产生正向商业博弈，使整个系统始终会有一个较为主力的临时商业既得利者（这个既得利益者会随着时间和价格挖矿难度等变量条件而变化）去无形推动整个生态。

8、创始人简介

中岛盛一：1980 年毕业于大阪大学物性物理工学科



作为三菱电机半导体事业部的非易失性储存其开发经理，持续从事工艺技术开发。
完成三菱电机的 EPROM,EEPROM,Flash 和微型计算机配备的闪存的全部开发。
负责三菱与意法半导体，摩托罗拉，日立各公司闪存开发协作。

三菱电机闪存部门负责人。
提出了世界第一个“Memory Solution”概念。
三年内将闪存业务（接手前：劣质业务，销售额为 1 亿美元，亏损额为 1 亿美元）成功转化为年销售额 10 亿美元，利润达 4 亿美元，占全球闪存份额的 10%。
成功地“改变销售方式”和“改变行业”，并在三年内建立了 10 亿美元的新业务。

创立 GENUSION，INC 以开发和商业化闪存，这是一种新结构。他用投资者 3000 万美元的投资，成功开发和生产 B4-Flash Memory（世界上最小的闪存 58 纳米 B4-Flash Memory）。

建立了拥有 B4-Flash 技术的 Pothos semiconductor, Inc 公司。
推动 B4 闪存的商业化，作为高性能，高可靠性的储存解决方案，该技术一段时间内无法被替代，在当下许多领域有独特的优势。

9、结论

随着新兴产业（包括新能源、大数据、云计算、物联网、人工智能等）不断发展发展，半导体芯片在各个行业产业链中愈发重要，几乎都离不开半导体的发展，把握住芯片，就等于把握住未来。B4 Flash Memory 以其独有的优势在半导体储存行业中独树一帜，肩扛着未来庞大市场的需求，为整个市场半导体储存市场指引着方向。而 BFM 是基于 Conditioned Proof Of Capacity(以下简称:CPOC)的新型加密货币。其主要的特点是使用 B4 Flash Memory 作为共识， 着重于在数据经济这个未来有着光明前景的方向发展，为区块链在数据经济的落地与大规模商业应用提供了重要价值介质。