# 涡轮网络 Volume Network(VOL)

# 白皮书

——探索演进路线的基于 HardDisk 的基础货币

版本号 1.2

# 一、序章

## 1.1 加密货币蓬勃发展

2008 年，中本聪在 metzdowd 的密码学邮件组列表中发表了一篇论文，论文描述了比特币的电子现金系统。2009 年 1 月 3 日，比特币创世区块诞生、第一批 50 个比特币同时被创造出来。比特币用分布式账本摆脱了“可信第三方”的制约，中本聪称之为“区块链”。

比特币作为加密货币，与传统货币相比有极大的优势：
去中心化：比特币是第一种分布式的虚拟货币，整个网络由用户节点构成，没有中央银行。算法是比特币安全的保证 。
全世界流通：比特币可以在任意一台接入互联网的电脑上管理。交易没有繁琐的手续与额度限制。知道对方比特币地址就可以进行支付。
方便使用：相比于现金和各类贵金属货币，比特币携带和保管的成本几乎为零，也不会出现损耗。

加密货币生态开始的过程似乎很慢，但近两年整个生态的进展越来越快。这从微软、戴尔和 Dish 等科技巨头均开始接受以加密货币作为支付方式可见端倪。这是一种革命性的解决方案，加密货币的影响已经惠及众多企业和行业，而金融和科技行业已经成为加密技术和区块链风暴中的漩涡：

- 金融业

金融机构正研究如何有效地利用其优势：银行正逐渐适应区块链技术，并使用这种技术来进行衍生品甚或棉花的交易。一个由多家银行组成的财团正支持 IBM 创建一项可用来进行跨国交易的区块链技术；澳大利亚股票市场是世界上第一个建基于区块链的股票交易平台。

- 银行业

全球有超过 20 亿人口没有个人银行账户。加密货币账户可让他们转账和接收付款。银行体系不稳定或不存在问题的国家，例如委内瑞拉，已经转向比特币等加密货币

- 电子商务

大型线上零售商已经开始接受比特币或以太币等代币进行支付。Overstock.com、亿客行（Expedia）和 Shopify 等大型企业都接受加密货币作为支付方式。商家和用户都可以更安全、更快捷地完成交易，防止信用卡欺诈，同时无需再担心支付服务供应商以各种理由冻结资金。

我们已经看到加密货币如何以更多人们无法想象的方式改变整个世界。

## 1.2 比特币及竞争币当前面临的问题

自从中本聪发表白皮书以来，比特币一直是作为一种点对点的电子现金而出现，这也是比特币的设计目的。后来，在发展过程中，随着人们逐渐发掘比特币作为价值储存、世界基础货币、全球结算网络、衍生金融体系和全球公证体系等方面的可能性，比特币被赋予了越来越重要的意义，然而，这些目的不可能同时全部实现，由此，由于对比特币未来的经济和政治前景的预期不同，比特币的生态中，开发团队、矿机厂商和矿工之间产生了越来越多的分歧。特别是在扩容之争和算力大战中暴露出来的研发团队中心化的问题，让人们无比担心比特币未来的政治风险。

比特币从来没有停止过分叉，在此前的分叉中，比特币 BTC 在加密货币领域的地位从未收到挑战，但是在 2017 年的加密货币牛市中，由于区块过小导致的网络拥堵问题，比特币的市场份额从早期的 90%以上暴跌至 34%左右，虽然现在又重新恢复至 50%以上，但下一次的上涨周期，BTC 依然存在拥堵问题，未来如何，难以预料。在大多数人看来，给区块扩容原本是共识，是简单的事情，只是如何扩容产生了争论。然而，看似简单的问题后续引发的争论、矛盾、甚至于战争，给 BTC 的发展蒙上了一层阴影，由扩容这一小问题引发出了种种问题，导致 BTC 以及众多基于算力 POW 的分叉币的未来从清晰逐渐变得模糊。另外，矿机巨头公司面临的上市波折，以及 Asic 矿机的滞销，导致众多数字货币的潜在用户通过挖矿方式进入数字货币市场的通道被斩断，从而使得资金进入数字货币市场的通道主要变成了购买 USDT，我们认为，这一方式对于数字货币市场未来的发展不利。同时，基于 GPU 和 FPGA 挖矿的众多数字货币例如 ETH、GRIN 等，由于 GPU 昂贵的价格，始终难以成为主流大众的选择，而 POS 方式的数字货币，并不能承担锚定现实世界资产的重任，也难以将更多的资金引入数字货币领域。

因此，我们创造了涡轮网络,我们希望，让矿工和新入场者通过硬盘挖矿的方式获得数字货币，其目的是让新的用户更多通过更低的门槛参与挖矿获得数字货币，并由此进入数字货币市场。

### 1.2.1 比特币生态的共识分裂问题

BTC 在过去两年分叉出了 BCH 和 BSV，其中过程曲折离奇，我们在这里不过多叙述。其中，BCH 的来源是由于比特币的 Core 团队拒绝弹性容量方案，而选择隔离见证和闪电网络方案的方式进行扩容，对于这一选择，其未来有可能造成比特币竞争力下降的情况下，由 ABC 团队和比特大陆发起的一次分叉。这一分叉产生了 BCH，在这一分叉之后，BTC 将逐渐走向全球结算网络和价值储备货币而非世界基础货币，并且，闪电网络将成为小额用户交易的主要通道，而 BTC 主链将成为一个结算网络，由此，BTC 主链的交易将逐渐减少。但是，随着小额交易的减少，矿工的收益也会逐渐减少，BTC 的安全程度有可能会降低，未来 BTC 的前景取决于 Core 团队。而 Core 团队对于密码朋克文化的坚持，坚持小区块和隐身于人群的乌托邦主义，将使得 BTC 有可能远离主流大众的需求。因此，开发团队中心化给 BTC 的前景带来了很大的政治风险，并且制约了生态的进步。

Bitcoin ABC 开发团队于 2017 年 7 月前后开发出 8M 区块容量比特币客户端，得到扩容支持者的支持，于 2017 年 8 月 1 日上线独立于 BTC 网络运行，有了现在的 BCH。此后一年，BCH 开发虽然有 Bitcoin Unlimited，Bitprim，nChain，Bitcrust，ElectrumX，Parity 和 VOLT 等多个团队参与，但主要开发工作和开发主导权在于 ABC 团队。

BCH 是一个坚持探索更新路线的数字货币，引入了包括逐块难度规则 DAA、二层智能合约虫洞等技术，但是由于 BSV 的分裂，给 BCH 的发展带来了难以预料的危险。算力大战爆发于 ABC 在 BCH 官网 Bitcoincash.org 发布 0.18 版升级之后，CSW 提出强烈批评，并且发布 BSV 版本，提出取消 ABC 的 0.18 版本升级，全网采纳 BSV 版本。BSV 由于 CSW 的支持，以及引入类似宗教发展的方式，将理性主义和个人崇拜引入其中，极大的分裂了 BCH 社区的共识，BSV 未来如何尚且不论，但是 BSV 削弱了 BCH 原本极大的发展潜力，导致全球世界基础货币，全球电子现金这一巨大的经济愿景的实现又变得困难。

从扩张战争开始，BTC、BCH、BSV 三个版本共存，给新的进入数字货币的人们带来了选择困难。而比特币社区的共识分裂，也使得电子现金这一伟大的目标逐渐被偏离。我们希望带来一种新的补充方案，让新的人群以极低的门槛认识和得到数字货币，就像当年 BTC 曾经那样

### 1.2.2 开发团队中心化及开发团队激励问题

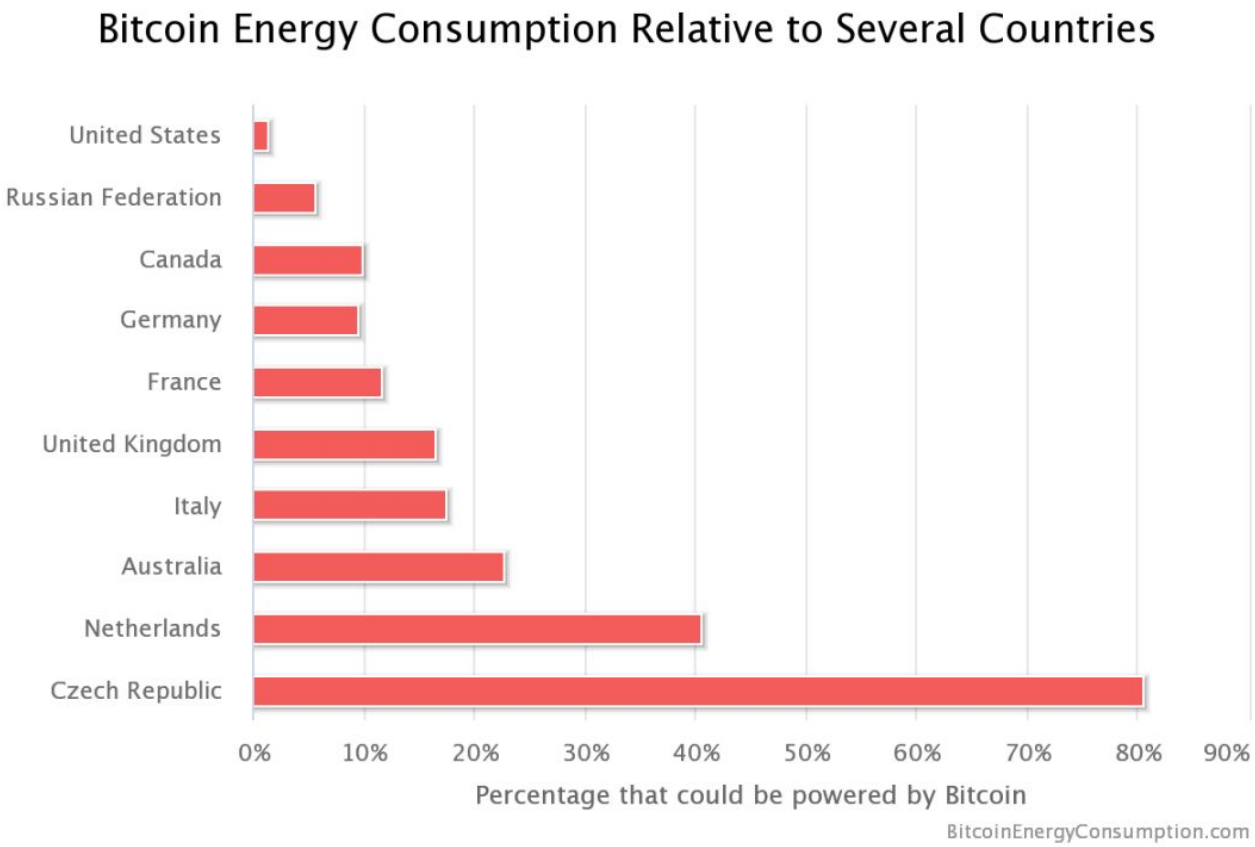
比特币生态的形成和发展，很大程度依赖于早期参与者的创新乐趣和理想主义热情，其中最主要的是开发者和 Geek 群体，然而，随着时间的推移和比特币价格的上涨，随着矿工和矿机厂商得到的巨大利益，开发者群体在比特币发展过程中，并没有直接利益收获。因此，随着比特币核心开发者组成 BlockStream 并开发闪电网络系统，代码审核权限集中化的问题越来越尖锐的暴露出来。

本质上来说，Core 团队对于闪电网络和全球结算网络愿景的不遗余力推动，本身就体现了开发者需要经济激励这一事实。然而，在现有体系下，包括 Core 团队和 ABC 团队，都无法直接从数字货币的发展中获得收益，这将带来极大的问题。

### 1.2.3 电力资源浪费带来的政府公关问题

加密货币的矿工们对他们挖矿时所耗费的具体电量三缄其口，但每个人在被问到时都宣称，这一行为的耗电量十分巨大。

据加密货币消息机构 digiconomist.net 发布的加密货币能源消耗指数显示，目前比特币挖矿每年消耗的电力大约在 42.15~54.11 太瓦时（TWh，1 太瓦时为 1 亿度电）之间，这一数字与各国的年耗电量相比，大概占美国全年用电量的 1.2%、俄罗斯的 5.1%、法国的 10.4%、英国的 14.7%、意大利的 15.7%、澳大利亚的 20.4%、荷兰的 36.4%、捷克的 72.2%。随着新矿工不断加入网络、挖矿难度逐步增加，这个数字会逐年攀升。甚至还有预测称，按照现在的耗电增速计算，到了 2024 年，虚拟货币挖矿耗电量就会占据全球所有的发电量。




这很糟糕。这意味着比特币每年相当于排放了 2000 吨的二氧化碳，这是对地球气候以及任何享受海岸、森林，不会受到蚊虫叮咬死亡威胁的人赤裸裸的的藐视。我们从另一种隐喻的角度来看，比特币 P2P 网络基本上就是一个分布式的超级人工智能，它正在把宇宙所有的能量（也就是物质）都变成比特币。

那么，我们真的会因为比特币挖矿而最终无电可用吗？

当前，世界上各国政府已经注意到了比特币的资源损耗趋势，中国发改委出台政策，将比特币挖矿作为落后产能要加以淘汰，4 月 8 日，国家发改委在官方网站上公布了一份名为《产业结构调整指导目录（2019 年本， 征求意见稿）》的文件，旨在鼓励、限制或淘汰各类产业，优化产业结构。其中在文件附件《产业结构调整指导目录》中列出了需要鼓励或淘汰的各类产业目录，其中在淘汰类产业目录中，出现了虚拟货币“挖矿”活动这一表述，文件还特别解释道，这是一种比特币等虚拟货币的生产过程。在文件分类中，挖矿活动属于“落后生产工艺装备”，淘汰期限为立即淘汰。值得一提的是，挖矿活动与一些毒害、污染环境的技术/工艺分类在一起。《产业结构调整指导目录（2019 年本， 征求意见稿）》公开征求

意见的时间为 2019 年 4 月 8 日至 2019 年 5 月 7 日，换句话说如果在 5 月 7 日前没有人对淘汰挖矿产业提出意见的话，挖矿活动无疑要被国家淘汰。

在这种背景下，以硬盘容量作为密码共识算法基础的 PoST 更适合作为一个基础的共识算法，来产生新的数字货币。

### 1.2.4 算力集中化带来的进入门槛问题

比特币的 POW 共识机制没有窍门。SHA-256 算法除了暴力破解以外别无他法。这意味着计算机要不停地运算，让风扇不停地转来冷却超热、超载的处理器。

而这就是平权主义瓦解的地方，算力集中化的矿池开始逐渐出现。

一开始的时候，加密货币极客可以在自己的家用计算机上用标准 CPU 跑挖矿软件。后来大家首先意识到 GPU（图像处理单元）要比老旧的 CPU 更适合进行哈希运算。仅仅几年后大家开始定制 FPGA（现场可编程门阵列）芯片，购买套件然后针对挖矿加以定制。再后来大家偏好的是 ASICs（专用集成电路），按照比特币算法来定制，并且部署到专门的数据中心里面。

按照过去一年出块统计看，世界前五大矿池已占全网 62.6%的算力，前十大矿池已占全网 86.3%的算力，个人挖矿已几乎不可能获得出块奖励。

当前，全球持有数字货币的人群只占总人口的很小一部分，越来越多的人正在逐渐的接收和了解数字货币，然而，比特币过高的进入门槛会将这些人挡在数字货币的大门之外。我们希望，通过涡轮网络的出现，将解决这一问题。

### 1.2.5 网络中心化

在比特币区块链这个区中心化的网络中，算力即是权力。

2018 年 11 月，比特币的分叉币比特币现金因社区意见不一致再次进行分叉，根据 Forl.lol 的统计数据，BCH 的整体算力哈希值从 11 月 10 日到 11 月 17 日期间从 9.54％上升到 15.43％，同时，BTC 的算力哈希值在那些日子里下降了 7％，从 90.46％下降到 84.57％。最终结果是由比特大陆为代表的 BitcoinABC 取得了这场胜利，BitcoinABC 在关键时刻利用 Bitcoin.com 矿池 4000P 的算力控制了全网 51％以上的算力。

这场算力大战表明，只需要有足够集中的算力和一点点贪婪之心，就可以操纵比特币网络。而这，正是与中本聪去中心化点对点的初心背道而驰的。

在涡轮网络的设计中，基于硬盘容量的共识，将使得整个密码共识过程更为分散，而且，无 Asic 的情况下，整个系统的算力将较为平均的分布在各个矿工的手中。

## 1.3 涡轮网络是什么，有哪些优势

涡轮网络项目致力于构建大规模在现实商业社会中应用的加密货币，我们坚信，真正的大规模是人人可参与挖矿，网络维护总成本尽量降低。

因此，我们提出了一种更节能环保、低门槛参与且安全防攻击的加密货币—涡轮网络，能够真正大规模在商业社会中落地应用。

### 1.3.1 超低门槛

PoW 挖矿需要昂贵、专用的 ASIC 钻机或 GPU，与此相比，您只需通过额外的笔记本电脑和外置 HDD 便能进行涡轮网络挖矿，只要能用一个多余桌面电脑和数 TB 的磁盘空间进入挖矿游戏，每天挖几个 VOL 基本不成问题。由于多余的储存空间很常见，硬件便宜，竞争也不那么激烈，更多的人可以参与到 PoST 挖矿中，这意味着网络是更加分散的。

我们认为硬盘挖矿才能真正的降低挖矿门槛，实现家家户户有矿机，人人都参与挖矿的愿景。

当前，普通硬盘 3T 容量的价格在 500 元人民币左右，只需要一台普通个人电脑，即可参与完全基于密码共识过程的涡轮网络的挖矿，这对于初次了解和进入数字货币领域的人来说，是一个非常低的门槛。

### 1.3.2 节能环保

硬盘天然存在耗电低，无热量，无需散热，低噪音，无法被 ASIC 化，购买门槛低的优点，每家部署几十块硬盘角落一丢就行，无需担心巨额的电费支出：

在涡轮网络中，使用 5T 硬盘挖矿平均功耗不到 7W。而比特币 ASIC 矿机耗电约 1350-2000W，而涡轮网络所需硬盘矿机仅耗电 70- 90W。仅为比特币 ASIC 矿机耗电量的 1/20。一台 ASIC 矿机，每年消耗电力约 17520 度，而硬盘矿机仅耗电约 700 度，硬盘矿机不仅耗电量极小，与比特币 ASIC 矿机相比，噪音极小且几乎没有发热量。

未来挖矿收益提高需要升级更大容量的硬盘，旧硬盘可以拿来存放影片、资料、做整列盘等。因此硬盘的残余价值和保值率是非常高的。

### 1.3.3 安全防攻击

时间证明是空间“耕作”的辅助机制。准确地来说，Proof of Time 是可验证延迟算法(Verifiable Delay Algorithm)，它是一种特殊的 Proof of Work，在验证过程中需要花一定的时长，经历特定次数的迭代。每次迭代过程可以加速，但不能跨迭代进行并行运算。同时它还需保证运算结果可验证且具有权威性：任意两个不同节点进行验证，其运算结果都是一致的，且网络中其他节点都可以对其结果进行验证。在此机制下，涡轮网络甚至可以设置，将一个区块 Proof of Time 的运算结果作为下一个区块的 Proof of Space 的运算起点。
有了空间证明和时间证明，每一个区块的产生以空间证明为起点，时间证明为终点，保证一个区块就是一个区块（也就是我们所说的 finalized），每个区块的权值相等，那么攻击者也就无法从孤块入手重写整条链。

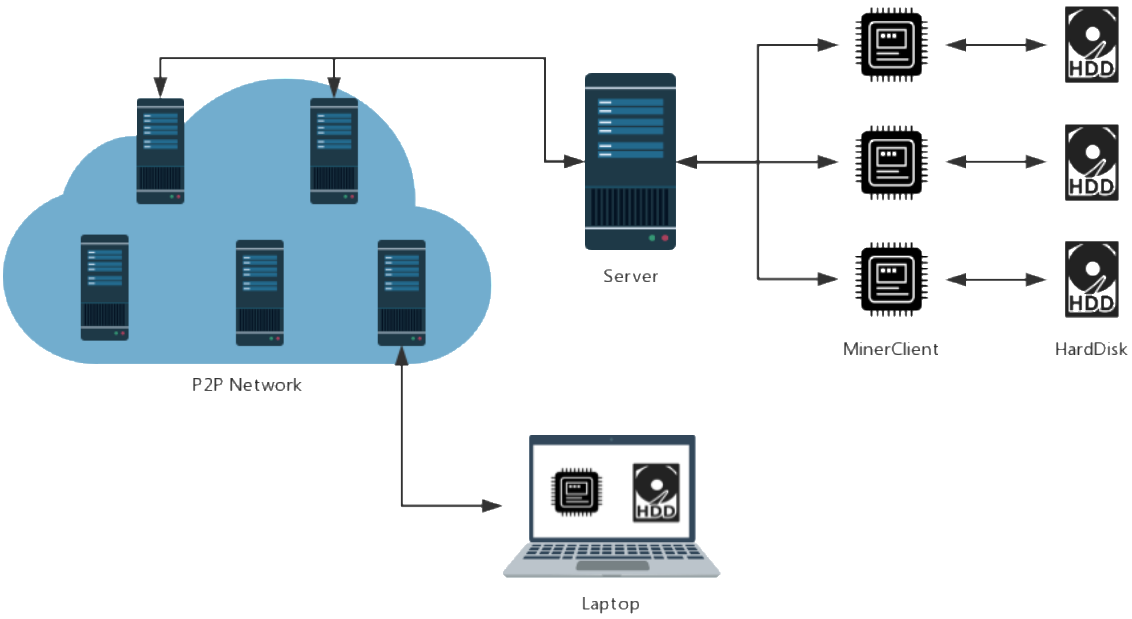
# 二、涡轮网络技术解决方案

涡轮网络采用 PoST（Proof of Space and Time，时空证明）作为共识算法基础。

## 2.1 涡轮网络网络架构

在深入挖矿细节之前，先了解一下涡轮网络的网络架构。

挖矿节点可是个人电脑，或者是矿池。挖矿节点需要连接到涡轮网络上的至少一个节点。挖矿节点需要存储挖矿私钥，可以在本地启动挖矿客户端，也可以连接其他多个挖矿客户端，再由客户端连接硬盘。




## 2.2 共识算法 - 时空证明（PoST）

PoST（时空证明）是在原来空间证明算法的基础上引入了时间维度的算子，利用可延迟验证函数的特性，强制要求矿工在得出候选块数据之后进行一定时间强度的数学运算，再结合可快速验证结果和候选块数据两方面要素进行块选择，从而缓解了空间证明算法中存在的类似自私挖矿、重写攻击等安全方面的漏洞。

PoST 共识算法可以拆分两部分：基于 Plot 的硬盘测绘算法和基于 VDF 的时间证明。

根据不同的硬盘大小，测绘可能需要几天甚至几周的时间。测绘过程中，我们使用称为 Shabal 的非常慢的哈希算法。由于 Shabal 哈希算法计算过程很慢，所以我们必须预先计算它们并将它们存储在硬盘上，这个过程称为硬盘测绘。

测绘过程中会创建相应的测绘文件以占据硬盘空间，测绘文件中会存储大量预先计算过的 Nonces。分配给测绘的硬盘空间越大，您可以存储的 Nonces 就越多。可以存储的 Nonces 越多，就越大概率挖到矿。

当生成一个 Plot 文件的时候，必须要提供一个涡轮网络账户。因为每个账户都不一样，即使 Nonce 的编号相同，每个矿工的 Plot 文件也都不一样。

同时，我们设计了一种基于 VDF 的时间证明算法，其中网络选择一个矿工来创建新区块的概率与当前这个矿工存储容量（S）和全网网络容量（A）的关系成正比。我们设计了算法，使得矿工必须提供存储并通过计算以证明数据被存储之后才能参与共识。

## 2.3 关键技术

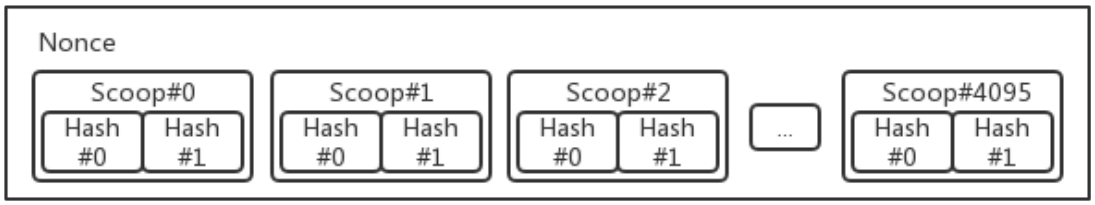
1、基于 Plot 的硬盘测绘算法
矿工首先根据自己的公钥以及 Shabal 算法，在硬盘上生成 Plot 文件，这一过程称为 P 盘。硬盘容量越大，Plot 文件中填充的 Hash 值数量越多，那么产块的概率就越高。
2、基于 VDF 的时间证明算法
矿工监听钱包收到的交易之后，组成一个 block，根据这个 block 的 hash 值，在硬盘上寻找一个最匹配的 Nonce，把 Nonce 转换为 Deadline。并要求矿工在对该 Nonce 进行一定时间强度的数学运算得出 VDF 证明，并且广播此 block 以及 VDF 证明。

下面我们详细介绍硬盘测绘算法、VDF 的时间证明算法的技术细节。

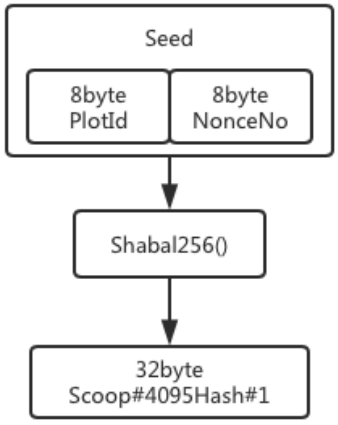
### 2.3.1 基于 Plot 的硬盘测绘算法

存储在硬盘上的预选计算好的 Hash 数据，称为 Plot 文件。P 盘就是在硬盘上生成 Plot 文件的过程。涡轮网络采用的是 256 位的 Shabal 算法，Shabal 是一种计算非常耗时的 Hash 函数，同时也是一种抵御 ASIC 的算法，这个算法比较适合做 PoST 共识。

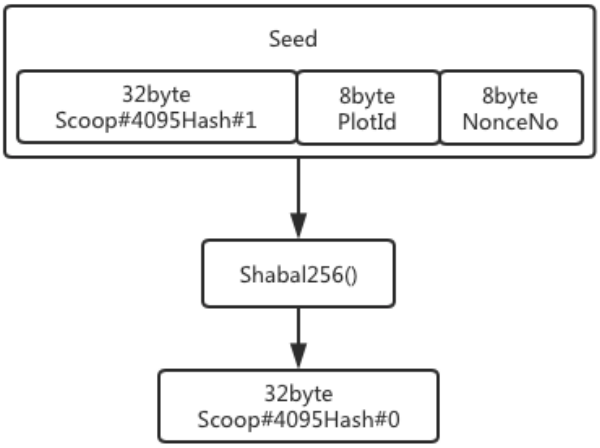
Plot 文件由大量 Nonce 组成。每个 Nonce 的大小是 256K。每个 Nonce 有个唯一的编号，从 0 到 18446744073709551615。每个 Nonce 分成了 4096 段。每一段称之为 Scoop。每个 Scoop 是 64 个字节，包含 2 个 Hash 值。



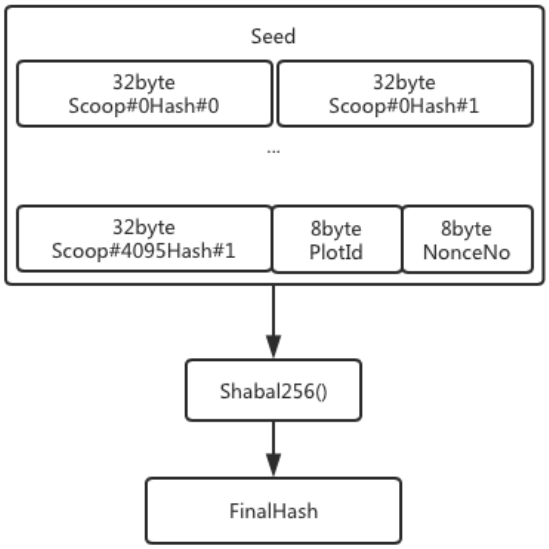

为了创建 nonce，首先制作第一个起始种子，种子包含 Plotter ID 和 nonce number，完成后我们用 shabal256 函数生成第一个哈希值，作为 Scoop#4095Hash#1。




随后把 Scoop#4095Hash#1 附加到起始种子。作为下一轮 shabal256 计算的种子。




随后把 Scoop#4095Hash#0 和 Scoop#4095Hash#1 附加到起始种子。作为下一轮 shabal256 计算的种子。依次类推，最后再生成 FinalHash 值：




再使用 FinalHash 异或其他所有 Hash，存入 Plot 文件中。

### 2.3.2 基于 VDF 的时间证明算法

从最近的 24 个区块计算 Base target。 Base target 用来调整挖矿难度。 Base target 越低，挖矿越难。因为难度的调整，涡轮网络能保证大概每 4 分钟生成一个区块。

加入挖矿池挖矿的话，涉及到奖励发放。 设置奖励发放，其实是告诉 涡轮网络： 1）你的所有收益分配给矿池。 2）矿池能利用你的 Plot 文件发现的 Deadline，并且矿池能生成区块签名。

在挖矿之前，矿工需要抵押一定数量的币，以获得挖矿资格。矿工发送抵押币的交易给全网，全网节点收到抵押币的交易后，在本地区块中记录抵押的信息。

挖矿的第一件事情是，矿工向钱包询问挖矿信息：区块打包签名， base target，下一个区块高度。钱包负责区块打包签名和下一个区块高度，矿工利用这两个信息，经过 Shabal256 算法生成 Generation Hash。

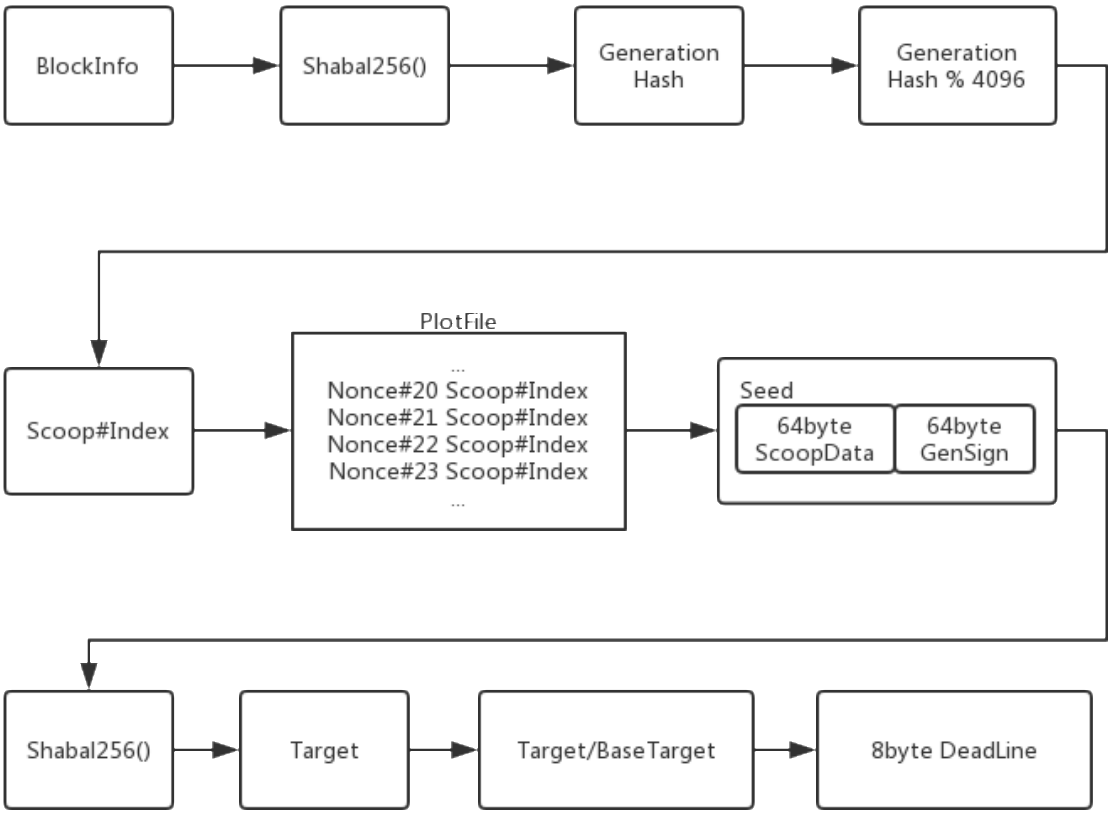
接着，通过模运算（4096），获得 Scoop 数值。

从 Plot 文件中，读取所有的编号为上述结果的 Scoop。对每个 Scoop，合并上区块签名，再经过 Shabal256 运算，得到 Target。 Target 再除以 Base target，获得 8 字节的 Deadline。矿工检查得到的 Deadline 是否足够低。如果足够低，则作为备选的出块数据。

将 Deadline 输入到可验证延迟函数（VDF）中，并在当前时间到 Deadline 这段时间内，执行一定时间百分比的 VDF 计算，得到至少 L 证据链和最终计算结果 R，其中（T、L、R）都是公开可验证的。

矿工根据（T、L、R）计算其是否满足出块要求，如果符合公式要求，且在上一个区块挖出后的 Deadline 的时间后，如果没有其他人在你之前挖出区块，你就能挖出该区块并获得奖励。

矿工提交信息给钱包：账户 ID 以及 Nonce 数值。如果你是独立矿工，你还需要提供密钥。如果是矿池，使用矿池的密钥。




钱包接收到矿工提交的 Deadline 相关信息后，创建相应的 Nonce ，验证 VDF 和 Deadline。如果 VDF 验证成功，钱包查看是否时间满足 Deadline，如果当前系统时间没到 Deadline，就继续等待。如果等待过程中，有其他钱包生成了合法的满足 Deadline 的区块，放弃该区块（因为该区块已经无效）。如果有多个矿工提交 Deadline，钱包选择最低的 Deadline。当 Deadline 的时间满足时，钱包开始生成区块，并广播此区块。

对打包进区块的每一笔交易，钱包都需要检查，比如说，交易的签名是否正确，时间是否正确等等。钱包会计算区块的所有金额以及费用。区块只记录的是交易的 ID 以及所有交易信息的 Sha256 信息。

其他节点钱包收到区块后，逐一验证区块的交易，并给与矿工奖励。在计算奖励时，钱包首先在本地区块中检索抵押信息，如果矿工抵押的币满足经济模型中定义的抵押条件，可以获得全额奖励。

# 三、通证经济模型

区块链平台本质是一个公平的价值流通市场，因此所有的经济行为的成本底层在于交易成本，VOL 币就是交易成本的载体，站在这个角度，VOL 币将用于以下激励用途：

1、记账（挖矿）奖励；

2、在共识中，VOL 的代币持有会影响个别场景下（如节点出块选择）的权重；

3、涡轮网络生态的参与者在底层代码开发、周边工具/服务提供、生态影响力宣传、应用场景落地等方面推动生态进展的奖励。

## 3.1 代币分配

Volume Network Token(VOL):

1.供应总量：100 亿 VOL

2.区块奖励：4000 VOL/块

3.预挖：预挖 3 亿 VOL 进行 IEO,其余 97 亿 VOL 正常挖矿产生

4.矿工挖矿：区块奖励其中 91 亿 VOL 奖励给矿工，即每个区块 3752.5 VOL

5.生态促进：区块奖励其中 6 亿 VOL 给到涡轮生态，即每个区块 247.5 VOL，将用于激励核心代码升级贡献者、矿池服务提供商、矿机厂商、推广团队

## 3.2 矿工收入计算

依据 PoST 共识机制，每个矿工的算力由其可用硬盘存储空间决定，收益由出块成功率和当前区块收益决定：

假设 A 矿工拥有 10T 硬盘，假设此时全网共 10P，且 A 矿工 CPU 处于平均水平，则 A 矿工出块成功的概率为 0.1%，区块奖励为 4000VOL，每 4 分钟出 1 块，一天 360 块

A 矿工平均收益为 360*4000*0.1%=1440 VOL/天

## 3.3 抵押挖矿加成

PoST 共识机制后续将加入 Staking，依据矿工抵押 VOL 币的不同比例，给予不同的挖矿概率提升，质押总额总体无限趋向于全网 100%的 VOL 发行量，随着全网矿工质押代币逐渐增加，单位质押量挖矿概率加成将逐步下降，单位算力质押量与全网质押量相关，计算公式如下:

$$f(x)=\begin{cases} x & x\in[0,1) \\ \frac{199}{999}*x+\frac{800}{999} & x\in[1,1000) \\ \frac{1}{60}*x+\frac{550}{3} & x\in[1000,10000) \\ \frac{1}{853800}*x+\frac{1494100}{4260} & x\in[10000,+\infty) \end{cases}$$

# 四、路线图

2019 年 3 月：核心贡献者团队搭建完成，涡轮网络项目的技术路线与经济模型调研

2019 年 4 月：项目正式启动，白皮书撰写完成

2019 年 Q2: 涡轮网络测试网上线，矿工可提前加入为主网挖矿做准备

2019 年 Q3: 涡轮网络的创世区块被挖出，开启一个创新性的挖矿征程

2019 年 Q4：

1 PoST 共识机制加入 Staking 功能

2 矿池增加反作弊检测功能

2020 年 Q1：GitHub 代码开源，PoST 共识机制引入 VDF 运算

2020 年 Q2-Q3：支持用户在 Lambda 网络与涡轮网络间动态切换，可同时存储文件与进行涡轮网络挖矿

# 五、核心团队

陈志强（Lucien Chen）：

涡轮网络项目创始人，前波场（TRON）联合创始人兼 CTO、第一位波场员工，曾成功主导 TRON 公链实现与应用生态落地。陈志强曾任职网易有道、腾讯、奇虎 360、阿里巴巴等一线互联网企业。在人工智能，推荐系统，分布式系统等有丰富的经验，具有亿级系统架构的开发能力，对高并发系统框架设计有丰富经验，在团队管理、战略规划和业务统筹方面都有丰富的实战经验，同时，陈志强在密码学方面也有着极深的造诣，也是比特币 Bitcoin 的早期支持者和投资者。

孙昊：

涡轮网络产品设计师，前波场（TRON）高级产品经理，前迅雷玩客云（OneCloud）第一位产品经理。在波场期间，先后担任过钱包、区块浏览器、应用商店、开发者工具等多个项目负责人。在迅雷期间，深度参与玩客云项目立项，协助将分布式存储网络与区块链结合起来，并参与玩客币（后改名为链克）的机制设计。熟悉各大主流公链机制和技术方案，对制度模式、经济模型等系统设计有丰富的经验和深刻的理解。

朱锦超：

涡轮网络项目经理， 前波场（TRON）DApp、TRXMarket 负责人。全面策划波场的 DApp 生态，并成功打造波场网络第一款千万级交易量的 DApp。主导完成波场网络第一家去中心化交易所 TRXMarket 从 0 到 1 的封闭研发，有着极强的协调能力、沟通能力和资源整合能力。另外深度参与过多个区块链项目的方案设计和矿机项目的落地。

解晓东：

涡轮网络区块链工程师，前波场（TRON）第二位员工及核心开发者。在波场期间，全程参与过 TRON 代码开源、测试网和主网开发，对区块链架构开发，区块链监控，区块链压力测试等有着丰富的经验。 解晓东也曾任职乐视网服务端开发工程师，构建视频直播业务平台架构，具有千万级用户软件的后端系统架构开发能力，对高并发、微服务等有丰富经验。

Lambda 核心开发团队：

涡轮网络初始代码贡献团队，Lambda 项目核心开发团队，主导 Lambda 项目开发与生态落地。Lambda 是一个安全、可靠、无限可扩展的去中心化存储网络，是对标 Filecoin 的去中心化存储项目。Lambda 核心研发团队核心研发团队均出自 OneAPM，在高峰时期，OneAPM SaaS

系统需要每天处理超过一千亿条的数据。为了满足这个业务需求，Lambda 团队成员开始用开源社区的方式来创建一个分布式的高可用数据库软件。在此过程中，得到了 Apache 基金会、Akka 社区、Druid 社区和 ClickHouse 团队的大力帮助，形成了现在的 Lambda 项目。

# 六、参考文献


[1]https://people.xiph.org/~greg/confidential_values.txt

[2]https://bitcointalk.org/index.php?topic=279249.0

[3] https://cryptonote.org/whitepaper.pdf

[4]https://eprint.iacr.org/2015/1098.pdf

[5]https://download.wpsoftware.net/bitcoin/wizardry/horasyuanmouton-owas.pdf

[6]http://blockstream.com/sidechains.pdf

[7]http://fr.harrypotter.wikia.com/wiki/Sortilège_de_Langue_de_Plomb

[8]https://bitcointalk.org/index.php?topic=281848.0

[9]https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt

[10] SpaceMint: A Cryptocurrency Based on Proofs of Space
Sunoo Park, Albert Kwon, Joel Alwen, Georg Fuchsbauer, Peter Gazi, Krzysztof Pietrzak

[11] Proofs of Space

Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak

[12] Synchronous Byzantine Agreement with Expected O(1) Rounds, Expected O(n2)Communication, and Optimal Resilience

[13] HOP: Hardware makes Obfuscation Practical

[14] Proof of Space from Stacked Expanders

Ling Ren, Srinivas Devadas