# 节能且可扩展的点对点加密货币系统

中文翻译：Disc.top 社区 （欢迎指正）

**概要：**本文提出了一种点对点的加密货币系统，它比 Bitcoin 更节能，保留了 Bitcoin 的大部分特性，比如点对点网络，最小的网络架构和安全性。不同的是 Diskcoin 使用的是条件容量证明（CPOC）一致性算法来减少电力消耗并且降低加密货币生产过程中的进入障碍，这种更加分散，也不会影响其安全性。

## 1. 介绍

Bitcoin 已经证明了点对点的电子现金系统确实可以在不需要信任或不需要中心化造币厂的情况下完成支付处理。然而，Bitcoin 使用的 POW 共识算法导致了算力垄断集中、巨大的能源消耗且进入门槛越来越高。

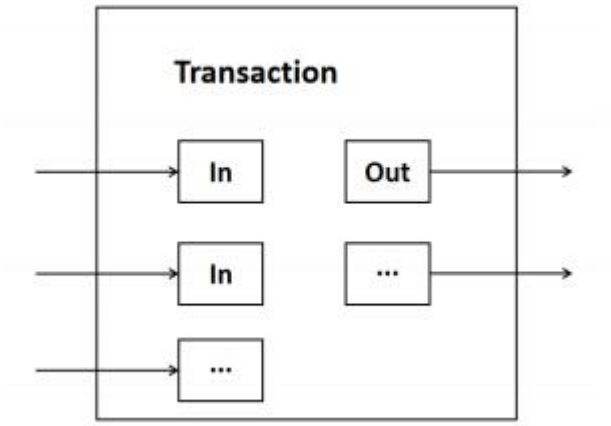
针对这种情况，Burst 团队于 2014 年启动了 POC 共识项目的研发，并获得了很多支持者。该共识算法基于容量证明，降低了挖矿门槛且大大的减少了采矿过程中的能源消耗。然而，Burst 也有其缺点，它缺乏稳定的激励机制，后期进入 Burst 的用户无法获得足够的代币奖励，并最终导致他们对社区参与热情不足。

2018 年，吸收了 BTC 和 Burst 优势的 BHD 诞生了，并创造性的提出一种双重激励方法，在一定程度上解决上述问题。

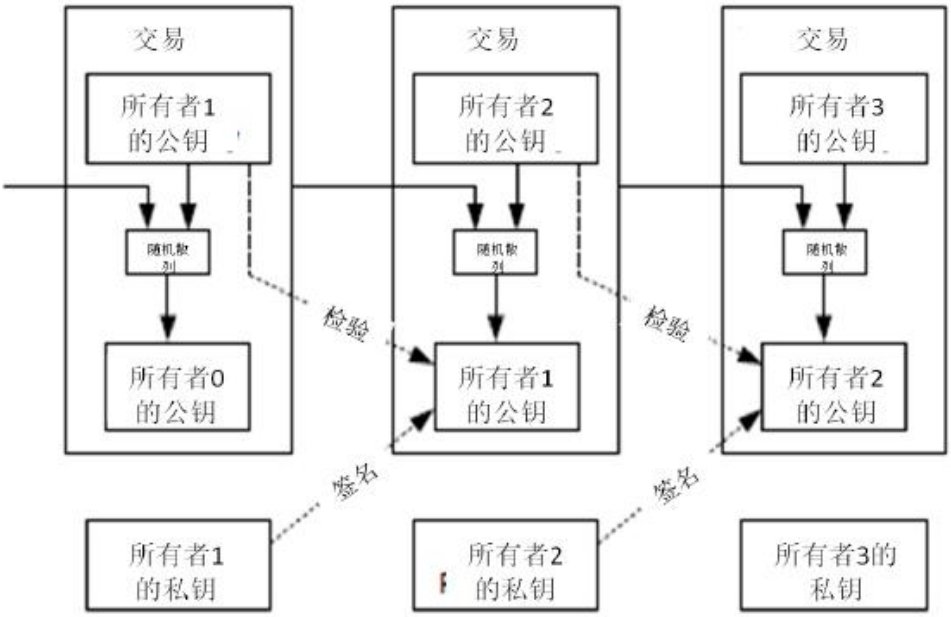
Diskcoin 吸收了上述三者的优点，并参考了 BCH 开发社区的思路，进行了一系列优化。

## 2. 交易

Diskcoin 交易结构与 Bitcoin 相似，称为 UTXO（未使用的交易输出）。



我们定义，一枚数字货币（an electronic coin）是这样的一串数字签名：每一位所有者通过对前一次交易和下一位拥有者的公钥(Public key) 签署一个随机散列的数字签名，并将这个签名附加在这枚数字货币的末尾，数字货币就发送给了下一位所有者。而收款人通过对签名进行检验，就能够验证该链条的所有者。

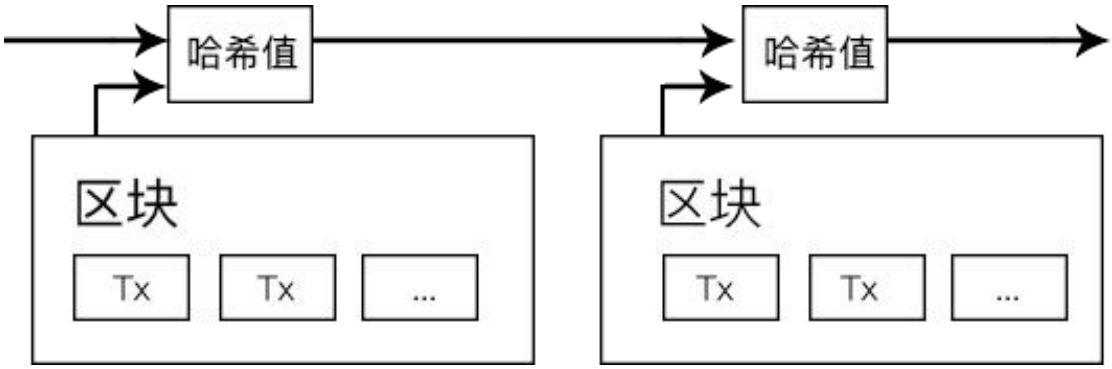



该过程的问题在于，收款人无法核实之前的所有者是否将币双重支付。我们需要一种方法让收款人知道以前的所有者有签名任何先前的交易，为了达到目的，实际上我们需要关注的只是于本交易之前发生的交易，而不需要关注这笔交易发生之后是否会有双重支付的尝试，为了能够确保不漏掉任何交易，唯一的方法就是获悉之前发生过的所有交易。

**时间戳服务**

我们提出一种“时间戳服务器”来引出解决方案。时间戳服务器通过对以区块(block)形式存在的一组数据实施哈希值而加上时间戳，并广泛发布这个哈希值，

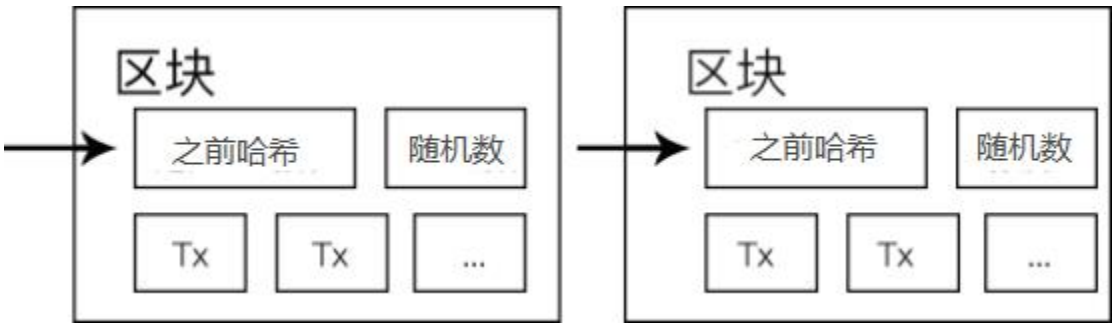
就像报纸和 Usenet（可订阅的新闻组）帖子一样。显然，该时间戳能够证实特定数据必然与某特定时间是的确存在的，因为只有在该时间存在了才能获取相应的哈希值。




每一个时间戳都在它的哈希值里包含了上一个时间戳，从而形成一条链，即每一次新增的时间戳都巩固印证了它们之前的所有记录。

## 3. 区块

与 Bitcoin 相似，用于 Diskcoin 交易的分类账建立并存储在一系列被称为区块链的连接块中。此分类账提供过去交易的永久记录及交易发生的顺序。




DISC 的每个块与 BCH 类似，将尝试尽可能多的交易直到达到 8MB 的限制，所有这些都以包含识别参数的区块头为前缀。区块中的每个交易由公共交易数据表示。 最大区块大小为 8M。 所有区块都包含以下参数：

**Block Header 区块头**

区块头以136字节的格式进行序列化，包括十个字段：version（版本），previous block hash（前一个区块的哈希值），merkle root hash （Merkle 树的根哈希值），timestamp（时间戳），difficulty target（难度目标），nonce(随机数)，generation signature(生成签名)，base target（基本目标），ploter ID，deadline(截止日期)。

区块需要这十个字段，需注意的是，哈希按内部字节顺序排列；其他值都是小端顺序。

**Coinbase Transaction 创币交易**

区块的第一笔交易是特殊的交易被称为“CoinBase 交易”，用于支付矿工的区块。Coinbase 交易是必需的，并且必须收集和支出由区块中包含的交易支付的任何交易费用。

有效的区块有权获得新创建的 diskcoin 值的区块补贴，并且还必须花费在 coinbase 交易中。交易费和区块补贴一起称为区块奖励。如果 coinbase 交易试图花费的价值超过区块奖励可用的价值，则 Coinbase 交易无效。补贴加上费用是最大的 coinbase 支付，但请注意，对于支付较少的 coinbase，它是有效的。

Coinbase 交易包含一个 000000000000000 的输入支出。用于提供签名的字段可以包含最多 100 个字节的任意数据。Coinbase 交易必须伴随区块高度开始以确保没有两个 Coinbase 交易有相同的交易 ID（TXID）。

**Block Serialization 区块序列化**

区块必须以二进制格式序列化，以便在网络上传输。根据当前的 Diskcoin 共识规则，如果 Diskcoin 区块的序列化大小不超过 8MB，则该区块有效。描述的所有字段都计入序列化大小限制。

## 4. CPoC

POC（容量证明）一致性算法源自 Burst，它始于 2014 年，并于 2018 年升级为 POC2。

Diskcoin 使用 CPoC（条件容量证明），它基于 POC2 并添加了抵押机制。 矿工需要放置相应的 Diskcoins 才能获得最大收益。在没有抵押的情况下，矿工可获得 40%的挖矿奖励；如果抵押足够，矿工将获得近 100%的挖矿奖励，剩余的将捐赠给 Diskcoin 基金会，以支付项目开发成本、运营推广成本，以及作为支持相关生态项目的基金。

CPoC 经济模型最早由 BHD 提出，Diskcoin 进行了一系列的优化。其中一个不同之处在于，在 Diskcoin 挖掘中需要抵押的代币的比例不是简单地固定或逐渐减少。相反，对于前 1800 个区块，矿工将以固定比例获得 40%的区块奖励，

并且从区块高度 1801 开始，将激活名为 DES（动态抵押）的算法。DES 将根据挖矿难度，生产的 Diskcoins 数量和 Diskcoin 抵押百分比自动调整放样百分比，以确保整个系统的良好运行。


## 5. 网络

Diskcoin 的网络类似于 Bitcoin。运转这个网络的步骤如下：

1) 新的交易向全网进行广播；

2) 每一个节点都将收到的交易信息纳入一个区块中；

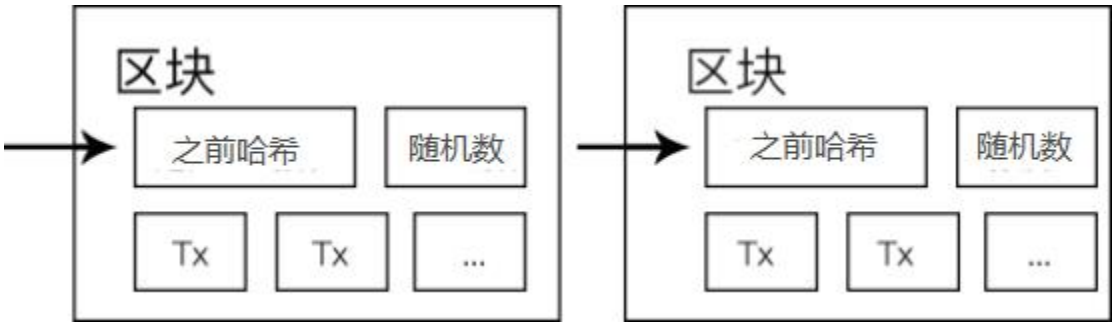
3) 每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明；

4) 当一个节点找到了工作量证明，便向所有节点广播这个区块。

5) 当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性；

6) 其他节点表示他们接受该区块，而表示接受的方法，则是在跟随该区块的末尾，制造新的区块以延长该链条，而将被接受区块的随机散列值视为先于新区快的随机散列值。

节点始终都将最长的链条视为正确的链条，并持续工作和延长它。如果有两个节点同时广播不同版本的新区块，那么其他节点在接收到该区块的时间上将存在先后差别。当此情形，他们将在率先收到的区块基础上进行工作，但也会保留另外一个链条，以防后者变成最长的链条。该僵局（tie）的打破要等到下一个工作量证明被发现，而其中的一条链条被证实为是较长的一条，那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。




实际上不需要抵达全部的节点。只要交易信息能够抵达足够多的节点，那么他们将很快被整合进一个区块中。而区块的广播对被丢弃的信息是具有容错能力的。如果一个节点没有收到某特定区块，那么该节点将会发现自己缺失了某个区块，也就可以提出自己下载该区块的请求。

## 6. 激励

按照惯例，每个区块中的第一笔交易进行特殊化处理，该交易产生一枚由该区块创造者拥有的新的数字货币。这样就增加了节点支持该网络的激励，并在没有中央集权机构发行货币的情况下,提供了一种将数字货币分配到流通领域的一种方法。稳步发行一定数量的新币相当于黄金矿工通过耗费资源将黄金加入流通。在本案例中，耗费的资源是磁盘空间时长和电力。激励也可以由交易费构成。如果某笔交易的输出值小于输入值，则差异部分将作为交易费添加到这笔交易的区块激励中。只要既定数量的数字货币已经进入流通，那么激励机制就可以逐渐转换为完全依靠交易费，那么本货币系统就能够免于通货膨胀。激励系统可有助于鼓励节点保持诚实。如果一个贪婪的攻击者能够调集比所有真实节点加起来还要多的磁盘空间，他将面临抉择：要么将其用于按照规则行事、真实挖矿产生新的数字货币，或者将其用于进行二次支付攻击。那么他就会发现真实挖矿是更有利可图的。因为该规则使得他能够拥有更多的数字货币，而不是破坏这个系统使得其自身财富的有效性受损。

## 7. 分发&挖矿

Diskcoin 的总供应量为 2100 万，每四年减半，通过挖矿分发。

Diskcoin 和 Bitcoin 的比较：

| 参数 | Bitcoin | Diskcoin |
| --- | --- | --- |
| 总供应量 | 21000000 | 21000000 |
| 出块时间 | 10 mins | 4 mins |
| 区块大小 | 1 MB | 8 MB |
| 初始出块奖励 | 50 BTC | 20 DISC |
| 减半周期 | Every 4 years | Every 4 years |

## 8. Block Creation 区块建立（Forging 锻造爆块）

“截止日期”、“基本目标“、”目标值“和”生成签名“，这几个数值来判定哪个矿工有生成区块的资格，哪个矿工有获得爆块奖励的权利，在有冲突时判定哪个区块被是最权威的。

### 8.1 Algorithms and Acronyms 算法&缩略语

#### 8.1.1 Deadline

当你挖掘并处理 plot 文件时，最终会产生称为 deadline 的数值。这些值表示在允许伪造块之前，自上一个块被伪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。

#### 8.1.2 Block reward

如果你足够幸运成功爆块，你将获得 Diskcoin 作为奖励。这被称为块奖励。 每锻造 525000 个区块，区块奖励减少 50%。 最初的奖励是每个区块 20 个 Diskcoins。 如果您在没有任何抵押的情况下进行挖矿，您将获得每区块 40% 的奖励。 你的抵押越多，你的奖励就越接近每区块 100%，其余的将被转移到 Diskcoin 基金会。

### 8.1.3 Base Target

Base Target 是根据每个区块来计算得出的。 该值调整了矿工的难度。 基准目标越低，矿工越难找到低 deadline。 它的调节方式是尽量让 Diskcoin 每个区块平均间隔时间为 4 分钟。

### 8.1.4 Network Difficulty

Network Difficulty(网络难度)，或简称 NetDiff，可以读作一个专用于对 Diskcoin 储存空间的一个估计值。这个值随块而变，以 base target 为基准。

### 8.1.5 Block Height

每个爆块都有一个单独的数字。每个新区块都会在先前区块编号上 + 1。这个编号称为块高度，用于标识唯一的区块。

### 8.1.6 Generation Signature

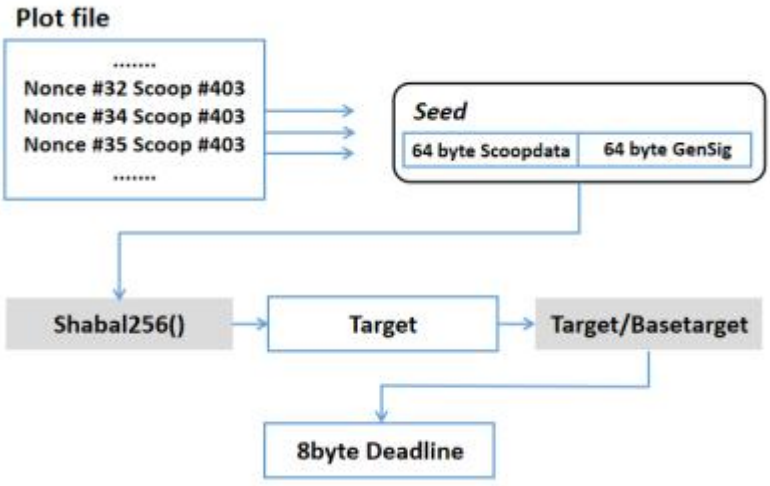
生成签名基于先前的块生成签名和块生成器。 然后矿工使用该值来锻造新块。 生成签名长度为 32 字节。

### 8.2 挖矿过程

矿工从钱包获取挖矿信息。 此信息包含新 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 与前一个区块生成器一起创建生成签名，并通过 shabal256 运行此方法以获取新哈希。矿工现在将采用新的 32 字节生成签名和 8 字节块高度，并将它们放在一起作为 Shabal256 的种子。 生成 Generation hash 的哈希值。

矿工对此哈希进行小规模数学运算，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。它将通过 shabal256 与 new generation signature 一起，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。



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。 在这些检查之后，矿工将信息提交给钱包。

### 8.3 区块锻造过程

#### 8.3.1 处理 Deadline

钱包收到矿工提交的信息，创建对应的 nonce，以便找到并验证自己的 deadline。完成此操作后，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。

#### 8.3.2 锻造

区块有效负载可以具有最大 8MB 的区块限制。

首先，钱包获取从用户或网络收到的所有未经确认的交易。钱包将尝试包含尽可能多的交易，直到达到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。

钱包还将总结所有增加的交易金额和费用。

## 9. 结论

我们在此提出了一种不需要信用中介的电子支付系统。虽然这种系统为所有权提供了强有力的控制，但是不足以防止双重支付。为了解决这个问题，我们提出了一种采用容量证明机制的点对点网络来记录交易的公开信息，只要诚实的节点能够控制大部分磁盘空间的情况下，就能使得攻击者事实上难以改变交易记录。该网络强健之处在于它结构上的简洁性。节点之间的工作大部分是彼此独立的，只需要很少的协同。每个节点都不需要明确自己的身份，由于交易信息的流动路径并无任何要求，所以只需要尽其最大努力传播即可。节点可以随时离开网络，而想重新加入网络也非常容易，因为只需要补充接收离开期间的工作量证明链条即可。节点通过自己的磁盘空间进行投票，表决他们对有效区块的确认，他们不断延长有效的区块链来表达自己的确认，并拒绝在无效的区块之后延长区块以表示拒绝。任何所需的规则和激励措施都可以通过这种共识机制来实现。

联系基金会：

www.diskcoin.org

disc@diskcoin.org

**References:**

1 Satoshi Nakamoto,“Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2009.

2 Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak3, “Proofs of Space”, https://eprint.iacr.org/2013/796.pdf, 2013.

3 Sunoo Park, Albert Kwon , Georg Fuchsbauer , Peter Gaˇzi , Jo¨el Alwen , and Krzysztof Pietrzak, ”SpaceMint: A Cryptocurrency Based on Proofs of Space”, https://eprint.iacr.org/2015/528.pdf, 2015.

4 Seán Gauld, Franz von Ancoina, Robert Stadler,“The Burst Dymaxion”, https://www.burst-coin.org/wpcontent/uploads/2017/07/The-Burst-Dymaxion-1.00.pdf, 2017.

5 4142454647484a4b5054575a,“BitcoinHD: Te Crypto Currency System Based on CpoC”, http://www.btchd.org/BHD-Whitepaper-1.0_en.pdf, 2018.

6 https://www.bitcoincash.org/spec/block.html