BLOCK COLLIDER WHITEPAPER

BLOCK COLLIDER TEAM

创建于: 2017年2月11日

修改于: 2018年1月17日

v0.9.9

目录

1 绪论. 3
1.1 动因 3
1.2 意义 4
1.3 使用案例 5
2 多重链机制 6
2.1 组合链 6
2.2 多重链冲突 9
3 在Collider上挖矿 10
3.1 共识方法：“距离证明” 10
3.2 编辑距离的计算挑战 13
3.3 NRG 16
3.4 交易挖矿 16
4 多重链交易动态 17
4.1 交易基础 18
4.2 标记的代币 19
4.3 承诺 19
4.4 回调函数 20
5 工具创新 23
5.1 区块漫游者 23
5.2 FIX协议（财务信息交换协议） 24
5.3 最优区块路线 24
6 展望未来 25
6.1协议发展考量 25
6.2 愿景与未来的方向 27
参考 27

“程序应该只关注一个目标，并尽可能把它做好。让多个程序能够互相协同工作。”
——道格拉斯·麦克罗伊，Unix pipes的发明者。[*14*]

1 绪论

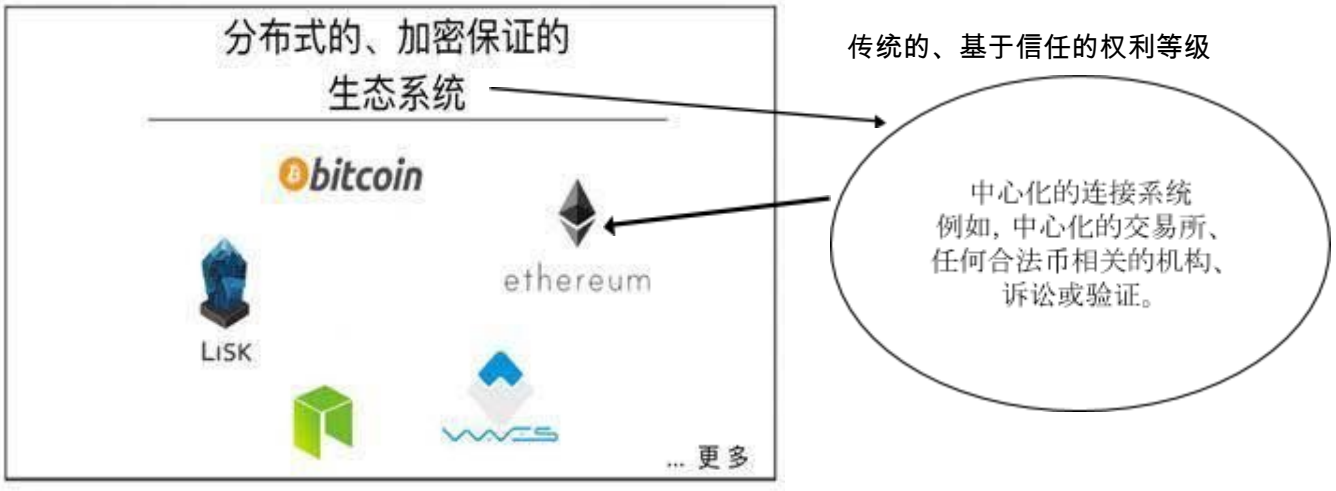
Block Collider多重链是一个由一系列来自于其他区块链上的区块组成的高速分布式账本，它将这些链整合在一起，并实现诸多交叉链功能。通过FIX协议（财务信息交换协议），多重链支持超低延迟的余额更新，并在重复工作及矿工网络速度上进行了创新，因此而产生的多重链在速度和吞吐量上都走在区块链的前沿。

Block Collider多重链仅由去中心化的点对点矿工合作创建——没有中心化的失败节点、神谕节点或验证节点。

1.1 动因

加密货币是“围墙花园”，它们不能被重复使用、触发或执行与其他区块链的交易。如果Alice想执行Bob的智能合约，她只能在Bob部署智能合约的区块链上发送加密货币。这种合作的缺乏扼杀了创新，并大大限制了实际的应用。

打包上块需要的时间和费用使很多重链都不适于大量的交易和贸易。为缓解压力而建立的侧链集中在网络上，并被一少部分矿池或初创公司掌握在手里，从去中心化设计的标准优势中孤立出来，并受到要求不必要的信任的权力结构的支配。



用多重链在链与链之间搭桥就像在建筑物之间修路。假设可以建造一个包含一切的建筑物，但实际上有些建筑物是用于办公的，有些用于居住——只要市民们在不同的时间点想要在在多个建筑中，路就是有价值的。

加密社区的存在证明了跨区块链各种各样的特征——有的链确认速度非常快，有的链有具有表现力的智能合约，有些只有纯粹的通货紧缩与保值性能。只要人们需要的特质是来自于不止一个链的，那么就需要在这些链之间搭建一个多重链。

这就是为什么Unix的设计理念提到：程序应该只关注一个目标，并尽可能把它做好[14]，并且操作系统应该使这些优秀的模块化部件简单高效（例如通过pipes）。Block Collider多重链通过提供链间交流与合作的机会，使这一理念适用于区块链。

1.2 意义

随着Block Collider多重链技术的采用：

- 交易和智能合约的启动或执行可通过其他区块链上的智能合约完成
- 安全的交易可以在没有“见证人”、“可信节点”或任何中心化机构见证下在各个区块链间传输完成
- 链与链之间交易可加速超过被连接上的两个桥接链的个体速度
- 智能合约可以被保证顺利自动执行
- 分布式应用程序开发人员可以模块化地组合来自整个区块链生态系统中特定区块链的独特功能
- 分布式应用程序开发人员可以构建链之间负载平衡工作的性能

所有这些功能都可以在不更改任何桥接链代码的情况下进行——该系统在设计上与现有生态系统兼容。而且，由于其快速的上块确认速度，以及由其架构所提供的大量的去重工作，Block Collider是构建真正去中心化系统的特殊平台。

1.3 使用案例

多重链技术是密码生态系统关键的下一步。以下是Block Collider多重链技术所支持的几个关键使用案例：

去中心化交易所

交易所是现在加密行业的首要瓶颈。在交易所上市是加密资产价格的主要驱动因素，并且交易所的技术问题，对整个行业造成了不利影响。Block Collider的多重链将允许加密货币之间的交换在没有任何中心故障点的情况下执行，这使得区块链的网络内在稳定性特性能够处理这一关键的行业痛点。

跨链智能合约对冲

黑客攻击是密码市场中许多参与者的首要忧虑，因为安全漏洞的存在，之前已有很多案例造成了重大的资本损失。由于Block Collider的多重链可以在某一事件一条链上被触发时，在另一条链上触发另一个行动，所以一个潜在的用途就是提供智能合约对冲。也就是说，当一个区块链上的账户（已知除了对冲提供者以外的任何人都无法访问）被清空时，另一个区块链上的账户将被记入此次损失的金额。 因此，第三方可以以通过数字加密的方式防控安全风险。

自动并有保证的智能合约执行

目前，智能合约的执行需要一个触发事件。一些中心化的服务用于安排触发，例如以太坊闹钟（the Ethereum Alarm Clock[4]）。Block Collider的多重链建立在对未来合约执行可以上链的保证上，所以这项基本功能不需要中心化机构或者第三方来提供服务。

2 多重链机制

2.1 组合链

Block Collider的多重链技术背后的关键架构要素，是将每个桥接链的当前状态封装到Block Collider多重链里。也就是说，在任何时间t，Block Collider正被挖出的（或刚刚被挖出的）最新的区块，指向每一个支持（或“桥接”）链的最新的区块。

背景：标准区块链

在常见的区块链中（包括比特币、以太坊及大多数其他的区块链），一系列块被连城一条链，以避免重复支付和未授权的信用/借记价值。每一个块都是一个组合，包含梅克尔根交易数据（Merkle root transaction data）、某些链上的状态根（a state root）、头部哈希（the header hash）以及一个对前一个块上头部哈希的引用。块本身可以由其头部哈希唯一地引用，所以这个哈希用作缓存键或查询键。

BTC Block Hash #0:
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

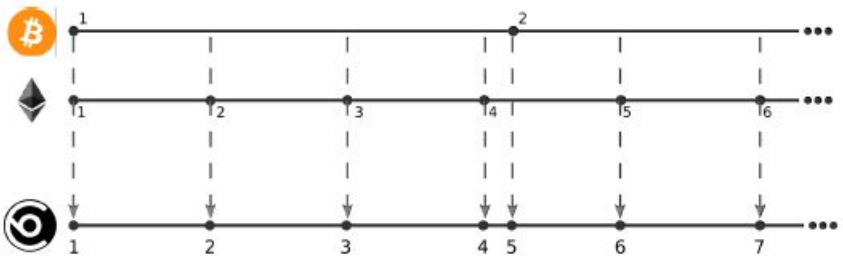
BTC Block Hash #1:
00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

这些哈希中的每个都形成一系列区块头，链中最新被验证的块有最大的“区块号码”并位于链的头部。编写本版本白皮书的时候，根据CoinMarketCap的数据，一共有609个区块链在挖矿，每个都以不同的速度在囊括了数以千计的矿机的网络上发布这些哈希值[8]。

“基本元组”：统一每个桥接链上的最新块

在Block Collider中的区块链，所有块都指向每一个桥接链的头部块——这个元组称为块的“基本元组”。更确切地说，一个Collider区块的基本元组可以指向任何在桥接链上最近被验证过的块，这些块的母块被前一个Collider区块的基本元组所引用。这使得Collider链可以充当所有桥接链的统一链。

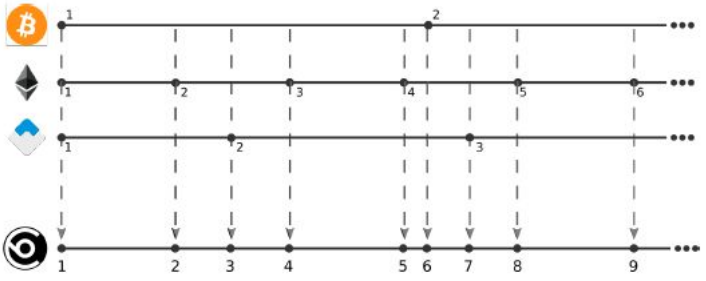
由于基本元组的组合性质，Block Collider的区块链永远比最快的桥接链还快。例如，当下以太坊每30秒产生一个新块，并且比特币每9.2分钟产生一个新块，一个由这两条链组成的Block Collider多重链，将为每个新的组合块形成一个新块，换言之大概是每28秒。参考以下例子（不按固定比例）：



注意在这个例子里，以太坊区块4被重复使用了一次——重复使用区块在基本元组中是一个常见现象，用以确保：

Block Collider block(BTC block 1, ETH block 4) < Block Collider block(BTC block 2, ETH block 4)

在以上例子中，以太坊区块链的ETH区块4是Block Collider是最快的链的一个实例。当我们在混合中再加入第三条链的时候，这个概念会变得更加清晰。在下面的例子中，每隔2个以太坊区块，就会有一个WAVES区块（组合区块）发出：



BTC block	ETH block	WAVES block	Block Collider block
BTC block 1	ETH block 1	WAVES block 1	BC block 1
...	ETH block 2	...	BC block 2
...	...	WAVES block 2	BC block 3
...	ETH block 3	...	BC block 4
...	ETH block 4	...	BC block 5
...	...	WAVES block 3	BC block 6
BTC block 2	...	...	BC block 7
...	ETH block 5	...	BC block 8
...	ETH block 6	...	BC block 9

请记住，这些表格代表了相同的经过时间。注意Block Collider链上区块发布率的增加，总块数从第一个例子中的7块增加到了第二个例子中的9块。另一个区块链（在本例中是Waves）的加入，增加了Block Collider的组合。

出块速率

由于只要任一桥接链发布新块，Block Collider多重链就会发布一个新块，Block Collider的新块数是所有桥接链新块数的总和。这意味着Block Collider多重链的出块速率（即给定间隔内被挖出来的块的数量）大概是所有支持链出块速率的总和（以新的桥接链的块进入Collider多重链所花费的时间为模）

由于区块的间隔（两个块之间的时间T）是速率的倒数（T=1/V）,因此这转换为Block Collider多重链和它的桥接链之间的谐波关系。这意味着，对于Block Collider多重链上任意一个桥接链i：

$$v_{bc} \approx \sum_i v_i$$

$$\frac{1}{T_{BC}} \approx \sum_i \frac{1}{T_i}$$

通过调整计算的难度阈值来挖矿，可以控制附加链的计算复杂程度，以便在等效哈希率下保持等待时间较低，即使速率必然增加。

在之前的例子中，Block Collider编队的第一循环“BTC+ETH”的矿工们在寻找“基本对（base pairs）”，在第二循环“BTC+ETH+WAVES”中矿工们在寻找“基本三元组（base triples）”，以此类推。用这种方法， Collider多重链利用桥接链的变动去创造一个单一的、快速移动的区块链，同时支持可信任区块间发行操作，该操作尤其对于高速交易或操作有用。

由于区块挖掘在所有区块链上的易变性，例如以太坊出块速度在6秒到2分钟之间，比特币一般在5-15分钟之间，对于矿工来说，试图抢先占领组合块以促使Block Collider链的序列支持一条链是几乎不可能的。这大大增加了多重链的阻挠攻击的计算难度，该攻击涉及转移Block Collider上的采矿权。

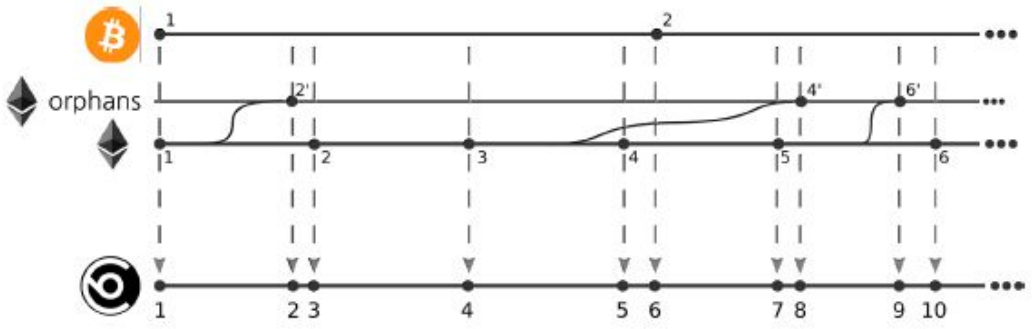
降低出块时间会导致过时率（stale rate）和激励中心化。为了解决这些问题，Block Collider将区块挖矿和交易挖矿分开。这个概念将在下一节中阐述。

2.2 多重链冲突

由于Block Collider上每个区块都来自于支持链，当一个支持链对于哪个区块作为头部存在不同意见时，Block Collider的矿工们将继承其中某些冲突。一个多重链策略是让这些冲突传递给Collider，让Collider区块链分叉来解决，就像它所含的那些链的分裂和解决一样。然而，这会在Collider上产生非常高的过时率，会导致的挖矿奖励产生中断，并且会在确保分叉解决方案上产生额外的问题。

相反，Collider允许任何最近的有效区块包含基本元组（包括孤块和叔块），这些区块的母块之前已经被一个基本元组引用过。“新近度（Recency）”在这里是指区块的深度并不明显低于链上可被观测到的深度最高的区块的深度，新近度的阈值对每个桥接链大小不同（并且由每条连的叔/孤块策略决定）。

为了计算出组合的Collider区块链的速率，孤块允许通过一个因素增加桥接链上相关区块的速率，该因素由该桥接链的孤块率决定。考虑一下例子：一个Block Collider多重链建立在BTC和ETH的链上，并且在ETH的每个偶数块上都有一个深度-1分歧。假设"’"表示一个区块变成孤块，例如“2’”，并且注意深度-1分歧意味着每个区块都有一个非孤块母块，那么我们可以观察到如下情况：



注意，无论是孤还是非孤的ETH块都可能首先出现在Block Collider链上，因为直到分裂被解决，否则无法确认其是孤块还是非孤块。还要注意，受限的后退是被允许的，但对于较低的过时率，这种后退是高度本地化的。最后，注意有效增加的Block Collider出块速率。由于ETH在这个例子里的过时率为⅓，所以它的有效速率增加后为 $(1-\frac{1}{3})^{-1}=1.5$ ，或增加50%。

3 在Collider上挖矿

3.1 共识方法："距离证明"

Block Collider使用中本聪共识机制的一个修改版去决定下一个头部区块。也就是说，它的核心是：

> 节点永远认定最长的一条链是正确的，并且会保持在这条链上工作并延长它。如果两个节点同时广播了下一个区块的不同版本，有些节点会接收其中一个早些，而另一些则会接收另一个早些。在这种情况下，它们均会在它们首先收到广播的那个区块后工作，但同时保存另一个分支以防它变得更长。这个困境将在下一个POW被找到并且其中一个分支变得更长后被打破，那些工作在另一个分支的节点将会转回到更长的那条链上。[15]

Block Collider通过引入一种新的算法对中本聪的共识机制作出修改，用于挖掘新块的计算挑战需求。该算法基于字符串编辑距离，将在本节后面进行介绍。这个挑战将把低于某一特定阈值的哈希值过滤掉的想法归纳为，在参考集合的某个距离内过滤哈希值——即，"距离证明（Proof of Distance）"。

和其他区块链一样，Block Collider的块包括交易、之前块的引用和其他区块链头部的证明形式，以便验证在每个块上完成的工作。然而，不像其他区块链，Block Collider的区块没有固定数量的交易。相反，每个块都有一个"距离平衡（distance balance）"，即该区块的交易距离总和必须低于某值，该值取决于区块矿工拥有的徽章（Emblem）数量。

徽章区块大小奖励

徽章是由Block Collider发布的加密宏观资产。矿工们根据他们拥有的徽章总量得到块

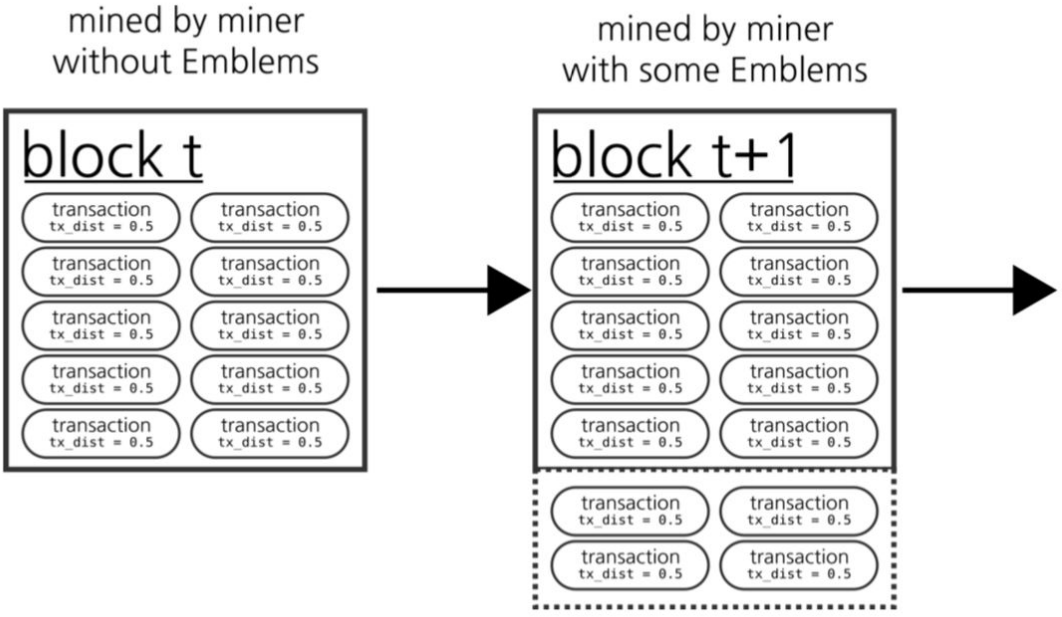
大小奖励，通过被允许在一个区块上额外增加空间打包交易，矿工们可以增加他们收集的手续费。依此类推，想象一个矿车——矿工们可以往矿车上放入的越多，如果发现了黄金，那么他们可能获得奖励就越大。

相比之下，比特币和以太坊的块由于大小限制或gas的限制导致他们只能容纳特定数量的交易。当然一些为避免巨大块带来的网络都塞而做出的限制是必须的，但独断的固定限制显然是等而次之的解决方法。区块大小可变允许了额外的激励，让矿工们更多地投入工作（字面上），从他们的工作中生产更多。此外，固定区块大小使得交易被纯粹地按照交易费排序，相反，Block Collider机制允许更灵活的旁路通过交易的“交易距离”影响优先级。

使用Block Collider多重链，每个块的上限即“交易距离”的最大总和（在本节稍后有更详细的解释），该值包含在每笔交易中。这意味着，如果一个块的最大距离总和为5，那么矿工将可以接受10笔距离为0.5的交易（0.5 X 10 = 5）。因此，距离较小的交易将更有机会以最低交易费进入一个块，所以用户可以提前挖距离以增加以更低交易费打包进块的可能性。否则，一笔交易可能不包含任何工作或显著的交易费，后者能激励矿工在打包交易时投入更多的算力。

不管用户是否预先挖掘他们的交易，徽章会增加矿工的最大距离总和，比如下面的例子，从10扩大到12：

这里的图片需要翻译



徽章不会增加矿工发现下一个块的可能性。无论块中被打包的交易数目多少，都必须

找到相同的距离分数（distance score）。另外，徽章奖励是次线性的（即，徽章所有权的奖励回报递减），这是为了经济平衡、防止中心化（因为徽章的边际效用对于徽章较少的那些效用最高）。

动态难度阈值

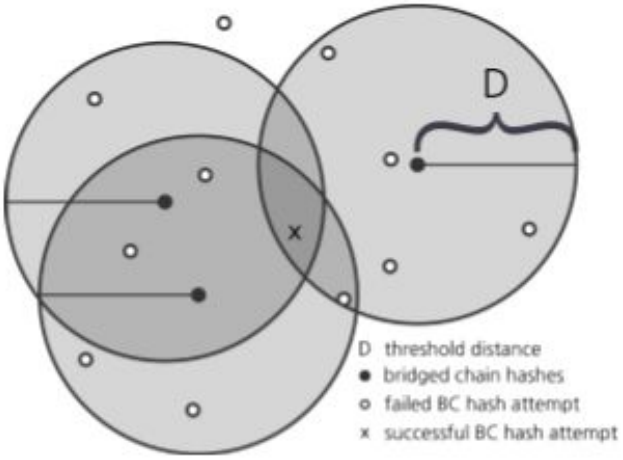
由于Block Collider多重链的块间距取决于其桥接链的块间距，保证块间距是不可能的。相反，对于六个计划中的分叉，每一个都有目标延迟周期，即：5.5秒、3.5秒、1.5秒和0.5秒。这意味着，在最开始，Collider多重链目标是在任意一个桥接链出新块之后大约5.5秒放出一个新块。

难度阈值的挑战是动态调整以适合这些目标窗口。如果观察到同一桥接链又增加了一个新块时还没找到解决方案，阈值会临时性地降低，使Collider的矿工更容易地以快于预期的速度马上跟上区块链的出块速度。除了在桥接链上提供特殊出块率调整外，当编辑距离特别难找时，还可以平滑情况（比如，当桥接链之间的哈希距离中心很远时，可以通过几何类比）

3.2 编辑距离的计算挑战

Collider多重链的挖矿是计算出满足成员链之间的最小编辑距离的哈希值，它的交易以及它之前的区块。Block Collider使用使用余弦相似度算法[17]来评估两个哈希值之间的相似度。

传统的基于哈希值的方法可以被认为是，在被发现的哈希的距离上寻找一个阈值，和一个任意参照点“0”——即，在距离“0”点为D以内的任意哈希值，同时也小于某个哈希阈值（也是D）。编辑距离将这种隐含的距离概念扩展到多维空间。由于编辑距离和更传统的工作量证明的挑战共享这个基本核心，两种方法都可以通过移动距离阈值轻松调整计算难度。



为了完成Block Collider为挖矿而设的计算挑战，矿工必须继续选择随机值并计算：

hash_attempt := hash(miner_public_key + nonce)

当结果满足时（双链情况），挑战可以终止：

RO(hash_attempt, BTC block hash) < D && RO(hash_attempt, ETH block hash) < D

或者等同地：

max(RO(hash_attempt, BTC block hash), RO(hash_attempt, ETH block hash)) < D

一旦矿工发现其结果散列满足约束阈值的随机数，他们将他们的结果广播到网络上，以赢得奖励，其中包括提交给该区块的交易中分配的一些费用。每一个Block Collider的块上都包括对前一个块的引用，以及它架构中所有相关区块链的头部状态。

编辑距离	传统工作量证明距离
从选定点测量	从零点开始测量
多维度	同一纬度
阈值可以轻松调整	阈值可以轻松调整

挖矿中的编辑距离：案例

设想一个三条链的Collider多重链。我们将从第三串字符开始，每个字符串表示来自另一个区块链的区块的头部哈希：

BTC: 000000000000000006abfe31e59af9f81b3fc84a1a25a8fdc095e429dc6dffa
ETH: 0x73413ff99013f6007b72e299aee87da63311602ae4dfb1466b254b7c89b8e1bd
NEO: 0b58e3e1980eb79c293ee1d047997c5a7092da8d49813c2407e90f85e0ba1f9e

如果说现在Collider多重链的阈值是0.29。为了在根链上挖掘一个新块，矿工将重复通过一系列字符集、数字或哈希字符串，直到它找到对于所有块来说都低于0.29的哈希值。通过英特尔酷睿i7处理器上的单个网络工作人员，原型矿工在32.6秒内发现了以下解决方案：

Solution: c53a147e80b2ae87c50d62dfdc82501d0405c9734d0daf6197918f182ca6c

在交易挖矿中编辑距离

在交易挖矿中，交易矿工首先必须计算交易数据，然后必须尝试连续的随机值：

hash_target := hash(transaction_data)
hash_attempt := hash(miner_public_key + nonce)

交易编辑距离就是the hash_attempt（以矿工工作为基础）和the hash_target交易ID（TXID）之间的距离：

tx_dist := RO(hash_attempt, hash_target) * byte_size(transaction_data)

每个区块最多只能包含一定数量的交易距离（tx_dist），该数量由挖出块的矿工拥有的徽章总数决定。挖掘交易的矿工为了更大机会被打包入块，可能会继续挖拥有较短距离的交易，或者直接广播它的结果并等待被打包。拆分交易和区块挖矿的意义已经在之前的章节中已经论述过了。

编辑距离的优势

从直观的角度来看，采用哈希数据将数据转换为不可回收的不同类型的空间——这就是哈希的目的，也称为“陷门函数”。由于Collider链正引用其他哈希去生成自己的哈希，为简单起见没有必要定义额外空间，并且所有操作都可以在没有任何陷门的介入下在哈希之间进行。这种承诺允许对哈希空间进行有趣的几何解释，因为余弦相似性是对称的，并且是一个结构良好的度量。

此外，作为计算编辑距离的副产品，该算法会生成关于如何编辑一个字符串以将其转换为另一个字符串的说明，以便验证编辑距离比计算更简单。这种不对称加剧了哈希空间猜测点中已经存在的不对称性，以找到合适距离内的一个点，这是计算挑战的关键特征。

最后，尽管许多哈希算法被有意设计成仅仅是为了提高计算成本，编辑距离目前还是一个值得被解决的问题。如果在人工构建的计算挑战的内部循环发现优化，则没有取得很大进展。通过将实际有用的问题置于Block Collider的计算挑战的核心位置，任何由此产生的优化解决方案的工作，也将以更好的核心算法的形式让计算机科学社区的其他成员受益。

Edit Distance computational challenge grants...
1. Natural multidimensional, geometric extension of minimizing a hash
2. Increased asymmetry in mining versus validation
3. Altruistically meaningful algorithm to optimize

3.3 NRG (Non-Relational Graphs)

NRG是Block Collider上由挖矿获得的链上货币。它主要用来鼓励实施转账和奖励矿工，和以太坊的“Gas”相似。但不同地方是，Block Collider的手续费也是用NRG支付。

和徽章一样，NRG总数固定，为98亿个。但不同于徽章的是，NRG可以挖矿获得。NRG的挖矿奖励随着时间递减，这样挖矿可以永恒持续下去。

3.4 交易挖矿

交易挖矿者必须提前评估好该笔转账所需的所有计算。然后，交易挖矿者需要找到一个随机值，该值是与转账数据的哈希值的编辑距离，并且包含了该挖矿者的公钥（在上文“编辑距离的计算挑战“中已做深入研讨）。接下来交易挖矿者可以继续按照较低的距离挖矿，但很大几率会很快被下一个区块包含进去，又或者矿工可以简单地将其结果广播出去，等待被其他区块包含。因此，交易挖矿者需要时刻注意着市场上包含转账服务价格的变化，来实现其经济效益最大化。

区块挖矿	交易挖矿
一个区块一个赢家	一个区块多个赢家
用于提高网络的安全	用于提高网络吞吐量
费用用NRG结算	费用用NRG结算
以计算编辑距离为基础	以计算编辑距离为基础
受网络速度和算力影响	受网络速度和数据库性能

如果转账矿工在某笔转账中不想收费（比如，转账矿工自己是交易方之一，又或者，该笔手续费已经通过其他方式支付给矿工了），转账矿工可以继续计算更低的距离数值，这样Collider链内支付的费用可以用算力代替。这样一种带外激励机制，促成了一种新的数字加密货币服务商的出现。因为交易距离较短的转账很有可能不需要手续费就进入下一个区块，新型的服务商可以利用算力来保证交易已经发布出去。

第二，尽管又一种新型的服务商出现了，但还是有很多交易崩溃或者没有被矿工记录。这样就给了没有硬件优势的小矿工机会，他们可以通过搜集那些被忽视的交易（很有可能从小客户身上）并且记录下它们，紧接着他们可以将这些交易广播出去并要求获得转账手续费的一部分。

将交易挖矿从普通区块挖矿分离出来的优势

鉴于其他的区块链正在探索一种策略，即将“叔块”（与当前区块竞争的其他区块）的工作包括在当前区块中，用以从先前的区块中获得一些优势。同样，Block Collider可以通过将交易挖矿和普通区块挖矿分离开来获得类似的优势。当区块矿工为了赢得下一个区块的奖励而竞争稀缺的不动产资源（矿机）时，交易矿工可以在一个不那么拥挤的环境中竞争，这样一来，区块矿工和交易矿工之间的重复工作可以大大减少。所以尽管Block Collider不会将之前加入进来的区块已完成的工作加入进来，但与其他区块链相比，之前区块损失的计算工作量大大地减少了。

区别交易挖矿意味着……

1. 减少重复工作，提高效率
2. 提高网络中心化的难度
3. 给矿工的职业分化提供了机会，用以提高效率

从经济学的角度来讲，我们可以将这种分离想象成分割一个垂直生产的行业—通过允许在两个不同空间的竞争，想要实现中心化必须要在两个不同空间中同时占据优势，这样一来，中心化的风险就减少了。特别是因为交易矿工和区块矿工有很多本质上的区别，比如说在内存，计算类型和结构上，区分开来可以提升效率。

4 多重区块链交易动态

在过去的几年中有若干次试图创造一个去中心化市场的尝试，比如Coinbase，Swap，ShapeShift和ox协议。尽管他们目标明确并且带来了一些新的交易功能创新，但是他们还是严重受限并且依赖于以太坊，特别是受限于以太坊的区块速度。目前，用户想要事项交易，必须等待下一个以太坊区块来确认他们的交易申请，然后对于交易的另一方还要至少等待一个区块的时间来接收并完成交易。如果每一个以太坊区块需要30秒，这样一个交易可能要几分钟才能

完成。当然，我们不可以排除一种不太可能出现的情况，即交易的双方的交易申请在瞬间在当前区块被矿工确认。但另一方面，当下任何一种不是采用以太坊合约的解决方案都是中心化的。

在之前章节介绍的基础上，Block Collider可以支持多种区块链的更加快速的交易，同时保证去中心化的要求。以Block Collider为基础的服务可以为用户的需求提供快速的更新，远远快于充当“桥”的区块链区块产生的频率。这样也能够促进跨链交易而不是代币的置换，代币置换是在中心化的交易所进行，也是以太坊网络里都在采用的一种方式。

4.1 交易基础

Block Collider的交易数据存储在一个分散的哈希表上（DHT），矿工们在这个表上同步节点数据并且检验工作。为了避免使用布隆过滤器（布隆过滤器无法只参考部分范围）而造成区块链延迟，节点的数据只能和DHT进行同步。这样一种储存数据的方法和IFPS所采用的十分类似，用户可以将所有的链上数据或者一部分本地储存下来。因为Collider多重区块链和许多区块链都能同步，它保持着能够短暂进入任一链的权限。这样Block Collider就可以在其他的桥接链中发起能够被立即执行的交易。

区块漫游者（能够发现并且分配区块的进程，将在接下来的章节阐述）是一种广播交易并用于在每一个成员区块链中执行的理想工具。矿工通过操作这些区块漫游者来标记提交的交易并且验证他们的手续费数额。当区块网络扩张之后，我们期望漫游者和矿工的分离会是经济的，这也是为什么这一进程只要求合法的私钥而不是加密钥匙对的原因。

4.2 标记的代币

Block Collider多重链使用标记货币，这是每个桥接链的价值单位。这些标记的货币只在能够支持代币资产或者允许侧链接入的区块链上使用。可以同彩色币进行比较。

例如，在以太坊区块链上，Collider使用一种标记的以太坊(M-ETH)，同时也是一种采用以太坊ERC20标准的代币。每一笔交易中包含这个代币，同时自动也是Block Collider多重链的有效部分。标记的区块将由漫游者进行观察（在下一章会作阐述）并且用于加快对等同步。下面有一个例子，尽管在以太坊中被执行了，仍然可以在Collider多重链中被调用。

0xd12Cd8A37F074e7eAFae618C986Ff825666198bd Transferred: TXID -23 M-ETH
0xBB9bc244D798123fDe783fCc1C72d3Bb8C189413 +22.999 M-ETH

使用字节来确认代币并不是Block Collider的专利，以太坊也使用同样的方式来确认转账的完成。所有的交易和区块都可以被提交到Block Collider中。如果某种代币比该代币所在区块链更有价值，理论上Block Collider上的矿工可以利用字节标记的方法区分，并将代币融合到自己的链上。

4.3 承诺

在Block Collider多重链上，承诺是一种加密的交易并且只能在遇到特殊事件或者其他区块链时才能解密运行。Collider承诺有两个关键：私密数据和比特过滤器。私密数据是一种加密并将在未来特定的时间被执行的交易。私密数据可以是内容，也可以是智能合约。比特过滤器将标记从哪里获取私钥来解密该笔交易。比特过滤器一定要是一个简单的比特层，为桥接链上的交易的哈希值提供一些边界信息。

交易矿工若想挖承诺需要先观察识别桥接链上，知道比特过滤器找到匹配的片段，并且矿工要成功解密私人数据。然后矿工将私人数据解析成一笔交易并且广播这笔交易，并从原始的承诺和桥接链交易（可能）中收取手续费。

承诺的案例

Collider多重区块链上的承诺功能很容易就实现了维基解密的完全去中心化。想象一下，Alice有她雇主的信息并且她认为该信息大众也该知晓，她想确保在无法进行可控发布的情况下，该文件的转储仍然能够实现。Alice可以将一份加密的复印文件放置在线上然后用一个Collider承诺来传播。具体而言，只要某些数据发布到任何桥接链上，Alice就可以设定一个保持沉默的承诺并且使用她的私钥签名。如果她停止了“心跳”广播，该承诺将解密并且发布一个交易，该交易将包含数据的私钥传播到Block Collider和其他所有的桥接链上。

4.4 回调

回调是一种以激励兼容的方式来执行用户之间的跨链交易。它们是“原子互换”的自然发展，它不仅可以交易硬币，还可以根据条件或其他区块链上的交易来执行任意交易。

回调分两个阶段执行;设置和履行。在设置阶段之后的每个行动都通过抵押来提供保证，抵押是由任何一方有机会终止交易来提供的。这样，如果一方违背了这个多阶段议定书，剩下的一方可以获得终止交易一方的抵押品。

在设置阶段，首先回调发起人发布回调交易，该回调交易设立奖金地址，并提供一部分信息以设置抵押地址。奖金地址是资助的，涵盖了矿工在交易过程中的部分费用。抵押地址是保存足够的价值储存的地方，以便如果一方退出交易，另一方可以始终由抵押账户中的金额得到补偿，并且使得退出交易永远不会符合任何一方的最佳经济利益。

为响应发起回调交易者，一个应答者发布了一个响应回调的交易，该回调交易将为一个奖金地址提供资金，并提供部分信息来设置抵押地址。来自双方的信息一起指定了抵押地址，根据交易的当前状态锁定和解锁[16]。

在履行阶段，回调发起人和应答者交替部分（或完全）履行交易。为使协议具有激励作用，每个抵押品所提供的抵押品必须抵消对方的潜在损失。简单来讲，抵押品必须至少与维持激励相容性所转移的东西有一样的价值。但是，通过允许部分履行，抵押品的价值可能比整个交易低k倍，其中k是整个交易分解成的部分件数。通过这种方式，交易执行的速度与任何一方愿意提供的抵押品数量之间有一个天然的折衷。

每个履行阶段都有一个到期计时器。如果定时器在适当的一方进行全部或部分交易之前到期，则认为交易已经失败，并且其抵押品被没收。这一过程是可以个性化定制的，所以除了抵押品被没收外，还会向欺诈方收取一个额外的便捷手续费。

回调案例

假设Bob想用5个以太坊来换0.2个比特币。Bob创造一个回调交易，提供一个奖金地址并资助这个地址用来支付挖矿费用，并提供部分信息来设置一个抵押品地址(C_{Bob})。Bob预计这笔回调交易将分5个阶段，所以他的抵押品地址一定要有至少1个以太坊（因为 5.0 ETH / 5 阶段 = 1.0 ETH）。

假设Alice和Carol都想成为该笔回调交易的另一方。她们同时提交了交易来回应Bob的回调交易，同时资助一个奖金地址和一个抵押品地址(C_{Alice}, C_{Carol})。区块矿工任意选择了一个（比如说选择了Alice）。因为没有被选中，Carol的余额不受影响。

现在设置阶段一定完成了，Bob和Alice进入到执行交易阶段，每个人都有至少1/5的交易价值在他们的抵押地址中。在第一阶段，Bob将五分之一他承诺的数额的以太坊（即1个以太坊）转移到Alice的账户中。他的转账解锁了他的抵押品，并且锁住了Alice抵押地址。然后Alice转移五分之一（即0.04 BTC）到Bob的账户里，这笔转账将解锁Alice的抵押地址并且重新锁住Bob的抵押地址。剩余部分将按照这样继续下去知道交易完成。

如果在任何阶段Bob或Alice没有按预期继续交易，那么在欺诈方的抵押账户中显然已足够为合作方提供赔偿，合作方可以在其他地方完成交易。

	Step	ETH_{Bob}	BTC_{Bob}	ETH_{Alice}	ETC_{Alice}	C_{Bob}	C_{Alice}
1	Bob creates callback transaction	**6 ETH**	**0 BTC**	**0 ETH**	**0.24 BTC**	—	—
2	Alice creates response callback	6 ETH	0 BTC	0 ETH	**0.2 BTC**	0 ETH	**0.04 BTC**
3	Bob funds his collateral	**5 ETH**	0 BTC	0 ETH	0.2 BTC	**1 ETH**	0.04 BTC
4	Bob transfers first piece to Alice	**4 ETH**	0 BTC	**1 ETH**	0.2 BTC	1 ETH*	0.04 BTC
5	Alice transfers first piece to Bob	4 ETH	**0.04 BTC**	1 ETH	**0.16 BTC**	1 ETH	0.04 BTC
6	Alice transfers second piece to Bob	4 ETH	**0.08 BTC**	1 ETH	**0.12 BTC**	1 ETH	0.04 BTC*
7	Bob transfers second piece to Alice	**3 ETH**	0.08 BTC	**2 ETH**	0.12 BTC	1 ETH	0.04 BTC
8	Alice transfers third piece to Bob	3 ETH	**0.12 BTC**	2 ETH	**0.08 BTC**	1 ETH	0.04 BTC*
9	Bob transfers third piece of to Alice	**2 ETH**	0.12 BTC	**3 ETH**	0.08 BTC	1 ETH	0.04 BTC
10	Alice transfers fourth piece of to Bob	2 ETH	**0.16 BTC**	3 ETH	**0.04 BTC**	1 ETH	0.04 BTC*
11	Bob transfers fourth piece of to Alice	**1 ETH**	0.16 BTC	**4 ETH**	0.04 BTC	1 ETH	0.04 BTC
11	Bob transfers final piece of to Alice	**0 ETH**	0.16 BTC	**5 ETH**	0.04 BTC	1 ETH*	0.04 BTC
12	Alice transfers final piece of to Bob	0 ETH	**0.2 BTC**	5 ETH	**0 BTC**	1 ETH*	0.04 BTC*
13	Alice reclaims her collateral	0 ETH	0.2 BTC	5 ETH	**0.04 BTC**	1 ETH*	**0 BTC**
14	Bob reclaims his collateral	**1 ETH**	0.2 BTC	5 ETH	0.04 BTC	**0 ETH**	0 BTC

注意到解锁的抵押地址（*号标记）意味着，如果说下一步交易超时，交易方可以收回抵押品。否则，交易法不可以收回该抵押品。注意到在每一个阶段中，

$$\frac{BTC_{Bob,t}}{BTC_{Bob,\text{total receive planned}}} + \frac{ETH_{Bob,t} + ETH_{\text{Bob unlocked collateral},t}}{ETH_{Bob,\text{total sent planned}}} = 1$$

所以如果Alice在某一阶段停止了交易，Bob并没有比没有收到按比例的交易金额更糟糕，对于爱丽丝也是一样。但是，由于抵押品的锁定性质，交易的任一方都会失去他的抵押品如果他选择停止交易，因此显得更加糟糕。交易所需的抵押越多，交易方会失去更多如果他选择停止交易。

同其他复杂的通信协议一样，用户不需要亲自执行这些步骤。Collider多重区块链将为这些交易提供模块，Block Collider团队将发布简易操作的软件来实现协议的交互。

5 关键性创新

为了开发出超越当前科技水平的技术，Block Collider团队在许多关键领域创造了新的方法和概念。以下是我们精心挑选出的一些。

5.1 区块漫游者

Block Collider是由一个快速分发融合无数其他区块链创造的区块，鼓励真实工作，并通过向新的客户节点（即便是不和Block Collider同步）传播链数据来回馈社区的过程而搭建的公有链。

为了将多种链融合在一起，Block Collider除矿工之外还引入了新的基于网络的工人，称为“区块漫游者”，他们将协助矿工将其他区块链中的区块数据传送回矿工进行处理。从一开始，漫游者就已经自动配置到由Block Collider核心开发人员和开发社区提供的挖掘应用程序中。

举例来说，一个穿越比特币区块链的漫游者持续在链的顶端寻找新的区块，并将区块数据传递给矿工。漫游者寻找节点的方式和传统比特币节点参与网络的方式一样。关键区别在于，区块漫游者可以由100个以上远程的客户端组成来寻找新的区块，而不是在以太坊网络中，只有固定25个。漫游者是为Waves，以太坊和小蚁等成员链设置的。

由于Block Collider的多重链特性，区块矿工受到激励来运行区块漫游者，因此他们不会落后于其他矿工。Block Collider的有效网络包括所有层叠在一起的桥接链网络，因此Block Collider的矿工尤其乐意于将区块传播出去。造假和不广播新区块永远不是一个明智的选择除非该矿工在每一条支链上都保持着最快的出块速度，但这同样不可能实现。

5.2 FIX 协议（Financial Information eXchange）

在发展新的金融科技时，对于低延迟交易订单数据和交易执行的追求为研发高性能计算机和基础网络建设提供了快速发展的机会。FIX协议是这其中最重要的元素之一。该协议是为了国际实时信息（证券和市场信息）交换而创造的。

Block Collider在两方面使用该协议。第一，在挖矿过程中，等待交易（包括费用和tx_dist）以及当前交易包含的价格被FIX协议分发出去。由于将交易数据提交到区块这个过程可以同客户订单的最终结算数据进行比较，需要实时的交易距离来保证有足够的区块空间来储存交易。第二，在挖矿之外，FIX协议也充当着一个为所有连接到Collider的区块链提供整个生态系统数据的角色。通过这样一个系统内置的协议，这些输送的数据可以作为机构投资者的一个简单切入点，来更轻松的了解到定价市场事件，交易量以及时间点数据。

5.3 最优区块路线

在区块链世界中，交易必须发生在不需要第三方公证的安全场景中。但是，在一些情况下（次级），对信任的要求降低可以帮助实现网络功能的最优化。

Block Collider在网络协议中构建了一个额外的概率“信任”层，它根据其他节点对网络状态和自己的信息所作的可验证声明来优化网络流。这样以来，对于节点真实地参与有一个软性激励，在这个参与中，作为一个诚实的用户可以提高节点接收数据块的速度，并在网络中传播自己的区块。

6 展望未来

接下来，Block Collider团队期望着Collider多重链的进化与发展。然而，在一个被设计成本质上不可以被信任的去中心化共识系统中，变革时尤其困难的。以下是我们对将要加入到我们奋发的软件中的更改以及我们打算推进的方向。

6.1 协议发展考量

适用于更多的桥接链

Block Collider旨在能够轻松添加新的区块链，这样每个新的区块链都不会为矿工或者漫游者的工作量产生有影响力的负担。计算难度将保持不变，除了约束条件中的附加条款。例如，从两条区块链增加到三条，区块挖矿临界值将作如下扩展：

```
max(R0(hash_attempt, BTC block hash), R0(hash_attempt, ETH block hash)) < D
```

```
max(R0(hash_attempt, BTC block hash), R0(hash_attempt, ETH block hash),
  R0(hash_attempt, WAVES block hash)) < D
```

再添加一条新的区块链，难度的临界值也会随之调整。

即使桥接链发生了一些灾难性事件，导致它停止输送区块，Block Collider仍将继续运行。Block Collider的设计能够保证交易的安全进行，只要它的数据和两个或更多的区块链进行同步。连续的区块只需要矿工观察和处理最新的和未被处理的区块。也许某一个连接的区块链会停止运行，但直到同化理事会（下文阐述）将其删除，Block Collider只会稍微减慢速度（因为新的被包含区块数量减少）。

计划硬分叉

在发布时，Block Collider将支持六个区块链。第六个区块链并没有在网站中列出，我们将秘密地在私人节点上与其他区块链平行运行，以避免市场因素影响该区块链上的定价。

在主网运行之后的前三点，硬分叉将最多被推到社区六次。这些分叉将包含错误修复和一些与其他区块链兼容性的提高，效率改进和一些超参数的修改（例如在观察到新的区块之后减少目标延迟）。在这些分叉的最后，投票协议将会经过测试并被确认为永久性控制Collider多重链的主要方式。

进化模式和功能开发

一旦最初的六个区块链被部署到Collider多重链中，并且核心协议通过了两年的孵化窗口，则协议切换到“进化模式”。在这个阶段中，有一个三个月的投票期，在此期间新的区块链可以通过简单多数投票进入Collider，而无用的区块链在三分之二多数统一的情况下被投票出局。

除此之外，进化模式允许“构架师投票”。构架师是一个同某一个项目或者建议相关的公开地址。这可以是要求资助开发新功能或者更改以前的功能的请求。要提交某一个项目，发起者必须要提供一定数量的徽章币。

进化模式有三个目的。首先，它给了徽章所有者在一个链条进化中的压注。其次，它允许Collider通过民主程序采用其他区块链的新功能。这也使得Block Collider能够随机应变，无论是政治环境的大规模变化，还是进入新的发币市场。最后，它允许Block Collider创建新的功能并有机地增加社区的参与。类似的计划可以在Dash Development Fund中找到，这可能是这种行为的理想例子[2]。

投票

在紧急情况下，有一个版本标记可以被矿工触发来转移到备用区块链上。版本标记与比特币中使用的标记一样，只支持以为数字，表示事态的严重性。但这不是一个“司马光砸缸”事件，但足以使矿工有能力摆脱对Block Collider产生负面影响、处于失修状态的其他区块链。

6.2 我们的愿景和未来的方向

最近在利用密码学解决协作问题的领域出现了巨大的进步，同时也吸引了大众的注意力。目前尚未发现有任何对未来的社会经济体系有影响的限制。这可能预示着一种新的范例，即个人可以通过加密其个人隐私信息来保证他们在这个世界上的权利和自由。

然而，就像我们所知道的，这个行业中的个体却被强烈地孤立起来。 虽然现存的各个系统授予用户一定程度上的自由，但用户仍然受到限制，并且必须留在单个系统中。 许多解决多重连接问题的解决方案都依赖于中心化，比如通过验证器，这与密码行业的价值和优势基本上是不匹配的。 通过将不同的链条以真正分散的方式整合到Block Collider的多重链中，我们希望通过密码技术实现更高水平的个人选择和自由。 未来，我们Block Collider希望能够融合更多链，并更紧密地整合链上的功能，这样个人可以在加密世界中有最自由的选择。

通过质疑区块链领域的主要假设，比如打破区块和交易挖掘的垂直整合以实现侧链的激励，通过徽章所有权开放区块大小的激励渠道，创新计算挑战的新算法，这些都证明着Block Collider对区块链生态系统的持续快速发展和基础创新有着卓越的贡献。

Block Collider团队致力于用数字加密实现自由，我们希望您能加入到我们的旅程中！

REFERENCES

[1] About the exchange. Shapeshift Website.

[2] Decentralized governance system. Dash Official Website.

[3] Colored Coins protocol specification. Colored Coins Github Repo, 2015.

[4] Ethereum Alarm Clock: It begins, 2015.

[5] Coinbase to launch standalone Ethereum messaging app token. The Coin Telegraph, 2017.

[6] Introducing Swap: A protocol for decentralized peer-to-peer trading on the Ethereum blockchain. Airswap Blog, 2017.

[7] Bitcoin Block Time historical chart. BitInfoCharts, 2018.

[8] Cryptocurrency market capitalizations. CoinMarketCap Website, 2018.

[9] Ethereum Block Time historical chart. BitInfoCharts, 2018.

[10] Benet, J. IPFS - content addressed, versioned, P2P file system. IPFS Website, 2014.

[11] Buterin, V. Toward a 12-second block time. Ethereum Blog, 2014.

[12] Lamoureux, R., and Morstatt, C. Financial Information eXchange protocol specification, 1992.

[13] Lerner, S. D. Even faster block-chains with DECOR protocol. Bitslog Blog, 2014.

[14] McIlroy, M. D., Pinson, E. N., and Tague, B. A. UNIX time-sharing system: Foreword, 1978.

[15] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system, 2008.

[16] Poelstra, A. Using chains for what they’re good for. Scaling Bitcoin Talk, 2017.

[17] "Cosine similarity." Wikipedia. January 26, 2018. AccessedFebruary 10,2018. https://

en.wikipedia.org/wiki/Cosine_similarity.

[18] Sompolinsky, Y., and Zohar, A. Secure high-rate transaction processing in Bitcoin. International Association for Cryptologic Research, 2013.

[19] Warren, W., and Bandeali, A. 0x: An open protocol for decentralized exchange on the Ethereum blockchain. 0x Whitepaper, 2017.