

HYCON 白皮书 v1.3

无限项目

中文版



摘 要	3
引 言	4
现有的区块链技术讨论	5
交易吞吐量	5
延迟	5
大小和带宽	6
安全性	6
浪费资源	6
可用性	6
版本控制、硬分支和多链	7
无限项目-核心目标	8
核心目标 1-市场需求识别	8
核心目标 2-灵活的货币	9
核心目标 3-以用户为中心的平台	9
核心目标 4-灵活创新	9
核心目标 5-安全的去中心化交易所	9
HYCON 技术规范	10
创世区块	10
哈希算法	10
共识机制——SPECTRE 协议	10
投票规则	11
举例说明 SPECTRE 在 DAG 中的应用	11
案例-双重支付	11
与链式区块链	14
无限 SPECTRE 的实现	14
块的“高度”和链接	15
网络基础架构 - Node.js,Typescript	15
序列化-协议缓冲器	16
采矿	16
概述	16

采矿过程的细节	16
Stratum 集成与 XMRig	17
挖矿奖励	17
钱包与账户	17
HYCON 钱包图形用户界面 (GUI)	17
HYCON 钱包	18
HYCON 地址	18
账户与余额	18
同步	18
结 语	19
参考文献	20
附录 A-创世区块	24
讨论	24
HYCON 创世区块的内容	25
附录 B-币的分布与预算分配	26
币的分布	26
预算分配	27

摘要

本白皮书首先概述了无限项目的远景，该项目计划分三个阶段推进：1) HYCON 币，即超连接币；2) 提供可定制企业区块链解决方案的开源无限平台（Infinity Platform）；3) 去中心化加密货币交易平台。HYCON采用SPECTRE协议，在保证安全的同时提高了交易速度，后文重点对这种快速又安全的加密货币HYCON进行了详细分析。本白皮书列举了一些现有加密货币所面临的难题及其自身局限性，并提出了HYCON的解决方案。此外，还介绍了HYCON的技术规范，并简要讨论了SPECTRE及其在无限项目中的实施情况。

引言

“ 现金 ， 作为几千年来人类最通用 、 最长久的发明之一 ， 在未来 15 年左右的时间里 ， 将最终融化为一串 0 和 1 组成的电子流。”——《经济学人》(2007)

在当今手机电子银行的世界里，钱正从有形的纸币和硬币转变为互联网上一串串跳动的数字。在这样的背景下，一种存在于加密字符串代码中、被称为“加密货币”的新的货币形式应运而生。这场数字货币的革命始于2008年，当时还不知名的中本聪 (Satoshi Nakamoto) 发布了比特币白皮书【19】。

现在，几乎每天都有新的加密货币诞生，而它们都有一个共同点：底层技术架构都是——区块链。

区块链本身就是系统上的一个共享公共账簿——从第一个区块问世一直到其结束。这个被称为区块链的账簿由一个个链接在一起的块构成，其中每个区块都包含了一定数量在特定时间被网络验证的交易。

无限项目将推出一种新的加密货币，叫做 HYCON，旨在解决现有区块链技术所面临的一些难题。下面是区块链开发现状的概要，重点介绍了需要解决的问题、无限项目本身的目标、HYCON 如何克服现有的区块链局限以及 HYCON 的技术规范。

现有的区块链技术讨论

为方便讨论，我们将重点说一说迄今为止最为广泛使用和研究的区块链技术应用的代表——比特币和以太坊。

Yli-Huomo 等人的研究成果【31】可以用作检验区块链技术的重要参考。其中总结了近期区块链技术的进展，并指出了区块链系统固有的局限性。虽然他们的研究完全集中在讨论比特币的文献上，但这一发现在我们的讨论中也同样适用，其中一些关键指标来自于Swan【29】。

研究指出了现今区块链系统的七大局限性：

- 交易吞吐量
- 延迟
- 大小和带宽
- 安全性
- 浪费资源
- 可用性
- 版本控制、硬分支和多链

交易吞吐量

典型的区块链（如比特币）需要 10 分钟或更长的时间来确认交易，平均交易速率约为每秒 4 个交易，最高可达每秒 7 个交易。以太坊每秒可以处理 10 个或更多交易，确认时间也比在比特币网络上快十倍。然而，对比 VISA 交易网络，就 1 能清楚看出当前区块链交易吞吐量的局限性：VISA 可在几秒钟内确认交易，平均每秒处理 2000 个交易，每秒交易量最高可达 65000 个【30】。从这些指标可以看出，目前最常用的区块链网络的吞吐量与传统的中心化支付网络（如 Visa）的吞吐量仍然存在着很大的差距。

限制区块链网络交易吞吐量的主要因素是节点间的延迟。虽然人们已经做出一些积极的尝试试图解决这个问题，比如比特币所采用的闪电网络【22】，以及已经作为一个微版本在以太坊区块链上运行的雷登网络【23】等，但就一个可行的长期解决方案各方还没有达成共识。

延迟

如上所述，因为网络的最大交易吞吐量受到节点间延迟的限制，延迟也就成为了区块链的限制因素。如果节点之间存在较高的延迟，矿工则更有可能是 在旧块上进行采矿。在比特币网络上，一个块同步到 50% 的节点的平均时间不到 2 秒，同步到 90% 的节点大约需要 13 秒（截至 2017 年 4 月）【4】。而在以太坊上，同步到 50% 的节点的平均时间小于 1 秒，同步到 90% 的节点大约在 10 秒内【11】。

对于比特币来说，出块时间与网络同步时间的比值很大，说明节点间的延迟尚不构成一个大的限制因素，而以太坊的出块间隔时间较短，在同步上耗费过多时间就会更有问题。不过以太坊采用了基于GHOST协议【27】的算法来激励矿工在最长的链上进行采矿，而不是试图使用由于高延迟和低间隔时间产生的分链。

大小和带宽

在讨论大小和带宽时，必须考虑到两个问题：整个区块链的物理数据的大小，以及通过网络发送的单个块的大小。根据要求，作为一个能挖出新块并与区块链网络交互的完全节点，必须保留一份完整区块链的本地副本。很显然，保留这份副本的存储空间需求是与链上的区块数量成正比的，这就有可能导致中心化，因为如果区块链变得足够大时，将只有少数几个节点有能力进行块的操作【15】。此外，当交易量开始突破可用带宽的限制，再加上块大小的硬性规定，挖矿费用会显著增加，导致核心协议改变以允许更大的交易量，比如改变块的大小，或减少出块的时间。最终，为了升级协议，不得不产生令人讨厌的硬分支。

安全性

工作量证明 (PoW) 区块链的最大卖点就是技术上很难被破解。攻击者若想要修改已经出现在区块链上的块，他们需要重做该块以及后续所有块的工作量证明。为了实现这样的攻击至少需要全网 51% 的哈希算力，因此也称为“51%攻击”。而这显然不太可能发生，因为拥有 51% 的算力所产生的采矿收益远比用来攻击获得的收益大。

第二种攻击方式被称作 Sybil 攻击，攻击者会在网上创建多个虚假身份，然后试图颠覆网络。在一个基于工作量证明 (PoW) 的系统中，比如比特币，你在网络上的影响力取决于你拥有多少哈希算力来计算新的块。而伪装成两名矿工将分割哈希算力。从而变得没有任何优势。

不过在区块链网络上还是有其他可以攻击用户资金的方法。通常，用户通过中心化的交易所来保存他们的密钥，一旦被入侵，攻击者将直接可以访问他们的钱包，以及加密货币。

区块链的另一个安全风险是在实施智能合约时出现的编码错误。成功利用智能合约漏洞完成攻击的著名例子发生在 2016 年 6 月 17 日，俗称“DAO 攻击”，攻击者使用一小段带有缺陷的代码执行了智能合约并获得了价值约五、六千万美金的以太币，并最终导致了以太坊被充满争议的硬分支分成两部分，创造出了以太坊经典 (ETC)【2】。

浪费资源

比特币对电力乃至环境的影响相当大。按照现在的估计，验证一笔交易需要 249 千瓦时的电力，比特币区块链上的矿工每年要消耗 32 太瓦时的电力来持续不断地开采出新的块【6】。虽然相对来说以太坊消耗电力较低，但其能量消耗和对环境的影响仍然很大【7】。实际上，如果你将维持比特币和以太坊正常运作的电力加起来，足以为新西兰提供一年的电力。目前，已经有人试图改变工作量证明 (PoW) 的区块链，取而代之的是权益证明 (PoS)，以太坊就是其最突出的支持者。

可用性

在比特币区块链上，大约每十分钟就会发布交易，但是之后通常需要等待 50 分钟甚至更久来

进行后续对交易的验证。这就类似于在现实世界中，从商店买了东西，却要等待一个小时排队付款。对于一个希望在真实世界中实时应用的程序，这显然是不可接受的。

其次，比特币以及目前可用的大多数加密货币都有着匿名，说得更准确点，假名的概念。区块链上的交易由所有参与者发布共享，并允许算法从用户的“私密”交易中提取交易数据进行校验，所以想要完成相对独立的交易，几乎不可能。再次以现实为例，想象用户给他的母亲汇款，根据交易信息，就可以看到：1) 交易双方现在以及过去发送和接收了多少比特币；2) 交易双方过去任意时间点的余额；以及 3) 用户给其他什么地方发送过或从什么地方接收过资金。所以基本上一旦将交易地址和真实的人链接起来，交易双方就可以看到对方的财务历史，甚至可以知道对方买了什么、赌了什么，甚至是得到过什么“匿名”帮助。正如美国联邦调查局 (FBI) 已多次证明的那样，比特币其实并非真正匿名。对许多用户来说，财务过度透明可能是使用比特币最大的缺点之一。不过，研究人员正研究这一问题的解决方案，比如在以太坊的大都会 (拜占庭) 升级中加入了 zk-SNARKS (零知识证明密码学)【24】(一种建立在 ZCash 上的隐私机制)。

版本控制、硬分支和多链

区块链分支带来的主要问题是共识机制和安全性的缺失。举两个夸张点的例子，一边是一个严重膨胀、占用了地球上 100% 的可用算力的区块链，另一边是 100 个互相竞争的链，各自拥有 1% 的可用算力。

第一个例子中，发动 51% 攻击、改变由真实节点维护的链，需要 51% 的可用算力。然而在第二个例子中，仅仅需要 0.51% 的可用算力就可以攻破任意一条链。

区块链靠着真实节点的综合算力高于恶意攻击的算力来维护共识机制。链一旦产生分支，算力被分配到每个分支上，由于发动恶意攻击所需要的算力减少，攻击就更有可能会成功。

硬分支通常是由于共识机制被破坏导致的另一种不太受欢迎的结果。区块链会因为其生态系统中不同干系人的不同意识形态产生分裂，或分支链。比较著名的例子有因为比特币的扩展问题致使其不能成为一种便捷、廉价的电子现金，从而分裂出比特币现金 (BCH)，以及前面提到过的以太坊经典 (ETC)，是从以太坊区块链不变性的哲学基础分裂而来。不过硬分支并不总是因为意识形态的分裂，很多时候也来自区块链系统核心协议的变更，比如以太坊 2017 年的大都会升级。这样的硬分支形成后，原链上的哈希算力仍然存在。但是在意识形态分裂产生的硬分支中，哈希算力被分给两条互相竞争的链，使得链不再安全，且易受攻击。

无限项目-核心目标

在无限项目的形成过程中，我们提出了下面两个关键问题：

- ✓ 鉴于现有加密货币的局限性，市场的需求是什么？我们怎样提供解决方案？
- ✓ 一种加密货币须具备哪些特性才能被广泛采用并融入到更为广泛的经济中？

考虑到这些问题，我们对现有的区块链进行了彻底分析——包括比特币、以太坊以及各种有前景的代币，揭示了每个项目的优势和弱点。然而很难找到一个能够回答我们最初提出的问题的项目。

因此，无限项目团队开始研究新的适合在现实世界中大规模采用的技术和算法，来帮助我们实现目标。与此同时，我们设计了无限项目的基本框架，并制定了以下 5 个核心目标：

无限项目核心目标

1. 确定加密货币的实际市场需求
2. 开发一种灵活的加密货币
3. 建立以用户为中心的区块链平台
4. 建立可持续创新的生态系统
5. 研究去中心化加密货币交易所的实现办法

核心目标1 - 市场需求识别

尽管目前许多区块链项目获得了主流的关注和认可，但没有一种加密货币在全球范围内渗入到电子商务中。更准确地说，大多数加密货币项目和现实世界解决方案之间依然存在着巨大的鸿沟。目前，仅有一小部分在线商家和少量其他服务接受或采用加密货币，使用比特币或其他任何当前可用的加密货币作为实际使用的电子货币是不可行的。

为了解决这一问题，并加速在真实环境中的应用，开发人员可以与特定领域或社区的专家一起工作，共同推动开发一种成功的、市场友好的货币来服务所有用户。

因此，要回答我们无限项目团队提出的其中一个关键问题——“什么才是市场想要的、以用户为中心的货币？”——我们必须首先定义所需的核心区块链技术，以便从市场和发展的角度找到一个双方都满意的解决方案。于是无限项目团队得出结论，在开发新的加密货币时，第一个关键成功因素（KSF）就是在提供市场需要的实际解决方案的前提基础上来进行设计和实施。

核心目标2 - 灵活的货币

无限项目团队决定放弃现有的许多加密货币项目中单一货币开发的传统观点，并引入一个灵活的、可以包含各种货币模型的实施平台的概念。

这就诞生了我们的“超连接币（HYCON）”。从一开始，HYCON 就被设计成便捷、廉价、可扩展且安全的加密货币，因此可以应用在各种现实世界的场景中。

HYCON 底层的无限区块链，也被设计成一个可互换的模块化结构，这将便于应用或改变底层技术以适应特定的需求。

核心目标3 - 以用户为中心的平台

可以说，比特币引发的范式转变中最重要的部分是推动了一种安全的、去中心化的、以电子方式交换价值的交易方式——它对所有人都开放，实现了脱离银行进行付款这一曾经看似不切实际的想法。

然而，阻碍加密货币得到更广阔应用的一大障碍就是其从概念层次到实际用户交互和体验的陡峭的学习曲线。无限项目通过简洁并便于操作的平台以及直观的钱包和交易平台界面，力图为用户减少这些障碍。我们的最终目标是让更多的人能够参与到区块链的范式转变中来。

核心目标 4 - 灵活创新

在无限项目的发展过程中，最重要的一个考量是如何帮助更多的人、更多的企业、政府、非政府组织等，去利用区块链的力量。因此，我们无限项目团队正在实施“无限平台”。这是一个灵活的区块链平台的概念，是从对现有的各类区块链、平台和加密货币的研究中演变发展而来的。虽然 HYCON 是无限平台的一部分，但它不会是其唯一的组成部分。

我们无限平台研究的目标是创建一个直观易用的平台，且可以通过多种方式实现。用例包括：实现基于 HYCON 的安全加密货币，便捷、廉价、可用作价值交换；建立去中心化的公司账簿，加强信息安全，促进更有效的数据存储和传输；提高证券交易所的加密安全等。使用无限平台构建的潜在使用场景和创新是广阔的，并且有着足够的灵活性为潜在用户提供他们所需的区块链解决方案。

核心目标5-安全的去中心化交易所

无限项目的一个活跃的研究领域是让用户能够以去中心化的方式兑换不同的加密货币。目前的交易所凭借着中心化得以低成本地快速交易加密货币，然而这种中心化要求用户将他们的法定货币和加密货币的资产委托给交易所。

可惜的是，尽管这些交易所经手的交易量巨大，但这些交易所使用的源代码通常不会被公开复审。全球范围内曾发生过多起攻击者从交易所中窃取用户加密货币的事件。交易所集中管理的用户资金和信息时至今日将继续使这些公司成为攻击目标。

作为无限项目未来研究的一部分，我们打算将原子交换的概念整合到 HYCON 中，以使我们的货币成为真正的交换媒介。通过 HYCON，其他多种加密货币都可交易，交易费将分配给维护网络的矿工们。原子交换将允许 HYCON 在等待另一种加密货币的支付证明时被第三方托管持有，从而方便了 HYCON 和其他加密货币之间无需授信的 P2P 交易。

HYCON 技术规范

特征	规范
哈希函数	Cryptonight & Blake 2b
共识协议	SPECTRE
链结构	有向无环图 (简称 DAG)
站间速率	1000ms
采矿方式	工作量证明 (PoW)

创世区块

韩国标准时间2018年1月4日凌晨3:15 (GMT+9) ， HYCON 发布了创世区块，可以在 GitHub (HYCON 存储库的一部分) 上查看【36】。有关创世区块的更多信息，请参阅附录A。

哈希算法

本白皮书在初版时，HYCON 采用 Blake2b 作为系统中唯一的哈希函数，而随着 ASIC 技术的最新发展【38】，Blake2b 逐渐被抗矿机 (ASIC-resistant) 的 Cryptonight 算法所取代，Monero 也采用该算法。Cryptonight 算法工作时使用伪随机内存读写操作，故与标准 ASIC 体系结构不兼容，却使得 CPU 与 GPU 的工作性能差别相对不那么明显。今后，为了防止采掘资源的中央化，计划遵循 Monero 设定的示例，并定期调整哈希算法，以在开采期间维持 ASIC 阻力。[43]

共识机制 ——SPECTRE 协议

比特币的共识机制是中本协议，与之不同，HYCON使用称作SPECTRE的协议作为共识机制【26】。SPECTRE在两组块之间采用投票算法，以成对的方式对它们进行排序，如块x应在块y之前，或块y应在块x之前，使得区块链变为有向无环图（简称 DAG）的形式。完整描述 SPECTRE协议的工作原理超出了本白皮书的范围，下面简单概括一下投票规则。

投票规则

要讨论SPECTRE的投票规则，最好采用可视化的过程表达方式。还应当注意，节点不能投票，也没有必要投票。投票来自块，而DAG结构决定了投票的方式。

SPECTRE 投票过程使用的标准如下：

两个重要术语是“旧” $past(x)$ 和“新” $future(x)$ ，它们分别代表了从 x 可达的块，以及将 x 作为先行块的区块。更具体地说，如果 x 属于 $past(y)$ ，则 y 就是 $future(x)$ 。即：

$$y \in future(x) \Leftrightarrow x \in past(y)$$

此外还要注意到虚拟块，表示为 $virtual(G)$ ，假设整个 DAG 都是它可以到达的块。

当指定一个块 z 为其它的块 x 和 y 进行投票时：

1. 如果 z 的先行块是 x 不是 y （ z 属于 $future(x)$ 但不属于 $future(y)$ ），那么它将投票给 x ；
2. 如果 z 的先行块既是 x 也是 y （ z 同时属于 $future(x)$ 和 $future(y)$ ），投票将取决于与 z 的可达块相同的虚拟块进行递归投票的结果；
3. 如果 z 的先行块既不是 x 也不是 y （ z 既不属于 $future(x)$ 也不属于 $future(y)$ ），投票将取决于以 z 为先行块的大多数块的投票；
4. 如果 z 是一个可以到达整个DAG的虚拟块（ $Virtual(G)$ ），它将遵从DAG的大多数块来决定投票结果；
5. 如果 $z=x$ 或者 $z=y$ ，只要 x 与 y 之间互相不可达，它将投票给自己。

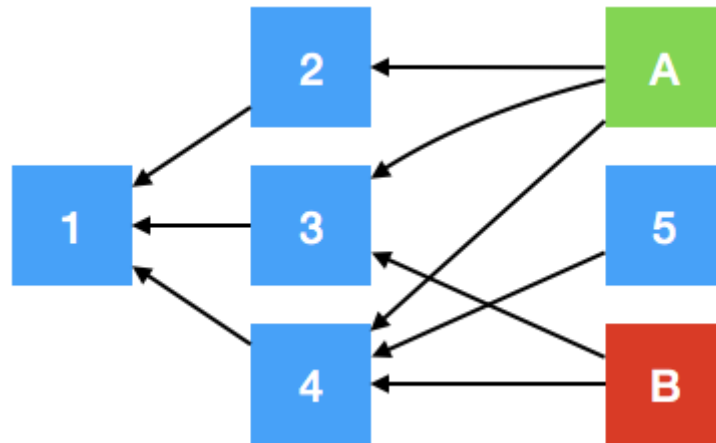
举例说明 SPECTRE 在 DAG 中的应用

为了更好地说明 SPECTRE 的工作原理，最好是通过实例，一步一步讲解投票过程的每个环节。下面的例子直接取自 SPECTRE 白皮书【25】。

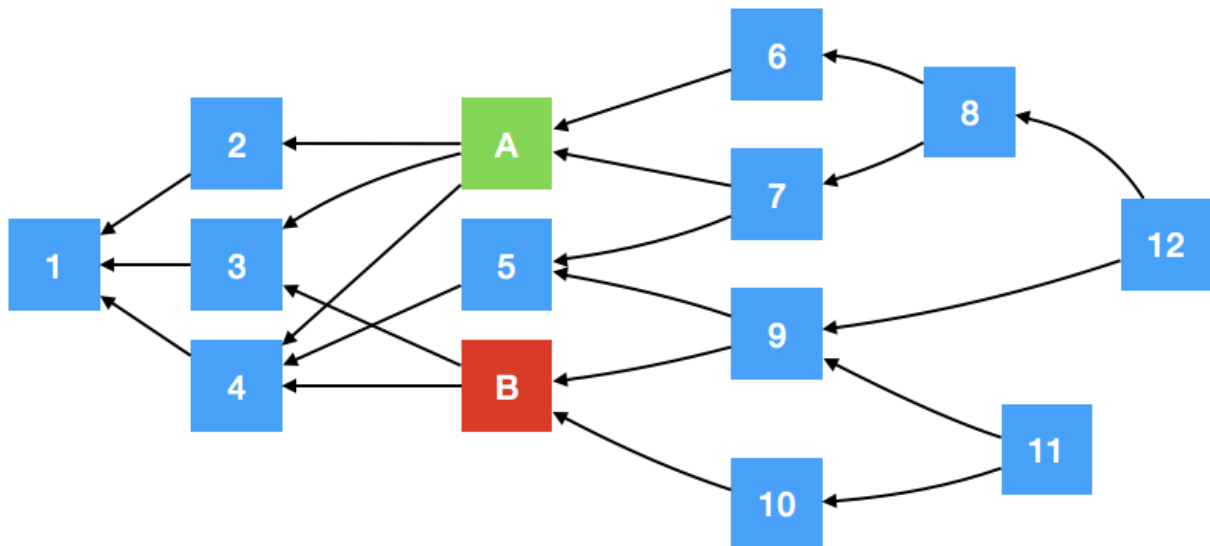
案例-双重支付

举一个最简单的例子，块A包含交易 t_1 ，块B包含与之冲突的交易 t_2 ，这些冲突可能是恶意的，也可能仅仅是由于节点间的延迟导致了交易被发布了两次，这样两个矿工就会收取相同的交易费。根据 DAG 结构的不同，块A和块B可能拥有不同的先行块和后续块，双重支付的解决方式也不尽相同。

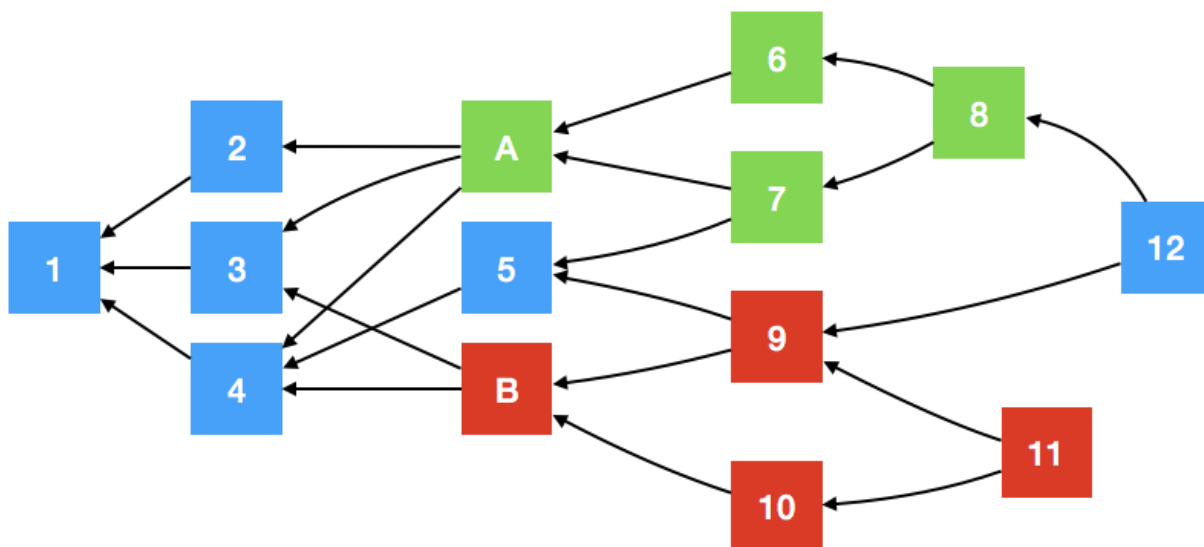
这个例子的初始情况可能如下所示：块A和块B几乎与块5同时添加进来。



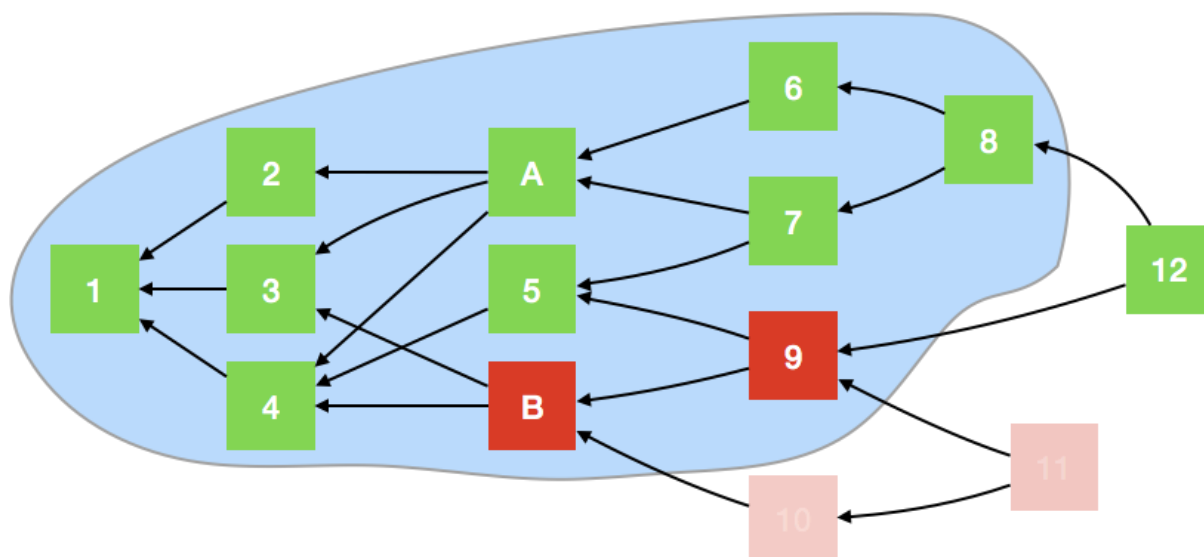
系统在这个阶段并没有意识到双重支付，因为互为冲突的块A和块B之后尚没有新块产出。但是随着DAG的发展，更多的块添加进来，双重支付的问题浮现，这时就需要分析整个DAG结构来决定块A和块B之间哪一个是先行块。



在上面的图中，块12是第一个把块A和块B作为先行块的区块，从而检查到双重支付。根据前面介绍的投票规则，块6、7、8都投票给块A，因为块B不是他们的先行块。同样的道理，块9、10、11都投票给块B。

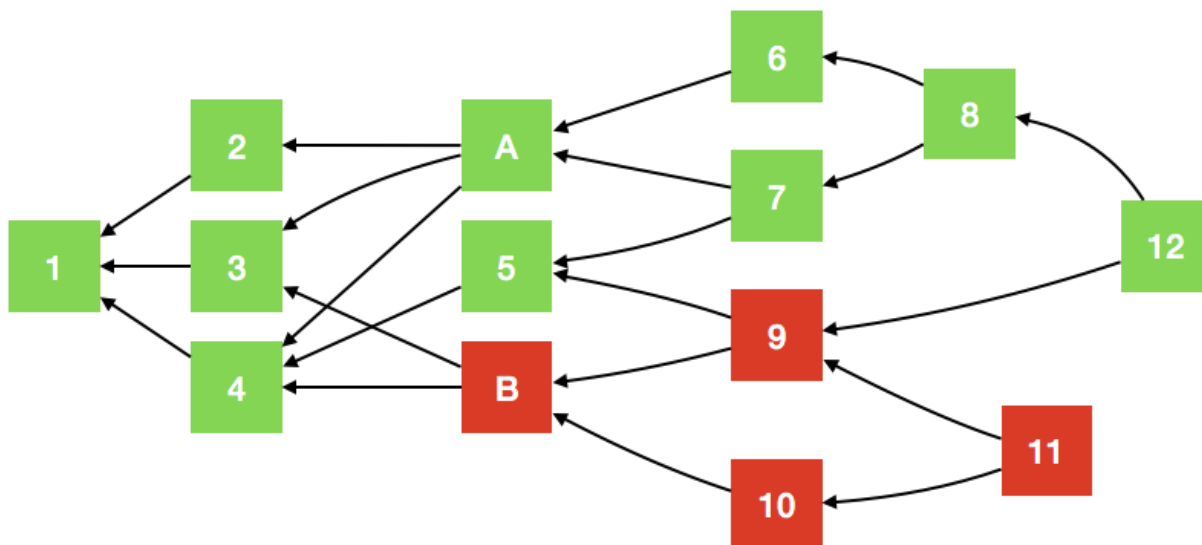


块12的投票是基于对其先行块的递归投票查询。因为块10和块11不是块12的先行块，故它们不包括在块12投票时的查询范围。块12投票时参考的查询范围如下图所示。



其中块1到块5不属于块A和块B的后续块，所以它们的投票结果取决于它们大部分的后续块。在这个递归投票的例子中，块1到块5的后续块更多的会投票给块A，故它们也投票给块A。块12的先行块里有9票投给块A，2票投给块B，所以块12会投票给块A。如果投票数相同，将由块12投出决定性的一票，故所有参与者都赞同块12的投票方式。由于块12只使用它的先行块（past(12)）来决定选票，所以它的投票永远不变。

DAG结构中接下来的投票是基于其他块的后续块。一旦块12的投票结果确认了，块5也会投给块A，因为后续块中有三票投给了块A（块7、8和12），多于块B的两票（块9和块11）。块4的后续块中，块A、5、6、7、8和12投给了块A，块B、9、10和11投给了块B，所以块4也投给块A。同理，块3、2、和1也都会投票给块A。所以，这个投票过程的最终投票统计为，块A得10票，块B得4票。



SPECTRE 一个有趣的特性是，它符合了其他区块链技术中采用的最长链选择模型，特别是在像上面演示的这样简单的例子里。可以看出，从块1经由块A到块12的路径，要比经由块B到块12的路径长，即最长的链路获胜。

与链式区块链

在讨论 HYCON 时，一个常见的问题是 DAG 的结构本身。HYCON 中使用的 DAG 结构采用了 1000 毫秒的区块间隔。在研究如何提高区块链上的吞吐量时，很明显分布式网络上的系统延迟是导致区块链无意分支的限制因素。与其回避这些分支，还不如将其纳入最终的结构中，并承担经常被误解和过分强调的 DAG。

DAG 优于链式区块链的地方是它缩短了出块的时间间隔，从而提高了交易的确认速度。目前存在的链式区块链中，新产出的块通过关联到前一个块的哈希值，被添加在链的末尾。与之形成对比的是，在 DAG 中添加新块时，只关联到当前 DAG 的末端。这样，不同节点都可以同时出块，而不用担心分支链的风险。新块可以有多个先行块，可以同时被添加进来，矿工们也可以仍然获得采矿奖励，而不用担心他们挖出的块成为孤立区块。可能发生的问题是，当节点发布了在其他地方同时发布的交易时，会产生双重支付的问题。使用 SPECTRE 的共识机制将决定哪些交易不该发布，而不是形成孤立区块。

无限 SPECTRE 的实现

SPECTRE 的投票过程是对资源的极大消耗，因此需要谨慎管理它的实施。为了便于开发，我们最初的原型是用 Python 编写的，但是无限 SPECTRE 的最终版本是用 C、C++ 或 Rust 之类的语言编写的，这样就可以完全控制数据结构和内存管理，从而获得更好的性能。

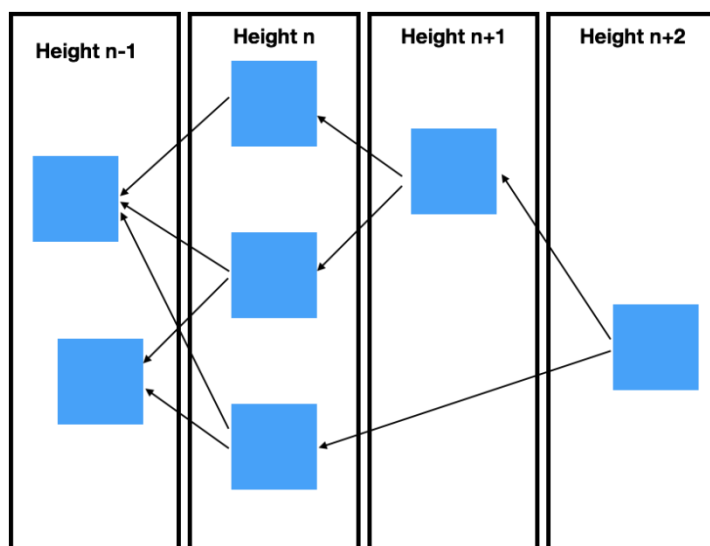
块的“高度”和链接

粗略地看一下 DAG 的结构，可以看出用在比特币或以太坊中的区块高度的传统概念需要进行细微的语义上的修改。在那些具有代表性的区块链中，高度代表了链接在创世区块上的块数。而在 HYCON 中，高度是一个更加笼统的描述，表示当前块在创世区块之上的 DAG 层数。其中的计算非常简单，新块的高度比它最高的父块的高度要高一层。

对于任一新块 B，与其父块 P：

$$Height(B) = \max(Height(p)) + 1; p \in P$$

用图表表示就如同下面提供的示例，新发布的块关联到最高的未被关联的块上，并将高度设置为比最高的关联块多一层。



网络基础架构——Node.js, Typescript

Node.js 对异步操作的内置支持是使用其作为系统架构的好处。Node.js 允许跨平台“事件驱动的非阻塞 I/O”，其中单个组件可以在正常操作流程之外等待运行结果。等待中的组件只在某个事件发生时触发和执行，例如从网络接收到消息或用户输入等，并在等待时允许执行其他代码。【20】

本质上是 JavaScript 的程序会被强制执行类型检查，而 Typescript 的采用就是因为其强大的类型检查功能。使用 JavaScript 的类型化版本，开发团队可以构建一个运用 Node.js 异步性的平台，同时，由于明确定义了类型，调试过程变得更简单。Typescript 文件在运行之前需要被编译，许多语法和类型错误在编译阶段更容易被发现，而不是像很多 JavaScript 程序中常见的那样，在混乱的回调中单步调试来搜索错误。

序列化-协议缓冲器

在区块链系统中，任意时刻都有任意数量的信息在网络上飞来飞去，重要的是节点软件能够以一致且正确的方式解码这些数据。由谷歌开发的协议缓冲器【14】允许在不同的平台上使用一致的消息定义，从而允许使用各种编程语言来开发运行在无限区块链上的节点。由于序列化层与编程语言无关，所以对于跨平台的程序是非常有用的。协议缓冲器还允许向后和向前兼容，使得更新更容易产生软分支，而不是硬分支。它还使第三方软件更加兼容，允许其他开发人员与 HYCON 网络进行交互。

采矿

概述

和大多数现有加密货币相似，采矿出块需要提供工作量证明 (PoW)。矿工根据 DAG 末端的哈希值计算下一个块的哈希值、块中所含交易的梅克尔树 (Merkle) 根，以及一个随机数，该随机数在超过当前难度的哈希值被计算出来之前一直变化。SPECTRE 的创始人认为使用该协议可以做到每秒产出 10 个块，而 HYCON 则以每秒 1 个块作为初始目标。虽然目前的原型采用了工作量证明，但是我们非常清楚比特币和以太坊所需的大量电力，所以正在考虑其他选择。其中一种不太为人知的方法是空间证明 (Proof of Space) 【32】。它要求矿工预先计算并存储大量数据，然后在其中搜索找到满足当前难度的答案。这种方法使用很少的电力，且已被 Burst Coin 和 Space Mint 证明有效。

采矿过程的细节

采矿开始时将对块头的内容进行编码和哈希计算，块头不会因为采矿而改变。这些内容包括与先行块的关联、块中所含交易的梅克尔树 (Merkle) 根、块的难度目标、块的时间戳，以及带有 Trie 前缀的 MPT 树 (Merkle Patricia Tree) 根，代表了该块中的交易结束后的状态。
(更多信息请参见《钱包与账户》一节)

Block Header (for pre hash)
Previous Blocks: Array of 32 Byte Hashes
Merkle Root: 32 Byte Hash
Difficulty: 4 Bytes
Timestamp: 8 Bytes
State Root: 32 Byte Hash

这些数据使用64位版本的Blake2b 进行哈希计算，为GPU和CPU矿工提供一个不变的哈

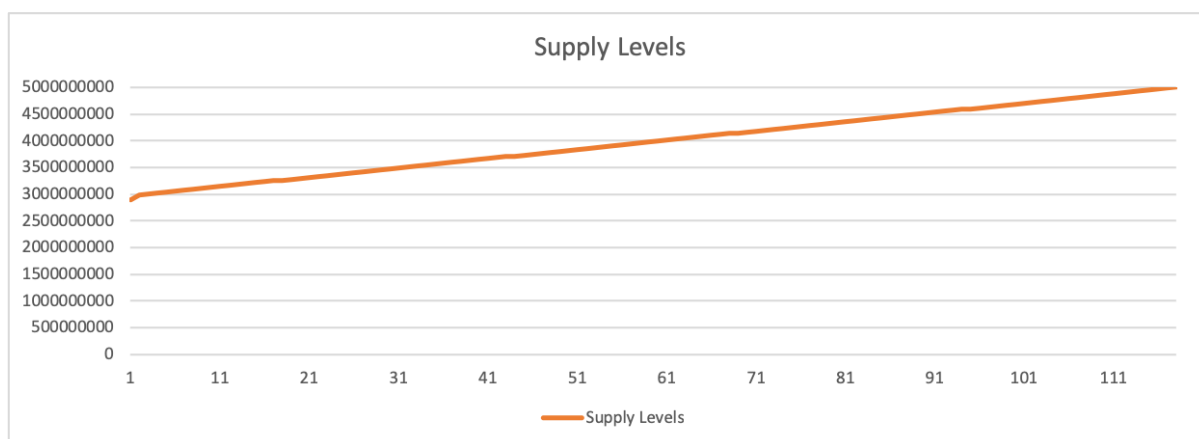
希预处理值。这一步很有必要，特别是对GPU挖矿，因为HYCON的块头通常因为有着多个父块而有着不同长度，而GPU挖矿软件在固定长度的数据结构下效果最好，所以需要进行哈希预处理。然后64位哈希预处理的块头，与一个8字节的随机数合并，该随机数在每次使用Cryptonight进行哈希计算时加1。合并后的数据再进行哈希计算，返回一个能代表整个块的32位哈希值。再将此哈希值与块头中指定的难度比较，如果达到正确的难度临界值，将返回随机数并将其包含在已完成的块头中发布。

Stratum 集成与 XMRig

HYCON使用Stratum协议来完成对使用修改版本的XMRig【39】的GPU 采矿的支持。

挖矿奖励

在成功完成一个新块的工作量证明后，矿工得到HYCON币的奖励。HYCON的采矿过程计划持续相当长的时间。采矿块的奖励最初设定为240HYCON。在GHOST协议更新后，这个值被降低到120HYCON，并降低到当前值即12HYCON/block。



钱包与账户

钱包图形用户界面 (GUI)

运行 HYCON 软件的完整节点可以访问本地托管的网页图形用户界面 (GUI) 进行钱包操作、交易，以及区块链的开采等。该图形用户界面使用 React 编写，支持轻量级的高性能接口。

HYCON 钱包

HYCON 钱包采用行业标准的椭圆曲线加密法进行交易签署，特别是 `secp256k1`【33】，并根据 BIP39【40】的规定使用恢复钱包的助记码，以方便集成第三方钱包供应商。根据 BIP32 和 44 的规定，还为 HD（分层确定性）钱包作出了规定。【41】【42】

HYCON 地址

HYCON 地址是从相关公钥的 32 字节 `blake2b` 散列中分片生成的 20 字节数组。对于人类可读性，地址输出为 `base58` 字符串，前缀为大写 H。字符串的最后 4 个字符用作地址的校验和。校验和分三步计算。首先，计算地址的 32 字节 `blake2b` 哈希。然后，这个哈希输出被编码为 `base58` 字符串。最后，这个字符串中的前 4 个字符被提取并附加到地址的字符串表示形式中。以这种方式使用校验和将意外使用错误输入地址的可能性降至最低。

HYCON 地址由 32 字节 `Blake2b` 解析的结果生成 20 字节。为了加毒地址的第一个文字是以大写 H 开始，`Base 58 string` 的结果构成。`string` 的最后四个字是地址的格子岛。格子岛算为三阶段。先计算地址的 32 字节 `blake2b` 海报价格后，结果以 `Base 58 string` 编码。最后还附上了带有 4 个字的地址。如果用这种方式使用格子岛，可最小化输入地址的可能性。

账户与余额

为了记录 HYCON 用户的支出与余额，需要用到一个会计模型。HYCON 采用的模型是基于以太坊所使用并在其黄皮书【34】中描述的，一种叫做 `Merkle-Patricia Trie`【35】（带 `Trie` 前缀的 `MPT`（`Merkle Patricia Tree`））的数据结构。每个块都包含块中交易结束后的状态。用 `MPT` 树根的 `blake2b` 哈希值表示，代表了所有 HYCON 账户的账户数据。

保存的账户数据包括某个 HYCON 账户的余额，与该账户相关的最近块的关联信息，以及一个随机数，代表该账户发起了多少交易。随机数用于防范重放攻击（`Replay Attack`），而前块的关联信息其实是一种优化，使交易历史查询更快，也使 `SPECTRE` 更容易追踪双重支付问题。

在会计模型中使用 `blake2b` 哈希，因为它允许处理大量交易和余额所需的合适的哈希。

同步

HYCON 将采用块头先行的办法在网络上发起同步。在第一次启动时以及随后的启动之后，节点发送一条信息到相邻的节点请求大量块头，并检查其中是否指明这些块紧随当前存储在本地数据库中最高块之后。收到块头时，如果这些块不在本地数据库中，节点将验证块，并从相邻的节点获取完整的块数据，再次验证通过后将块添加进本地数据库。由于只有父块被添加后，子块才可以添加进数据库，这个过程必然是连续的。

结语

本白皮书始于对现有加密货币局限性的探讨，也是整个无限项目的基础。无限项目的愿景是提供一个便捷、安全、可扩展、以用户为中心的区块链，以及可被广泛采用的加密货币生态系统。结合 SPECTRE 协议和 Black2b 哈希算法，我们提出了一种既安全又方便的新型加密货币。通过采用本白皮书所阐述的办法，HYCON 加密货币与无限项目为全球加密货币环境提供了一种有价值的、差异化的补充。

参考文献

- [1] Blake2.net. (2017). BLAKE2. [online] Available at: <https://blake2.net/> [Accessed 16 Oct. 2017].
- [2] CoinDesk. (2016). Understanding The DAO Attack - CoinDesk. [online] Available at: <https://www.coindesk.com/understanding-dao-hack-journalists/> [Accessed 20 Nov. 2017].
- [3] Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Siler, E.G. and Song, D., 2016, February. On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security (pp. 106-125). Springer Berlin Heidelberg.
- [4] Decker, C. (2017). BitcoinStats. [online] Bitcoinstats.com. Available at: <http://bitcoinstats.com/network/propagation/> [Accessed 10 Nov. 2017].
- [5] Decker, C. and Wattenhofer, R., 2013, September. Information propagation in the bitcoin network. In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on (pp. 1-10). IEEE.
- [6] digiconomist.net. (2017). Bitcoin Energy Consumption. [online] Available at: <https://digiconomist.net/bitcoin-energy-consumption> [Accessed 16 Nov. 2017].
- [7] Digiconomist. (2017). *Ethereum Energy Consumption Index (beta) - Digiconomist*. [online] Available at: <https://digiconomist.net/ethereum-energy-consumption> [Accessed 8 Dec. 2017].
- [8] The Economist. (2007). The end of the cash era. [online] Available at: <http://www.economist.com/node/8702890> [Accessed 27 Sep. 2017].
- [9] Ethereum Blog. (2014). Toward a 12-second Block Time - Ethereum Blog. [online] Available at: <https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/> [Accessed 27 Sep. 2017].
- [10] Etherscan.io. (2017). Ethereum Average BlockSize Chart . [online] Available at: <https://etherscan.io/chart/blocksize> [Accessed 16 Nov. 2017].
- [11] Ethstats.net. (2017). Ethereum Network Status. [online] Available at: <https://ethstats.net/> [Accessed 16 Nov. 2017].

[12] Goland.org. (2017). How to make block chains strongly consistent – Stuff Yaron Finds Interesting. [online] Available at: http://www.goland.org/why_block_chains_are_strongly_consistent/ [Accessed 27 Sep. 2017].

[13] Goland.org. (2017). The block chain and the CAP Theorem – Stuff Yaron Finds Interesting. [online] Available at: http://www.goland.org/blockchain_and_cap/ [Accessed 27 Sep. 2017].

[14] Google Developers. (2017). Protocol Buffers | Google Developers. [online] Available at: <https://developers.google.com/protocol-buffers/> [Accessed 20 Oct. 2017].

[15] James-Lubin, K. (2015). Blockchain scalability. [online] O'Reilly Media. Available at: <https://www.oreilly.com/ideas/blockchain-scalability> [Accessed 16 Nov. 2017].

[16] Koteska, B., Karafilovski, E. and Mishev, A. (2017), Blockchain Implementation Quality Challenges: A Literature Review : Proceedings of the SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications, Belgrade, Serbia, 11-13.9.2017.

[17] Malanov,A, (2017). Six main disadvantages of Bitcoin and the blockchain. [online] Kaspersky.com. Available at: <https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/> [Accessed 16 Nov. 2017].

[18] Motherboard. (2017). One Bitcoin Transaction Now Uses as Much Energy as Your House in a Week. [online] Available at: https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change [Accessed 20 Nov. 2017].

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

[20] The NodeSource Blog - Node.js Tutorials, Guides, and Updates. (2014). Why Asynchronous?. [online] Available at: <http://nodesource.com/blog/why-asynchronous/> [Accessed 16 Nov. 2017].

[21] Park, J.H. and Park, J.H., (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry, 9(8), p.164.

[22] Poon, J. and Dryja, T.. (2016). The Bitcoin Lightning.network [online] Available at: <https://lightning.network/lightning-network-paper.pdf>.

[23] Raiden-network.readthedocs.io. (2017). Raiden Specification — Raiden Network 0.2.0 documentation. [online] Available at: <https://raiden-network.readthedocs.io/en/stable/spec.html> [Accessed 7 Dec. 2017].

- [24] Reitwiessner, C. (2017). zkSnarks in a Nutshell [online] Available at: <http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf> [Accessed 23 Nov. 2017].
- [25] Sirer, E.G. and Song, D., 2016, February. On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security (pp. 106-125). Springer Berlin Heidelberg.
- [26] Sompolinsky, Y., Lewenberg, Y. and Zohar, A., 2016. SPECTRE: A Fast and Scalable Cryptocurrency Protocol. IACR Cryptology ePrint Archive, 2016, p.1159.
- [27] Sompolinsky, Y. and Zohar, A., 2015, January. Secure high-rate transaction processing in bitcoin. In International Conference on Financial Cryptography and Data Security (pp. 507-527). Springer, Berlin, Heidelberg.
- [28] Son, M. (2017). Bitcoin's Rise Happened in Shadows of Finance. Now Banks Want In. [online] Bloomberg.com. Available at: <https://www.bloomberg.com/news/articles/2017-10-05/bitcoin-s-rise-happened-in-shadows-of-finance-now-banks-want-in> [Accessed 7 Dec. 2017].
- [29] Swan, M., 2015. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".
- [30] VISA (2017). Visa Inc. Facts & Figures . [online] Available at: <https://usa.visa.com/dam/VCOM/global/about-visa/documents/visa-facts-figures-jan-2017.pdf> [Accessed 20 Nov. 2017].
- [31] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE, 11(10), p.e0163477.
- [32] Dziembowski, Stefan; Faust, Sebastian; Kolmogorov, Vladimir; Pietrzak, Krzysztof (2015). "Proofs of Space". 9216: 585–605.
Available at: <https://eprint.iacr.org/2013/796.pdf>
- [33] Secg.org. (2010). Standards For Efficient Cryptography 2, [online] Available at: <http://www.secg.org/sec2-v2.pdf> [Accessed 20 Jan. 2018].
- [34] Wood, G., 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151.
- [35] Ethereum. (2018). *ethereum/wiki*. [online] Available at:

<https://github.com/ethereum/wiki/wiki/Patricia-Tree> [Accessed 22 Jan. 2018].

[36] Team Hycon. (2018). *Team-Hycon/Genesis-View*. [online] Available at: <https://github.com/Team-Hycon/Genesis-View> [Accessed 22 Jan. 2018].

[37] Cryptonight Hash Function Cryptonote.org. (2018). [online] Available at: <https://cryptonote.org/cns/cns008.txt> [Accessed 2 Feb. 2018].

[38] JustCryptoNews. (2018). *Sia Coin - BitMain Antminer A3 Blake (2b) ASIC Miner Announced*. [online] Available at: <https://www.justcryptonews.com/340/sia-coin-bitmain-antminer-a3-blake-2b-asic-miner-announced> [Accessed 2 Feb. 2018].

[39] Monero (XMR) CPU Miner - GitHub. (2018). *xmrig/xmrig*. [online] Available at: <https://github.com/xmrig/xmrig> [Accessed 6 Feb. 2018].

[40] Palatinus, M., Rusnak, P., Voisine, A., Bowe, S.. *bitcoin/bips/bip-0039*. [online] Available at: <https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki> [Accessed 6 Feb. 2018].

[41] BIP32. (2012). *bitcoin/bips*. [online] Available at: <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>.

[42] BIP44 (2014). *bitcoin/bips*. [online] Available at: <https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki>.

[43] The Monero Project. (2018). Monero: A Scheduled Network Upgrade is Planned for April 6. [online] Available at: <https://getmonero.org/2018/03/28/a-scheduled-protocol-upgrade-is-planned-for-April-6-2018-03-28.html>.

附录

附录 A-创世区块

讨论

HYCON 的创世区块发布于韩国标准时间 2018 年 1 月 4 日凌晨 3 点 15 分 (GMT+9)，恰逢比特币发布创世区块 9 周年。以下是创世区块所包含信息的摘要。在 HYCON 团队的 github 库中可以找到该块以及用不同编程语言编写的解码软件。

块本身包含一个块头和 6 个交易。这 6 个交易代表了 HYCON 币的产生以及最初的分配。有关通证及预算分配的详细信息，请参阅附录 B。

块头包含挖掘难度、交易的梅克尔树 (Merkle) 根、状态树根，以及块的时间戳。

块数据的其余部分由单个交易组成，这些交易加载账户，用于将来分发通证。为了大规模发 HYCON 币，以这种方式对创世区块内的交易进行编码通常被认为是最透明的办法，因为它将允许这些账户的资金从一开始就被追踪。

创世区块的内容

解码后, HYCON 创世区块的内容如下:

块头

难度: 0 梅克尔树根:

cff5f8a5381ce41e26bf3f5f7b658dcef0d4935dfd791460614feb894ff36457

状态树根:

e08408cb5bf38fb2652676af953d169c7997dd2af88299163b9a389b9d6a3ed4

时间戳:Thu Jan 04 03:15:05 KST 2018

交易

首次币发行账户

账户地址 (未加工的): 9565e92e694ef206abe21d65d3a93996682d41f7

Amount: 2,000,000,000 HYCON

空投账户

账户地址 (未加工的): fa7042154efb88d06c198ef106ca31aed57e6875

Amount: 400,000,000 HYCON

团队账户

账户地址 (未加工的): 8bab45e2f5c79c00d539ae1a65dbd1f8fd416ca7

Amount: 500,000,000 HYCON

发展基金

Account address(raw): 7a7b31e5aced4889a75d1042a6f1204d2a889af8

Amount: 500,000,000 HYCON

漏洞悬赏

账户地址 (未加工的): 571a6e4554afbb09ee7da1ae20c18dbca9fab46

Amount: 500,000,000 HYCON

企业社会责任

账户地址 (未加工的): 11d8046e6cd88f9e580b84a0b10c7c452f0030fc

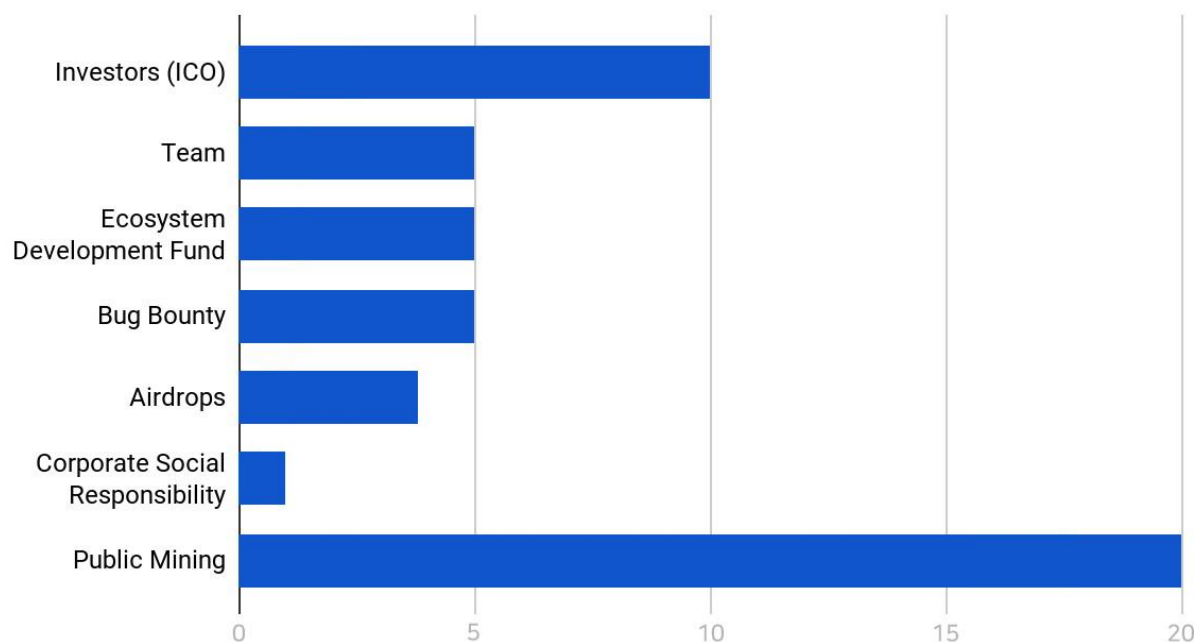
Amount: 100,000,000 HYCON

附录 B-币的分布与预算分配

币的分布

HYCON币的总数量为50亿。分配方式如下：

HYCON Distribution



如上图所示，大部分的HYCON币将通过公开采矿获得，为20亿HYC，其余30亿在创世区块内产生，并被分配给负责币流通的HYCON账户中。

这30亿HYC分成6个用途。最大的部分（10亿HYC）分给了首次币发行的参与者以及发行前的投资人。团队、生态系统发展基金，以及漏洞悬赏项目各分5亿HYC。1亿HYC分给了HYCON的企业社会责任。剩下的4亿HYC将通过活动及其它尚未定下来的方法进行空投。

应注意，Genesis 区块为 ICO 基金分配了 20 亿美元，但在与社区协商之后，可供使用的代币数量减少了一半，即可供使用的代币数量减少了 10 亿美元。

预算分配

我们首次币发行时分配资金的主要重点是促进更智慧的发展以及确保项目的长期未来。因此，筹集到的资金中有 70% 将投入到 HYCON 和无限项目未来的研发中，包括无限平台与无限去中心化交易所的研发。值得注意的是，虽然这些都是单独的项目，HYCON 的首次币发行却是唯一为推动整个项目前进而采取的筹资活动。

Budget Allocation

