HYCON WHITEPAPER v1.2

HYCON 白皮书 v1.2

INFINITY PROJECT

无限项目

ABSTRACT 摘要

This paper begins by outlining the vision of the Infinity Project, which is planned for a 3 phase roll-out: 1) the ‘HYCON’ coin 2) the open-source Infinity Platform for customizable enterprise blockchain solutions, and 3) a decentralized cryptocurrency exchange platform. However, this whitepaper’s main objective is to provide a detailed analysis of ‘HYCON’, a fast and secure cryptocurrency that makes use of the SPECTRE protocol to enable high transaction speeds while maintaining security. Identified herein are a sample of the challenges and limitations of many existing cryptocurrencies and solutions proposed by the HYCON coin. Additionally, the technical specifications of HYCON will be introduced, as well as a brief discussion of SPECTRE and its implementation in this project.

本白皮书首先概述了无限项目的远景，该项目计划分三阶段推进：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。

INTRODUCTION 引言

> “...cash, after millennia as one of mankind’s most versatile and enduring technologies, looks set over the next 15 years or so finally to melt away into an electronic stream of ones and zeros.”
> “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。”
>
> **The Economist (2007)** 《经济学人》（2007）

In today’s world of electronic and mobile banking, money is transforming from something tangible, held in one’s hand, into digital numbers that are moved around the Internet. In this environment, it was a natural progression for new forms of currency to emerge, which exist only as cryptographically secured strings of digital code, known as ‘cryptocurrency’. This digital currency revolution began in 2008 when the still anonymous Satoshi Nakamoto published the Bitcoin whitepaper [19].
在当今手机电子银行的世界里，钱正从一种攥在手里、看得见摸得着的东西，变化成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】。

Today, new cryptocurrencies are released on an almost daily basis, sharing one unifying concept: the underlying technological architecture that is the blockchain.
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。

A blockchain itself is a shared public ledger of transactions that records and maintains that record of all transactions made on the system - from the genesis of the first block until the present moment. The ledger - the blockchain defined above - is built using a linked list, or chain of blocks, where each block contains a certain number of transactions that were validated by the network in a specific timespan.
区块链本身就是一个共享公共账簿，记录并维护着系统上的所有交易记录——从第一个区块问世一直到此时此刻。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。

The Infinity Project will introduce a new cryptocurrency called HYCON, designed to address some of the challenges faced by existing blockchain technologies. What follows is an outline of the existing state of blockchain development with a focus on the problems that need to be addressed, the goals of the Infinity Project itself, how HYCON proposes overcoming existing blockchain limitations, and the technical specifications of HYCON.
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。

DISCUSSION OF EXISTING BLOCKCHAIN TECHNOLOGIES 现有的区块链技术讨论

For the purposes of this discussion, the Bitcoin and Ethereum blockchains will be the focus as they are the most widely used and well studied implementations of blockchain technology to date.
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。

A useful reference point for examining blockchain technology is the work of Yli-Huomo et al.[31]. Presented therein is a comprehensive summary of recent work on blockchain technology and the limitations inherent to a blockchain based system. While their research was focused entirely on papers discussing the bitcoin blockchain, the findings presented are broadly applicable for the purposes of this discussion. The key discussion metrics used were drawn from Swan [29] and again, these are applicable here.
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】。

This research highlights seven limitations of current blockchain systems:
研究指出了现今区块链系统的七大局限性：

- Throughput 交易吞吐量
- Latency 延迟
- Size and Bandwidth 大小和带宽
- Security 安全性
- Wasted Resources 浪费资源
- Usability 可用性
- Versioning, Hard Forks, and Multiple Chains 版本控制、硬分支和多链

Throughput 交易吞吐量

A representative blockchain such as Bitcoin takes 10 minutes or longer to confirm transactions, achieving 7 transactions per second maximum throughput, with current transaction rates in the region of 4 per second. Ethereum can process 10 or more transactions per second, with confirmation times approximately 10 times faster than those found on the bitcoin network. However, benchmarking the current throughput capacity of these blockchains against the VISA network is a useful comparison to understand current limitations of these blockchains: the VISA network can verify transactions in seconds, process 2000 transactions per second on average, and features a maximum capacity of 65,000 transactions per second.[30] As can be seen by these metrics, there is still a large discrepancy in the throughput of today’s most used blockchain networks when compared to traditional, centralised payment networks like VISA.
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，与传统的中心化支付网络（如 VISA）相比，当今使用最多的区块链网络的交易吞吐量也还存在着很大的差距。

A primary factor limiting the throughput of blockchain networks is the latency between nodes. While there have been some promising attempts to address this problem, such as the lightning network [22] due to be adopted by Bitcoin, and the Raiden network [23] that is already running as a micro version on the Ethereum blockchain, consensus has yet to be reached on a viable, long-term solution.

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。

Latency 延迟

As mentioned above, latency and throughput go hand in hand as limiting factors, because the maximum throughput of a network is limited by the latency between nodes. If there is a high latency between nodes, the risk of mining on an old block is increased. On the Bitcoin network, for example, the average time taken for a block to propagate to 50% of the nodes is just under 2 seconds, with 90% of nodes reached after approximately 13 seconds (as of April 2017) [4]. For Ethereum, the average time for propagation to 50% of nodes is less than 1 second, with 90% of nodes reached in approximately 10 seconds [11].

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】。

For Bitcoin, the ratio of the block mining time to the network propagation time is large, meaning that latency between nodes does not act as a large limiting factor. With Ethereum’s shorter inter-block time, the wasted time could be more problematic, but Ethereum uses an algorithm based on the GHOST protocol [27] to incentivise mining on the longest chain instead of attempting to continue to mine on parallel chains that were created due to high latency, or low inter-block times.

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。

Size and Bandwidth 大小和带宽

There are two considerations that must be addressed in a discussion regarding size and bandwidth: the physical data that represents the full blockchain, and the size of individual blocks being sent over the network. With the requirement that a *full-node,* which can mine new

blocks and interact with the blockchain network, must maintain a local copy of the entire blockchain, it is clear that the storage capacity required to maintain this local ledger is directly proportional to the number of blocks on the chain, thus leading to a risk of much higher centralization if the blockchain becomes so large that only a few nodes are able to process a block [15]. In addition, when transaction volume starts to push the limits of the available bandwidth, coupled with a hard-cap imposed by the block size, mining fees can increase significantly, which could lead to changes in the core protocols to allow for greater transaction volume: i.e. larger block sizes, or shorter block times. In this eventuality, a hard fork, which is generally considered undesirable, would be required to make the necessary protocol upgrades.
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。

Security 安全性

One of the biggest selling points of POW blockchains as a technology is the fact that they are very difficult to hack. In order for a fraudulent user to alter an entry that is already present on the blockchain, they would need to redo the proof of work for that block as well as all subsequent blocks that reference it. The computational resources needed to successfully perform an attack of this nature is equal to the hashing power of 51% of the network, hence the name, “51% attack”. However, this is an unlikely prospect as the mining benefits of possessing 51% of the network would outweigh those to be gained by acting fraudulently.
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。

A second method of attack is referred to as a Sybil Attack, where a fraudulent entity creates multiple fraudulent identities for use on the network, which then try to subvert the network to their advantage. In a POW based system, such as Bitcoin, your ability to influence the network is determined by how much hash power you use to find new blocks. Pretending to be two miners would require the hash power to be divided, resulting in no advantage.
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出新的块。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。

There are, however, other ways to attack user funds on a blockchain network. Often, users rely on the safe storage of their private keys by centralized exchanges, which, if compromised, can provide an attacker with access to their wallets, and by extension, their cryptocurrency.

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。

Another security risk in the blockchain space is found in the implementation of *smart-contracts* that feature coding errors. A particularly well-known and successful exploitation of a smart contract occurred on June 17, 2016 and is now colloquially known as the “DAO attack”, wherein an attacker was able to use a small flaw in the code that executed the smart contract to obtain an estimated $50~60 million worth of ether, an event that eventually led to the controversial hard fork that split the Ethereum network in two, creating Ethereum Classic. [2]
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】。

Wasted Resources 浪费资源

The electrical and by extension environmental impact of the bitcoin blockchain is considerably large. At current estimates, 249 kWh of electricity is required to validate a single transaction, with upwards of 32 TWh used by miners annually to continually add new blocks to the Bitcoin blockchain.[6] While the figures involved are lower for Ethereum, the energy outlay, and thus environmental impact, is still massive.[7] In fact, if you were to combine the amount of energy used to protect the Bitcoin and Ethereum networks, there would be enough to power the country of New Zealand for a year. There are currently movements away from proof of work blockchains, with Ethereum being the most prominent proponent for a move towards proof of stake.
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。

Usability 可用性

On the Bitcoin blockchain, transactions are published as part of a block approximately every 10 minutes, and it is standard to wait up to 50 minutes or more after each transaction has been published, to allow for subsequent verification. Taking a real-world example, this would be analogous to attempting to pick up groceries from a store and then having to wait in line for an hour while your payment is processed. For real-time application to a real-world use case, this is clearly unacceptable.
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。

A second, more nuanced concern with Bitcoin, and the majority of currently available cryptocurrencies, is the concept of anonymity, or pseudonymity as is the common case.

Transactions are public and shared by all participants on the blockchain. For transactions where discretion is required, this is not always desirable as the data could be examined, allowing algorithms to extract transaction data from a user’s “private” transactions. To again use a real world example for illustrative purposes, suppose a user sends money to their mother; based on the transaction information, it is possible to see: 1) How much bitcoin has been sent and received by each user now and throughout the entire history of those particular addresses, 2) The balances of both addresses at any given time in history, and 3) To which other addresses each user has sent funds to or received funds from. Essentially, senders and recipients of transactions can see the financial history of the other, and could even have the ability to know what was bought, what was gambled on, or even which entity received ‘anonymous’ support, once you are able to link a particular address to an individual. As the American FBI has proven several times now, Bitcoin is not truly anonymous. For many users, financial transparency is perhaps one of the largest disadvantages of using Bitcoin, however, researchers are working on fixing this problem with solutions such as zkSNARKS [24] (zero-knowledge cryptography), which is a privacy mechanism built into ZCash, and added to Ethereum with the Metropolis (Byzantine) upgrade.

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 zkSNARKS（零知识证明密码学）【24】（一种建立在 ZCash 上的隐私机制）。

Versioning, Hard Forks, and Multiple Chains 版本控制、硬分支和多链

The primary problem of forking on a blockchain is one of loss of consensus and security. Take the hyperbolical example of a severely bloated blockchain which makes use of 100% of the computing power available in the universe, and a contrasting example wherein 100 competing chains each possess 1% of the available computing power.

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。

In the case of the first example, a 51% attack would truly require 51% of the computing power available in order to overtake the chain maintained by honest nodes, however in the fragmented case, only 0.51% of the computing power available in the universe would be required to corrupt any individual chain.

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。

Blockchains rely on consensus being maintained by having the combined computational power of honest nodes outweigh the power available to malicious ones. With a fragmentation of the chain and reduced computational power being applied to each fork, an attack has more chance of being successful, with a lower entry point in terms of resources required to be met.
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，而发动恶意攻击所需要的算力减少，攻击就更有可能成功。

Hard forks are another generally undesirable outcome that often result from a loss of protocol consensus. Ideological differences between different stakeholders within a given blockchain ecosystem can lead to a split, or a fork of the chain, with well-known examples being the breakaway of Bitcoin Cash due to Bitcoin's scaling issues and inability to be used as a fast and cheap means of electronic cash and the previously referenced Ethereum Classic, which forked away from Ethereum on the philosophical basis of blockchain immutability. However, hard forks are not always contentious and often come about through changes in core protocols of a blockchain system, such as with Ethereum's 2017 Metropolis upgrade. After a hard fork, the overall hash power that was applied to the original chain may still be there, however in the case of an ideological hard fork, it is then split between two competing chains, leaving them possibly less secure and more vulnerable to attack.
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。

INFINITY PROJECT - CORE GOALS 无限项目-核心目标

During the formation of the Infinity Project we asked the following 2 key questions:
在无限项目的形成过程中，我们提出了下面两个关键问题：

✓ Given current limitations of existing cryptocurrencies, what are the needs and wants of the market and how can we provide solutions?
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？

✓ What properties are necessary for a cryptocurrency to be widely adopted and integrated into the wider economy?
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？

With these questions in mind, we conducted a thorough analysis of existing blockchains - including Bitcoin, Ethereum, and a variety of promising Altcoins - to uncover the strengths and weaknesses of each project. However, it was difficult to find a project that perfectly aligned with our initial questions posed above.
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。

Therefore, the Infinity Project team began researching new technologies and algorithms that were more suitable for mass, real-world adoption, to help us meet our goals. At the same time, we started to design the basic framework of the Infinity Project, and formulated the following 5 core goals:
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：

INFINITY PROJECT CORE GOALS 无限项目核心目标

1. Identify actual market needs for a cryptocurrency 确定加密货币的实际市场需求
2. Develop a cryptocurrency that is flexible 开发一种灵活的加密货币
3. Create user-centric blockchain platform 建立以用户为中心的区块链平台
4. Develop an ecosystem that promotes sustainable innovation 建立可持续创新的生态系统
5. Investigate methods for a decentralized cryptocurrency exchange 研究去中心化加密货币交易所的实现办法

Core Goal 1 - Market Need Identification 核心目标 1-市场需求识别

Although many blockchain projects have gained mainstream attention and recognition recently, no cryptocurrency has penetrated digital commerce on a global scale. More precisely, a great divide still exists between most crypto projects and real world solutions. Cryptocurrency acceptance and adoption is currently limited to a very small group of online merchants and a handful of other services, making it infeasible to completely rely on Bitcoin or any other currently available cryptocurrency as the de facto digital currency of choice.

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。

To help overcome this and issue and expedite use cases and adoption, it is useful to work jointly with experts in a given field or community, along with developers, in order to drive the development of a successful, market-friendly currency that best serves all users.

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。

Therefore, to answer one of the two key questions posed by our Infinity Project team, "What is the user-centered currency that the market wants?", we must define the core blockchain technology required in order to find a mutually desirable solution from both a market and development standpoint. This led the Infinity Project team to conclude that the first key success factor (KSF) when developing our new cryptocurrency is to design and implement it based on the premise of providing practical solutions that the market needs.

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。

Core Goal 2 - Flexible Currency 核心目标 2-灵活的货币

The Infinity Project team decided to step away from traditional viewpoints of monolithic monetary development present in many existing encryption projects, and introduce the concept of a flexible implementation platform that can incorporate various monetary models.

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。

By extension, this led to the creation of our "Hyper-connected Coin" (HYCON), which from its very beginnings, was designed to be fast, cheap, scalable, and safe, and thus ready for adoption and usage in a variety of real-world situations.

这个平台加以扩展，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。

The underlying Infinity blockchain that it's built upon has been designed with an interchangeable, modular structure, which will facilitate the easy adoption and alteration of the underlying technology to suit specific needs.
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。

Core Goal 3 - User-Centric Platform 核心目标 3-以用户为中心的平台

Arguably, one of the most important parts of the paradigm shift that Bitcoin ignited is the facilitation of a secure, decentralized exchange of value electronically - one that is open to all, and opened the door to the once unrealistic notion of making payments without banks.
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。

However, a steep learning curve from the conceptual level down to the actual UI and UX of most cryptocurrencies is one of the key hurdles currently hampering greater adoption. The Infinity Project seeks to reduce these barriers to entry by providing a more straightforward and user-friendly platform, in addition to an intuitive wallet and exchange platform interface. Ultimately, our goal is to allow more people to harness the paradigm-shifting power of blockchain technology.
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。

Core Goal 4 - Flexible Innovation 核心目标 4-灵活创新

One of the most important aspects considered during the development of the Infinity Project was how to help more people, businesses, governments, NGOs, etc., harness the power of blockchain technology. Thus, our Infinity Project team is researching the implementation of the Infinity Platform, which is a flexible blockchain platform concept that evolved from the study of various other existing blockchains, platforms, and cryptocurrencies.
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努力推进“无限平台”的实施。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。

The goal of our Infinity Platform research is to create a platform that is intuitive to use and one that can be implemented in various ways. Example use cases for the Infinity Platform include: implementing a secure cryptocurrency based on HYCON that is fast and cheap to use as a means to exchange value; the creation of decentralized corporate ledgers to enhance information security and facilitate more efficient data storage and transmission; and adding cryptographic security to stock exchanges. Potential use cases and innovations built with the Infinity Platform are vast, and can adapt to offer potential users the flexibility to create the blockchain solution they need.
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。

Core Goal 5 - Secure Decentralized Exchange 核心目标 5-安全的去中心化交易所

An active area of research for the Infinity Project is giving users the ability to exchange different cryptocurrencies in a decentralized manner. Current exchanges rely on centralization to cheaply and quickly trade cryptocurrencies, however this centralization requires users to entrust their fiat and cryptocurrency holdings to the exchange.
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。

Unfortunately, the source code that powers these exchanges is often not publicly available for review, despite the huge volumes of transactions that pass through these exchanges. Globally, there have been multiple incidents where exchanges have had their user’s cryptocurrencies stolen by malicious actors. The centralization of user funds and information existing on exchanges today will continue making these companies targets.
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。

As part of the Infinity Project’s future research, we intend to integrate the concept of atomic swaps into Hycon to allow for our currency to become a true medium of exchange. Through HYCON, multiple other cryptocurrencies will be tradable, and transaction fees will be distributed to the miners who protect the network. Atomic swaps will allow HYCON to be held in escrow pending the proof of payment of another cryptocurrency, and thus facilitate trustless P2P trading of HYCON and other cryptocurrencies.
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 TECHNICAL SPECIFICATIONS HYCON 技术规范

Characteristic 特征	Specification 规范
Hash Function 哈希函数	CryptoNight & Blake 2b
Consensus Protocol 共识协议	SPECTRE
Chain Structure 链结构	Directed Acyclic Graph(DAG) 有向无环图（简称 DAG）
Block Speed 站间速率	1000ms
Mining Method 采矿方式	工作量证明（PoW）

Genesis Block 创世区块

The HYCON Genesis Block was published on January 4th, 2018, at 3:15am KST (GMT+9). It is available to be viewed on GitHub as part of Team Hycon's repository[36]. For more information

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。

Hashing Algorithms 哈希算法

The first version of this document cited Blake2b as the only hash function being used as part of the HYCON system. However, due to recent developments in ASIC technology[38], it was decided to move away from the Blake-2b hash and to instead use the ASIC resistant hash Cryptonight, which is also employed by Monero. What makes Cryptonight interesting is that it uses pseudorandom memory read/write operations as part of its hashing operation. This leads to performance being loosely comparable whether on a CPU or GPU, while also rendering it incompatible with standard ASIC architecture.

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。

Consensus - SPECTRE Protocol 共识机制——SPECTRE 协议

In contrast to the Nakamoto protocol used for consensus on the Bitcoin blockchain, HYCON implements a protocol called SPECTRE to maintain consensus [26]. SPECTRE generalises a blockchain into the form of a directed acyclic graph(DAG) by employing a voting algorithm between pairs of blocks in order to specify their order in a pairwise manner, i.e. block x should be applied before block y or block y should be applied before block x. While a full description of the SPECTRE protocol is beyond the scope of this whitepaper, a basic outline of the voting rules is provided below.
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。

Voting Rules 投票规则

In order to discuss the voting rules in SPECTRE, it is useful to refer to a visual representation of the process. It should also be noted that no votes are communicated between nodes and there is no need to explicitly participate in a vote. Rather votes come from blocks and the way in which they vote is implied from the structure of the DAG.
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。

The criteria used in the voting process in SPECTRE are as follows;
The important terms to be noted are $past(x)$and $future(x)$, which designate the blocks that are reachable from x, and the blocks which reference x as an antecedent respectively. More specifically, block y is in $future(x)$ if x is in$past(y)$. i.e.
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：

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

It should also be noted that the virtual block, designated $virtual(G)$, is a hypothetical block that has the entire DAG as its past.
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。

For some block designated *z* voting on some other blocks designated *x* and *y*:
当指定一个块 z 为其它的块 x 和 y 进行投票时：

1. If z is in $future(x)$ but not in $future(y)$ then it will vote in favour of x.
   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. If z is in $future(x)$ and $future(y)$ the vote will be determined recursively based on the prospective vote of a virtual block with a past equal to $past(z)$
   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. If z is not in $future(x)$ or $future(y)$, then the vote will be decided by the majority vote from the set of blocks designated by $future(z)$
   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. If z is a virtual block with $past(Virtual(G))$ i.e. its past = the entire DAG, it will vote in accordance with the majority vote of the DAG.
   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. For the cases $z = x$ or $z = y$, the block will vote for itself to be correct, provided that y is not in $future(x)$, or vice versa.
   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。

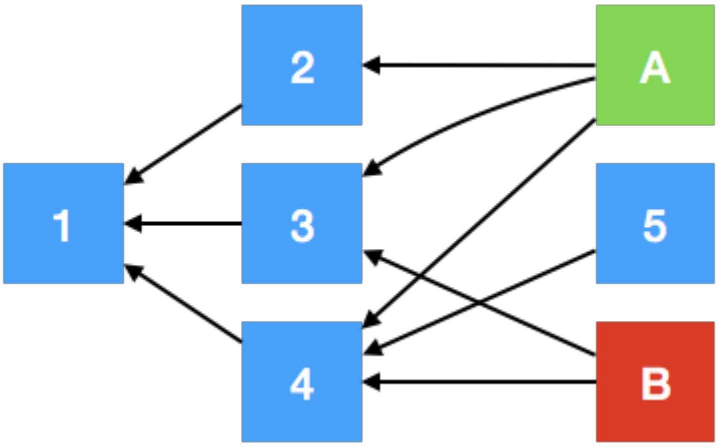
Application of SPECTRE Protocol to Example DAGs 举例说明 SPECTRE 在 DAG 中的应用

To best illustrate the application of SPECTRE, it is useful to work through an example of the protocol in action step by step and provide snapshots of the state of the voting process as it proceeds. This particular example is drawn directly from the SPECTRE whitepaper. [25]
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】。

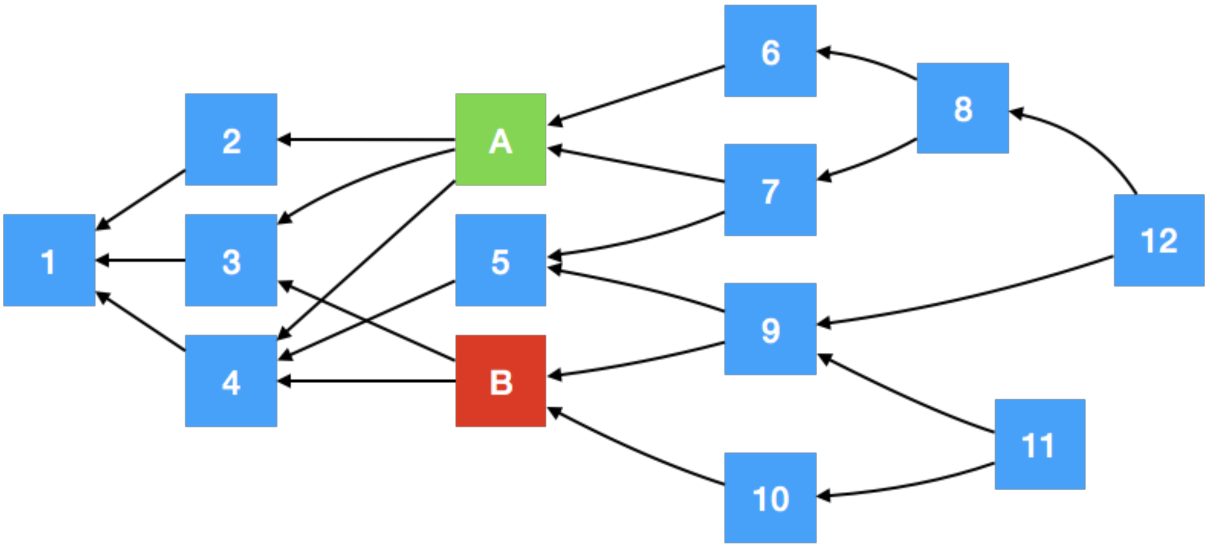
Example Case - A Double Spend 案例-双重支付

Take the simplest possible case where a block *A* contains a transaction *t1* and a second block *B* contains a conflicting transaction *t2*. These conflicts could be malicious, or merely caused by latency between nodes leading to transactions being published twice, such that two miners are collecting the same transaction fee. Depending on the structure of the DAG the result of this double spend will be resolved differently as the two blocks will have differing pasts and futures.
举一个最简单的例子，块 A 包含交易 t1，块 B 包含与之冲突的交易 t2，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。

The initial case for this example looks as follows with blocks A and B being published at approximately the same time as block 5.
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。

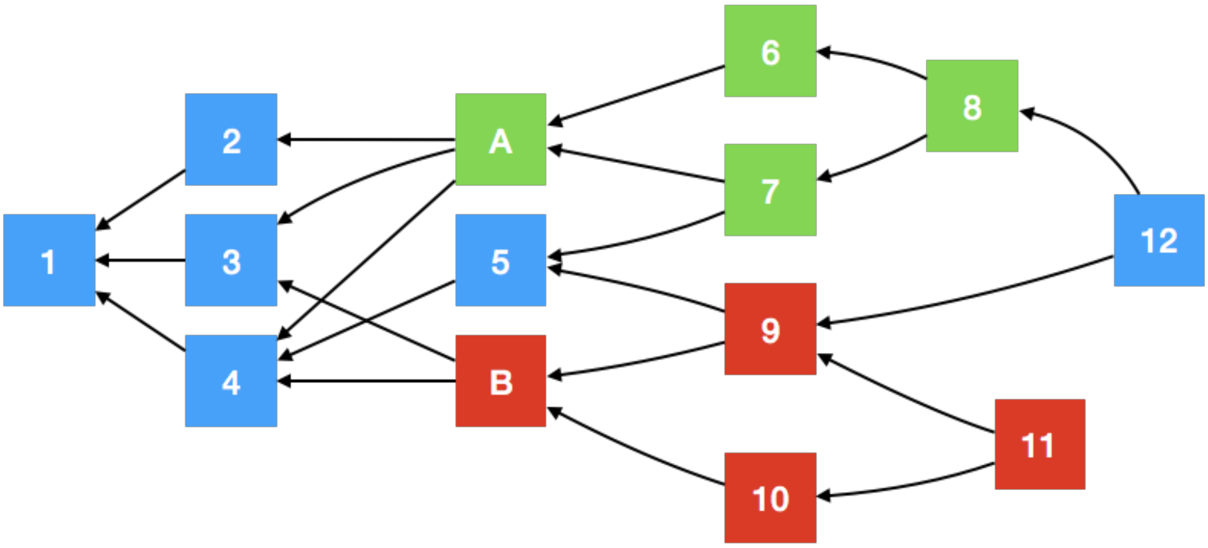


At this stage the system is unaware of the double spend, as no subsequent blocks have been published referencing both of the conflicting blocks. However, as the structure of the DAG develops and more blocks are added, the double spend is discovered and the structure of the DAG will be analysed to determine which block takes precedent.
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。



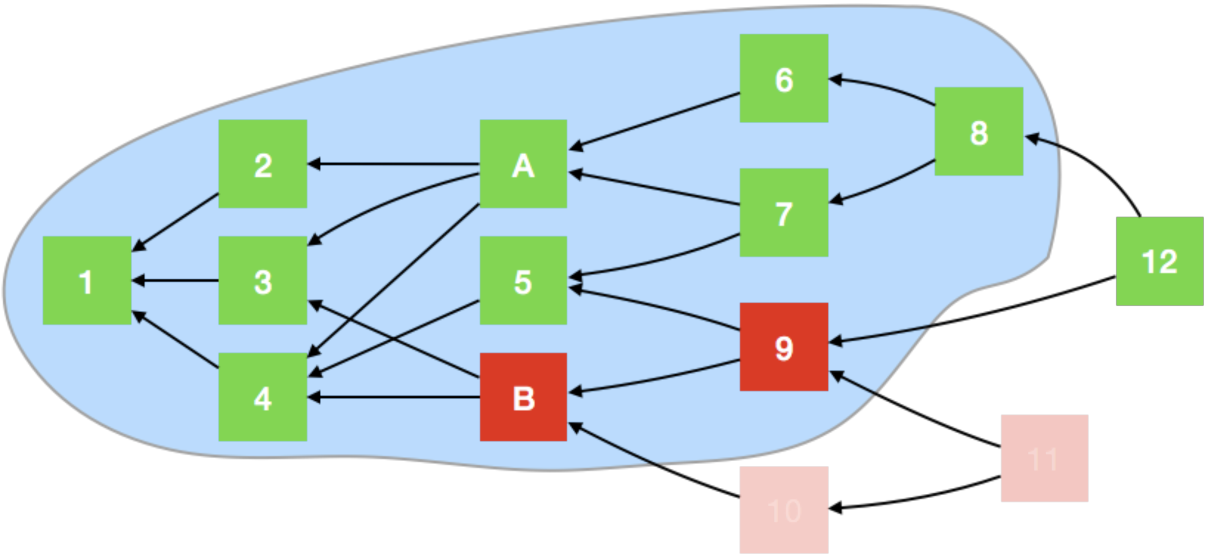
In the above diagram, block 12 is the first block published with reference to the double spend between A and B. Following the rules listed above, the votes can be counted as follows. Blocks 6, 7, and 8 all vote for block A, because block B is not present in their past. Similarly, the votes of blocks 9, 10 and 11 are for B, for the same reason.

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。



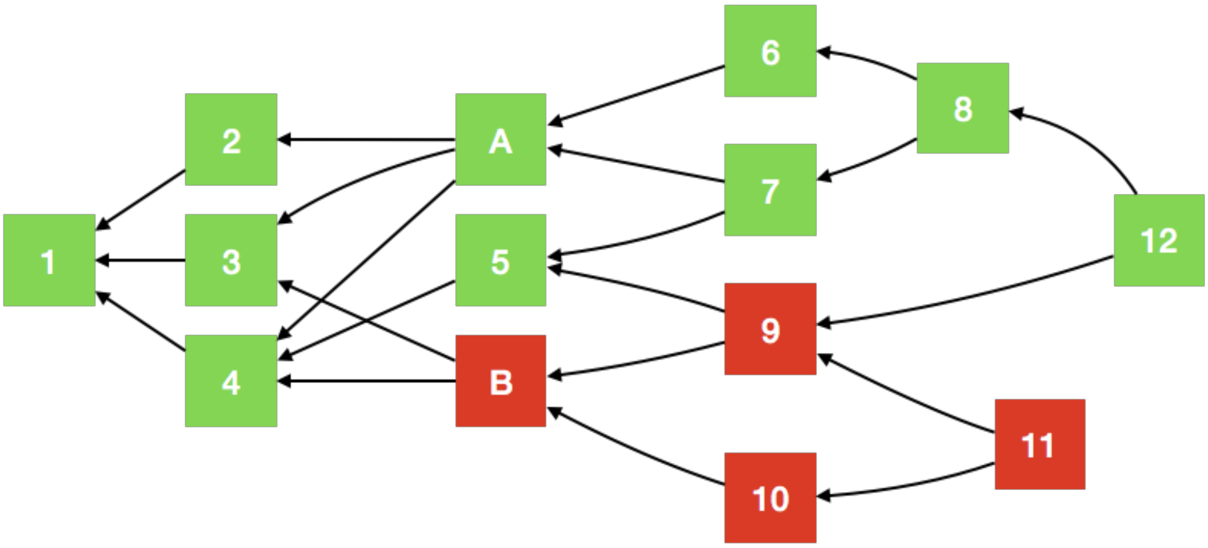
Block 12 votes based on a recursive call over its past. As blocks 10 and 11 are not included in $past(12)$, they are not considered when determining block 12's vote. The voting area for block 12 is shown below.

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。



Blocks 1-5 are not in the sets of blocks $future(A)$ or $future(B)$, so they will vote the same as the majority of their futures. In the case of this recursive vote, these blocks all have more votes for block A in their future and so also vote for block A. Block 12's past contains 9 votes for block A and 2 votes for block B, So block 12 will vote for block A. If there had been a tie, Block 12 would break the tie deterministically so that all servers can agree on which way block 12 votes. Since we only use $past(12)$ to determine the vote of 12, its vote will never change.
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里，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。

The remainder of the voting process in the DAG is based on the future of the remaining blocks. Once Block 12's vote has been confirmed, Block 5 votes in favour of A because the votes of 7, 8, and 12 outweigh the votes of 9 and 11. Block 4 sees votes for A from A, 5, 6, 7, 8, and 12, with blocks B, 9, 10, and 11 voting for B, thus Block 4 also votes for A. It is a similar case for blocks 3, 2, and 1, which all cast their votes for A. Leading to a final vote tally for this voting procedure of 10 votes in favour of A and 4 votes in favour of B.
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。



An interesting property of SPECTRE is that, especially in simple cases such as the one illustrated here, it replicates longest-chain selection models used in other blockchain technologies. Following the route from 1 -> 12 passing through A, and the same route but passing through B, it can be seen that the route 1->A->12 is longer than the route 1->B->12, i.e. the longest chain wins.

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。

DAG Versus Blockchain DAG 与链式区块链

The advantage of a DAG over a blockchain is primarily that it allows for shorter intervals between blocks, which in turn leads to higher transaction confirmation speeds. In contrast to currently existing blockchains, where newly mined blocks are chained on to the end of the blockchain by referencing the hash of the previous block, a new block to be added to the DAG references the current tips of the DAG instead. This allows blocks to be published simultaneously from different nodes, without running the risk of forking the chain. As new blocks are permitted to have multiple antecedents, they can be added concurrently and thus miners can still reap the mining rewards without having to worry about their blocks being orphaned. Where problems occur is if nodes publish transactions that have been simultaneously published elsewhere, leading to possible double spends. Using SPECTRE, it is possible to achieve consensus about which transactions should be rejected without orphaning the entire block.

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。

INFINITY SPECTRE Implementation 无限 SPECTRE 的实现

The voting procedure in SPECTRE is quite a drain on resources, so its implementation needs to be carefully managed. Our initial prototype was written in Python for ease of development, however, the final version of the INFINITY SPECTRE implementation is to be written in language such as C, C++ or Rust, such that complete control over data structures and memory management is maintained allowing for better performance.

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。

Block “Height” and Chaining 块的“高度”和链接

As can be gathered from a cursory glance at the DAG structure, the traditional idea of block height as used in Bitcoin or Ethereum requires a slight semantic modification. In those representative blockchains, the height represents the number of blocks that have been chained on top of the genesis block. In HYCON the height is a more general descriptor representing the number of DAG layers above the genesis block the current block is. The calculation to be applied is quite simple. The height of the new block is one more than the height of its highest parent.

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。

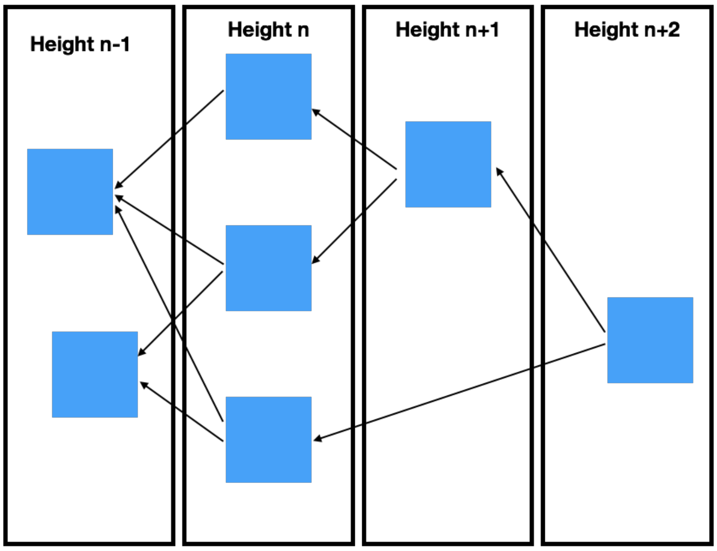
For any new block $B$with set of Parents P:

对于任一新块 B，与其父块 P：

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

Diagrammatically, this situation looks like the example provided below. Newly published blocks reference the highest available unreferenced blocks, and have a height set as one more than the highest referenced block.

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。



Network Infrastructure - Node.js, Typescript 网络基础架构——Node.js，Typescript

The advantage to using this setup for the system architecture is Node.js' inbuilt support for asynchronous operations. Node.js allows for cross-platform “non-blocking evented I/O”, where individual components can wait for the results of operations outside of the flow of normal operation. The waiting components are only triggered and executed on the occurrence of a certain event, such as a message being received from the network, or input from a user, allowing other code to execute during the waiting period. [20]

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】。

The use of Typescript was decided upon due to the strong type checking that it enforces on what is essentially Javascript. Using a typed version of Javascript allowed the development team to build a platform that takes advantage of the asynchronicity provided by Node.js while also making debugging a simpler process due to explicitly defined types. As the Typescript files require compiling before being run, many syntax and type errors can be caught easily at the compile stage, rather than by trawling through a maze of callbacks step by step in the debugging process as is common in Javascript applications.

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查错误。

Serialization - Protocol Buffers 序列化-协议缓冲器

In a blockchain system there are any number of messages flying around the network at any given time. It is important that the node software is able to decode that data in a consistent and correct manner. The use of protocol buffers, which are developed by Google[14], allow for consistent message definitions that can be used across different platforms, to allow for nodes running the infinity blockchain to be developed in numerous programming languages. The serialization layer is language agnostic, which is highly useful for cross-platform applications. Protocol buffers also allow for backwards and forwards compatibility, increasing the chance that an update will only require a soft fork, rather than a hard fork. It is also makes it easier for third party software to be compatible, allowing other developers to interact with the Hycon network.

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。

Mining 采矿

Overview 概述

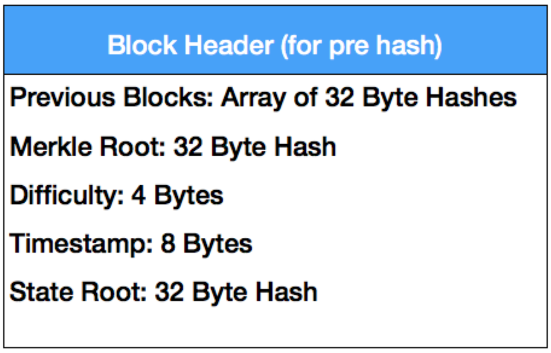
Publishing of a block will require proof of work, similar to the majority of existing cryptocurrencies. Miners will calculate the hash of the next block based on the hashes of the tips of the DAG, the merkle root of the transactions to be included in the block, and a nonce, that will be altered until a hash that exceeds current difficulty is calculated. While the creators of SPECTRE state that 10 blocks per second is feasible using the protocol, HYCON will initially have a target of 1 block per second. Although the current prototype uses proof of work, we are very aware of the large amount of electricity being used to secure the bitcoin and ethereum networks, and are considering alternatives. One of the lesser-known methods that we are considering is Proof of Space[32], which requires miners to pre-compute and store large amounts of data, then search through the files for a solution that satisfies the current difficulty. This uses very little electricity and has been demonstrated to be effective by Burst coin and Space mint.

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。

Mining Process in Detail 采矿过程的细节

The initial stage of the mining process is the encoding and hashing of the contents of the block header, which will not change as a result of the mining process. These contents are the references to the previous blocks, the Merkle root of the transactions to be contained within

the block, the block target difficulty, the block timestamp, and the root of the Merkle-Patricia Trie representing the current world state after the transactions in this block(see Wallets & Accounts section for more information).
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

This data is hashed using the 64 Byte version of Blake 2b to provide an unchanging pre-hash to be furnished to a GPU or CPU miner. This step is necessary, particularly for GPU mining, as HYCON block headers have variable length due to multiple possible parent blocks. GPU mining software works best when furnished with a fixed length data structure so pre-hashing is necessary. The 64 byte header pre-hash is then combined with an 8 Byte nonce, that is incremented by one for each hash attempt using the Cryptonight hash algorithm. The combined header pre-hash and nonce are hashed together to return a 32 byte hash representative of the block. This hash is then compared to the difficulty specified in the block header, and if the correct difficulty threshold is reached, the nonce is returned to be included in the finished block header and published.
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 Integration & XMRig Stratum 集成与 XMRig

HYCON makes use of the Stratum protocol to allow for support for GPU mining using a modified version of XMRig[39].
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。

Mining Rewards 挖矿奖励

On successful completion of the Proof of Work for a new block, the miner is rewarded with HYCON. The mining process for HYCON is planned to last for 50 years. As a consequence of this drawn out timeline, as well as the high rate of block publication, the reward for

publishing a block is necessarily low, with a high volume of transaction fees likely to be a higher revenue source than the specific reward from publishing a block.
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 50 年。根据这样的时间表以及高出块率，完成新块开采的报酬必然是很低的，而更多的收入可能来自大量的交易费用，而不是出块的奖励。

Wallets & Accounts 钱包与账户

HYCON Wallet GUI HYCON 钱包图形用户界面（GUI）

A full node running the HYCON software has access to a locally hosted web GUI allowing for wallet operations, transactions, and blockchain exploration. The GUI was written using React to allow for a lightweight high-performance interface.
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 Wallet HYCON 钱包

HYCON wallets employ industry standard elliptic curve cryptography methods for transaction signing, specifically sep256k [33], as well as implementing mnemonic codes for wallet recovery as specified by BIP 39 [40], to allow for ease of integration for third party wallet providers.
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 sep256k【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。

Accounts & Balances 账户与余额

In order to keep track of the spending and balances of HYCON participants, it is necessary to implement an accounting model. The model chosen for use in HYCON is based on the one used in Ethereum and described in the Ethereum Yellow paper[34], a data structure called a Merkle Patricia Trie[35]. Each block contains the world state as a result of the publication of its contained set of transactions, the value of which is the hash of the merkle patricia root representing the account data for all HYCON accounts.
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。每个块包含着块中交易结束后的状态，用 MPT 树根的哈希值表示，代表了所有 HYCON 账户的账户数据。
The account data that is stored is the balance of that particular account in HYCON, a reference to the most recent block referencing that particular account, and a nonce value representing how many transactions that particular account has initiated. The nonce value is used to protect against replay attacks, and the previous block reference is an optimisation to allow for quicker transaction history querying as well as easier tracking for SPECTRE in the case of a double spend.
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。

Synchronisation 同步

HYCON will employ a headers first approach to initial synchronisation with the network. On first startup, and subsequent startups thereafter a message is sent to connected peers asking for a number of headers with a block height subsequent to a certain block height (the currently stored maximum block height in their local database). On receipt of those headers, the blocks are verified and if they are missing from the local database, the full block data is requested from a connected peer. The received blocks are verified again on receipt and then added to the database if they are validated. As blocks can only be added to the database once their parent blocks have been included this process is necessarily sequential.

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的块之后。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。

CONCLUSIONS 结语

This whitepaper’s discussion began by exploring the limitations of existing cryptocurrencies, which was the basis for the entire Infinity Project. The vision of the Infinity Project is to provide a fast, secure, scalable, and user-centric blockchain and cryptocurrency ecosystem available for mass adoption. Through the combination of the SPECTRE protocol and BLAKE-2b hashing algorithm, we have proposed a new cryptocurrency that is both safe and expedient. With the adoption of the methods elaborated herein, the HYCON cryptocurrency and Infinity Project offers a valuable and differentiated addition to the global cryptocurrency landscape.

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。

REFERENCES 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., 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.

[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].

APPENDICES 附录

APPENDIX A - GENESIS BLOCK 附录 A-创世区块

Discussion 讨论

The HYCON genesis block was published on January 4th, 2018 at 3:15am KST(GMT+9) to coincide with the 9th anniversary of the publication of the Bitcoin Genesis Block. Below is a summary of the information contained within the block. The block, along with decoding software written in several programming languages, is available online at the Team Hycon github repository.

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。

The block itself contains a header and six transactions. The six transactions represent the minting of the HYCON that is to be initially allocated. See Appendix B for full details of the token and budget allocation.

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。

The block header contains the mining difficulty, the root of the merkle tree of the transactions, the root of the world account states, and the timestamp of the block.

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。

The remainder of the block data is made up of the individual transactions which are loading up the accounts to be used for future token distribution. It was felt that encoding the transactions within the genesis block in this manner was the most transparent method for preparing for the wide release of HYCON, as it will allow all of the funds from these accounts to be tracked from the beginning.

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。为了大规模发行 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。

Contents of HYCON Genesis Block HYCON 创世区块的内容

When decoded, the contents of the HYCON genesis block are as follows:
解码后，HYCON 创世区块的内容如下：

Block Header 块头
Difficulty 难度: 0 Merkle Root 梅克尔树根:
cff5f8a5381ce41e26bf3f5f7b658dcef0d4935dfd791460614feb894ff36457

State Root 状态树根:
e08408cb5bf38fb2652676af953d169c7997dd2af88299163b9a389b9d6a3ed4

Timestamp 时间戳: Thu Jan 04 03:15:05 KST 2018

Transactions 交易
ICO Account 首次币发行账户
Account Address(raw)账户地址（未加工的）:
9565e92e694ef206abe21d65d3a93996682d41f7 Amount 数量: 2,000,000,000 HYCON

Airdrop Account 空投账户
Account address(raw) 账户地址（未加工的）:
fa7042154efb88d06c198ef106ca31aed57e6875 Amount 数量: 400,000,000 HYCON

Team Account 团队账户
Account address(raw) 账户地址（未加工的）:
8bab45e2f5c79c00d539ae1a65dbd1f8fd416ca7 Amount 数量: 500,000,000 HYCON

Development Fund 发展基金
Account address(raw) 账户地址（未加工的）:
7a7b31e5aced4889a75d1042a6f1204d2a889af8 Amount 数量: 500,000,000 HYCON

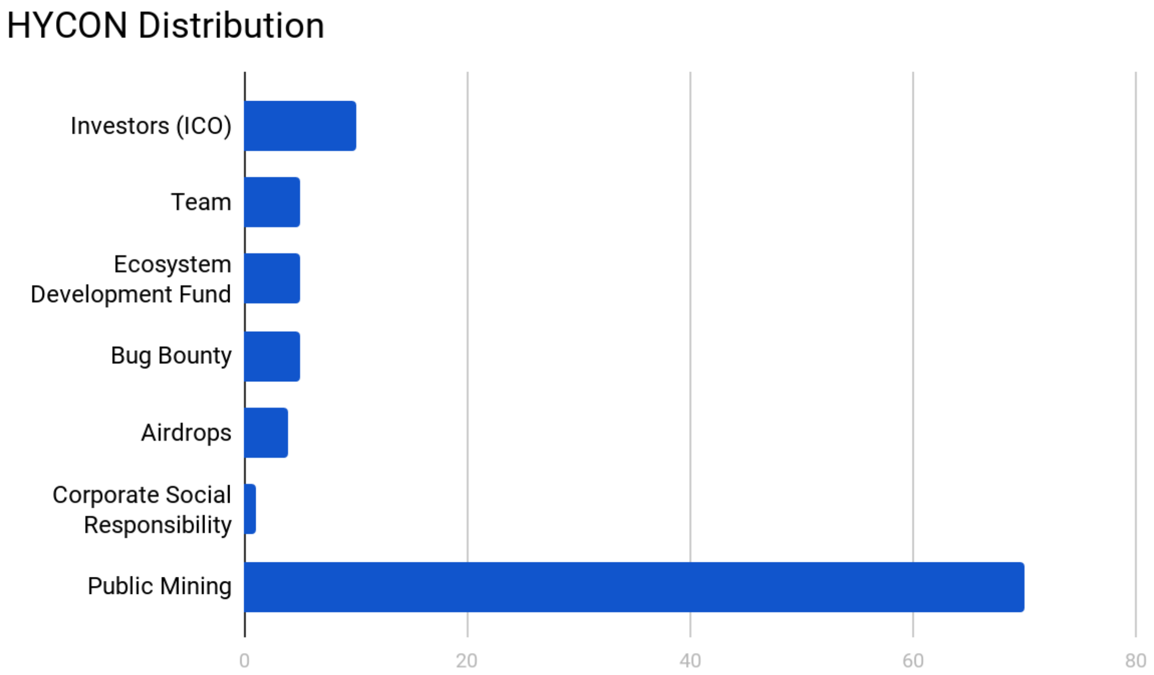
Bug Bounty 漏洞悬赏
Account address(raw) 账户地址（未加工的）:
571a6e4554afbb09ee7da1ae20c18dbca9fabc46 Amount 数量: 500,000,000 HYCON

Corporate Social Responsibility 企业社会责任
Account address(raw) 账户地址（未加工的）:
11d8046e6cd88f9e580b84a0b10c7c452f0030fc Amount 数量: 100,000,000 HYCON

APPENDIX B - Coin DISTRIBUTION & BUDGET ALLOCATION 附录 B-币的分布与预算分配

Coin Distribution 币的分布

The total available number of HYCON to be issued is 10 Billion. The method for allocation is as follows
HYCON 币的总数量为 100 亿。分配方式如下：



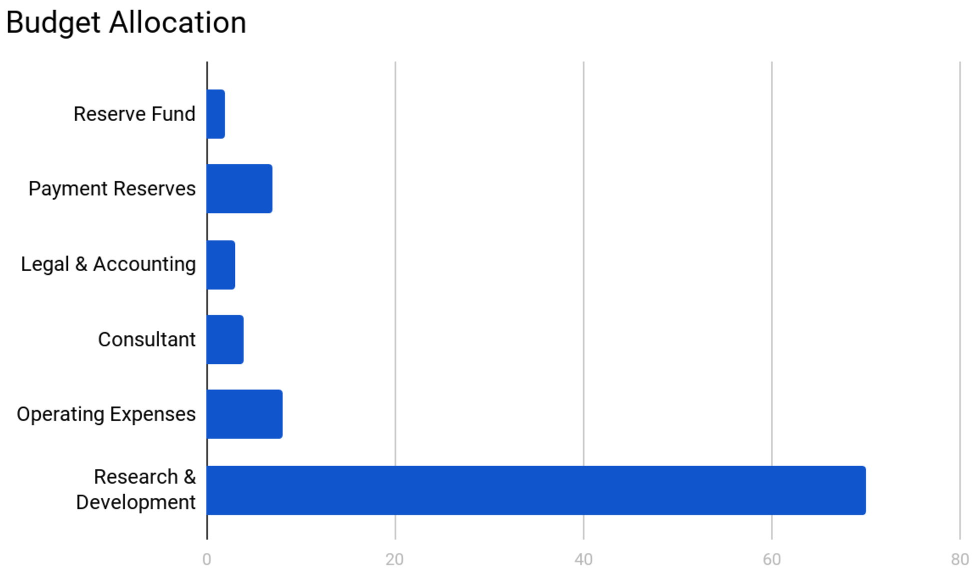
As can be seen in the above chart, the majority of HYCON coins will be available through public mining, with 70% (6 billion HYC) allocated for that purpose. The remaining 30% of coins have been minted within the Genesis block and allocated to HYCON accounts responsible for the distribution of those coins once the network is live.
如上图所示，大部分的 HYCON 币将通过公开采矿获得，大概占 70%（60 亿 HYC），其余 30%在创世区块内产生，并被分配给负责币流通的 HYCON 账户中。
This 30% has been allocated for six purposes. The largest portion is for the participants of the ICO and other pre-investors, with a total of one third of the initially minted coins (10% of HYC total; 1,000,000,000 HYC) being allocated thus. 5% of the total HYC, (500,000,000 HYC) will be provided to the team, to the Ecosystem Development fund, and to the Bug Bounty programs respectively. 100,000,000 HYC or 1% of total HYC will be allocated towards the Corporate Social Responsibility of HYCON. The remaining 400,000,000 HYC, (4% of total HYC) of the minted coins are to be airdropped through events or other yet to be decided upon methods.
这 30%分成 6 个用途。最大的部分分给了首次币发行的参与者以及发行前的投资人，占最初铸币的三分之一（占 HYC 总量的 10%，10 亿 HYC），HYC 总量的 5%（5 亿 HYC）分别分给了团队、生态系统发展基金，以及漏洞悬赏项目。HYC 总量的 1%（1 亿 HYC）分给了

HYCON 的企业社会责任。剩下的 4 亿 HYC（HYC 总量的 4%）将通过活动及其它尚未定下来的方法进行空投。

Budget Allocation 预算分配

The primary focus for the allocation of funds from our ICO is to facilitate the securing of talented development and securing the long term future of the project. As such, 70% of the funds raised will go into funding the future research and development of HYCON and the Infinity Project, including the Infinity platform and the Infinity decentralised exchange. It is important to note that while these are separate projects, the HYCON ICO is the only fund raising drive being taken to ensure the liquidity of the entire project moving forward.

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
Reserve Fund
Payment Reserves
Legal & Accounting
Consultant
Operating Expenses
Research & Development