商业白皮书

版本 1.0

本白皮书仅供讨论之用，不代表任何形式的投资建议。此外，该白皮书不构成出售股票或证券的要约，也不构成购买此类股票或证券的请求。该白皮书上的任何信息都不以影响任何投资决策为目的，也不应成为任何投资决策的基本原理。Skycoin并非投资咨询公司，任何证券投资建议，或任何税务或法律建议都应由投资咨询公司提供。Skycoin鼓励读者寻求适当、独立的专业建议，以知晓任何对Skycoin和区块链整个行业投资的法律和税务要求。只有在独立理财顾问的帮助下，结合在籍国或居住国的环境，在Skycoin或其它代币进行收购、控股或交易的场所内进行投资。请注意，对任何参与代币销售则属非法行为的人士，本白皮书不构成出售要约，或不构成对购买要约的请求。参与代币销售则属非法行为的人士不应参与代币销售。请与您的律师或会计师协商，了解自身是否能参与该代币的销售。本白皮书不应该被理解为投资合同。白皮书（1.0版本）或将进行修改，我们会及时在网站上更新最新版本的白皮书。对于每个更新周期，我们会对更改的地方做出注释，并写明更改理由。新版本的白皮书（根据版本编号）或涵盖推翻之前版本的内容，或对之前内容进行澄清或反驳，在这种情况下，最新版本应该被视为最准确的最新版本。因此，Skycoin官方网站以外渠道发现的白皮书可能包含过期或不准确的信息。

目录

SKYCOIN项目概述 2
简介 3
项目发展 5
Skycoin 6
优势 6
供应与分配 7
Obelisk 7
比特币及其它方法存在的问题 7
解决方案:Obelisk共识算法 8
币时 10
Skywire: 新一代互联网 12
搭建新一代互联网的必要性 12
Skywire概述 13
Skywire/Meshnet图解 14
通信协议 15
支付协议 16
Skyminer硬件平台 16
第一代Skyminer技术规格 16
应用生态系统 17
Skyledger 17
CX/CXO开发框架 18
Skysuite: 本地应用程序 18
CXO图解 19
Skywire应用计划 22
团队|创始人 24
团队|投资人及顾问 25
团队|运营 27
附件 28
参考文献 28

Skycoin项目概述

Skycoin是一个完整的生态系统，加密货币只是生态系统的一部分。Skycoin还包括取消采矿奖励、开发节能定制硬件、实现能与Visa相似项目匹敌的交易速度，以及创造更安全、更高效的互联网。

上述成就得以实现，得益于Skycoin生态系统的5个稳健的组件核心：

Skycoin: 由带宽支持的快速、安全的货币。

Skywire: 真正的去中心化网状网络。

Skyminer: Skywire真正的去中心化网状网络。

Skyledger: 开放的去中心化区块链网络。

Skysuite: 分布式应用程序套件。

架构概述

构件		
Skycoin	REPO	比特币
CX	REPO	以太坊
CXO	REPO	IPFS, FileCoin, Bittorrent, Mega, Dropbox, Google Drive
Skywire	REPO	MPLS, IPv4/IPv6, OpenFlow, Tor, I2P
Sky-Messenger	REPO	Tor, Telegram, Skype, 微信, WhatsApp
BBS	REPO	Steemit, 4chan, Facebook, Twitter

本白皮书将阐述Skycoin生态系统，以及五个支柱如何实现去中心化等承诺。并让全球企业和个人安全地采用区块链技术。

简介

中心化 *(Web 2.0)*

Web 2.0带来了互联网服务提供商，它们为超过2亿2500万人提供了超高速互联网。这创造了例如Uber、Airbnb和Ebay等在内的共享经济，使得全球商业及其分布进入前所未有的阶段。互联网催生了无缝支付方式的出现。人们只需要点击几个按钮，就能通过Paypal和其他电子钱包进行即时交易和全球汇款。这些技术很伟大，但它们有一个重要的缺陷——权力的集中。

去中心化 *(Web 3.0)*

Skycoin增加了现有协议所缺乏的性能。Skycoin建立的快速、可扩展和真正的分散区块链平台将使Web 3.0成为现实，帮助我们摆脱高昂的网络费用以及政府和公司对信息的控制和对隐私的侵犯。

Skywire

Skywire及其隐私协议用户能获得价格更低、更快的互联网，该互联网由用户控制，且对为其他用户提供带宽的用户进行奖励。Skywire是网络中立性解决方案、工具，确保用户私密浏览而不受第三方追踪和控制。

Skyledger

Skyledger为用户带来新一代的去中心化应用程序，所有用户、区域都能使用到这些运行速度快、稳定、具备无限扩展性的应用程序，从中受益。

Skycoin

Skycoin让中心化支付能在数秒内完成，且无需手续费，实现真正的去中心化国际汇款，其转账速度不亚于所有早期使用的支付网络及电子钱包。Skycoin正在开发第一个完全可扩展的协议，为下一代去中心化应用程序、服务和支付提供支持。

为了确保生态系统的稳定，Skycoin持有者会收到第二种货币——币时。系统鼓励用户持有Skycoin以获得币时，使用币时支付Skycoin转账和换取生态系统的服务和功能。币时也可以通过基金会场外回购进行交易，随后进行销毁，减少币时。

除了其现有的核心组件，Skycoin也拥有功能齐全的软硬件：Skycoin钱包实现无缝交易；Skyledger应用率每天都在增长。Skycoin已完成搭建其第一代硬件，目前正在生产各种新一代组件。

项目发展

Skycoin最初是对比特币波动性的审计，后来经过6年的编写（*以及重写*），以解决诸如重复Coinbase输出、签名不变性、交易不变性问题以及关键问题：比特币的共识算法（*工作量证明或*PoW）。

基于PoW，矿机通过比赛解决难解的加密谜题，竞相在区块链中加入下一组交易或区块。第一个提供解决方案的矿机获得报酬和交易费。尽管许多人对这一证明体系表示赞赏也能从中获利，但审计团队只看到危险信号：比特币巨大的计算能源需求将大部分采矿集中到世界上电力价格低廉的地区。

其中一组在自乌克兰北部，他们组成了一个完整的比特币行业，配备了采矿池、硬件和交换设备——被GHash.IO所取代，GHash.IO是一个控制超过60%采矿能力的采矿池(Noble, 2014)。这只是一个例子。位于中国的三大矿池(“十佳和最大的比特币矿业池”，2017年)和ASIC（专用集成电路）挖矿硬件单 一生产商控制这挖矿，因此“中心化”的现状并不能体现中本聪的初衷。

Skycoin团队开始最早的研究，寻求方法解决 PoW算法问题，同时另一场围绕中心化的冲突在加剧——网络中立性的斗争。互联网服务供应商(ISP)控制互联网的物理架构，并可基于不同或分层定价，限制向网络用户提供服务的质量。此外，ISP能够通过向第三方出售信息(例如位置、浏览历史、未加密的信息内容等)来开发客户，这种情况到目前仍未改变。

网络中立性和PoW表面上是两个不同的问题，但Skycoin的团队发现两者存在同样的根本性缺陷：倾向于中心化的系统。Skycoin的研发最终会构成Skywire的关键基础，Skywire是一个真正的去中心化互联网，让用户摆脱对ISP的依赖。

今天的Skycoin项目已经在全球15个开发团队的努力下，落实了多项创新项目(如Skycoin、Skywire、Skyledger等)。Skycoin继续在发展，但在2018年，Skycoin团队将正式向公众推广Skycoin。

Skycoin | 优势

加密货币驱动的Web 3.0

Skycoin项目是最早开发的加密项目之一，而Skycoin是项目最早的产物。Skycoin作为基础设施项目，根植于去中心化的创始理念，运行在完全不同的共识算法上，即“ Obelisk ”或 “ 信任网络 ”。有了“ Obelisk ”，Skycoin不易受到PoW和权益证明（PoS）的弱点影响。

快速

2秒完成交易。没有瓶颈问题或费用问题，Skycoin比其他加密货币速度更快，且能与信用卡和Apple Pay竞争。

零手续费

Skycoin交易需要币时， Skycoin持有者每小时持有一枚币所获得的单独的货币。

安全

在Golang上建立起来，实现从无到有，Skycoin充分利用了经受时间考验的加密标准，确保交易不能被篡改。Skycoin不受51%攻击、逆转、复制和延展性等威胁。

隐私

Skycoin交易结构是为无缝应用CoinJoin协议而设计的。一旦整合，Skycoin将多个钱包的交易混合在一起，确保交易之间无法进行区分。

可持续性

没有PoW和PoS典型的计算能源需求，Skycoin可以在30瓦特的手机处理器上运行。

激励性

Skycoin不仅是一种加密货币，它从Skywire网状网络中获得内在的价值。用户通过提供资源赚取Skycoin，使用Skycoin支付获得网络资源。

实物支撑

Skycoin的实际应用意味着它有真正的资产支撑：带宽。

供应与分配

Skycoin的供应是不变的。总供给上限为1亿个，不得创造或销毁Skycoin。Skycoin的分发是公开的。随着公众获得越来越多的Skycoin，分发速度将会减慢。这种方法确保了Skycoin在用户和社区成员手中，而不是矿池和投机者手中。

Skycoin的使命是通过Skywire网络实现互联网更美好的未来。无主的可分配的币将用于支持网络的长期发展（例如资助更多的用户搭建节点）。由于这种以增长为导向的方法，Skycoin不需要大量的前期资金。撰写该白皮书期间有7500万个未分配的Skycoin，但这些币需要在第一批2500万（25%）分发之后才能分发。在每年第一批25%的 币分发后，会解锁另外5%的币。

初始的25%之后的分发是硬编码到协议上的，其时间是锁定的，因此币的分发保持在最大值5%以下。通过创建一个硬编码的、时间锁定的分配策略，Skycoin能确保分发过程公平，不偏离团队初衷，分配率与用户增长保持一致，且能防止通货膨胀。

Obelisk

Obelisk是Skycoin独特的共识算法，是整个Skycoin基础设施的核心。信任网络共识改变了我们理解和使用区块链技术的方式。Obelisk消除对高昂的采矿资源的需求，摒弃采矿激励的恶性循环，大大地提高了交易的速度及安全性。

比特币存在的问题及PoW的缺陷

比特币早期的编程有一个基本的误判，即通过采矿搭建经济激励的框架，有利于实现去中心化。相反，PoW使得矿池的影响力集中在那些使用廉价电力的资源密集型矿机中。这些具有影响力的群体可对网络进行广泛的更改(如分叉)。

中本聪认为采矿控制是比特币网络面临的最大的非加密威胁网络，因为当超过50%的哈希算力限制在一个行动者手上时，就会出现51%攻击。

这也意味着其网络的运作既不经济也不环保。能源研究员Sebastiaan Deetman（2016年）称“比特币网络不断扩大，可能导致电力连续消耗（相当于）丹麦2020年的总电力消耗。”挖矿所需的连续处理能力输入也使得每月成本上千万，其可持续性不强。

巨大的采矿成本只能靠大量新资本和新用户加入来抵消。但是，很少比特币和以太坊以外的币能有这种紧密关系来维持这种增长。

权益证明的中心化倾向

尽管PoS算法能解决51%攻击的安全问题，但是PoS算法甚至比PoW网络更易受中心化的影响。

由于PoS，参与者持有特定加密货币的多少(或“份额”)决定了其对技术网络进行更改的投票权。参与者在不考虑处理能力的情况下，也可以开采相当于其股份的部分加密货币。这一原理显著地加强了51%攻击的经济壁垒。在公开市场上获得大部分网络代币的成本可能超过了潜在收益。此外，如果一个攻击者成功地成为网络的多数利益相关者, 由于网络稳定性受到影响、市场回应，攻击对他们的影响最为严重。

尽管它提高了人类攻击网络的壁垒，但PoS创造了一个与PoW相同的集中脉冲。在PoW的支持下，对实施网络技术变革的投票权“分配在矿机、开发人员和其他关键成员中”。（Young，2016年）PoS系统则让“主要利益相关者在不考虑社区、企业、矿机和开发人员意愿的情况下，做出任何他们想要的改变。这种投票权的集中，以及对网络的控制，违背了基于分布式账本的加密货币的目的，因为它违背了分配网络中所有元素以避免权力集中的原则。（Young，2016年）

解决方案：Obelisk – 分布式共识算法

为了解决集中的问题，Skycoin使用了分布式的共识算法，Obelisk。根据信任网络，Obelisk分散各要素对网络的影响。网络由节点（*如计算机*、Skyminer等）而不是矿机组成，每个节点都订阅许多被信任的节点。拥有更多订阅者的节点具有更大的影响力。

每一个节点都会分配到作为“公共广播渠道”的个人区块链上，其每一个举动都将被公开记录，是可见的。由于所有共识决策和通信都是通过每个节点的个人区块链进行的，社区可以很容易地对节点进行审计，防止作弊或勾结，但同时不会影响隐私。节点由其加密公钥编址，节点的IP地址只向其直接连接的节点公开。此外，没有固定的端口，也没有已知的有线格式的明文。

根据每个节点的个人区块链留下的公共记录，网络可以切断与不诚实或恶意节点的联系，应对缺陷的问题。根据同样原理，如果社区认为网络的权力过于集中（或不够集中），社区可以改变集体的信任关系，平衡网络的权力。

节点对社区的责任，第三方审计以及共识的透明促进集体决策，为网络带来高度民主和分散的元素。
（延展阅读及技术证明请参阅附录。）

Obelisk的共识解决方案

伸缩性强、能耗低
Obelisk共识算法是一种可扩展的算法，其计算成本低，　是PoW的替代品，能促进算法得以在价格低廉的硬件运行且生成区块。越多人加入，中心化则越难以实现。

有力地防御协同攻击

Obelisk可以抵御大规模、有组织的恶意节点网络协同攻击。该算法是非迭代的，能快速收敛，可以在在只有近邻连接的稀疏的网络（如网状网络）上运行，也能在连接图（即不需要DAG-type连接）的周期里很好地运行。

抵御“51%攻击”

信任网络共识防止中心化趋势。Skycoin不依赖于采矿奖励，因此不易受到PoW/PoS漏洞的影响。

未必有足够的资源汇集扰乱网络，它会对网络用户影响甚微。入侵者仍然需要他人在交易链中的私钥来制造任何破坏。Skycoin没有交易可锻性。此外，依据每个节点包括入侵者的公共记录，确保检测到问题时迅速将其与网络分离。

隐藏IP地址

节点由其加密的公钥编址。一个节点的IP地址只向其直接连接的节点公开。

时钟同步独立

该算法不使用“ 挂钟 ”（即日历日期/时间）。相反，使用从有关信息的验证共识和区块链提取的区块序列号来计算节点的内部时间，即通俗来说是“ 区块时钟。 ”

存在两种类型的节点：共识和区块生成

一个共识节点从一个或多个成块节点接收输入。每个节点的算法是独立的，但它们都在相同的数据结构上运行。两种类型节点一直对数据来源进行验证，检测欺诈性数据。欺骗性的或无效的消息被检测到，会被除掉，且永远不得传播——参与可疑活动的对等节点会被切断，其公钥也被禁止使用。

币时

Skycoin交易不收取费用。交易费用类似于区块奖励，会刺激矿工抬高费用，影响网络的发展，仅带来负面效果的经济激励。通过取消交易费用，Skycoin为所有持有者带来公平的投资利益。

Skycoin交易收取的是币时，而不是Skycoin或美元。要赚取币时，用户只需持有Skycoin。每1个地址持有1个Skycoin1小时可获得1币时。因此，持有1000个Skycoin 1小时就可以获得1000个币时。若交易所持有Skycoin，则交易所拥有其赚取的所有币时。

除交易费外，币时还可以通过充当混合抵押币来提高Skycoin　CoinJoin基础设施内交易的隐私，从而防止参与者退出或降低CoinJoin交易速度。

支付币时可在Skycoin生态系统中使用不同的功能，如专用虚拟网络服务、Popcorn Time（爆米花时间）网站电影下载以及Skywire额外带宽等。若持有者对币时的货币价值更感兴趣，可通过场外回购（*OTC*）的方式轻松获取币时，保证其基础价值。此外，Skycoin去中心化交易所启动后，币时持有者可通过交易所将币时兑换成其他各种货币。

为了防止通货膨胀并合理使用币时，每小时只产生最多1亿个币时。每次交易会销毁Skycoin输出生成的币时，销毁数量为交易中即将耗费的累计币时50%（四舍五入），从而使币时减少，币时数量得到限制，并在循环中达到平衡值。

OTC回购

为了确保建立一个健康的币时经济机制，并回馈在测试中获得币时的硬件测试人员，Skycoin基金会将开始资助OTC回购币时。回购的资金来自未分配的币。该基金会将销毁其购买的币时以增加币时的稀缺性和价值。

硬件钱包

硬件钱包用于安全存储加密货币资金的物理电子设备，旨在将私钥与网络环境隔离开来，黑客需实际拿到该设备才能访问私钥。目前，硬件钱包有多种价位供用户选择，支持不同的加密货币，满足用户偏好。

Skycoin认为硬件钱包是储存加密货币最安全的手段。为了最大限度地提高硬件钱包的使用率，除推出自己的硬件钱包之外，Skycoin将在不久之后与几款最受欢迎的硬件钱包合作。Skycoin硬件钱包将支持储存数十种替代货币以及Skyledger上的货币，可以说是Skycoin移动钱包和桌面钱包带来的最大便利。

Skyminer

搭建新一代互联网的必要性

互联网一直是实现个人赋权的工具和推动商业创新的平台。然而，当今的互联网并未扩展到满足企业和消费者的需求。

从最基础的层面来说，由于缺乏基础设施，且连接和设备成本高昂，全球超过一半的国家和地区处于离线状态（Taylor，2016年）。 然而，当7.67亿人每人每天依靠不到1.90美元维持生活时（《2016年贫困和共享繁荣报告2016》，2016，第3页），经济因素是导致这些人置身“网”外的决定性因素。 由于消费者必须支付互联网服务供应商（ISP）规定的价格，在市场的作用下，较为富裕的国家得以连接上互联网，也正是那里可能发生有关收益的争议。

发达国家带来的盈利机会相当具有说服力，但并不意味着互联网接入不受限制。网络用户和ISP的关系长期以来一直存在争议——ISP负责制定规则，消费者按规则付费。近期网络中立性原则被废除，随即引发了大量的公众抗议。然而，无论消费者能否成功地抵制中立性被废除，都无法改变他们为获得这一重要服务而对ISP的依赖。

那些处在收益争议风口的企业，也表达了反对的意见。不过这些企业面临的是现有互联网的另一个问题。作为新兴技术的引领者，他们有雄心抱负，但受到带宽和服务质量（QoS）的限制。使用案例包括：

- 移动增强现实/虚拟现实
- 无人驾驶车
- 物联网（IoT）

网络容量是阻止这些技术和其他新兴技术应用的最后一个障碍之一。随着媒体对质量的标准提高以及更多设备连接，代宽需求也将继续上升。由于物联网技术在人类生活中扮演着更重要的角色，为了确保操作安全，延时、冗余和服务质量将变得越来越重要。

历史已经表明循环创新的必然性。当一项服务不能满足其用户的需求时，用户最终会做出某种程度的回应，并为下一轮创新奠定基础。需求是创新的源泉，而现在最需要做的，莫过于建立一个新的去中心化的互联网—Skywire。

Skywire提出的最低要求，降低了准入门槛，其呈现出的分布式网状网络也意味着隐私、安全和独立性。Skywire的速度和适应能力也提供了无限的创新空间。但更重要的是，Skywire改变了长期以来一个小型中心机构掌权的局面，实现了权力的平等分配。

Skywire概述

Skywire项目旨在创建更快、更实惠、更为便捷的激励型网状网络，且提供比当前互联网质量更高的服务。

为实现这些目标，网状网络必须具备：

通讯协议

免受传输控制协议/互联网协议（TCP / IP）限制。

支付协议

补偿运营商提供给网络的资源。

硬件平台

能够跨越最后一英里，并提供扩展网络所需的网络、存储和计算资源。

应用生态系统

推动网络应用和网络资源需求。

Skywire团队投入近四年时间开发出可靠的解决方案满足了以上要求。如今Skywire路由和支付协议已准备好投入使用，第一代硬件设备已经完成并已发出。应用程序（包括第三方和本地应用）开发正在全面展开。一切都已准备就绪，Skywire已为构建新的更好的互联网做好准备。

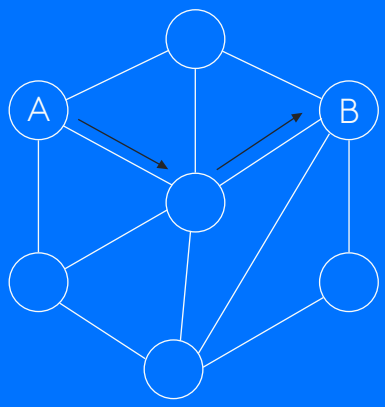
Skywire/Meshnet

客户端运行专用虚拟网络客户端

所有客户端流量均通过TUN/TAP适配器传输

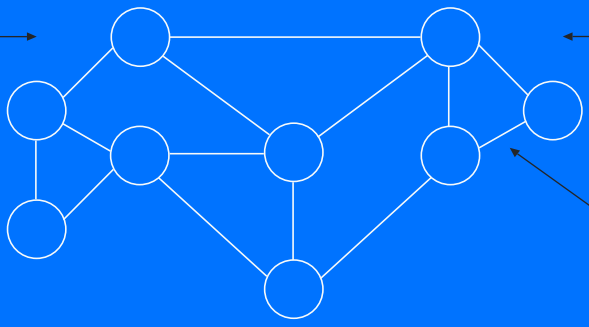
专用虚拟网络客户端tongg Skywire连接服务器

源路由可避免hot potato BGP路由并通过DOS标准实现路由选择。



VPN将流量传输回旧的IP4 / IP6互联网

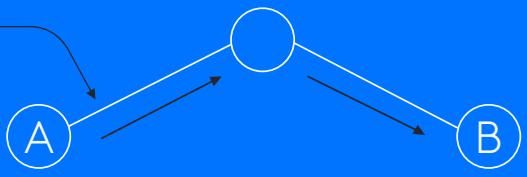
Skywire节点由其公钥标识。



Skywire节点通过固定的网状点对点拓扑进行连接。

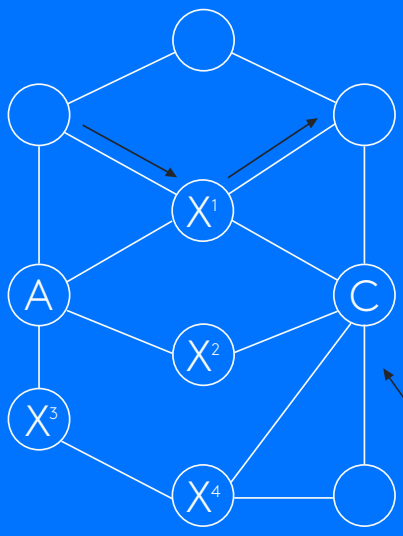
节点之间的连接称为传输。

节点可制定数据包转发规则，称为路由。
R：A->B->C。



多跳数据传输有助于防止资源耗尽攻击，如分布式拒绝服务。节点可使用Skycoin来获取、保留和分配网络资源。

节点根据其消耗和生产的资源的实用性和平衡状况来接收或消费币。



规模不变，可在多种距离范围内操作。适用于国家，城市，工厂内部的家庭网络和物联网（*IOT*）的网络。

网络使用源站路由选项并支持多重连接。

网络支持不同的路由以满足应用服务质量要求。

节点可制定数据包转发规则，称为路由。 R：A->B->C。

R: A > X1 > C

R: A > X2 > C

R: A > X3 > X4 > C

Skycoin应用程序在自己的网络上运行并使用独立的命名空间。

通讯协议

目前几乎所有的互联网流量都使用传输控制协议/互联网协议（TCP / IP）通信协议。这些协议已有40多年的历史，也不适用于网状网络。TCP将所有的数据包丢失现象都解释为拥堵，并自动缩减连接速度以减轻拥堵。此外，由于每个节点必须独立查找发送下一个数据包的位置，因此基于IP的路由速度较慢且计算量大。

Skywire通信协议采用多协议标签交换（MPLS）技术，在任何媒介上实现了高延展性和高速的数据传输。在MPLS技术支持下，通过网络的路由在发送流量之前便得以确定。嵌套标签描述了其通过网络的路由，可被出站的数据包接收。当一个节点收到一个数据包时，它只读取最外面的标签并进行相应的操作，与IP路由表查找相比，大大地减少了计算量。

当前的互联网刺激ISP尽快通过所谓的“ hot potato路由 ”将其流量转储到其他网络上。这种做法有利于ISP，但对通过网络传输的流量不利。由于跳跃次数增加，hot potato路由会导致传输延迟大大增加。Skywire完全避开了这个问题。Skywire源节点始终倾向于以低延迟、低成本的方式发送流量，同时保护路由。转发流量越多，运行节点的收益也就越多，从而激励了网络拓扑的高效运行。此外，源节点可以完全控制路由，同时修改路由协议以适应其需求。常见方案包括：

- 优化网络电话（VOIP）或游戏的低延迟网络路径
- 针对视频和文件共享应用程序的高吞吐量网络路径进行优化
- 将路径绑定到目的地以实现冗余，减少延迟和吞吐量

相对于TCP/IP而言，Skywire的通信协议在私密性和安全性方面具有更大的优势。数据包路由上的每个Skywire节点只能看到数据包的前一跳和下一跳，而看不见发出者、接受者或内容，这是针对IPv4的重大改进。公钥哈希代替了IP地址，对Skywire网络上的节点进行唯一标识。由于源节点可以通过公钥验证目的地的真实性，因此成功防止了中间人攻击。

Skywire是端对端加密的，所以持有流量的人无法得知流量的内容。相比之下，代管TOR退出节点的原理也大致相似。但是，TOR退出节点会在主机系统上存储数据的副本，主机因而容易受到法律问题的困扰。如果一个节点被怀疑为恶意节点，该节点将会进入黑名单并因此被禁止重新连接到主机。

支付协议

目前所有互联网替代品都存在一个严重的缺陷：由志愿者无偿运营，因此大多数用户访问网络资源，却没有给予回报。 Skywire通过其内含的支付协议解决了这个问题，每个节点都可以作为一个自动计量、计费和结算的微型ISP有效地运作。

节点希望转发流量并获得补贴（即Skycoin和币时），这相当于Skycoin的“挖矿”，许多用户会通过这种方式最先赚取到他们的Skycoin。路由上的每个节点记录自己转发的流量，源节点则记录自己发送的流量。带宽支付通过不知情的第三方托管系统自动定期结算。

源节点持有由第三方托管的币。假名帐户为与第三方创建。每个节点都可以通过第三方来验证信息源节点及其支付能力的声誉，而无需知道第三方的身份。从第三方的角度来看，所有节点都将显示为多个分离的假名帐户。

小额交易将通过区块链之外进行内部结算。一旦余额超过阈值（目前为1 skycoin），区块链外的交易可以撤回到新生成的、从未使用过的地址，从而减少区块链膨胀并鼓励小额交易在区块链外进行。

有关Skywire的其他信息，请参阅附录。

应用生态系统

Skyledger

Skyledger是可扩展的、安全的、分散的第三方应用启动平台——帮助更多企业采用区块链架构的必要解决方案。由于其速度更快、安全性更高和隐私性更强，区块链最终可发挥其潜力，为现代企业提供可靠、快速、多功能的基础平台。

通过Skyledger，客户可以根据自己的需求定制私人区块链，享受Skycoin技术带来的所有成果：

- 能耗低
- 近乎即时的交易时间
- 无交易费用

由于每个企业各自拥有自己的区块链，它们不会面临以太坊ERC-20等平台上出现的拥堵问题，从而 消除了目前阻止许多企业应用区块链技术的限制。如，能源公司在法律上必须遵守严格的操作准则 （如交易速度、报告、计量）。考虑到其商业价值和法律义务，企业担心影响其运营，不会冒险 使用不相干组织的流量。使用Skyledger，这个问题可以完全避免。

企业已经开始采用Skyledger作为其区块链解决方案的基础：

SPO

SPO是基于Skyledger的去中心化服务，运行存储和数据传输，是一个对等加密互联网浏览器，且内置防垃圾邮件和由用户控制的数据提要过滤多种功能，确保实现未来网站定制创建、购物、游戏、视频等应用。

MyDailyLife *(MDL)*人才中心

MDL旨在为2.3万亿美元的娱乐行业建立信任托链。 MDL平台具有独特的基于消费者的生态系统市场和微型KOL（重要意见领袖）合作伙伴计划，可帮助提高其收入。

CX/CXO开发框架

Skycoin生态系统包括自己的编程语言和不可变的对象系统，为Skywire网络的应用逻辑和数据分发提供基础。

CX编程语言

CX编程语言是由Skycoin团队开发的能构建智能合同的确定性语言，且安全性更高、功能更多。CX可用于创建分布式应用程序、视频游戏以及程序FPGA芯片。技术型用户可在Skycoin博客上查阅详细的语言概述（*参见附录*）。

CX对象系统*(CXO)*

分布式内容共享协议CXO支持结构化数据的点对点复制，其中数据只能由发布者修改。通过CXO，发布者创建数据提要并使用自己的私钥署名。其他节点可以订阅此数据提要，使其在网络的使用范围更广。但是，若无发布者的私钥，其他节点便无法更改数据提要，因此即使文件不是从发布者的源节点直接下载的，也能确保数据的完整性。

CXO将有关区块链的不变性和内容分发网络（CDN）的可扩展性结合起来。当内容不一定存储在区块链上，但需要易于获取、可验证时，这一点作用尤为突出。例如，将社交媒体平台的所有内容直接存储在区块链中，平台会因为更多人使用而膨胀。使用CXO存储和分发内容可以完全避免这一问题。

Skysuite：本地应用程序

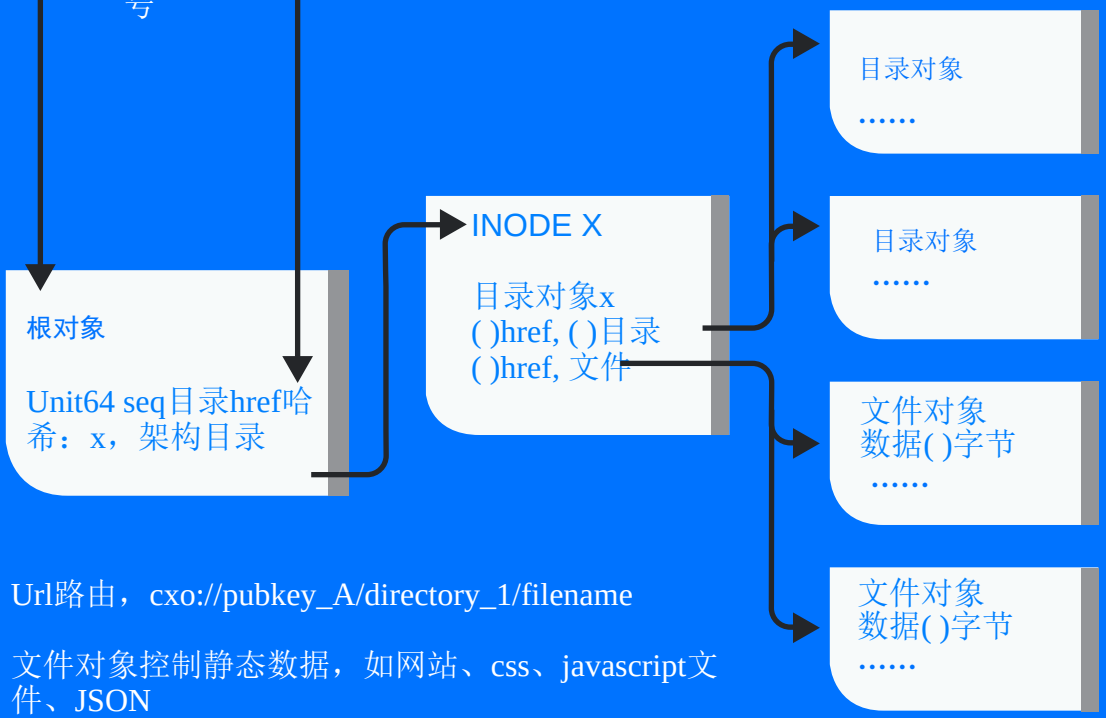
Skycoin团队开发了一套在Skywire网络本地运行的独立的应用程序。第三方应用与这些应用结合，使得对Skycoin生态系统服务的需求不断增多。一些应用目前正在开发中，包括Sky-Messenger，IM客户端；Skycoin BBS，社交媒体平台；Cryptosphere，专用虚拟网络客户端；还有 Kitty Cash，广受欢迎的Cryptokitties游戏的继承者。

CXO

发布者控制数据存储内容及更新内容

发布者使用私钥签署根对象

更新数据存储内容序列号



Url路由，cxo://pubkey_A/directory_1/filename

文件对象控制静态数据，如网站、css、javascript文件、JSON

SHA256哈希可识别并捕捉对象

文件若无变动，则无需从新下载，节约网络带宽并加速内容传递

Skyminer硬件

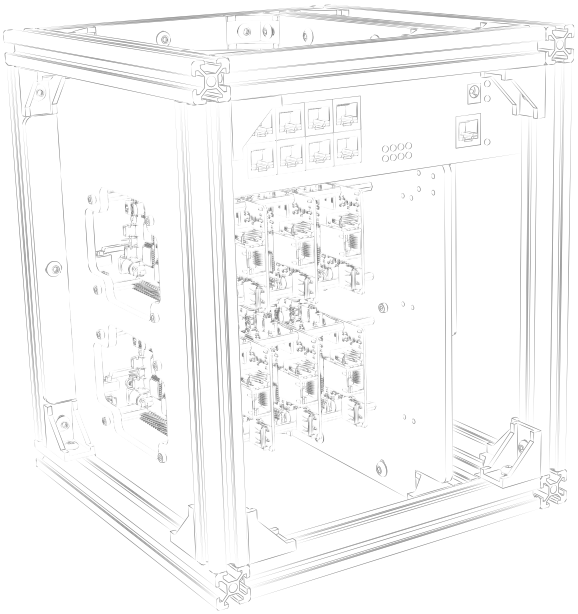
Skyminer是一款定制的专用虚拟网络，其具备计算能力、网络和存储功能，是Skywire网络基础设施的核心。

Skycoin生态系统的设计就是要让每一位用户，不管通过怎样的途径、掌握怎样的技术知识，都能获得Skycoin生态系统的服务。Skyminer是用户访问生态系统的主要驱动力。Skyminer硬件成本低、效率高，因此购买及运行其硬件的成本也相对较低。Skyminer“即插即用”功能目前正在开发中，旨在帮助不懂技术的用户轻松部署自己的节点。

为实现Skycoin开源项目的根本目的，我们将推出完整的Skyminer零件清单和组装指南，所有想使用Skyminer的用户都可获得这些资料。

第一版Skyminer技术规格

- 定制PCB板
- 16端口OpenWRT路由器
- 16 GB RAM（*32 x 512MB DDR3*）
- ARM Cortex ™-A53 CPU
- 8 x 16GB Class-10 A1 Micro SD
- 六核Mali450 GPU
- LAN带宽: 8 x 100Mbps
- 千兆以太网，8 + 1端口交换
- 64-位Linux *(Alpine Linux)*



组件生产

Skycoin团队在逐步提高Skyminer的产量。主网建成后，Skycoin计划让一家工厂每周生产1000组Skyminer，并计划在2019年第一季度之前扩大到2家工厂，每家每周生产10,000组Skyminer。

硬件研发

Skyminer有两个领域需要重点研发。第一个是天线硬件。Skycoin团队正在开发两种主要的天线：

1. 短程（*最远*5*公里，视距清晰*）天线，用于城区的点对点接入
2. 远程（*最远*15*公里*）天线连接人口稀少的社区

这些天线将使用多输入多输出（MIMO）传递信息，实现性能最优化，同时扩大有效范围。为满足全球客户群的需求，天线具备两种电源配置：

1. 低功率天线，符合美国联邦通信委员会对无照传输的规定和类似的国际规定（CFR，标题47，第15节）
2. 高功率天线，可在其获准的地理区域上使用

第一代Skywire天线组件现在正处于测试阶段，预计将于2018年中推出。

第二个研发的重点领域是Skywire矿机组件。研发团队最初开发太字节存储阵列和比第一代Skywire矿机组件解密流量更快的专用FPGA芯片。研发团队计划与硬件供应商合作，在不提高硬件价格的情况下，优化硬件。

Skywire应用计划

部署全部完成后，要通过Skywire直接访问互联网骨干网，Skywire就必须提供：

- 人口密集地区节点之间的短程连接
- 人口稀少地区节点之间的远程无线连接
- 连接到光纤骨干网的回程连接

凭借目前的技术，以上目标均可实现。Skywire将通过三个阶段的发展推出其网络。

第一阶段：测试网

第一阶段已正在推进。基于软件的测试网已于2017年底开始运行。第一台Skyminer设备，当时被称为Skyminers，已经发货，基于硬件的测试网将于2018年第一季度末开始运行。通过测试网，研发团队可以确保Skywire具备条件，获得更广泛的应用。运行官方Skyminer和精选自制矿机的用户，会因其参与测试网而获得Skycoin奖励。

在这个阶段，网络的运行作为Skywire节点之间的覆盖流量必须通过现有的互联网，除非节点通过以太网或WiFi直接连接。

第二阶段：主网

第二阶段标志着主网的正式启动和实现真实网状网络功能的开始。 Skywire节点将通过WiFi相互连接并分享带宽。短程和远程无线天线在这个阶段已经可以使用，让对等节点间的距离分别达到5公里和15公里。

在这个阶段中，带宽市场不会达到自给自足的临界质量，因此Skycoin基金会暂时资助节点运营。为奖励早期使用者的措施，正在运行的所有节点每天都可以收到平均分配的Skycoin。随着节点数量增加，这种补贴会相应减少，通过使用而获得奖励相应增加。到最后，运行节点的奖励会完全来自于使用。

第三阶段：回程

回程在传统意义上指连接网络边缘和主干网的网络部分。在Skywire中，回程是指无线网状网与光纤连接点之间的连接。建立Skywire回程连接比建立点对点连接涉及到的更多，因为它要求在数据托管中心或其他网络点与光纤建立直接连接。

由于促进回程连接的节点将流量聚合到互联网骨干网中，它们比网状网上的典型节点需要更多的前期投资和硬件容量。目前拥有光纤连接的二级网络运营商可以轻松设置自己的Skywire设备，辅助回程连接，从而开拓出利用未使用的带宽赚钱的方法。

一旦实施回程连接，网状网将不再依赖3级ISP（例如康卡）。为了进一步提高性能和冗余，回程连接应在尽可能多的光纤之间建立。

第三阶段完成搭建Skywire架构，但这项工作绝不止步于此，并将不断研发，升级网络硬件，提高网络的效率和性能，确保Skywire网络始终可以满足用户的需求。

团队|创始人

杰出的人创造伟大的事业。Skycoin的团队集合了最杰出的人才，共同创造未来。

Synth
创始人
Synth是比特币最早的开发者之一。8年前创办了skycoin，以期创造一个崭新的去中心化的网络。目前为数个加密货币项目担任顾问。Synth有数学、分布式系统和符号逻辑学背景。

Houwu Chen
创始人
Houwu是以太坊的开发者之一，也是Skycoin分布式网络及加密货币的中心共识协议Oblelisk白皮书的作者。他曾在清华大学攻读博士学位。

Steve Leonard
创始人
Steve编写了Skycoin多数初始软件。在Skycoin之前，他创建了几个广为流行的商务电子后端。他具有函数编程、化学和数学背景。

团队|投资人及顾问

Michael Terpin
CoinAgenda创始人兼首席执行官
Michael Terpin，Transform Group的创始人兼首席执行官，Marketwired创始人。2013年初，共同创立了BitAngels，推动CoinAgenda系列会议。联合创立了早期的区块链孵化器bCommerce Labs和Dapps基金。目前担任Alphabit基金ICO投资委员会主席，并为众多区块链公司和基金会提供建议。Terpin为150多家区块链公司和基金会的公关工作贡献力量。

Mike Doty
ARK联合创始人| Bitseed联合创始人
Mike Doty拥有超过25年的机械工程和设计经验，专长涵盖制造、设计、分析、测试和系统集成。Doty拥有加州理工学院的工程和应用科学学士学位。他是注册质量工程师（CQE）和注册可靠性工程师（CRE）。

Richard Kastelein
Blockchain News创始人（2017年并购）
Cryptoassets设计集团总监
Blockchain Partners合伙人
Richard Kastelein是一位多项奖项加身的出版商、创新执行官和企业家，是六家区块链初创公司咨询委员会成员。Kastelein在Blockchain News上撰写了超过1200篇关于区块链技术和创业公司的文章，并发表在《哈佛商业评论》、《Wired》和《Venturebeat》等知名刊物。

Dr. John Henry Clippinger
首席创新官 / Swytch.io创始人 / Tokencommons.org创始人 /
MIT媒体实验室的科学家
John Henry Clippinger目前是麻省理工学院媒体实验室人类动力学小组的研究科学家，同时还是ID3的共同创始人和执行董事。此前，Clippinger博士是哈佛大学法律实验室的创始人兼联合主任。他同时也是eG8论坛、全球领导力电信委员会以及世界经济论坛风险分析网络的成员。

Patrick Dai

Qtum创始人兼首席执行官

Patrick毕业于德雷珀大学，在完成博士课程之前离开中国科学院。他曾在阿里巴巴工作。拥有区块链技术开发方面的专业知识，并一直致力于推动其发展。

Josh Ogle

Samples.com和The Original Agency首席执行官|天使投资人

Josh有着引导和扩大企业、帮助企业重新定义市场领域的经验。不管是商业渠道还是代理工作，在他的指引下，每家企业都走向繁荣。他为企业带来了一种通过凝聚力和生产力经营和发挥规模效应的方式，以最大限度地发挥他们的潜力。作为康奈尔大学的校友，他对未来科技和区块链技术的发展充满信心。

Alphabit

数字货币基金

Alphabit由伦敦对冲基金Light Peak Capital的前货币交易员Liam Robertson共同创立。Alphabit是一个3亿美元的基金，业务内容为开放式共同基金和对冲基金的交叉。Alphabit之前的投资包括Videocoin和Stormx。

TokenKey

由Chris Emms创立的Tokenkey是一支专业化的全球团队，他们为区块链项目提供从最初提出想法到最后交付的帮助。他们的服务包括：白皮书和商业计划、代币经济学、审计和评级、架构和合规、公司实体和法律、数字资产创建、咨询委员会、代币发行和交易所上市、监护和托管、营销和公关、社区管理和奖励以及加密货币交易和套利。

SharkCIA

市场和策略

SharkCIA是一个专门从事研究、投资以及营销区块链公司的机构。SharkCIA的成员来自世界各地，团队经验包括提供黑客式增长、公共关系，基层社区扩展、战略建议以及帮助较为不知名的项目获得更广泛的认可和增加市值。

Hive Chain Labs

来自硅谷的Hive Chan Labs和Hchain资本致力于跨学科区块链项目的研究和孵化。Hchain是区块链的信仰者，并持有“使区块链无处不在”的愿景。他们的投资案例包括ICO.com、 TKN.com、Scry、 RChain以及Polkadot等。

团队|运营

Sam Fong Sing

首席运营官

2017年Sam开始了Skycoin中国团队的战略发展。Sam是一个区块链基金会的联合创始人，以及在上海和新加坡设有办事处的管理咨询公司bluePro Consulting的创始合伙人。他曾担任世界500强公司的高级职位。Sam是南澳大学的校友。

Jesse Sun

东部地区运营

Jesse Sun创办和运营的基金投资于区块链初创公司、应用程序、加密货币以及比特币开采。在加入密码世界之前，他是一名管理顾问。Sun拥有曼彻斯特商学院的MBA学位和同济大学硕士学位。

附件

《加密货币网络分布式共识算法》
由用户johnstuartmill及一名匿名用户提供

Skywire：一个新的互联网

CX 概述

Resources

10 个最佳最大的比特币采矿池
(2017年11月)

10 个最佳最大的比特币采矿池2017
(2017年11月)

到2020年，比特币消耗的电力将相当于丹麦消耗的电力
Deetman, S.(2016年3月29日)

全球findex数据库2014
Demirguc-Kunt, A., Klapper, L., Singer, D., & Oudheusden, P. V. (2015年).

比特币出现以前的加密货币简史
Griffith, K.（2014年4月16日）

2017年开发年度报告(2017年)

两位研究人员认为比特币的末日即将来临
Noble, Z.(2014年6月17日)

贫困与共享繁荣2016 (2016年)

有线电视公司如何阻止你使用光纤
Smith, D.(2014年6月6日)

研究表明47%的世界人口现在使用互联网
Taylor, A.(2016年11月22日)

工作量证明与权益证明：优势和劣势
Young, J.(2016年9月14日)

Skycoin.net