CHIA NETWORK INC.

商业白皮书

1.0.1 版 - 2021 年 2 月 9 日-2021 年 3 月 1 日修订

天下数据 于 2021 年 3 月 18 日汉化编辑

Chia(奇亚)QQ 交流: 228877063

介绍

比特币及其底层区块链被许多人视为货币、金融、商业和社会本身不可逆转、变革性进化的前沿。

比特币被异想天开地描述为 "神奇的互联网货币"。那些认为这是不屑一顾的人低估了可编程数字货币将要产生的变革性影响。本白皮书将试图解释我们认为数字货币和区块链最终能对商业和社会产生的影响。我们相信，区块链应用于货币和货币相邻的用例，有能力改变金融、财富、安全、数字安全，并最终改变整个信任的概念。

以此原则为根本，设计良好的数字货币应该比现金更容易使用，更难被盗。适当规则下，数字货币的安全不应该依靠专家团队来保障。丢失钥匙应该很容易找回。任何人，包括家用电脑上的个人，都应该能够参与交易的验证。任何人都应该能够种植(farm)我们的采矿版本,而不是少数强大的大型实体。

使用架构良好的数字货币，任何人都应该能够成为自己的银行，因为它更快，更便宜，最终更安全。我们相信，chia(奇亚)是一种建立在我们新的区块链上的新数字货币，具有与其他数字货币完全不同的功能和安全性，将最终实现 "神奇的互联网货币 "的承诺。

简史:从 **Bitcoin** 比特币 **…**到 **Chia(**奇亚**)**

和所有新技术一样，数字货币和区块链的影响在短期内被高估，长期内被低估。迄今为止，比特币已经引领了潮流，就像 ARPANET 和早期的 ISP 为互联网、网络铺平了道路，最终形成了我们目前所处的 "有一个应用 "的世界。

越是研究比特币，越是微妙、强大、迷人。中本聪共识证明，一个全球共享的数据库可以不相信任何人。然而，比特币协议所使用的工作证明方法中包含了一个假设，即未使用的 CPU 周期在全球数百万台计算机中是一种巨大的过剩商品。这个前提最终没有被证明是正确的，但寻找一种巨大的过剩商品是有先见之明的。专用的一次性硬件和廉价的电力，在工作证明计算方面反而比通用 CPU 好得多。

这种发展削弱了比特币的另一个核心原则--去中心化，因为专业的 "挖矿 "硬件越来越多地被少数几个大型实体所拥有和运营，这些实体是在靠近廉价电力的特制大型数据中心。因此，本来是一个去中心化的共识网络，却出现了中心化。这种集中化降低了信任度，并引发了有关电力消耗、电子垃圾、碳排放和地缘政治的难题。

在中本聪的白皮书发布 11 年后，世界已经从比特币实验中学到了很多东西。密码学的研究进展也在不断推进。在 Chia(奇亚)，我们开始利用这些经验，站在 Merkle、Rivest、Hellman、Finney、Wuille、Boneh 等巨人的肩膀上，应用新的密码学，其中一些是我们帮助发明和完善的，创造比特币实验的下一个篇章。

我们正在对比特币进行加倍的努力。我们正在采用和帮助比特币采用新的技术，比如 bech32m, graftroot, 和 taproot。Chia(奇亚)的交易率和区块大小仅仅是基于更现代化的工程就有效地翻了一倍。

我们的币使用了比特币未使用的交易产出（UTXO）模型的改良版本。Chia(奇亚)是自比特币以来第一个新的中本共识，并利用了中本聪之前未被阐述的许多见解，比如自然日志管理与工作难度重置

相关的关键区块链常数。我们为这个项目带来了先进的工程设计、部署互联网规模应用的经验和严谨的科学态度。

我们还发挥创造力，解决推动全球采用数字货币的其他重要方面。我们有一个独特的计划，利用企业和后来的上市公司形式，给这个新的互联网货币提供透明度、控制力、监管的认可和公众的支持。

我们将利用我们在这些技术方面的专业知识和市场战略，跟随开源先驱 RedHat 和 MySQL AB 的脚步，扩大全球开源软件支持业务。我们相信，大型机构、企业和其他实体将能够毫无顾忌地获得使用像 chia 这样的数字货币的效率和好处，因为我们将在那里为他们提供支持。

我们同样注重 "Cypherpunks(密码朋克)写代码 "的精神。我们将投资并支持各种形式和规模的开发人员，因为他们在我们的基础层区块链之上建立了前所未有的新应用。我们认为这是我们的杠铃式上市策略。我们认为，只有最大的实体、最小的个人开发者和像你这样的个人，才有需求--现在--可编程的互联网货币。有一天，我们都可能会用 Chia(奇亚)在旧金山买咖啡，但现在我们认为银行和政府以及 De-Fi 集体会用它来建立新的金融技术，解决跨境支付，并发明一个不需要信任那么多中间人的新未来。

我们明确的目标是间接的为 SWIFT、DTCC 以及西联汇款等服务。然而，如果这些实体真的采用我们的技术来改进他们的产品，我们也不会感到惊讶--就像唱片公司最终采用 iTunes 和 Spotify 时一样。

Chia(奇亚)是对基于工作证明的区块链进行改进的尝试，我们称之为空间和时间证明的新共识算法。空间证明不需要消耗大量的电力和浪费的单用途 ASIC 硬件来验证交易，而是利用当今世界上已经存在的过度供应的剩余磁盘空间。

我们观察到，许多需要可编程互联网货币的项目和企业计划转向 Ethereum，却发现了 Ethereum 的智能合约编程语言 Solidity 的苛刻限制。糟糕的设计和安全性使得企业项目几乎不可能采用

Ethereum 来转移生产或规模化的资金或投资。接下来最有可能的替代品，如 Ripple 和 Stellar，也存在重大问题，迫使政府和银行不得不试验性地使用 "内网 "版本的区块链软件代替。内网区块链是私有的，有权限的，与老式的数据库相比，好处不多。它们失去了开放的、去中心化的、安全的区块链的所有积极网络效应。

我们认为，央行数字货币计划、金融机构内部代币化和外部支付、全球企业供应商管理、DeX/DeFi，甚至个人跨境支付，都将在 Chia(奇亚)区块链上发挥最佳效果。

现金、股票、城投债、企业债、期货、数字货币之间的人为壁垒应该会下降。这些工具都应该连接到一个全球市场--部分由你的智能手机为你管理--每天全天交易。购买股票应该像按下按钮一样简单，用特斯拉股票购买特斯拉汽车或一杯咖啡也应该同样简单。玄妙的结算方式不应该阻碍你交易任何特定股票、债券或期货合约的愿望。

你有权私下、安全、稳妥地持有你的财富，并以一种你能用数学方法预测通货膨胀的方式持有它。

你应该有权力非常清楚地知道，当你购买一项资产时，你是在信任谁。

我们也相信，你应该能够安全地购买资产，使用不需要你信任任何人的市场。

Chia(奇亚)是数字世界的绿色货币。

公司愿景

我们成立 Chia Network Inc.的目的是为了推动对 Chia(奇亚)的应用，并为我们如何使用我们的资源提供控制、信任和透明度。一旦我们在公开的证券交易所注册我们的股权，这些控制将是特别强大的，如果你选择成为股东。

我们已经看到了在我们这个项目之前在这个领域的骗局和闹剧，我们将转而拥抱监管机构。投资者应该通过公开信息披露得到保护，这不应该引起争议，当然也不应该在没有这种法律规定的透明度的情况下向公众出售投资。

Chia(奇亚)网络打算向政府、金融机构、企业和大型存储买卖双方出售软件服务和支持其开源区块链和智能交易软件。Chia 还期望促进 DeFi、DeX、跨境支付和新的终端用户钱包创新的草根发展，以加速开发尚未发明但只有安全的分布式可编程货币才有可能的新应用。我们的工具将使这些开发者能够创造出比之前更方便用户使用的应用和钱包。

公司有一个新的和优越的方法来资助、构建和支持区块链，通过一个最终公开的、盈利的、开源的开发公司，持有一个预挖农场（相当于一个预挖矿场）的 Chia(奇亚)币.奇亚网络打算将公司的股权在一个主要的证券交易所上市，以加强其开源软件支持业务在政府、金融机构和企业中的可信度和监管确定性。

公司认为，其企业价值将初步反映其资产负债表上所持有的奇亚的价值。随着企业软件业务的发展，我们相信我们的软件服务和支持业务将增加公司的企业价值，并有助于推动商业和全球范围内对奇
亚果的采用。ChiaNetwork 的资产负债表应允许公司的公开交易股权发挥类似于奇亚币 ETF 的功能。
公司预计其在公开市场上的股权估值将与奇亚币在数字货币交易所的价格变动相关联。

公司业务

公司于 2017 年 8 月 1 日在特拉华州注册成立，由 BitTorrent 的发明人 Bram Cohen 创立。自成立以来，公司一直专注于开发 Chia Network 的区块链，并开始推广其潜在用途。Chia Network 的区块链将是一个全球开源的去中心化网络，使用其原生加密货币运营支付结算系统，将被称为 Chia(奇亚)或 XCH。Chia Network 的区块链旨在更加高效、安全和易于使用。

公司是一家位于加州南旧金山的特拉华州公司，目前有 21 名全职员工和相当于全职的承包商，以及 15 名兼职顾问。16 名员工主要专注于研究和开发活动，5 名员工/承包商专注于公司的管理和实施其商业计划。

公司大事记

Pre Alpha 阶段***:***

2018 年 1 月，奇亚网络在 BPASE'18 上发表了 Beyond Hellman's Time-Memory Trade-Offs with Applications to Proofs of Space 学术论文，并募集了 330 万美元的种子轮融资，于 2018 年 3 月完成。该轮融资包括 Naval、A16Z、True Ventures、Greylock、Galaxy Digital、Metastable 等投资。2018 年 5 月，我们发表了《Simple Proofs of Sequential Work》，在 Eurocrypt 2018 上获得最佳论文。

2018 年 8 月，公司通过 GitHub 向公众发布了第一个开源库 bls-signatures。该库和公司最近发布的源代码已经收到了超过七十五个来自第三方开发者的拉取请求，并吸引了超过三十五个第三方贡献开发者。Ethereum 2、Dash 和其他项目都是奇亚网络区块链组件的贡献者。它们与 Filecoin、
Algorand 一样，也是 Chia Network 部分新技术的采用者。

公司于 2019 年 1 月发布了开源的可验证延迟函数（VDF），这是一种用于加密协议的时间证明基元。为了优化实现和吸引开发者，公司宣布为我们的 VDF 举办 pairof 实现比赛。在两次挑战中，

参赛者竞相创造出更快的公司 VDF 实现，或提交安全漏洞证明。经过两轮的 VDF 竞赛，VDF 算法比原来的参考实现快了 4 倍。随后，千家网络聘请了其中一名参赛者，并与其中一名获奖者签订了合同。

2019 年 7 月，Chia(奇亚)网络发布了空间证明软件、绿皮书，申请了第一批临时专利，并宣布举办空间证明大赛，对算法进行优化。

Alpha 阶段*:*

2019 年 12 月，公司发布了 Chialisp 的 alpha 钱包模拟器和脚本语言文档，以及 Chia Network 的 testnet 区块链的 alpha 实现。

测试阶段*:*

2019 年 4 月，公司发布了区块链的测试版，其中包括 testnet 区块链上的完整钱包功能、交易和智能币。数千名开发者和社区成员已经安装了 Chia Network 的区块链软件，并在 testnet 网络上拥有节点。

2020 年 7 月，公司完成了行业范围内的合作，创建了 IETF BLS 签名标准，并更新了我们对该标准的实施。随之，我们得以最终完成空间证明的实现。自此，我们的社区一直在创建耕种文件(Plots
Files)以便将来在我们的主网上工作。

在历 2020 年下半年，我们的无激励的 testnet 按公共节点数一直处于区块链的前 15 位。尽管在这段时间内，发布之间的多个硬分叉（对区块链进行不兼容的修改）步伐很快。到目前为止，2021 年 1 月初达到了约 30PB 的网络存储峰值。我们估计在发布时，Chia 主网将有 40 到 60PB 的专用存储空间，然而要提醒的是，这只是一个估计，可能会有偏差，偏向于较高的水平。

2020 年 11 月，公司发布了新的共识算法，该算法基于 2020 年 2 月在斯坦福区块链 2020 上发表

的论文《Proof-of-Stake Longest Chain Protocols Revisited》中的一个想法。这篇论文背后的研究人员后来在 2020 年 5 月发表的《 Everything is a Race and Nakamoto Always Wins 》(万物皆赛，中本聪常胜)中独立证实了原来 Chia 共识的安全保障。

新的 Chia 共识方法将 Chia 的安全性提高到了与工作证明相同的 51% 攻击阈值，只有一种远距离攻击的安全阈值较低（约 46%）。这一个较低门槛的攻击在我们的新共识中也比原来的共识更难。新的共识有额外的终端用户特征，交易区块大约每 45 - 49 秒到达一次，产生更可靠的预期区块时间。还有更快的确认积累，更快速地增加了交易是最终的确定性。在前三年中，通过每十分钟奖励 32 个农户分得的 64 个 Chia(奇亚)来增强农户的能力。每个三年期后，共将有四次减半的养殖奖励。

公司计划在 2021 年 3 月 17 日或之前发布 Chia(奇亚)网络的区块链主网。最初将有六周的时间，交易将被禁止，只有种植奖励（Farming），奖励给农民。这是为了稳定链，并给更多的时间进行测试。

市场概况错综复杂的遗留金融体系

全球银行和货币通常容易受到外来冲击、政府管理不善和金融危机的影响。全球金融体系巴尔干化(碎片化)，不透明，并依赖过时的技术。较新的金融技术通常被设计成只能在一个国家的管辖范围内工作。另外，国际金融技术解决方案往往价格昂贵，需要复杂的协调。此外，现有的地方银行变化缓慢，采用新技术的速度慢，并面临任意的监管和政治限制。

为了应对加密货币的兴起，SWIFT 和其他机构开始对一些国际转账进行现代化改造.....具有讽刺意味的是，亲手将现金交付到国际目的地通常仍然更便宜、更快捷、更可追踪，而且更省时。然而，实物交付现金有监管和安全风险，如进口的资本控制，资本报告，出口限制和欺诈。

比特币是在 2008 年全球金融危机引起的动荡中推出的。中本聪在比特币的起源区块和源代码中都加入了伦敦时报的标题 " Chancellor on brink of second bailout for banks "。自比特币推出以来，

持续的金融震荡持续困扰着世界。近期的全球乱象包括：塞浦路斯银行面临灭顶之灾的威胁、委内瑞拉的恶性通货膨胀、中国收紧资本管制、香港担心银行账户被查封、黎巴嫩银行关闭以防止银行挤兑、阿根廷 2019 年的恶性通货膨胀、2020 年 3 月 COVID-19 诱发的股灾。

除了这些外部冲击外，"9-11 "后世界银行环境的持续变化迫使各国寻求低效的变通办法，以开展合法的国内业务，并在代理银行减少的情况下生存。这些金融冲击是比特币价格和采用的重要驱动力。

"中本聪共识 "的分散式银行

中本聪发明了一个被称为 "中本聪共识 "的模型，它允许全世界的比特币节点运营商安全地充当结算交易的 "银行"，即使没有一个节点运营商能够单独控制交易。然后，他们会因为对验证网络的贡献而获得币的奖励。这个过程通常被称为挖矿，它确保没有一个实体拥有或运营网络。

由于这种基础设施大多是去中心化的，面向互联网的，而不是建立在传统的银行基础设施之上，因此它存在于全球任何互联网连接的设备上，任何人都可以使用。比特币最近已经成为一种流动性较强的全球货币，价值超过了 6000 亿美元美，元，大多数日子的交易量超过 550 亿美元。自从我们写下上一句话后，这些指标几乎无一例外的增加了。这个全球性、流动性、无权限的网络开启了一个新的金融科技产业，建立在比特币之上，而不是银行。

在比特币之后，又出现了 Ethereum(以太坊)，这是一个在架构和能源效率方面类似的网络，但有希望实验性的 Solidity 智能合约语言，它的应用范围从筹款代币到去中心化交易所和金融（DeX/DeFi)，再到虚拟猫的饲养游戏。

这两个区块链平台经历了成长的阵痛。比特币的工作证明现在每年利用约 87 太瓦时，截至 2020 年 12 月，这个能耗水平与芬兰国家相当。这个能源利用水平理所当然地引起了争议。比特币的品牌也遭受了大型交易所的重大攻击，以及来自企业和政府的采用担忧，这与其与洗钱和在线毒品市场的早期使用有关。此外，比特币脚本是有限的，发展缓慢，并且通常需要对比特币协议进行重大修改，可能需要数年才能部署。这些限制阻碍了构建优越的羁系和控制。

Ethereum 与比特币一样依赖 "浪费 "的 Proof Work 挖矿，并且还存在其他问题。几乎每一个部署的 Solidity 智能合约都吸引了大量的余额，都以某种方式受到了损害。Solidity 脚本语言使得编写金融软件比保护金融软件更容易。Ethereum 因被称为 "ICO "的筹款机制而闻名，筹款人在 Ethereum 网络上创建新的代币，以比特币和乙醚出售--其中许多代币的监管合规性很差或根本没有。最近的去中心化金融应用暗示了金融技术的革命性变化，但由于 Solidity 糟糕的安全立场以及 Ethereum 和 Solidity 使用的账户/全局状态模式，它们也受到了漏洞的困扰。

Chia(奇亚**)**网络

利用空间和时间证明的可持续中本聪共识

Chia Network 的区块链依赖于一种新的中本共识算法，称为空间证明和时间证明。这些新方法不会像 Proof Work 那样消耗大量的电力和单一用途的硬件。Chia Network 的区块链（和 chia）旨在成为 Proof of Work 的 "绿色"、生态友好的替代品。闲置的空间是一种分布广泛、抗 asic、供应过剩的商品。电价与运行存储基本无关，随着消费者 SSD 价格低于硬盘价格，电价将变得更加无关紧要。我们预计，chia 耕种(farming)将比 Proof of Work 或 Proof of Stake 更加分散，而且能源和资源密集程度也会大大降低。

中本聪选择 Proof of Work 来解决围绕信任一群匿名个人同意交易账本的关键问题。在网上，伪造多个角色相对容易，因此一个人在社交媒体平台上可能看起来像 1000 个不同的人。工作证明迫使每个人都付出一些可证明的努力，使他们不太可能控制一个以上的逻辑账户或所谓的角色。

此外，"工作证明 "创造了一种方法，以数学上被证明为随机的方式选择下一个验证一组交易的人。这让网络中的参与者保证验证他们交易的人不会是他们刚刚卖船的同一个人，以避免出现验证者可能会使支付给卖船人的款项消失，从而永远不会显示为完成的交易。随机选择下一个交易区块的验证者，可以避免购船者在没有付款或重复消费的情况下，一帆风顺。Satoshi 曾希望 "工作单位 "是大家电脑上未使用的 CPU 容量。然而，在 CPU 上具有所需属性的算法，很容易在专用的 ASIC 芯

片中被加速，从而推动证明工作的成本向最廉价的电力来源发展。这使得那些拥有大量资本和获得廉价电力的人，能够比在家里使用笔记本电脑的人每分钟和每美元证明更多的工作。

空间证明是一种证明你在硬盘上保留一些未使用的存储空间的方式。Chia(奇亚)网络的区块链用户会通过安装软件，将硬盘上未使用的空间绘制(plots)出来，软件会生成并将磁盘上的密码数字集合存储成地块。这些用户被称为农民(farmers)，与 Proof Work 的矿工不同。当一个新的区块在奇亚网络的区块链上广播时，农民会扫描他们的地块，看看他们是否有一个与前一个区块衍生的新挑战号接近的数字。这种检查空间证明的操作速度很快，效率也很高.据悉，农民在一个树莓派上就可以耕种一 PB 的土地（plot files）。农场主赢得区块的概率是指农场主每次挑战的空间占整个网络总空间的百分比，平均每天有 4608 次挑战获胜的机会。

将存储作为商品来保证下一个验证器的唯一身份，具有中本聪希望的闲置 CPU 的特性。企业和终端用户倾向于购买比他们今天所需的更多的存储，以预期他们未来的存储需求。

重要的是，没有比利用希捷、英特尔、西数、三星等公司生产的闲置硬盘和固态硬盘更便宜地存储每 TB 随机数据的技术方法。存储还具有这样的特性：当有人完成耕种后，他们可以将其重新用于其他有价值的用途，比如存储公司的数据库或增加更多孩子的照片。这些空间证明也给了很好的保证，将随机选择验证下一个交易区块的中标农户。

由于空间证明只需要很少的时间来查询，为了防止拥有大量空间的攻击者创建备用的竞争性交易历史和期货，Chia(奇亚)网络区块链有第二个组件，叫做时间证明。时间证明需要实际的 "挂钟 "时间在区块之间传递。时间证明由一个可验证延迟函数来实现，它需要一定的时间来计算，但验证速度非常快。VDF 的关键思想是它需要顺序计算，因此拥有许多并行机器或 CPU/GPU/ASIC(如在工作证明挖掘中)不会产生效益，因此电力浪费最小。并不是每个人都需要运行一台 VDF 服务器（我们称之为 Timelords），但希望为网络增加更多冗余和安全性的用户可以这样做，因为最快的那台总是会先完成，网络上只需要一台 Timelord 就可以完成一个区块并将链子向前推进。时间证明还增加了

额外的保证，即下一个区块的验证者将以一种完全不可预测的方式被选择，因此用户可以有信心，对他们当前交易感兴趣的一方被选为下一个验证者的可能性非常小。

和比特币一样，Chia(奇亚)网络的区块链上的工作难度也是动态调整的，所以 32 个区块完成的目标时间平均为 10 分钟。并非每个区块都是交易区块，预计每 10 分钟会有 9 到 14 个交易区块。耕种(Farming)难度会根据网络空间的大小和最快的 Timelord 的速度进行调整，以保持目标时间的规律性。无论哪一个变化，如果区块释放速度过快，难度都会增加。如果区块完成得太慢，难度就会降低。随着农耕竞争通过增加网络空间而上升，农民可以期待特定存储量的奖励会下降。

Chialisp

Chialisp 是 Chia(奇亚)网络基于功能语言 Lisp 的智能币语言。Chia 区块链上几乎所有的东西都是币。智能币集智能合约和智能交易功能于一身。Chilalisp 在设计上追求安全和简单，同时允许强大而广泛的功能。在 Chia(奇亚)网络的区块链上运行的应用程序旨在拥有适合银行、支付和金融应用的功能。我们推出的主要重点将是核心功能，如财务控制、支付清算和结算，以及管理资产的发行。

Chia(奇亚)网络的区块链将使用户能够定制托管和清算安排。Chialisp 将使 Chia(奇亚)控制与内部会计控制相匹配并超越内部会计控制，并以可审计的方式保障资金不受意外损失、盗窃或黑客攻击，并具有不同的风险容忍度。Chialisp 的设计是为了让智能币轻松地作为 SSAE 18 SOC 1 或 SOC 2 报告的控制措施，并在 GAAP 或 IFRS 财务审计中得到依赖。

这对于那些没有自我保管数字货币的人来说可能听起来很无聊，但对于那些已经有了数字货币的人来说，它让随身携带数字货币的感觉不像是走在城市的糟糕部分，现金从杂货袋中掉出来，而更像是拥有自己的便携式银行金库。

Chialisp 将在比特币中使用的简单可靠的方法内运行，即作为唯一的共享状态（UTXO 模型）来跟踪当前可消费的硬币。Chialisp 的特点是加强了对净结算的支持，允许打开和删除支付渠道的交易与正常转账无法区分。Chialisp 的规则是在区块链上执行的，以实现这些控制的卓越安全性。

随着 2019 年 12 月 Alpha Testnet 的推出，Chialisp 向 chia 的开发者和部署者提供了一套参考智能币和钱包。奇亚网络参考智能币涵盖的初步用例包括高级多签名支持、原子交换、授权受款人白名单、提现回溯托管、提现率限制、慢速纸钱包、数字身份钱包和彩色币。公司于 2020 年 4 月发布了彩色币的参考智能币，并预计将于近期发布数字身份智能钱包。

Coloured coins 是奇亚实现所谓的 "彩色币"。这是一个术语，宽泛地描述了一类在区块链之上表示和管理现实世界资产的方法。Chia 彩色币将由一个嵌入到几个最小面额的 chia（一个 mojo，即一万亿分之一的 chia）中的智能硬币来表示，它允许任何人在 Chia 网络的区块链之上定义和发行

资产。所发行的资产也将继承 Chialisp 智能币的所有功能，从而可以拥有原生 chia 所享有的所有保管和控制权。增加 DID（分布式身份）钱包功能将允许发行者只自动向完成 KYC/AML 或经国家注册机构验证的人发行资产，但其方式是保护隐私的，并依赖于 W3C 去中心化标识符标准。

多重签名和原子交换*:*

多重签名和原子交换是更复杂的智能交易的基石，也是许多更简单的控制和保管安排的核心。这使得公司可以要求三个签名者中的两个人从钱包中花钱，或者完成比特币和 Chia(奇亚)币之间的交易，而不需要信任其他方提出并完成互换。IETF BLS 签名协议也使多个签名方案变得更容易，对参与者来说也更安全，因为签名可以合并，不必按顺序或在同一时间或地点发生。

授权收款人钱包*:*

例如，授权收款人白名单允许公司将支出权从控制员下放给工资管理员，管理员只能向控制员或财务总监设定的地址付款。这就减轻了电子邮件钓鱼企图成功或黑客攻击薪资管理员的可能后果。这也使得挪用公款变得困难。我们打算使用我们的分布式身份钱包来使之变得特别灵活，但首先以父钱包、子钱包的形式实现了我们的参考版本。

转账收回*:*

当一个组织在区块链上发币给另一个组织时，有两件事需要发生。必须发生一定量的区块确认，以向接收方证明发送的币是有效的，而不是双重消费，收到的币将来不会被网络认为是有效的。第二个活动只是确认支付交易实际上正在进行中，因为它可能需要一些分钟才能被收件人认为是最终的。转账收回增加了一个时间段，在最初的转账移动到区块链上后，发送方可以撤回资金。通过添加第三个密钥，可以收回或加速交易底层币的转移，可以降低发送交易的风险，实现托管业务模式。通过较短的恢复托管期--以比收件人的区块数少 1 个区块为例，否则他们会认为是最终的区块数--发送者现在可以在发送交易后检测到错误，纠正收件人地址中的错别字，将坏的交易抓回，并重新发送一个正确的交易。对于某些严格控制的用例，可以实现一个较长的回收期，如果后来发现钱包的所

有转账都是不正当的，就可以对其进行审核并取消。在网络购物模式中，消费者可以将回收托管期委托给运输公司，当托运人收到包裹时，运输公司会将资金发放给零售商，如果货物没有在约定的时间内送到托运人手中，则将资金返还给买家。

限额钱包*:*

限额钱包允许创建钱包，在指定的时间内只能花费一定数量的币。你可以把一年的生活费放在钱包里，但限制每周只能花掉钱包里资金的 1/52。如果钱包被盗，或者被第三方入侵，一旦确认失去控制，你可以用主钱包将尚未被盗的资金余额转回来。Chia(奇亚)在 2020 年 8 月的 testnet 上发布了一款限额钱包。

延迟恢复功能的纸钱包*:*

当前加密货币的最佳实践是保留一个纸质钱包备份你的活动钱包或热钱包。这是必须的，原因很多，包括硬件可能会出现故障，而且很容易让你的硬件丢失或被盗。然而，纸钱包很有可能被盗，并完全控制和窃取你的所有资金。延迟恢复功能的纸钱包允许你存储一个智能交易，可以启动一个延时过程来恢复你的热钱包中的资金，但它不是你的私人密钥的副本。如果有人盗取您的纸钱包并开始恢复，您的活动钱包可以识别这种情况，并将资金转移到您控制的新钱包。启动备份恢复可以选择要求交纳保证金，以进一步阻止纸币钱包盗窃资金的企图。

数字身份钱包*:*

Chialisp 实现了具有深度恢复选项的数字身份钱包，并允许个人和组织在无权限区块链之上添加身份和权限。用户可以以假名的方式将身份控制权委托给家人或法律顾问，其方式既可以被委托人恢复，也可以让委托人自己的身份被恢复和使用。这使得某些类型的信托/受托人关系成为可能，也是数字继承的一条途径。这也让奇亚网络区块链上的资产提供者有一种方法，让最终用户完成 KYC/AML 等流程，并从他们的数字身份钱包中出示该证明，以便能够获得股权、对冲基金的认购或

政府支持的稳定币。如果资产发行商或验证服务确定某人的身份发生了变化，他们也可以轻松撤销这些凭证。

彩币*:*

彩色币允许个人、金融机构、企业和政府发行链上资产，这些资产继承了 Chia Network 区块链的智能交易能力，并依赖于时空证明提供的全球去中心化安全验证。ERC-20 代币是目前最被认可的彩币形式，但其局限性很大。他们所依赖的 Solidity 智能合约存在着安全风险。此外，对于终端用户来说，它们并不像是 Ethereum 区块链的原生部分，而且需要钱包和数字货币交易所单独启用每个资产。最近的安全研究表明，它们也很容易在交易所被伪造。Chialisp 彩色币继承了 Chialisp 的所有能力，这使得它们更适合高合规性的资产发行，并使它们能够更原生地适用于奇亚钱包。

与 Solidity 不同，Chia(奇亚)色币可以用来创造短暂的价值，因此在奇亚区块链上的应用一般不需要闪贷。这一直是 Ethereum 上 DeFi 的致命弱点之一。短暂的彩色币与 Chia 的原生交换能力和任意复杂度的部分完成交易相结合，是 DeFi 项目试图构建的那种套利应用和交易的优越构件。

奇亚彩币的应用*:*

在企业方面，一家美国的对冲基金可以利用奇亚彩币来管理认购所有权，并让投资者出示数字身份证明其公民身份、投资者资格和 KYC/AML 状态--所有这些都可以原生到奇亚网络的区块链上。政府可以向任何完成了所需 KYC 数字身份证明的人发行其国内货币支持的稳定币。Chia Network 的区块链上的彩色币可以用于存储或开环的公司礼品卡，债务发行，股权发行，以及任何相关的资产发行，跟踪和管理。

由于 Chialisp 是一种通用的开发语言和环境，所有这些示例功能都可以根据用例的需要进行混合和匹配。开发人员可以利用 Chialisp 提供的工具集创建新的和目前无法想象的功能，而无需改变 Chia Network 的协议或环境，同时 Chialisp 将提供这些控制和应用的安全性和可审计性。我们相信，Chialisp 将成为新兴的 De-Fi 运动的最佳工具。

Chialisp 和 BLS 签名的选择使支付渠道的实施比目前比特币或 Ethereum 的支付渠道更简单、更直接。支付渠道领域的发展速度很快，因此公司希望在奇亚网络主网推出后，采用第二层社区出现的最佳技术。战略储备金

公司预计在主网启动时，将建立 2100 万个 Chia（Chia 网络的战略储备或预挖农场），并将这些放在我们的资产负债表上。公司设立 2100 万是为了向前人的工作致敬。预测推动采用奇亚区块链所需的资源是具有挑战性的，特别是那些以奇亚计价的资源。因此，我们希望我们保守地偏向于让公司和最终股东拥有超额的奇亚战略储备。如下文所述，我们相信，上市公司结构与健全的公司治理相结合，将提供一个审慎的框架来管理战略储备，并允许我们使用传统的公司工具以公平的方式向股东分配多余的 Chia（如果有的话）。

挖矿释放策略

耕种奖励(farming)将在 Chia(奇亚)网络区块更新后创造新的 Chia。我们的耕种奖励计划直接仿照比特币的奖励计划。我们将这些奖励呈现在一个理想的情况下，但现实通常与理想相差甚远。由于加入网络的空间和 Timelord 速度增加或减少的波动，实际的发放时间表会像比特币的发放时间表在历史上一样略有不同。我们可能会根据我们在比特币中观察到的情况增加一个时间调整系数，试图让耕种奖励最终比比特币更接近这个理想。理想化的时间表如下。

- 64 chia：在主网启动后的前三年，每 10 分钟将产生.
- 32 chia：在主网启动后的第四年至第六年，每十分钟将产生
- 16 chia：在主网启动后的第 7 年至第 9 年，每 10 分钟将生产
- 8 chia：在第 10 年至第 12 年中，每 10 分钟将产生
- 4 chia：在第十二年之后，每年每十分钟.

在奇亚网络的区块链上，通过耕种奖励(farming)可能产生的奇亚币总数没有上限，也没有限制。在启动后的第六年年底，截至该日产生的所有耕种奖励(farming)将占当时所有奇亚币的 42%。从主网启动后，随着尾随排放在第 13 年开始放缓，养殖奖励大约需要 21 年才能与奇亚网络的战略储备规模持平。

Chia Network 的区块链的释放时间表被称为释放计划，这比封顶供应增加了显著的安全优势。封顶供应区块链的奖励最终将完全只来自交易费用，这可能会导致矿工有动力在交易费用较低的时期覆盖最近的历史，而不是挖掘新的区块，特别是如果费用在白天很重要，并且每天晚上（一般从太平洋时间午夜到太平洋时间凌晨 4 点）接近零，这就是今天发生的模式。因为第 12 年以后，排放率固定在每 10 分钟 4 Chia，所以通货膨胀率占供应量的比例是永远下降的。通胀率在释放后的第 25 年跌破 0.50%。我们的目标是交易费和爆块释放要达到一个合理的平衡点。高到足以强烈激励农民将其加入其中，而又不至于相对于固定奖励太高，以至于有强烈的动机去覆盖历史。我们还认为，固定的供应量不一定是理解通货膨胀最重要的东西，但能够直接计算出任何特定时间总供应量的共同预期，就能获得大同小异的财政和安心的好处。

XCH 释放时间表（减产计划）：

		第 1 年	第 2 年	第 3 年
耕种奖励		3,363,840	3,363,840	3,363,840
累计耕种奖励		3,363,840	6,727,680	10,091,520
累计奖励占发行上限百分比		13.81%	24.26%	32.46%
当前流通量		24,363,840	27,727,680	31,091,520
减半周期*:*		第 4 年	第 5 年	第 6 年
耕种奖励		1,681,920	1,681,920	1,681,920
累计耕种奖励		11,773,440	13,455,360	15,137,280
累计奖励占发行上限百分比		35.92%	39.05%	**41.89%**

当前流通量		32,773,440	34,455,360	36,137,280
减半周期*:*		第 7 年	第 8 年	第 9 年
耕种奖励		840,960	840,960	840,960
累计耕种奖励		15,978,240	16,819,200	17,660,160
累计奖励占发行上限百分比		43.21%	44.47%	45.68%
当前流通量		36,978,240	37,819,200	38,660,160
减半周期*:*		第 10 年	第 11 年	第 12 年
耕种奖励		420,480	420,480	420,480
累计耕种奖励		18,080,640	18,501,120	18,921,600
累计奖励占发行上限百分比		46.26%	46.84%	47.40%
当前流通量		39,080,640	39,501,120	39,921,600

After a final halving, XCH continues trailing emissions:

减半周期*:*		第 13 年	第 14 年	第 15 年	第 16 年	第 17 年
耕种奖励		210,240	210,240	210,240	210,240	210,240
累计耕种奖励		19,131,840	19,342,080	19,552,320	19,762,560	19,972,800
累计奖励占发行上限百分比		47.67%	47.95%	48.22%	48.48%	48.75%
当前流通量		40,131,840	40,342,080	40,552,320	40,762,560	40,972,800
Trailing emissions:		第 18 年	第 19 年	第 20 年	第 21 年	第 22 年
耕种奖励		210,240	210,240	210,240	210,240	210,240
累计耕种奖励		20,183,040	20,393,280	20,603,520	20,813,760	**21,024,000**
累计奖励占发行上限百分比		49.01%	49.27%	49.52%	49.78%	**50.03%**
当前流通量		41,183,040	41,393,280	41,603,520	41,813,760	42,024,000

50 年总流通量	**47,910,720**				

这个释放计划时间表受比特币的释放时间表影响，并针对 Chia(奇亚)区块链的一些不同的数学基础进行了调整，比如平均每天 **4608** 次奖励机会，以及较快的减半速度。

下表比较了比特币在每四年减半期间的挖矿总量和 Chia(奇亚)币在每三年减半期间的产出量:

	BTC	XCH
第一次减半	10,500,000	10,091,520
第二次减半	5,250,000	5,045,760
第三次减半	2,625,000	2,522,880
第四次减半	1,312,500	1,261,440
第十一年末*	18,593,393	18,501,120

- 两者 11 年实际结果对比，其中 BTC 是预估值。

Chia(奇亚)网络战略储备的治理

本公司相信，"治理 "Chia Network 的战略储备和支持发展优越的金融基础设施的最佳方式是采用经过 400 年考验的股份公司技术，并采用当前公司治理的最佳实践。在适当的时候，本公司打算将本公司的股权在全国性证券交易所上市。公司对 Chia(奇亚)网络战略储备的管理和使用，可能会对采用 Chia(奇亚)换钱和金钱相邻的使用案例产生重大影响。我们相信，公司形式与透明的披露激励机制比目前其他支持或管理公共区块链的尝试更好。当然，由于网络的去中心化性质，Chia(奇亚)网络的区块链和非本公司持有的 Chia(奇亚)币将在本公司存在或不存在的情况下工作和交易。一旦启动，本公司对 Chia(奇亚)区块链没有直接的控制权，因为奇亚区块链的规则只能通过让大多数运行节点独立升级到新版本来更新。需要注意的是，正如我们在下文中所概述的那样，公司不打算再进一步耕种这个区块链。此外，与股权证明区块链不同，币的所有权对 Chia 区块链的治理或验证没有影响。

Chia(奇亚)在瑞士设立了子公司，负责管理欧洲的业务。我们预计一旦疫情缓解，将在新加坡设立子公司，以管理亚洲的业务。Chia Network 的战略储备将在主网启动时由美国母公司和瑞士子公

司平均分配。一旦公司能够将其更复杂的完善系统投入使用，公司可能会使用智能币来限制预挖 Chia 的总供应量，使其限制在股份行权计划表中。此外，公司打算建立内部控制，使其对投资者和币种用户的承诺需要我们独立董事的董事会批准，而不受任何单一股东控制 Chia(奇亚)网络战略储备能力的限制。本公司还计划采取一定的保证措施，例如，在未向公众提前 90 天公示的情况下，不会对其限售战略储备奇亚币的承诺进行更改。此外，在我们成为 1933 Act 法案和 1394 Act 法案下的申报公司之前，本公司不打算向股东发放 Chia(奇亚)币或股息币，也不打算使用币回购股权。我们在下面的 "公司治理 "和 "战略储备控制 "部分概述了这些控制措施。

我们的上市公司战略提高了监管的清晰度，因为公司打算成为一家申报上市公司，其股权在美国证券交易委员会的监管框架下交易。本公司相信，这将有助于区分奇亚币的商品属性与公开上市的奇亚网络公司的股权。

上市公司创造了透明度，并向大公司和政府等客户保持信任。这种透明度和监管基础设施使公司能够对 Chia(奇亚)网络战略储备的使用方式和时间实施可靠的控制，并使 Chia(奇亚)网络能够在政策变化影响任何一个市场之前向股票市场和硬币市场发出通知。

我们也希望我们的用户、农民和开发商能够以股东的身份拥有部分战略储备，并享受美国公开股权市场的投资者保护。我们认为，让每一个可以投资股权的人都能接触到 Chia(奇亚)战略储备，是一种让所有人的利益在 Chia(奇亚)的长期成功和可编程互联网货币的广泛部署中保持一致的优越方式。

Chia(奇亚)币在数字货币交易所的价格与公司股权估值之间的预期相关性，应允许企业客户和第三方在公司股权和 Chia(奇亚)币之间进行对冲。这将使希望在商业中使用奇亚币的组织能够获得限制其受 Chia(奇亚)币波动影响的方法。借用 Chia(奇亚)币进行国际贸易融资的公司可以购买 Chia(奇亚)网络股权的跨式和看涨期权，以限制他们对 Chia(奇亚)币价格波动的风险。这也将趋向于把对 Chia(奇亚)网络区块链不断增加的价值的长期投资转移到股票市场--目前股票市场在全球范围内有更广泛的部署和便利的访问。我们最终计划改变这种情况，希望尽我们所能实现。

对战略储备的控制

我们的董事会已经通过了以下关于本公司使用预挖农场的限制。如果没有董事会的多数票，这些限制不得更改，其中必须包括至少一名独立董事。

我们打算由 3 名外部董事组成 5 人董事会。目前，我们的董事会由三名成员组成：Bram Cohen、Gene Hoffman 和 Chuck Stoops。Cohen 先生和 Hoffman 先生并不是独立董事，因为根据证券交易所的规则，这个概念被定义为独立董事，而 Stoops 先生符合独立董事的条件。此外，Stoops 先生符合审计委员会主席的资格。

我们正在与另外一名独立董事候选人进行讨论，并已开始寻找第三名候选人。一旦两个董事会空缺得到填补，董事会预计将提高批准门槛，要求外部董事也必须获得多数票。

这些控制措施需要修改，如果没有至少 90 天公示将不会被实施，这些通知将在公司网站、Keybase 渠道和/或其他类似的高度可见的方法上发布。

重要的是，如果公司发现自己破产了，董事的信托责任就会转移到债权人身上，因此在这种不太可能的情况下，公司可能无法遵守这些限制。此外，法院命令可迫使本公司绕过这些限制。

这些限制如下:

1. 本公司将不会出售战略储备中的 Chia(奇亚)。本公司也不会签订任何期货合同，允许或要求本公司以后将 XCH 转让给第三方，对投资者来说这超出本报告所述的惩罚条款。
2. 如果本公司在主网启动后的两年内未尝试提交注册声明，或在主网启动之日起三年内未对本公司股权进行有效登记，则按照 SAFE 协议（未来股权简单协议）现有投资者有权要求按 XCH 当时的市场价格赎回部分战略储备。此外，在注册声明生效后，如果公司的企业估值在 30 天内不超过公司资产负债表上 chia 值的 65%，投资者可以按当时 XCH 的市场价格赎回其投资金额。如果该等惩罚性赎回权被触发，投资者只能收回当时其初始投资额的市场价值，而不是任何收益。本公司预计将这些 SAFE 转换为股权或优先股权，从而取消这些惩罚

限制或以更新的限制取代。在公司股权的注册声明或等值物生效之前，Chia(奇亚)网络不打算向投资者转让任何奇亚。

3. 本公司不会也没有用奇亚发放给本公司的雇员、相当于雇员的独立承包商、高级职员或董事。
4. 本公司不会有意在主网上耕种 Chia(奇亚)。本公司将有耕种容量来支持我们的各种试验网，但配置错误可能导致意外耕作(farming)的发生。本公司计划实施控制和监控，以防止或检测公司所属设备的任何意外耕种(farming)。然而，本公司并不限制我们的员工或承包商在其个人时间使用其个人拥有的硬件进行耕种(farming)。

公司拟将该战略储备用于但不限于以下用途:

1. 向政府、金融机构、做市商和企业借出 Chia(奇亚)，用于其与 Chia(奇亚)相关的项目，如资产发行、支付国际发票和在各种数字货币交易所提供流动性。这些贷款将提供给信用良好的实体，一般需要以 Chia(奇亚)计价的利息，并以 Chia(奇亚)全额偿还。出于营销目的，公司可能会不时提供负利率以促进采用。例如，允许存储供应商提供以 Chia(奇亚)而非非货币向其外国供应商支付 105%的发票，而 Chia(奇亚)只期望归还 95%的贷款。
2. 在我们公开登记股权后，用 Chia(奇亚)资助股东活动，如回购股份或向股东分红。
3. 利用 Chia(奇亚)投资于有前景的项目，以扩大 Chia(奇亚)在货币和金融科技市场上的功能和影响力，但在我们公开注册股权之前，不能投资。

4. 我们可能会使用 Chia(奇亚)增加额外的耕种奖励(farming)或以其他方式激励农民(farmers)或开发人员验证或开发网络或软件。我们有举办软件增强竞赛和耕种(farming)竞赛的历史，并计划使用奇亚作为这类竞赛的奖品。

同样，我们不计划使用 Chia(奇亚)来资助股东活动，如回购或分红，或投资使用 Chia(奇亚)的公司或项目，直到 Chia 网络公司股权的注册声明或其等价物生效之后。我们相信，在主网开始交易后不久，奇亚区块链将充分去中心化，这样它将满足所谓的 "Hinman Test"。美国证券法规通常只关注证券的销售，因此我们不打算出售预挖农场的组件，直到我们通过成为报告公司解决任何信息不对称问题，并且我们从我们的监管机构那里得到安慰，他们不认为公司未来销售的任何 Chia(奇亚)是一种证券。然而，如果他们认为有必要进行某些报告或注册，我们作为一个已经上市的实体，将更有能力满足这些要求。

我们相信，这些控制措施是有效的，并且随着我们在 2021 年上半年增加独立董事会成员，这些控制措施将变得更加有效。单纯的股东投票是无法改变这些控制措施的。此外，我们董事会越来越独立的性质将确保战略储备被用于深思熟虑地增加全球对奇亚的采用。在国家级股票市场上市后，这些控制措施将因其执行力和约束力而获得证券监管的额外好处。

战略储备旨在创造一个长期的、可持续的方法来资助 Chia 网络区块链的持续发展和部署。从长期来看，我们的上市公司结构将为我们提供有序向股东转移价值和资金的工具，以资助我们技术的开发和部署。如果变得合适，我们可能会将企业软件或贷款业务剥离给股东。最终我们可以选择建立一个持续发展的信托基金，并将 Chia 网络公司的剩余资产全部分配给股东，留下发展基金、贷款业务和企业软件业务--后两项业务归股东所有，战略储备金的余额由股东掌握。

然而，很难预测未来十年，更别说三十年了。我们认为，既要考虑 Chia 区块链的长期可持续性，也要计划确保一个生态系统的发展，不依赖任何一方。如果 Chia 区块链像我们希望的那样被广泛部署和有用，它将成为银行和政府用于全球互动的轨道。这最终意味着，我们必须计划随着时间的推移尽量减少我们对地缘政治风险的暴露，但要与保留资源以实际达到这种采用水平相平衡。

收益和上市

公司预计主要通过以下方式实现收入和构建股东价值。:

- 为 Chia(奇亚)币、Chialisp 和 Chia 智能币在商业中的使用提供安装、开发、持续服务和支持，并发行使用 Chia 彩色币的资产。
- 为 Chia(奇亚)币、Chialisp 和奇亚智能币在商业中的使用提供安装、开发、持续服务和支持，并发行使用奇亚彩色币的资产。
- 为做市商、政府、金融机构、企业和开发商赚取 Chia(奇亚)币贷款利息，供其在日常经营中使用。

服务和伙伴关系

公司将采取哑铃式投资技术利用 Chia 网络的区块链、Chialisp 和 Chia(奇亚)为企业、金融机构、政府和开发商提供服务。我们相信，政府、银行、企业以及开发者、创新创业公司和分布式开源项目对我们的技术有迫切的需求。包括但不限于以下这些服务:

- 软件服务和支持协议;
- 与现有企业资源规划软件或金融机构基础设施的集成服务;
- 定制功能/智能币开发/彩色币开发;
- 将服务整合到大型存储部署和共同购买协议中，以支持大型存储部署的购置;
- 构建开发者工具，支持和投资开发者，支持开发者活动和黑客大会.

公司将追求的目标是建立一个全球软件解决方案团队，直接或与其他软件供应商和金融服务公司合作，促进可编程数字货币的采用和使用。本公司相信，就像 Redhat 的出现使企业和政府能够安全地采用 Linux 一样，建立一个与独立软件供应商和软件集成商合作的全球服务和支持业务对于企业、金融机构和政府在全球商业中实际采用 chia 至关重要。

公司打算为其他公司和开发商推出使用 Chia(奇亚)区块链和 Chialisp 的功能提供定制开发、支持和联合营销--特别是那些针对最终用户的功能。这些合作伙伴关系将推动对奇亚的采用和需求，也可以为公司提供收入和战略机会。

数字货币交易所

公司经常与包括数字货币在内的数字资产交换平台进行沟通。2019 年 9 月 Coinbase 宣布，这些资产推出后，chia 是他们目前考虑纳入的十七种资产之一。2020 年 9 月，Bitstamp 宣布，chia 是他们正在探索支持的数字资产之一。公司预计将为此类平台提供技术支持，并可能参与联合营销。

存储生态系统

Chia(奇亚)耕种(farming)奖励将提高存储市场中存储的价值。存储服务提供商能够按订单出售更多的存储，因为他们知道可以从超额分配的存储中赚钱。这就降低了买方对他们需要多快、多少存储的估计过于保守的风险。存储制造商也可以通过改变他们的驱动器烧入和质量保证(QA)流程来为自己创造收入，以谋划和耕种 Chia(奇亚)。制造商可以为大客户设置驱动器，让 QA 流程策划和耕种(farming)奖励到客户的奖励地址中,从而增加存储客户的单位价值。

大型存储采购商例如云供应商，需要常年在数据中心 7X24 小时运行存储设备。由于云存储是一个低利润率的业务，每 TB 购买和安装成本的任何增量下降都会迅速增加利润率。chia 网络希望大型存

储服务商在用户购买请求存储空间之前，利用 Chia 耕种来提前收回一部分成本

中型存储购买者通常没有专职于存储的全职 IT 人员。 这个市场的大部分份额都外包给了大型存储购买者的云提供商。 那些不倾向于在 3 到 5 年内购买存储的需求估计会增加。 他们的 IT 团队可以在几个星期内专注于安装新的存储区域网络（SAN）或网络连接存储（NAS），然后对该存储进行例行维护，直到数月或数年之后再增加容量。 选择在存储的未使用部分上耕种 Chia 将使购买者及其 IT 团队可以预先购买并安装更多容量，从而降低了他们低估存储需求的风险，并减少了 IT 团队必须花费的时间 专注于向 SAN 或 NAS 添加存储。

终端用户在传统设备上投入的存储空间，往往有 50%的剩余容量没有使用。随着从硬盘向固态硬盘的过渡，固态硬盘价格的提高导致存储空间的超额分配较小。然而大部分终端用户的存储方式即将转向 SSD 固态硬盘存储，随之而来的是存储厂商将大部分的研发支出放在 SSD 上。这很可能会使存储成本像历史上的机械硬盘一样快速下降。行业分析师目前预测，消费类 SSD 将在 5 到 8 年内变得比同等大小的硬盘便宜，我们在下面将会讨论。这很可能会让终端消费者回到购买两倍于他们所需的存储设备的状态。我们打算通过与存储和设备制造商的合作，让最终用户轻松地将其未使用的存储分配到 Chia Network 的区块链上，并直接或从存储或设备制造商创建的池子中获得奖励。

目前，二手硬盘的市场受到一定的限制。企业倾向于在三年后替换掉数据中心的所有硬盘。这些驱动器通常具有显著的剩余使用寿命，但由于它们达到了平均故障时间的年龄，因此不能信任它们用于关键数据存储。这些数据中心淘汰下来的硬盘是极好的耕种(farming)工具，我们相信我们将为它们创造一个市场，使它们远离垃圾填埋场，提高剩余价值利用。

在 NAND/SSD 存储方面的两个方面耕种(farming)Chia 也是大有可为。当然，到 2031 年，可能比这更快，消费类 SSD 将比相同尺寸的硬盘便宜。这将导致 Chia(奇亚)地块耕种所需的能源大幅减少。此外，还有一类 NAND 存储，今天一般被认为是废物，可以很容易地转化为商业上可行的耕作空间。

最后，如果事实证明我们低估了过剩存储的可用性，并且 Chia 的采用开始给存储业务带来压力，那么影响将是降低每个人的每 TB 存储成本。我们认为这是一种社会公益，即使我们希望 Chia(奇亚) 的影响只是为了更好地利用现有未充分利用的存储空间。

DeFi

我们认为，彩色币（Coloured coins）和 Chialisp 是 De-Fi 的优越发展环境。Chialisp 的固有属性和我们完善的 UTXO 模型几乎消除了智能交易外部的借贷需求，以完成同样的交易、交换和套利机会。根据应用的不同，交易对手风险有限或无限，Chia 的原生交换功能，通过部分完成的交易，也将成为无信任发行、交换和价格发现的绝佳组件。我们相信，设计良好的交易所报价和市场将是处理价格发现等事情的优越方式，因为预言机(price oracle)问题对于目前的区块链和智能合约来说仍然具有挑战性。

向无银行账户和银行账户不足的人提供这类工具非常重要，特别是在经济基础设施远不稳定的非 30

国集团国家。拥有贷款、预测市场和期货合约的替代办法，可以对作物产量或小企业资本形成产生直接影响，这对最不富裕的人来说特别重要。

国际支付

公司认为，Chia(奇亚)的主要用例之一是国际支付，特别是在政府或金融系统不稳定的地区。在短期内，Chia 网络打算支持并可能投资于能够将 Chia(奇亚)兑换成当地货币的公司和开发商，就像 Localbitcoins 和 Paxful 目前为比特币做的那样。从长期来看，从存储生态系统和云计算/存储提供商开始，Chia Network 计划在亚洲启用并推动采用 Chia(奇亚)币来结算国际发票，在亚洲，存储制造商和云提供商采购硬件和组件。Chia Network 计划拥有公开交易的股权，这将允许企业以新颖的方式使用股权期权，以减少他们在持有硬币进行日常使用时对任何相关硬币价格波动的风险。Chia Network 预计大量收入将来自与交易所和国际业务的服务和支持合同，以及相关的 chia 借贷利息收入。

我们同样致力于帮助开发者合作伙伴使用我们的技术和工具，为跨境支付等应用创建卓越的数字钱包。我们计划同时培养像 Paxful 这样的货币到加密货币的市场，以及能够使用手机给你移民国家的家人汇款的一般使用案例。像西联汇款这样的这些服务的选择不是即时的，也不是你在家里就可以

做的事情。这是在考虑到高额费用之前。我们相信，经济上处于不利地位的人，当他们可以有一个低费用的，更容易使用的应用程序，以节省他们的时间和金钱时，遭受这些较高的费用。

竞争分析

公司认为，Chia Network 的区块链和智能币平台将为现有竞争平台提供优势。Chia Network 的区块链既要面对现有平台（如 Ethereum）、R3 等 "内网 "区块链以及传统金融基础设施的竞争。除了比特币越来越清晰的投资用例之外，金融机构基本上已经放弃了使用比特币和 Ethereum。Chia(奇亚)网络区块链比现有金融机构更开放、更方便，比工作证明区块链更高效、更少浪费，比 Ethereum 更适合安全的智能金融交易，同时比工作证明链和股权证明链更去中心化。

公司认为，私有链或许可链不太可能获得大规模采用，类似于 20 世纪 90 年代末企业试图通过推出内部网络来推迟采用互联网。非许可区块链和公共区块链的核心价值之一是，它们允许彼此不信任的各方一起并肩进行交易。

许可链几乎是一个矛盾体。区块链被设计成 7X24 普遍可用和容错的。增加一个权限系统就增加了一个单点故障，使得一个有权限的区块链无法做出普通区块链作为基本属性的高可用性的有力论断。
区块链遵循梅特卡夫定律，网络上每增加一个参与者或节点，区块链就会变得更有价值和效力。从定义上看，权限制度限制了增加新用户的便利性，从而限制了这种网络的效果和价值提升。政府或企业从有权限的区块链中获得的效率提升并不像从无权限的区块链中获得的效率提升那样。

许可链也严重削弱了非许可的去中心化区块链所创造的无信任感。很难想象乌克兰会加入俄罗斯许可的区块链，或者巴基斯坦要求印度允许其参与印度控制的区块链。杰夫-贝佐斯的蓝色起源不太可能加入埃隆-马斯克的 SpaceX 运营的太空产业交易区块链。但是，一个无权限的去中心化区块链允许所有这些激烈的竞争对手信任一个交易，甚至是彼此之间的交易--或者是在他们自己交易旁边的网络上。

目前正在花费大量的精力试图解决我们认为的棘手问题，将利益证明作为使用较少电力保障公共区块链安全的替代策略。在一些项目为这些问题创造了解决方案的范围内，我们认为他们在假设中做出的权衡是劣质的，因为它们容易导致中心化，并且在国际地缘政治压力下不如中本共聪共

识那么稳健。我们支持 VDF 的开发和商业化，是一些股权证明问题的潜在解决方案来源，Ethereum 2 采用基于 RSA 的 VDF 等项目就是证明。VDFs 创造了一个随机性的来源，以减轻攻击，验证者可以影响自己的选举来验证。

Proof of Stake 有三个属性，作为一个全球可编程货币我们认为无从选择。利益相关者倾向于将验证向最富有的验证者集中，并且通常会随着时间的推移集中控制。我们认为，当政府成为利害关系人时，这个因素的表现会特别差。利益关系证明也容易受到长距离攻击。一个人可以借到非常大的价值，并在短期内进行抵押，然后解押并卖出头寸来偿还贷款。利用仍然包括大额股权的链条，人们可以生成一个替代的未来，并将其引入新的、"更好的 "链条，在这个链条上，大额价值从未被出售。最后成功地实现了对股权证明链的 51%攻击并且被永久记录下来，他们永久拥有该区块链的完全控制权，不像中本共聪共识链可以从 51%攻击中恢复。

Chia Network 的无权限和去中心化区块链将增强政府和金融机构的基础设施。银行和支付网络将能够创建安全、快速、不依赖任何第三方的资金转移机制，包括 Chia Network。政府和银行可以安全地与全球各地的代理银行和供应商进行业务往来，而不受地缘政治局势或其他国家或银行试图限制其活动的影响。一个开放的全球去中心化网络将使金钱和财富的转移变得值得信赖、可靠，而且效率大大提高，而不必依赖中间商、其他银行或其他国家。Chialisp 将让他们对自己的交易或彩币
(Coloured coin)发行的资产进行所需的限制和控制，同时让基础价值由可编程货币的去中心化全球网络担保，并可在该网络上转移。

执行官员和董事

Bram Cohen:董事、董事长、首席执行官和创始人，2017 年 8 月至今。

Bram Cohen 是 BitTorrent 的发明者，BitTorrent 是互联网上使用最多的点对点文件共享协议。2009 年，BitTorrent 占所有互联网流量的 43%至 70%，最近看到使用的复兴，占 2018 年全球上游互联网带宽的近 21% 。Cohen 先生经常被指责为中本聪，但他否认了这一说法。Bram 于 2004 年创立了 BitTorrent, Inc 并担任其初始 CEO。在 BitTorrent 工作期间，他曾担任工程经理、产品经理和 BitTorrent 董事会成员等多种职务。在那里，他管理着 BitTorrent 实验室，这是 BitTorrent 的一个研发部门，在那里他主持成功地重新架构了一个新的 BitTorrent 客户端：uTorrent Web。他于 2017 年 8 月离开 BitTorrent，创立了 Chia 网络。自 Chia Network 成立以来，他一直担任 Chia Network 的董事长和 CTO，并自 2019 年 6 月起担任 CEO。他目前是 Flibe Energy 公司的顾问，该公司是一家致力于设计和开发液态氟化钍反应堆（LFTR）的工程公司。Bram 是世界上最畅销的拼图设计师之一 。

Gene Hoffman:董事、首席运营官兼总裁，2019 年 12 月至今，业务发展高级副总裁，2019 年 8 月至 2019 年 12 月，董事会顾问，2017 年 8 月至 2019 年 8 月。

Gene Hoffman 是一位连续创业者和前上市公司 CEO。他已经建立并向 PGP 公司、Vivendi-Universal 和 Amdocs 出售了三家公司。2003 年至 2016 年，他是 Vindicia 的联合创始人、董事长兼首席执行官，该公司是一家消费者订阅基础设施公司，于 2016 年出售给 Amdocs。从 2017 年到 2019 年，他担任 Chia 网络董事会的顾问，直到 2019 年 8 月全职加入公司。他曾在八家不同的技术和能源公司担任董事会成员，并在两个非营利性董事会中任职，其中一个是他共同创立的。

他有 21 年在高合规安全环境中工作的经验，其中 12 年管理 PCI 和 SSAE-16 合规性，存储了

220,000,000 张信用卡。Hoffman 在企业软件和 SaaS、消费者订阅、密码学和软件开发领域建立并扩大了公司规模。他在公共和私人市场上筹集了超过 1.55 亿美元的资金，收购了四家公司并出售了三家公司。1997 年，他在 PGP 公司工作时，通过亲自出口 PGP 源代码书，帮助结束了美国对密码学的出口管制。霍夫曼是多项专利的共同发明人，目前是 Directly 和 Iris.tv 的顾问。

Mitch Edwards：首席财务官兼总法律顾问, 2019 年 1 月至今

Mitch Edwards 先生领导我们的财务和法律部门。Edwards 先生拥有丰富的经验，曾担任公共和私营互联网、科技和区块链公司的 C 级主管。从 2015 年到 2017 年，他在 Overstock.com（Nasdaq： OSTK）担任代理首席执行官和总法律顾问。他负责监督 Overstock.com 的区块链并购活动、全球首次注册公开发行区块链证券，以及区块链证券交易所 t-Zero 交易所的开发。在加入 Overstock.com 之前，从 2012 年到 2014 年，Edwards 先生曾担任 Razer Inc.（HKG:1337）的首席财务官兼总法律顾问。(HKG:1337)的首席财务官兼总法律顾问，该公司是一家总部位于新加坡的全球领先的 PC 游戏公司，在那里他领导了国际扩张、并购和上市准备工作。从 2010 年到 2012 年，Edwards 先生担任 Skullcandy Inc.的首席财务官和总法律顾问，负责该公司的首次公开募股、纳斯达克上市和全球扩张，在加入 Skullcandy 之前，他曾担任 BitTorrent, Inc.的首席财务官和 GC。Edwards 先生拥有斯坦福大学法学院的法学博士学位，并在牛津大学获得了法理学和国际商法的学士/硕士学位，他是该校的马歇尔学者。爱德华兹先生还获得了北大经济学学士学位，并在该校的毕业典礼上作了毕业演讲。他还曾在白宫和美国最高法院工作。

Chuck Stoops -理事

Stoops 先生拥有 20 年的财务和技术行业经验，擅长帮助高增长公司转型为全球强者。Stoops 先生出身于 "四大 "会计背景，2004 年加入 PayPal，成为其财务领导团队的第二位成员。在 PayPal 工作期间，他帮助指导该支付公司快速扩张到国际市场，包括规划和谈判在新加坡的国际总部投资，以及在卢森堡建立一个完全特许的 PayPal 欧洲银行。2009 年底离开 PayPal 后，Stoops 先生曾短暂加入 Skype 的财务团队，帮助公司准备 S-1 申请，并最终在 2011 年初成功出售给微软。2012 年，Stoops 先生成为 Netflix 的第一位国际员工，担任欧洲财务主管，直到公司将欧洲业务从卢森堡迁至阿姆斯特丹。当时 Stoops 先生已经在卢森堡安顿好了，2013 年选择回到 PayPal，这次担

任欧盟法律顾问和首席数据保护/隐私官。2014 年底，Stoops 先生加入日本跨国公司乐天，担任其欧洲总法律顾问和数据保护官，他再次获得了欧洲银行的正式执照，同时管理监管事务，并为该集团在欧洲的控股企业提供咨询，包括 Viber、Kobo 和几个国家的电子商务市场。在此期间，Stoops 先生曾担任 eBay、黑莓(RIM)、Skype 等集团公司的董事，精通集团财务报告和控制。目前，Stoops 先生是一家处于早期阶段的银行技术创业公司的负责人，该公司计划在卢森堡获得欧盟监管牌照。 Chuck 是 "交换空间 "公司的积极顾问和投资人，尤其是区块链、支付、身份和忠诚度领域的公司。

Stoops 先生是任何有用的金融普惠项目的倡导者，这些项目可以帮助社会中服务不足和银行不足的群体。Stoops 拥有华盛顿和杰斐逊学院的文学士学位和两个法律学位；佩珀代因大学的法学博士和乔治城法学院的法学硕士。他居住在卢森堡。

知识产权

本公司根据开源 Apache 2.0 许可证对其软件进行授权。本公司目前正在申请临时专利，这些专利涵盖了我们的空间和时间的组合证明、我们的工作难度调整、我们阻止无休止攻击的多链方法以及我们的新共识算法，这些都在我们的绿皮书和我们的新共识工作文件中有所概述。本公司已在全球主要市场注册了 "Chia "和 "Chialisp "商标，并计划将该商标自由授权给与 Chia 网络区块链兼容的软件和应用。本公司没有授权也没有依赖其他公司或个人的知识产权在本公司软件中使用，或已在开源许可下获得特定的版权许可，以包含奇亚区块链软件的某些依赖性。本公司可能决定将其专利与其他公司共同使用，以达到相互防卫的目的。

资本化

自成立以来，公司已经通过 SAFE 协议筹集了约 1600 万美元资金。这些资金主要分三轮，有三种不同标准的价格上限，和转换功能。最后一轮 500 万美元的融资已于 2020 年 8 月完成。没有向任

何投资者被承诺以 chia 作为投资回报。某些投资者拥有赎回权，如果公司在上述特定时间段内未将股权上市公开交易，则将以 Chia(奇亚)币的当时价格计价。本公司预计将这些 SAFEs 转换为股权

或优先股权，并且不打算在本公司股权注册声明生效前向投资者提供 XCH。

我们的投资者包括 Slow Ventures、Naval Ravikant、Breyer Capital、Collaborative Fund、IDEO Colab、a16z Crypto、True Ventures、Galaxy Digital、Cygni Capital、Greylock Partners、DCM、Metastable、StillMark Capital 和 Kamal Ravikant。

为简单起见，并考虑到未来的估值可能会有很大的变化，我们将在假设下一轮资本募集的货币前估值为 250,000,000.00 美元的基础上讨论我们的模拟资本结构。以下百分比没有考虑到未来一轮资金前估值会造成的稀释。我们在计算中包括了所有已发行和未发行的限制性股票奖励、期权或认股权证，以收购 Chia 网络的股票，就像完全归属一样，但不包括为尚未发行的进一步股票奖励保留的股份。

没有一个股东会持有超过 50.0%的公司股份。作为一个整体，投资者将持有本公司 35.1%的已发行股份。单一投资者或基金持有本公司已发行股份的比例不得超过 10%。科恩先生将拥有大约 47.4%的股份，其中包括他的创始人的股权和他随后在保险箱中的现金投资（按折算）。

上市准备情况

公司一直认为最终公开发行股票或上市是我们产品和业务战略的一个组成部分。为此，我们聘请 Edwards 先生担任我们的首席财务官和总法律顾问，并聘请 Hoffman 先生担任独立董事，但现在担任总裁和首席运营官。由于 Hoffman 先生不再符合担任审计委员会主席的独立性要求，我们聘请了符合审计委员会主席资格的独立董事 Stoops 先生。

自成立以来，我们的财务报表每年都由 PCAOB 注册会计师事务所 Armanino LLP 进行独立审计。公司的财政年度截止到 3 月 31 日，公司从成立到 2021 财年已经完成了财务审计。2022 财年截止到 2021 年 3 月 31 日。

结论

金融的未来从现在开始。

Chia(奇亚)是数字世界的绿色货币。