白皮书

版本 1，2021 年 7 月

乔尔・卡斯尔

创始人，KAJ LABS & LITHOSPHERE

joel@kaj labs.com

l ithosphere.network

kaj labs.com

为数字经济打造智能智能合约

抽象的

在地理学中，岩石圈是类地行星或天然卫星最坚硬的外壳。在地球上，它由地壳和上地幔部分组成，在数千年或更长时间的时间尺度上具有弹性。- 维基百科

在过去 10 年中密切关注区块链领域，KaJ Labs 基金会可以从早期网络的错误中学习建立一个更好的区块链网络。

此时，所有类型的代币都完成了一些价值转移和分配的基本功能，但距离现实世界所需的功能齐全的金融服务还有很长的路要走，这就是为什么说到区块链在区块链应用中的应用。金融界，只听雷声，不下雨。人们需要基于区块链技术的新一代金融基础设施，它具有完备的金融功能，能够连接不同的社区和代币，能够尽快弥合中心化和去中心化组织之间的鸿沟，以迎来价值互联网时代。

我们在信息互联网的曙光中创建了一个全新的“电子邮件系统”，而不是改造“邮政系统”。同样，当价值互联网到来时，我们想要构建一个新系统：基于各种代币的价值转移基础设施。

岩石圈（Litho）已为 DeFi 时代做好准备！通过对代币私钥的分布式管理，并通过为中央组织和外部数据源提供端口，在各种代币之上建立一层控制管理，Lithosphere 将连接各种过去和下一代智能合约，解决关键问题当前价值互联网互操作性不足的问题。

岩石圈对所有人开放。它连接中心化和去中心化组织，容纳身份验证方法和匿名交易机制，并通过整合当今存在的和未来可能存在的加密货币和区块链来引入链上数据和链下数据。岩石圈是一台图灵完备的虚拟计算机，它让 DeFi 在未来拥有跨越多个代币的无限遐想空间，开启了今后不可想象的可能性。本白皮书介绍了 Litho 项目的总体概念、关键技术和发展策略，在审视价值互联网的历史的基础上，提出了去中心化银行的前景。

设计理念

区块链的出现和意义

由于缺乏信心，传统的市场经济成本很高。个人持续处理信任的主要方法是通过中心化的组织或公司。现代人类文明的快速发展得益于具有相似理想的人们被组织成政府、政党和企业等机构。然而，中心化组织面临着巨大的挑战：首先，由于组织之间缺乏信任和观念上的争论，各种团体卷入了暴力对抗、多年战争，甚至核恐怖主义。二是资源越来越集中在少数人手中，阶级差距拉大。最后，还有“单点故障”的概念，例如太阳风。

由于少数机构垄断了大量的权力、财富、技能、数据等资源，因此背信弃义或被黑客攻击的后果将是严重的。Lithosphere 的愿景是连接所有区块链，并通过允许它们相互交易来打破区块链之间的障碍。最终目标是创建一个连接的区块链网络，一个能够以去中心化方式相互通信的区块链网络。

有了 Lithosphere，区块链可以维护主权、快速处理交易并与生态系统中的其他区块链进行通信，使其成为各种用例的最佳选择，而不是仅限于一个区块链网络，即 Polkadot / 比特币 / 以太坊 / Cardano。

岩石圈的一个很好的用例是 NFT 的转移。目前，NFT 只能传输给给定网络内的各方。目前无法将以太坊 NFT 发送给智能链 (BSC) 用户，反之亦然。有了 Lithosphere，生态系统中的用户将能够从任何支持拜占庭容错 (BFT) 共识的区块链接收和发送代币。

从机构的中央信贷授权到用于记录价值交换的不可侵犯的数学原理的转变是一个重大进步。货币本质上是一种共识。它是一个标准的会计符号，用于更方便的价值交换。回顾人类的金融史，从以物易物，到以牛羊贝壳作为万能等价物，再到使 用贵金属作为货币，再到目前使用具有强大信用基础的纸币，人类货币是接近抽象数学，它作为符号或分类帐的性质更加明显。由于区块链，人类会计概念变得更加符合数学。

它帮助整个会计系统摆脱单一机构的控制，走向更加公平和透明的道路。普惠金融是一个概念，旨在为世界各地的弱势个人和小企业提供进入金融系统和低成本金融服务的途径。全球有 25 亿人无法使用银行、开设储蓄账户或获得信用卡，从而将他们与全球经济隔绝。银行对跨境转账收取高昂的费用。普通投资者只能从银行等金融机构购买非常低端的金融商品，在谷歌、阿里巴巴等科技公司上市之前，他们无法参与早期投资。

许多中小型企业虽然信用良好、业绩优异，但也难以获得银行的贷款支持，因为它们不是80/20规则下传统银行的目标客户。区块链技术的发展正在改变上述条件。比特币用于支付萨尔瓦多等其他国家的工人工资。参与比特币和以太坊等知名区块链项目的首次代币发行 (ICO) 的投资者获得了初始投资数百倍的回报。由于区块链技术，普惠金融达到了新的高度。许多组织正在探索将传统形式的资产（例如商业票据和忠诚度积分）记录到区块链中的方法，通常以联盟链的形式。加密货币作为金融交易中的一种支付方式正变得越来越被接受；许多组织正在探索将传统形式的资产（例如商业票据和忠诚度积分）记录到区块链中的方法，通常以联盟链的形式。出现了可与传统金融机构相媲美的数字资产交易所。

交换数字资产的银行功能由这些交易所执行。它们类似于证券交易所，因为它们提供了一个购买和交换代币的平台。跨境代币转账平台的功能可与跨境银行汇款的功能相媲美。然而，这些平台在不同程度上以中心化的方式运行，这不仅引入了与中心化相关的安全问题，而且阻碍了区块链技术的广泛使用。基于这种现象，我们需要一个分布式的“银行”，通过区块链可以将多种数字货币和数字资产移入、移出和交换。我们需要一个可以开发和执行基于数字货币和数字资产的金融产品和合约的位置，以及保护交易隐私的安全环境。当然，这样的“银行”除了借记贷记、汇款、结算、金融产品销售等少数服务外，与传统银行完全不同。任何有足够专业知识和现金的公司或个人都可以打开他们的业务窗口。他们可以提供多种服务，同时维护分布式区块链基础设施的安全性，从而为更多人提供更多金融服务。更准确地说，这是一个建立在数字资产和分布式金融市场上的未来金融基础设施。任何有足够专业知识和现金的公司或个人都可以打开他们的业务窗口。他们可以提供多种服务，同时维护分布式区块链基础设施的安全性，从而为更多人提供更多金融服务。更准确地说，这是一个建立在数字资产和分布式金融市场上的未来金融基础设施。
任何有足够专业知识和现金的公司或个人都可以打开他们的业务窗口。他们可以提供多种服务，同时维护分布式区块链基础设施的安全性，从而为更多人提供更多金融服务。更准确地说，这是一个建立在数字资产和分布式金融市场上的未来金融基础设施。

设计目标

区块链的主要好处在于，它有助于解决困扰人类的信任问题，使区块链技术提升人类文明水平。由于人类需要减少交易费用，它的增长势不可挡。因为每条区块链都可以进行点对点的价值传输，与原来的信息互联网（IoI）不同，区块链技术将我们从IoI时代推向了价值互联网（IoV）时代，可以说是第三个互联网的产生。

Lithosphere 基于对跨链技术、人工智能和机器学习的研究，以及去中心化的特点及其应用场景，确立了以下目标，以开发更广泛传播的区块链技术和数字资产应用：

跨链资产转移：

- 连接大型数字货币网络（如比特币和以太坊），在不改变原有链的机制的情况下完成资产交易。这使得 Lithosphere 能够以非常便宜的成本整合新创建的数字货币网络。
- 将岩石圈与财团链相结合。这处理从原始链到岩石圈的资产转移、从岩石圈到原始链的资产转移以及岩石圈上的资产交易。
- 确保跨链交易安全，跨链交易服务稳定。

交易隐私保护：

- 允许交易方选择是否私下执行交易。为数字资产转移和交易提供隐私保护。为数字资产持有
- 者提供匿名保护。
-

功能扩展性：

- 成为不可替代资产和数字货币交易的去中心化平台。为多种数字货币经营一家存款和借贷公司。
-
- 使用数字货币作为数字资产交易的工具。创建全新的数字金融资产并进行
- 兑换。

由于信息互联网，世界发生了巨大的变化。由于价值互联网，人类文明注定要经历巨大的社会变革。这得益于基于区块链技术的价值互联网所具备的数字化、智能化、去中心化、普惠等品质。数字化和智能化可以帮助价值互联网更高效地运行，这些元素已经存在于信息互联网上，但现在正在应用于价值互联网。去中心化是一个更重要的特征，因为它将有助于消除中心化组织造成的瓶颈。人们可以通过私钥更好地维护自己的个人财产权；他们可以更好地解决与共识机制的冲突，

当人们可以轻松地通过互联网传输信息并使用算法编程信息时，人们就加入了信息时代的互联网；当他们可以轻松地通过互联网发送价值并使用智能合约编程价值时，他们将进入价值互联网时代。价值互联网的优势使其比传统协作模式具有“高维度”优势。在区块链上，所有类型的“价值”都将被表达并易于交换和编程。结果，人们的协作关系和人类文明无疑将发生巨大的变化。

价值互联网将允许个人像被告知一样处理价值，其主要作用将是传达价值。

然而，要实现这一目的，互联网的价值必须在三个方面提高。互操作性是第一位的。价值存在于许多区块链、中心化组织和数据中心，价值互联网需要公链或其他解决方案，可以跨区块链、中心化组织和数据源进行交互，以及转移价值和执行智能合约。第二个因素是可扩展性。价值互联网必须适应各种情况，包括银行、工业和政府管理。最后要考虑的一点是有用性。价值互联网需要强大的生态系统和无缝运行各种应用程序的能力，以便开发人员可以快速创建应用程序，而消费者可以轻松使用它们。

然而，与信息互联网相比，价值互联网仍处于早期阶段，存在互操作性、可扩展性和可用性限制。

在互操作性方面，虽然信息互联网已经能够将文字、照片、音频和视频作为一个统一的信息进行传输和编程，但价值互联网仍在努力解决区块链之间的价值交流，尤其是链下值和数据。

价值互联网不仅需要跨链连接，还需要与中心化实体和外部数据源的连接。不同区块链上的代币无法相互交易，因为现有区块链无法相互通信（状态机同步）。由于区块链目前无法与区块链之外的中心化组织进行通信，因此很难将链下资产映射到区块链上。由于现有的区块链无法读取链下数据，因此其上的“智能”合约是盲目的或愚蠢的，无法看到或与外界交流。

以跨链技术为例，跨链通信，尤其是构建跨链智能合约，现在极具挑战性。现在有成千上万种不同类型的代币可用，但每一种都只能在单个区块链上自由移动，并拥有自己的钱包生态系统、智能合约创建工具等。现有的区块链网络本质上是岛屿生态系统，价值互联网距离真正可互操作还有很长的路要走。

在可扩展性方面，当信息互联网通过将各种数据编码为比特，将各种场景的通信逻辑编程为应用程序而不断扩展的同时，价值互联网才刚刚起步，将各种价值代币化为代币，映射各种场景的交易作为智能合约的逻辑。

价值互联网规模由于缺乏兼容性而受到严重限制。链下价值向价值互联网的转移受到了难以将涉及多种货币、众多组织和多种数据源的实际应用场景映射到区块链以构建分布式解决方案的困难。

在可用性方面，虽然信息互联网的处理能力、存储容量和同步速度足以处理大多数信息管理需求，但价值互联网只能适应更大的项目。在标准化、平台化、功能模块化、应用生态、互操作性、抗量子攻击等方面，价值互联网还有很多工作要做。

互操作性是上面列出的三种障碍中最紧迫的，因为它允许我们在区块链之间移动资产，设计各种货币的智能合约，并提高更新的可扩展性。另一方面，可用性是一项长期的努力，但阻碍价值互联网发展的互操作性和可扩展性需要快速解决，并已成为需要解决的两个最紧迫的障碍。

智能合约和去中心化金融 (DeFi)

价值互联网的目标是将不同的价值链接到区块链，以便智能合约可以控制它们。价值互联网实现了个人之间去中心化、去中介化、包容性和可编程的协作。由于这些明显的好处，不同的价值将竞相映射到区块链。随着区块链限制得到解决，价值互联网无疑将以更快的速度扩展。

将价值映射到区块链的过程需要将金融逻辑与业务逻辑解耦，这意味着价值互联网是由一个重要的金融组件创建的。价值互联网金融应用是指价值互联网上具有特别显着金融特征的应用。去中心化金融是指价值互联网上的链上金融操作，以及相应的链下金融活动（DeFi）。

由于价值互联网建立在使用用户数据报协议的点对点网络上，因此存在一定的障碍。未来价值互联网的性能将逐步接近信息互联网，业务场景和金融交易可以在同一个软件中编写。但是，鉴于目前的情况，我们预计这将需要很长时间。目前的价值互联网将主要支持金融应用，即 DeFi 应用将是主要应用。

信息互联网已经对人们的生活产生了重大影响。由于价值互联网，我们也可能预期我们的生活会发生重大变化。我们可能熟悉互联网上提供的多种形式的信息，但很少有人谈论价值互联网的“价值”。

首先，价值互联网上的价值是由区块链表示的代币，将价值映射到价值互联网的过程称为资产代币化。如果链上的代币代表底层链下资产的所有权、收益和控制权，则连接的资产将以链上代币表示并构成价值互联网的一部分。价值互联网让越来越多的价值通过这个过程进入自身，通过分布式账本防止“双花”，让没有中介的价值传递像发送信息一样简单，编程价值像编程信息一样简单，使得价值互联网的前景与我们之前在电信方面看到的相似。

其次，代币化是资产证券化的一种形式，其中链下价值作为加密资产映射到链上。由于代币可以无限分割并随时间和空间转移，因此它们可以用于抵押、贷款和保险等金融交易。因此，通证化被定义为将资产证券化并将链下资产转换为可以使用私钥进行管理的加密资产的过程。

最后，价值互联网将包含更广泛的价值。只要通证化有利可图，身份、签名、数据、投票权和其他数据就会映射到价值互联网。因此，价值互联网将比传统金融市场拥有更广泛的价值。

定位

我们根据 DeFi 的光明前景和当前价值互联网提出的挑战提出了岩石圈项目。Lithosphere 的目标是打造数字经济时代的平台级公链，可以连接各种价值，提供完备的金融功能，沟通多元社区和代币，架起中心化和去中心化组织的桥梁，将价值互联网作为借助区块链、人工智能等技术尽快实现。

岩石圈建筑与技术

分布式私钥管理和智能合约虚拟机

由于 DeFi 资产以代币的形式显示，如果可以实施多代币智能合约，它们可以大大提高价值互联网的互操作性，并且可以更容易地提高可扩展性。目前的跨链技术多为侧链技术，采用双向挂钩将交易转移到侧链，多重签名退出侧链。这样的方法只能产生原子转移，结果几乎各方面都不尽如人意。我们需要创建一个公链，允许其他代币以更具创造性的方式映射到它，以便可以创建多代币智能合约。我们可以通过这种方式大幅提升价值互联网的互操作性，而这条公链无疑将成为最重要的 DeFi 基础设施之一。它不仅可以在区块链之间传达价值，还可以实现与中心化组织和链下数据源的接口，以提高价值互联网的可扩展性。在一条新的公链上，各种代币将如何表达？我们设想各种区块链上的代币私钥可以通过公共链以分布式方式安全地控制，这样，区块链就可以管理代币的控制权。它将像价值互联网上的一条“高速公路”，可以轻松实现各种代币和多代币智能合约之间的价值转移，提供各种 DeFi 服务。各种代币将如何表达？我们设想各种区块链上的代币私钥可以通过公共链以分布式方式安全地控制，这样，区块链就可以管理代币的控制权。它将像价值互联网上的一条“高速公路”，可以轻松实现各种代币和多代币智能合约之间的价值转移，提供各种 DeFi 服务。各种代币将如何表达？我们设想各种区块链上的代币私钥可以通过公共链以分布式方式安全地控制，这样，区块链就可以管理代币的控制权。它将像价值互联网上的一条“高速公路”，可以轻松实现各种代币和多代币智能合约之间的价值转移，提供各种 DeFi 服务。

由于几乎所有的区块链代币都是由私钥控制的，因此价值互联网上的价值可以通过智能合约进行分布式管理，只要其代币的私钥可以由公共链的分布式节点控制。有了图灵完备的智能合约，公链还可以以更复杂的形式提供去中心化金融（DeFi）的各种功能。

这个连接所有代币的区块链，对于各种应用场景不需要复杂的逻辑。其目的是在所有区块链上创建一个管理层，使所有代币能够进行交互。因为它不需要运行繁重的应用程序逻辑，所以在目前的可用性下，它能够完成各种 DeFi 功能。

无数分布式密钥管理 (MDKM)

岩石圈基于密码共享领域的分布式密钥生成（DKG）理论和成果。公钥和私钥都是由合作通信的节点生成的。公钥在公链中广播，私钥通过可变秘密共享（VSS）以分布式的方式由各个节点分别存储。公用公钥由DKG算法生成，再由相应算法生成Lock-in的账户地址，实现去中心化控制。

这里我们参考基于椭圆曲线密码学分布式密钥生成协议的VSS和DKG领域以及应用研究的过程如下：

给定椭圆曲线E，存在一个有限域GF(q)，q是一个质数，有n个参与者集Q = {P1, P2, ..., Pn}，pi表示第i个参与者Pi的身份，而Pi表示 ∈ GF * (q)，其中 GF * (q) 是 GF (q) 上的乘法群。同时，pi 和 I 在计算过程中可以互换。E/GF(q)表示E上的加性基团。T为E/GF(q)，E/GF(q)的阶数为素数或素因数，将此素数或素因数标记为p。

在这个密钥生成协议中 ，假设标量乘法和点乘法都在 δ 并且其他操作在 GF (q) 处完成。为了计算 Q (x) T，我们首先计算 Q (x) 然后 p(x) mod p，Q (x) mod p 是 T 上的标量乘法。让我们假设 E 有另一个基点 T′ 在椭圆曲线上 δ。

阈值签名

阈值签名技术可以解决岩石圈离开节点创建的签名问题，同时也提高了区块链网络的稳定性。根据分布式密钥生成网络中节点自适应的研究，Lithosphere 会在极端情况下选择合适的节点加入并刷新共享的密钥参数，以保证链的成功运行。

石版币

Litho 是岩石圈的原生硬币。跨链和链内交易都会消耗一定数量的 Litho。Litho 还用于跨链验证节点的保证金。Litho / $LITHO 是 Lithosphere 网络中的首选货币，尽管也可以使用另一种加密货币，因为 Lithosphere 区块链支持互操作性。

LAX - 算法稳定币

Litho 算法稳定币 (LAX) 类似于在以太坊区块链上运行的算法稳定币协议，但与美元币 (USDC) 和 Tether (USDT) 等币种不同，后者由经审计的美元或 PAX Gold 等加密资产支持(PAXG)，Litho USD 硬币不与美元或任何加密抵押品挂钩。Lithosphere 协议不是使用加密货币、法定货币或商品作为抵押品，而是在称为“重新调整基准”的过程中每 24 小时调整其 LAX 加密货币供应以维持稳定的价格。

共识机制

岩石圈采用了权益证明共识机制。

Lithosphere 的目标是利用区块链技术构建一个基础设施平台来运行去中心化的应用程序，在平台上，多种类型的代币将能够通过智能合约自由交互，实现价值互通。Lithosphere 旨在实施 Myriad Distributed Key Management，为 DeFi 构建智能合约。

当未注册的资产从原始链转移到 Lithosphere 时，Lithosphere 将根据跨链交易信息构建新资产，利用内置资产模板部署新的智能合约。当注册资产从原链转移到 Lithosphere 时，Lithosphere 将在现有合约中发行等量的代币，确保原链资产仍可在 Lithosphere 上交易。

跨链整合

资产映射是指在 Lithosphere 上为受控项目生成匹配令牌的过程。由于映射，一个令牌可以与其他映射资产自由交互。锁定和锁定操作用于建立和解除分布式控制。

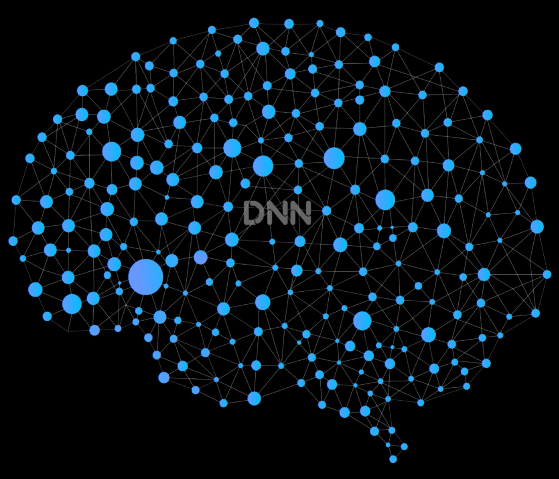
跨链交易

资产锁定是为所有密钥管理的代币启用无数分布式密钥管理和资产映射的过程。

Asset Lock-out)是Lock-in的逆向，由控制权限管理和资产映射拆解两部分组成。锁定完成后，数字资产的控制权返回给所有者，恢复完整的密钥存储和集中的密钥管理。通过提高当前数字资产的安全性、流动性和 DeFi 应用，采用多样化的密钥分发管理将提升数字资产的价值。

深度神经网络 (DNN)

David Yang 博士提出了用于岩石圈智能合约的深度神经网络 (DNN)。DNN 在区块链应用中非常有用，例如 DeFi 和 NFT 交易。然而，由于这些平台的两个基本设计问题，在当今的区块链平台上训练/运行大规模 DNN 作为智能合约的一部分是不可行的。首先，现在的区块链通常要求每个节点随时保持完整的世界状态，这意味着节点必须执行每个区块中的所有交易。对于涉及 DNN 的计算密集型智能合约来说，这是非常昂贵的。其次，现有的区块链平台期望智能合约交易具有确定性，



可重复的结果和效果。相比之下，DNN 通常在 GPU、TPU 和/或计算集群等大规模并行计算设备上训练/运行无锁，这些设备通常不会产生确定性的结果。

Lithosphere 首次在智能合约中实现了 DNN，通过将大规模深度神经网络 (DNN) 纳入代码中，使智能合约变得智能，具有众多潜在应用。例如，在去中心化金融 (DeFi) 中，DNN 可能有助于检测异常的代币价格变动，这可能是闪电贷攻击的一部分。去中心化自治组织 (DAO) 可能会与通过强化学习不断训练的 DNN 自动交易代币。内容创建者可能会应用生成对抗网络 (GAN) 来生成视觉艺术图像，然后将它们标记为可在去中心化交易所中交易的不可替代的代币 (NFT)。

LEP100 多链通证标准

LEP100 是多代币的新标准，允许单个合约代表多个可替代（货币）和不可替代代币（NFT），以及由 Lithosphere 的创建者 Joel Kasr 提出的用于提高 gas 效率的批量操作。最重要的是，LEP100 代币可以兑换任何其他代币等价物。LEP100 代币使用原生 Litho 代币 (LITHO) 提供燃料。

. 当与 LEP100 代币挂钩时，您还可以与使用任何主要数字资产的任何网络挂钩。代币是多合约兼容的，并具有转移、返还余额和检查代币拥有情况等基本功能。与 ERC20 或 BEP20 不同，LEP100 代币允许单个合约代表众多可替代和不可替代的代币，从而可以在日常使用中广泛应用。它是 DeFI 平台、游戏平台、NFT 和其他高需求合约兼容平台的最有效代币。LEP100 还可以轻松集成到任何以太坊 dApp 或其他链中，因为它可以交易 ERC20、ERC-721、ERC-1155、BEP2 和 BEP20 代币。LEP100 建立了管理跨链代币的最佳实践。由于它们的相似性，代币与 ERC20、ERC-721、

LEP100 代币标准还允许在智能合约中进行代币时间切片。当一个token被切片时，它被分成两部分：一个是有时间限制的切片（这里的TL代表Time-Lent），另一个是无限的末端（这里的TL代表Time Restricted，因为它的效用是有限的）一段时间但未锁定）。如果需要，两个切片都可以再分成两个时间片，从而实现复杂的 DeFi，例如期权和期货交易。

验证器

在经典的拜占庭容错 (BFT) 算法中，每个节点具有相同的权重。在岩石圈中，节点拥有非负的投票权，拥有正投票权的节点被称为验证者。验证者通过广播加密签名或投票来参与共识协议，以就下一个区块达成一致。

验证者的投票权在创世时确定或由区块链确定性地更改，具体取决于应用程序。例如，在 LithoSwap 等权益证明应用程序中，投票权可能取决于作为抵押品的抵押代币数量。

线性通信 BFT 共识

Litho 协议利用 BFT（BFT 代表拜占庭容错）算法来实现这一点。拜占庭容错共识算法可保证多达三分之一的拜占庭或恶意行为者的安全。分布式系统中的拜占庭故障是最难处理的。

由 BFT 提供支持的 Lithosphere 等区块链框架允许公共和私有区块链相互转移代币。

BFT 驱动的区块链网络（Lithosphere）允许与其他 PoS/快速终结性区块链（如 Cosmos、Binance 或权威证明和 PoW 区块链）进行互操作。

岩石圈采用了一种新的共识算法，即由 David Yang 博士提出的 LinBFT。线性通信 BFT 协议（LinBFT）适用于无需许可的公有区块链系统，其中没有公钥基础设施，基于经典的 PBFT，有 4 大改进：

- 每块共识。每个块都有共识，而不是一组块。这限制了区块提议者的权力，从而减轻了自私挖矿。
- 轮换领头羊。LinBFT 协议为每个区块更改领导者（即区块提议者），这降低了领导者遭到拒绝服务攻击的风险。
- 改变诚实。在 Pyramid LinBFT 中，只要超过 2/3 的所有参与者对每个块都是诚实的，参与者可以对一个区块是诚实的，而对另一个区块是恶意的（例如，一个包含参与者感兴趣的交易）。换句话说，每个参与者都可能在某个时候是恶意的，但区块链始终保持安全。
- 动态参与者集。LinBFT 允许节点在纪元开始时加入和离开协议。因此，不同的区块可能会被完全不同的节点集验证。

此外，在普通情况下，LinBFT 只涉及一轮投票，而不是 PBFT 中的两轮投票，这减少了通信开销和确认时间，并采用了权益证明机制来奖励所有参与者。使用从以太坊测试网获得的数据进行的大量实验表明，LinBFT 始终且显着优于现有的区块链生产中 BFT 协议。

无数分布式密钥管理

Myriad Distributed Key Management 通过多个节点，根据目标区块链采用的数字签名算法，在目标区块链上分布式生成公私钥对和地址以及交易签名，从而实现账户的控制和管理和目标区块链上的资产以分布式方式。

这样的技术路线使得 MDKM 能够兼容尽可能多的加密算法控制的数字资产，无论这些数字资产是在中心化还是去中心化的基础上产生的。通过MDKM支持签名算法，可以控制和管理一系列具有相同签名算法的加密数字资产。

目前大部分（超过80%）加密数字货币采用与比特币和以太坊相同的ECDSA签名算法，因此MDKM首先选择实现对ECDSA签名算法的支持。此外，MDKM 将支持使用不同签名算法的加密货币，例如 Stellar 的 Ed25519 签名算法[JL17]，以及 Schnorr 的签名算法。

LEP100 代币标准

所有 Lithosphere 代币都遵循 LEP100 规范。Lithosphere 网络是一种多链架构，允许任何人开发 dApp 和其他基于区块链的数字资产。它还确保跨链交易、最小的gas消耗和安全交易的快速交易。

LEP100 使 Lithosphere 区块链上的代币能够正常运行。因此，每个人都可以从低交易费用中受益。

此外，无论区块链网络的结构如何，跨链 DeFI 机制都提高了所有小合约的互操作性。Lithosphere 环境非常支持，Litho Launchpad 通过各种 DeFI 程序为所有引导程序提供资金。

为什么你的 DeFi 项目应该使用 LEP100 代币标准?

LEP100 代币可用于代表各种资产，包括股票、法定货币和加密资产。来自各种区块链的其他代币可以很容易地与 LEP100 代币挂钩。因此，它使开发人员能够使用相同的代币构建不同版本的加密资产。

所有转移 LEP100 代币的验证者都将获得 LITHO 作为奖励。奖励以交易费用的形式支付。与 ERC20 等其他代币标准相比，它的所有交易的 gas 价格最低。它建立在 Lithosphere 网络上，可提供超过

10,000 TPS 与以太坊的 ERC20 的 15 TPS 和比特币的 4 TPS 相比。

将 DeFI 项目与 LEP100 代币集成很简单。您还可以在 DEX 上免费列出项目，例如 LithoSwap、PancakeSwap 和 Uniswap

LEP100 代币特性

LEP100 代币提供了许多出色的功能，包括

- 高速交易速度：LEP100 代币标准可实现高速交易速度，使其具有极强的可扩展性。
- 低交易费用：与以太坊网络不同，用户不会被收取高昂的天然气价格。
- 跨链兼容性：ERC20、ERC-721、ERC-1155、BEP2和BEP20网络和区块链支持LEP100代币。
- 与当今市场上几乎所有主要的加密货币钱包兼容。
- 易于在交易所出售：LEP100 代币易于在交易所上市，并且被出售的可能性更大。

验证节点

为了赚取部分交易费用，验证者完成对岩石圈交易的记录。根据其拥有的权益，验证者收到相应的密钥份额并计算关联的签名份额以附加到交易中。根据密钥份额百分比，验证者获得与验证交易相关的交易费用。如果密钥共享信息不可用或丢失，则无法收取交易费用。如果节点签署了错误的交易，验证者的凭据也将被删除。

综上所述，验证节点激励系统将鼓励 Authenticators 提供适当的交易证明，Validators 忠实地完成 Lithosphere 记录，以及 Record-keeper 保持在线并保持其关键份额的安全。

验证节点仅适用于在岩石圈网络中拥有足够大股份的个人。一般节点是不符合验证节点条件的节点。一般节点无法参与跨链交易验证过程，但可以将其权益提交给受信任的验证节点。委托验证节点收到的交易费用按照委托权益比例分配给普通节点。如果委托的验证节点受到惩罚，一般节点将遭受类似的损失。

由于这种激励机制，岩石圈的利益相关者可以获得与权益相关的优势，同时也有动力将他们的权益提交给受信任的验证节点。这增强了岩石圈的安全性和稳定性。

锁定账户生成方案

锁定账户生成方案基于阈值密钥共享和安全多方计算。

介绍

分布式密码学的理论基础和分布式计算的一个基本挑战都是安全的多方计算。

该假设基于 1982 年出版的《姚的百万富翁问题》一书。简单定义，安全多方计算是指一组称为 P1 Pn 的参与者协作安全地计算函数 f(x1, xn
) =(y1, yn)。然后 n 个参与者中的每一个都有函数 f 输入之一。Pi有秘密输入xi，计算后得到输出yi。在这种情况下，即使有人在整个计算过程中作弊，安全性也需要确保计算结果的有效性。这意味着在计算完成后，每个参与者必须收到正确的结果 yi，并且所有参与者的输入都受到保护。通过计算，Pi除了(xi,yi)无法获得更多信息。

通用节点

阈值密钥共享方法旨在解决安全密钥管理问题。根据当代密码学设计原则，密码学的安全性取决于密钥的安全性。如果安全密钥被泄露，密码学的安全性将受到威胁。因此，密钥管理在密码学安全研究和设计中至关重要。当一个帐户由具有不同兴趣的众多人维护时，安全地处理密钥分发可能具有挑战性。密码学家 Adi Shamir 设计了 Shamir 的秘密共享阈值密钥共享技术来解决这个问题。

一个密钥被分成 n 块并交给这个系统中的 n 个参与者。每个参与者都有一块密钥共享，并且必须使用最少 k 个密钥共享来重构密钥。因此，一个账户上的每项活动都需要至少 k 个人的合作来维护账户的安全性和可靠性。

基于安全的多方计算和阈值密钥共享，我们创建了锁定帐户创建技术。岩石圈验证者（记录管理员）负责维护和管理锁定帐户的密钥，以确保它们的安全和可靠。此外，在没有设置拓扑的 ad-hoc 网络中，该技术降低了密钥丢失的危险，并提供了高度的灵活性和稳定性。

以下是锁定账户生成方案：

设计说明

第 1 步：选择一个安全的随机数。
在岩石圈上，有 n 个验证器，称为 P1.....Pn。每个验证器选择一个安全的随机整数 di 以及一个 k 阶多项式 fi (x)=di+ai,1 x+ +ai,k-1xk-1。该技术通过安全通道将 fi (j) 传递给其他验证器，并将 di G 广播到每个网络节点，G 是椭圆曲线的基点。

第 2 步：验证消息是否正确。
Pj 将在收到其他验证器的消息后检查消息的正确性：lag=Check(f1
(j),.....,fn (j)) lag=Check(f1 (j),. ,fn (j)) lag=Check(f1 Pj 接受并在本地存储如果 flag=true。如果 flag =false，Pj 拒绝消息，需要其他验证器重新提交。

第 3 步：您将获得分发的密钥。
当所有的消息都被传递和签出后，每个验证者会收到他们的密钥份额如下： fj(k),k=1,.....,n key sharek=(j=1) fj(k),k
=1,....,n

第 4 步：确定锁定帐户的地址。
锁定账户地址=GenerateAddress(d1 G,.....,dn G) n 锁定账户上的任何活动都需要至少 k 个验证者的参与。

方案生成

在锁定帐户创建过程中，私钥不会在整个网络中生成或重建。需要至少 k 个验证者的参与来生成锁定帐户的签名。他们使用自己拥有的密钥份额独立计算签名份额，然后使用签名份额来重建完整的签名。锁定账户的签名方案如下：

计算步骤 1 中的签名份额 使用密钥份额，几个 n 岩石圈验证器计算消息的签名份额。

第2步： 分发签名。
每个验证者将他或她的签名份额传输给其他人。

第 3 步： 重新组合并广播整个签名。
当验证者获得超过 k 个签名份额时，它会重建整个签名并将其广播给其他验证者：

签名=构造Sig（签名share1，.，签名sharek）

第四步： 他们生成锁定账户的完整签名，其中包括以下信息：signature sharej=Generate Sig(m,key sharej)

优点

即使部分网络瘫痪或某些重要份额丢失，整个系统仍保持稳定和安全。为了减少密钥共享带来的威胁，每个验证器的密钥共享都会定期更新或在满足触发情况时更新。

轻松集成和高效数据存储

原链的初始交易用于对锁定账户进行任何操作。没有新的交易类型或验证机制。因此，理论上任何链都可以以低成本与岩石圈合并。同时，不同于多重签名账户方案采用智能合约逻辑实现多方管理，Locked Account创建策略采用密码学原理实现多方管理。最后一笔交易只有一个签名，而不是多个。因此，这种技术的数据存储效率更高。

智能合约代币交易匿名

为了在 Lithosphere 上的智能合约代币交易中实现匿名，使用了环签名和一次性账户。为了使发件人匿名，环签名将交易发件人与一组虚假成员结合在一起。每笔交易都会生成一个无法连接到实际所有者的一次性帐户。

几乎所有的跨链交易方案都需要一种锁定源链资产的技术。被锁定的资产只有在满足触发条件后才会解锁并返还至原账户或其他账户。

Hashed TimeLock Contract 系统、可信第三方托管账户策略和多重签名账户方法是现有技术的示例。

完全去中心化，无需第三方参与

安全多方计算用于生成锁定帐户。此程序不需要值得信赖的第三方参与方或背书。我们所需要的只是验证者进行信息交换和计算的安全路由。锁定帐户生成技术比受信任的第三方托管帐户方案更便宜且更灵活。

安全稳定

Shamir 的秘密共享方案（又名 Shamir 的 (k, n)-阈值秘密共享方案）用于将锁定帐户的密钥分发给 Lithosphere 验证器。每个验证者持有密钥份额的一个组成部分。即使有几个验证人下线或丢失了他们的密钥份额，锁定帐户的签名仍然可以产生，并且交易仍然可以在至少 k 个验证人的情况下完成。因此，锁定帐户的创建策略可以确保这一点。

一次性帐户系统

一次性帐户方法作为匿名的基础特别重要。每个用户都有一个主账户和几个子账户。因此，如果有人希望在智能合约代币交易中保持匿名，除了原始账户之外，他们还必须创建一个相关账户和一个一次性主账户。

环签名方案

2001 年，引入了环签名方法。这是一种有点不同的组签名方案。组签名方案需要可信中心和安全设置，这意味着签名者可以被信任中心跟踪。通过消除可信集线器和保护系统，环签名方法克服了这个主要问题。

自从引入环签名方法以来，已经开发了许多基于椭圆曲线密码（ECC）的实用系统，例如陷门方法。活门环签名、可链接环签名、匿名可撤销环签名和可否认环签名是环签名系统的四种类型。

Lithosphere 开发了基于 ECC 的环签名方法，以在智能合约代币转移中提供匿名性。

环签名方案分为三个部分。下面以签名者(P,x)为例进行说明：

使用 GEN 获取公共参数。签名者使用方法 GeneratePublicKeySet() 和公钥作为参数来构建一个包含来自全局状态的 n 个成员的公钥集：
publickeyset=GeneratePublicKeySet(P)
I=GenerateKeyImage((P,x))=I=GenerateKeyImage((P,x))=I=GenerateKeyImage((P,x))=I=GenerateKeyImage((P,x))=I=GenerateKeyImage((P,x))=I
环签名：创建环签名。签名者使用 GenerateRingSignature( ) 为消息 m 生成环签名，使用公钥集、I 和 x：
ringig=GenerateRingSignature(m,public keyset,I,x) VERIFY THE RING SIGNIFICANCE VerifyRingSignature()，返回 true 或 false使用公钥集、I 和环：lag=VerifyRingSignature 验证消息 m 的环签名。(m,publickeyset,I,ringsig) 如果标志为真，则环签名有效。否则，它是无效的。

环签名方案中的关键图片和环签名无法与公钥集中的签名者匹配。任何人都可以检查签名是否真实，但没有人可以识别签名者。

基于密码学的安全保证

许多现有的跨链交易采用逻辑安全机制，依赖于参与者注意自身利益。换句话说，如果这意味着损害他们的利益，玩家不会破坏跨链交易。这被称为“理性参与者假设”。Lithosphere 采用阈值秘密共享技术，以及独创的椭圆曲线加密技术，保证了原始签名方案的安全性。

基于多方计算的锁定账户管理解决方案；

基于环签名和一次性账户的智能合约代币交易隐私保护方法。

开始跨链交易后，所有后续操作都在 Lithosphere 验证器节点之间自动执行，不需要交易参与者的协调。这就留下了密码方法的安全性来确保系统的无缝运行。

智能合约

识别和定义各方的财务联系 智能合约改进。

智能合约是一种从时间序列和空间位置上定义多个参与者之间一种或多种数字资产的关系和价值交互条件的合约，用于完成多个参与者之间一种或多种数字资产的金融交易。

通过数字资产锁定映射到 Lithosphere 链上的资产，允许 Lithosphere 的智能合约同时指定许多不同数字资产之间的连接，称为数字资产。

各种数字资产的所有者或消费者被称为多个参与者。它们在 Lithosphere 链中表示为账户，包括用户和合约账户。加密智能合约中的合约参与者可能包括众多用户账户以及许多合约账户。

通过智能合约进行金融交易的定义成为对各种数字资产和不同时空所有权之间联系的描述，因为金融的核心是跨时间和地点的价值交换。

以下是当前智能合约的局限性：

- 只能在同一链上的两方之间对同一数字资产进行操作；只能转让数字资产的所有权，使使用和所有权
- 不可分割；
- 只能由交易触发，没有链下触发条件或合法的链下信息输入。
- 实现多方、多种数字资产间的所有权和使用权的应用；有效获取链下数据输入；
-
- 以封闭或并行的方式调用智能合约中的其他智能合约，就像智能 合约是智能合约一样。

Myriad Token 管理中的 Key Distribution 允许各种数字资产之间进行交互，并成为 Lithosphere 智能合约的定义和编程对象。因此，它有能力和需要实现多角色、多令牌和使用权分离（权利）等 DeFi 功能。

智能合约处理许多不同帐户类型同时还定义众多用户和各种智能合约之间的连接的能力被称为多角色。

在使用 Lock-in 将不同的数字资产映射到 Lithosphere 之后，Lithosphere 上的智能合约可能会同时描述许多不同数字资产之间的关系。

使用权分离是指将数字资产的使用权（权利）和所有权分离的能力。目前的智能合约只能将代币作为一个整体从一方转移到另一方，一方获得数字资产的所有权而另一方获得使用权是不可行的，这意味着传统智能中所有权和使用权是分开的。合同。在单个智能合约中建立两个以上的用户账户或合约账户很简单，允许所有权和使用账户以及金融活动（如跨各种数字资产的抵押贷款）分离。

如果数字资产之间的链接仅在空间方面进行指定，则数字资产的转移将成为可能。如果这种关系以时间为特征，则是它们之间的借用关系。当用对象属性来描述连接时，它代表对象的所有权和使用权。因此，将一个或多个时间、空间、对象属性等关系的逻辑抽象化，可以构建各种数字资产之间从简单到复杂的各种交易，甚至引出尚未实现的金融创新，无限想象。

合约多重触发机制触发条件多样化

由于目前的智能合约是通过对合约的转移来触发的，所以目前智能合约的实现是基于数字资产所有权的转移。

例如，当用户开始向智能合约转账时，节点必须首先验证转账的合法性，其中包括确定用户当前在区块链上的财务余额是否支持该交易。智能合约然后运行接受礼物的相关函数，并根据函数预定的响应条件对其进行判断。例如，智能合约会检查捐赠的全部金额，只有在没有超过配额的情况下才会接受。最后，修改后的合约值或智能合约状态将被放入区块中，以表明交易已经发生。

从前面的分析中我们可以看出，智能合约的功能会涉及到对一些标准的判断，但是如果智能合约没有被首先触发，这些条件是不会被检查的。即使满足要求的情况，也不会触发智能合约中以下规则的执行。许多金融交易场景，例如被动量化交易策略，如果智能合约不能由交易以外的因素触发，则无法执行。因此，改进触发机制是改进 DeFi 应用程序智能合约的第一步。除了支持现有的主动触发方式外，还引入了两种新的触发机制：时间触发和事件触发。

多种触发机制的三种触发方式如下：

- 主动触发方式类似于当前的智能合约触发方式，兼容所有智能合约。
- 定时触发模式是指智能合约被时间点或持续时间等时间环境激活的能力。
- 事件触发模式是指当某个事件发生时，智能合约将被激活，例如随着时间的推移通常的掉期，时间触发模式将完全支持此类应用。例如，捕获事件在自动交易和量化交易中至关重要。必须使用事件触发模式来启动此类事件。

目前，智能合约只能处理来自其区块链内部的信息，但是，在多个触发机制的情况下，一些触发信息将来自外部。因此，智能合约将提供外部信息输入接口，并使用不同的技术来验证链下数据的有效性和真实性。

为此，Lithosphere 将首先通过 HTTP 或袜子将外部数据传输到节点，具体取决于第三方数据源提供的通用 API。Lithosphere 将封装来自某些广泛使用的链下数据源的数据调用，其功能类似于为节点获取提供数据的系统调用。但是，节点可以使用上述数据收集路线创建其数据源以获取重要数据信息。

共识过程验证获取的链下数据的有效性。当节点发现链下数据与特定的智能合约触发情况相关联时，节点将运行并广播智能合约。如果恶意节点故意在全网广播智能合约，网络可以在执行阶段简单地终止智能合约，如果它被判断为恶意，因为智能合约在执行前会被其他诚实节点重新验证。此类恶意行为不会对智能合约的实际运行产生任何影响，也没有机会从不劳而获或套利的利润中获利。

激励方法还可以帮助解决链下数据输入有效性的问题。由于数据确认需要网络共识，节点只能通过追求更快更可信的数据源，准确验证触发情况，才能增加收益。由于有效市场和资源配置的性质，高效网络节点将得到奖励。最终数据的有效性不受少数流氓节点生成的数据的影响。

增强功能和兼容性

Lithosphere 的智能合约将基于以太坊等区块链智能合约进行升级和开发。将根据与现有智能合约的兼容性添加功能添加，例如触发机制。已经在以太坊和其他区块链上运行的智能合约将能够简单地转移到 Lithosphere，智能合约开发人员将能够在 Lithosphere 上快速创建。

下一步将是优化编程语言和虚拟机，以获得更健壮的应用程序开发环境，并为编码知识较少的开发人员提供更直观的应用程序开发工具和调试环境。

合同内附电话

上述对当前智能合约的改进，最终将让 Lithosphere 上的智能合约在时间和空间上根据各种条件、各种价值和参与者之间定义关系和交互规则，让 Lithosphere 上的智能合约构建 DeFi 应用程序。

在 Lithosphere 上，智能合约不仅可以更改帐户状态和数据，而且如果满足某些条件，它还可以在执行过程中调用另一个智能合约。

必须完成以下活动才能实现智能合约 A 对智能合约 B 的调用：

(1)创建一个封闭的调用智能合约。

在智能合约A的代码中添加调用智能合约B的预设条件判断和预设条件规则，生成目标智能合约地址索引参数。触发智能合约 A 时的数据输入，以及数据计算的结果，为条件判断提供了基础。如果满足预定义的条件，节点将下载并执行智能合约 B。

调用条件分为规则和时间两部分。规则是智能合约中的预编程计算例程。时间条件可以是智能合约中预先定义的在智能合约执行时触发的条件，也可以是定期检查智能合约状态的条件。

(2) 进行封闭呼叫的程序。

一世。当智能合约 A 被激活时，它会根据预设的调用情况判断是否需要执行智能合约 B。

ii.当满足调用情况时，调用预设的计算函数，并将结果作为智能合约B的输入。

三、执行智能合约A的节点将智能合约B下载到本地计算环境，将上一步确定的数据作为智能合约B的输入数据，开始执行智能合约B。

上述过程可用于执行智能合约 A 对合约 B 的调用。 我们将它们之间的逻辑链接称为智能合约的封闭调用，因为智能合约 B 以智能合约 A 的状态为触发器和输入数据.

智能合约不仅根据其业务逻辑做出决策，还可以根据预定义的标准调用其他智能合约。因此，在不同的智能合约之间创建类似网络的调用交互很简单，在连接的金融应用程序之间建立价值交互，从而允许创建复杂的应用程序。因此，复杂的金融服务，例如基于未来现金流的贷款申请，可能会使用封闭的智能合约调用来开发。由于这些特性和多触发机制，岩石圈平台可以实现复杂的金融活动，这将在多触发机制部分进行解释。

合约开发

要履行智能合约，需要完成以下步骤：

(1) 构建智能合约

岩石圈智能合约是当前智能合约的演变。合同应该有两个组成部分：定义和描述。

定义部分一致且符合以太坊智能合约。因此，当前的以太坊智能合约与岩石圈兼容。它包含合同状态、合同价值以及用于定义响应条件和规则的方法。

(2)发布智能合约

智能合约发布后，定义部分将记录在当前智能合约之后的区块链上。描述部分将与当前区块链中所有智能合约的触发条件合并，创建一个调用列表，该调用列表将被记录在区块中，并且可供全网访问。

调用列表中的每一行条目对应一个智能合约。除了描述中的材料外，每条记录都有一个索引地址，对应于存储的智能合约。

下一步将是优化编程语言和虚拟机，以获得更健壮的应用程序开发环境，并为编码知识较少的开发人员提供更直观的应用程序开发工具和调试环境。

时序和触发条件

主动触发器类似于以太坊中智能合约的激活方式，即通过转移到合约地址。以下步骤将用于创建新的时间触发模式和事件触发模式：

(1)通过节点判断触发条件

为了执行，调用列表被下载到本地节点。为了确定列表中的每个项目是否与触发条件匹配，节点将轮询列表并下载匹配或本地数据。

(2)触发智能合约

当记账节点在特定时间轮询时发现满足某个智能合约的条件时，该节点从调用列表中获取智能合约地址并发送特定交易以激活智能合约。同时，全网记账节点将下载所选交易的智能合约。

(3)执行智能合约

一个智能合约的执行方式与当前的智能合约相同，即在节点的运行环境（虚拟机）中执行。合约的不同之处在于它具有额外的触发条件，并且可能通过触发条件整合到其他合约中，从而导致发生连锁。

快速开发和接口

Lithosphere 将为智能合约和函数库提供开发环境。开发人员可以使用这些功能来加速智能合约的创建。为了更简单地访问和交互数据，开发环境将不同的区块链、智能合约、数据源等封装为接口。

下面是一些典型的接口：

(1)密钥管理

- 初始化密钥对、创建并返回公钥地址都是必须实现的功能。

- 输入公钥地址和关联签名后返回签名哈希值。

(2)区块链数据采集

如果将区块链视为允许分布式应用程序（DApp）的系统，那么收集区块链数据的智能合约将与获取区块链系统的全局变量相同。智能合约可以使用此接口访问区块链上的以下信息：

瞄准特定的块高度。发件人的信息。收件人的信息。

(3)智能合约的调用

智能合约用于实现岩石圈的所有功能。
转移智能合约的使用可用于在智能合约中进行转移。为了涵盖典型的金融应用，Lithosphere 将采用更基本的智能合约。因此，在 Lithosphere 上开发智能合约需要将简单的智能合约嵌入到传统的金融应用程序中，然后通过添加更复杂的功能来增强其功能。

Lithosphere 将识别基本的金融合约，从而产生一个供开发人员使用的智能合约库。

(4)链下数据源接口

在触发情况下，智能合约使用链下数据。此类数据通常是使用第三方提供的标准 HTTP 或基于袜子的 API 获取的。例如第三方接口调用函数会通过HTTP获取目的URL地址，并返回一个JSON包。

该接口方法还可以用于从其他区块链获取信息，例如查询和确认另一条链中的交易是否被其所在区块确认。

Lithosphere 将使用基金会来发现第三方接口并创建第三方接口供智能合约调用。

(5)快速发展

Lithosphere 将为常见应用提供多个智能合约模板，供应用开发者在项目早期参考和使用。但是，应用程序开发人员仍必须满足某些代码标准。

随着平台的底层功能和常见的金融基础应用程序变得更加丰富和复杂，应用程序开发人员可以通过创建前提条件来使用智能合约来实现所需的金融应用程序。. 为了进一步完善这样的开发环境，大幅降低开发者的开发门槛，Lithosphere 的计划包括可视化和模块化的应用开发工具、编译环境、应用测试环境，这将使智能合约开发者能够专注于金融应用的创新和Launchpad 来启动 dApp。

(6)编程语言和虚拟机

为了与智能合约的互操作性和现有智能合约的快速移植，Lithosphere 最初将采用以太坊的 Solidity 编程语言。未来我们会提供多种语言的编译器，以适应更多的智能合约开发语言。

我们将创建一个智能合约沙盒系统，使用浏览器或编程编辑器执行特定的故障安全检查和燃料成本最小化。

使用多个触发器实现复杂的金融功能

现有的智能合约只能被动地等待交易的触发被交易执行，这就提出了需要引入可信经纪人来确定谁有权在什么条件下触发智能合约的问题。在 Lithosphere 平台上，智能合约将通过代码（无论是普通智能合约还是封闭合约）来描述各方之间的关系。多个触发器将自动执行这些智能合约，允许它们一个接一个地参与，而无需人工交互。因此，多方可能会使用智能合约代码相互信任，以执行一系列复杂的金融活动。岩石圈智能合约提供独立规划所有权和使用权的能力，

由于此功能，智能合约现在可以执行广泛的金融活动。例如，如果您想借钱，您可以设计 Lithosphere 智能合约来借入代币、返还新币并支付利息。以 Lithosphere 平台为例，智能合约可以自主管理一个基金，包括将各种代币的使用权纳入智能合约、保管各种数字资产、产生管理费、支付股息等。以各种衍生品为例，智能合约可以使用外部数据源触发器获取保证金并执行修改保证金、清算和结算等操作。

社区运营方案

KaJ Labs 基金会作为该项目的主要赞助商，其目标是打造一个有前途的区块链生态系统，而不是像典型的企业和创业计划那样实现企业盈利能力。造福所有代币持有者的 Lithosphere 平台不归任何单个实体或个人所有。整个区块链代币社区拥有 Lithosphere 平台。Lithosphere 使令牌的使用更加灵活和可访问，并赋予令牌提供复杂 DeFi 服务的潜力。所有代币的价值都会增加。

实际上，价值互联网的跨链生态是一个浩大的工程。Kaj Labs 基金会要推进生态系统的发展，这个生态系统必须有全社区的加入和参与，其区块链必须通过不断的迭代来增强。这正是区块链项目的特点。区块链计划始于需要解决的关键需求或问题，参与者和有需要的人必须不断调查这些需求或问题，以鼓励持续进步。同时，它将吸引更多的人加入社区，从而促使需求将项目转向更好的方向并鼓励其技术进步。回声的目的是产生激励、应用和使用的正反馈循环。因此，

以下人员组成社区：

- 核心开发团队和 Kaj Labs 基金会。他们是项目平台的发起人和推动者。

希望成为项目一部分的程序员。如果他们对项目或项目技术感兴趣，他们可以加入基金会开发团队或作为第三方独立创建和优化岩石圈。

- 岩石圈中的参与节点 他们通过跟踪分类帐和操作智能合约同时维护岩石圈来赚钱。

- 岩石圈平台的用户。对于 DeFi 和其他服务，他们使用 Lithosphere 平台。 • 在 Lithosphere 平台上，DeFi 服务提供商，例如支付机构、中心化或去中心化交易所、借贷机构和其他金融服务提供商。

- Lithosphere 代币持有者，例如私募股权公司、早期投资者、后期投资者和潜在投资者。

- 其他参与岩石圈开发的各方，如媒体、政府等。
社区运营的目标是聚集尽可能多的力量，并以最有效的方式进行安排，以便岩石圈能够迭代、改进、影响和服务于更广泛的社区。

社区的发展与核心社区和外围社区密不可分。两者互惠互利，以核心社区为焦点。另一方面，外围社区必须继续参与关键社区的创建，因为核心社区将源自外围社区并借鉴外围社区，外围社区将需要核心社区的资源来支持它们。我们发现比特币、以太坊和其他项目都以同样的方式发展。核心社区包括早期采用者、区块链技术社区和区块链价值社区，而外围资源包括额外的投资者、用户、开发者、记者和其他利益相关方。

项目推广方式

- 该概念将社区运营分为两类：核心和外围。前者更喜欢离线模式，而后者更喜欢互联网模式。以下是关键社区运营的策略：

- 岩石圈基金会团队：团队将获得代币奖励。一个原因是为了补偿之前使用的资源，另一个是允许任何人成为股东，并期望他们在未来为岩石圈做出贡献。

- 区块链技术社区。

- 技术是区块链发展中最重要也是最困难的方面。我们将通过线上和线下的方式，发现和培养一批顶尖人才，利用创始团队的技术专长和社会资源，推动技术社区的发展。

- 区块链价值社区：利用区块链技术社区，我们可以组织与持有者的聚会，传播区块链知识，同时也促进与私人价值社区合作的机会。

推动区块链技术的运动

价值互联网目前存在可用性瓶颈，未来需要继续努力改进。价值互联网的用处与岩石圈项目密切相关。为了贡献区块链技术的实用性，我们将启动“区块链技术推广运动”。对于 Kaj Labs 基金会来说，这将是一个长期项目。

以技术沙龙、训练营和研讨会的形式，这一运动将继续积累技能和技术信息。我们将鼓励参与者提供内容，这些内容将在众多网站和媒体上发布。为了发展区块链技术社区，我们将提供每月培训课程，以招聘传统互联网员工和其他技术人员。

区块链技术推广运动将汇集包括大学、研究机构、企业、机构、政府和联盟在内的各方力量，建立合作伙伴关系，汇集资源，支持区块链技术的进步。

区块链接口运动的标准化

价值互联网具有需要多方解决的互操作性和可扩展性问题。岩石圈项目与这两个障碍的突破性发展和进步密不可分。通过建立“区块链接口标准化运动”，我们将帮助加强它们。对于岩石圈基金会来说，这将是一个长期项目。

该运动不仅会鼓励区块链之间的接口标准化，还会鼓励去中心化和中心化组织之间的接口标准化，以及区块链和外部数据源之间的接口标准化。

岩石圈应用

借贷

随着数字货币作为价值交换媒介和价值存储载体的重要性日益增加，使用数字货币创造新价值和赚取收入是不可避免的趋势。例如，比特币用于资助区块链矿业公司和其他加密计划。随着数字货币应用种类的增加，数字货币的直接投资选择也扩大了。

用数字货币创造价值的人更需要数字货币，而拥有数字货币的人想要升值，因此对数字货币的借贷需求将会上升。

考虑加密货币以太坊 (ETH)。在 Lithosphere 上，服务提供商创建存款应用程序并使用智能合约设置利率。

通过跨链交易，用户将以太坊区块链中的 ETH 发送到 Lithosphere 智能合约地址。Lithosphere 上的存款会生成一个凭证（看起来像存款银行收据的 Lithosphere 代币），记入用户的 Lithosphere 帐户。然后智能合约会为您计算利息。当用户想要提现时，将凭证发送到一个中间地址，进行跨链交易。在原链上，代金券对应的ETH被解锁，发回原用户账户。存款准备金（锁定在与中间地址对应的原始链上的资产）始终可见。

支付结算

企业越来越多地接受比特币等数字资产作为支付方式。未来将有更多应用程序使用一系列数字货币进行支付。目前有多种支付方式可供选择，包括 VISA、Paypal 和支付宝，每种都有自己的一套支付和结算程序。岩石圈是一个多币种分布式平台，它将许多银行分类账组合成一个统一的分类账。无需安装多个数字货币钱包，任何企业或用户都可以使用 Lithosphere 钱包进行多币种支付和结算。

交易和交换

目前，需要集中交易所和场外交易市场才能完成数字货币交易。每笔交易都取决于交易所和中介机构的信心。在多种货币与 Lithosphere 挂钩后，交易所和中介机构可能会使用智能合约来实现多货币拍卖交易和一对一的遏制交易。在 Lithosphere 上，隐私保护交易机制支持需要隐私保护的交易。将数字货币导入 Lithosphere，在 Lithosphere 上开始私人交易，以及将数字货币移回原始链，都可以通过 Lithosphere 实现。通过隐藏资金追踪路径，在一定程度上保护了原链的隐私。岩石圈可以处理 10,

1,700 TPS。Visa 平均每秒处理约 1,700 笔交易（根据官方声称的每天超过 1.5 亿笔交易的计算得出）。

投融资

传统机构越来越多地转向联盟链来存储商业发票、忠诚度积分、未来收益权和应收账款等资产。未来将有更多的金融资产记录在基于联盟链的分布式账本上。当这些财团链连接到 Lithosphere 时，它 们就成为金融资产提供者，投资者可以用他们的数字货币获得这些资产。这类似于在银行购买金融商品，就像在传统银行公司中一样。主要区别在于可以有更多的中介机构参与，资产所有者可以直接为自己融资。

在区块链世界中，初始代币发行（ICO）/初始交易发行（IEO）已成为一种流行的筹集资金的方式，并且这种做法正在扩展到非区块链领域。越来越多的项目将智能合约直接用于 ICO，尤其是那些建立在以太坊或 BSC 上的项目，这使得该过程更加开放和公平。然而，专门接受 Ether 的 ICO 会惹恼拥有其他数字货币的投资者。ICO 发行者可以使用 Lithosphere 创建一个支持多币种投资的智能合约。投资者可以更轻松地使用以太坊、比特币或任何其他与 Lithosphere 相关联的区块链代币进行投资，发行人可以更简单地管理他们的资金。此外，当新的区块链发布时，Lithosphere 跨链交易可用于将众筹股份转换为当地货币。有了 Lithosphere，我们正在进入一个基于区块链的数字版权发行新时代

更多应用

上述金融应用旨在帮助读者更好地掌握岩石圈的基本原理和价值。更多的例子包括基于数字货币的多币种信用卡、捆绑一系列资产的资产支持证券、基于数字货币的点对点借贷公司和众筹等。

主要银行将区块链技术视为一项基本战略，但他们也在研究如何利用它来改变传统业务。

银行业务，例如货币兑换，一直在数字货币领域蓬勃发展。在这些领域，区块链在两条平行的轨道上发展，但随着数字资产的出现和越来越多地融入实际经济，这两条轨道最终会交叉。银行资产负债表将在很大程度上转移到区块链上，数字资产将被纳入银行资产负债表（支持数字资产贷款和存款的银行）（法定货币由区块链代币表示和核算）。这种未来的整合将得到 Lithosphere 的分类账间技术的支持。

当前岩石圈特征

互操作性

通过去中心化托管模型 (MDKM) 实现跨链互操作

用于 NFT 的下一代区块链

一个可扩展的、去中心化的、跨链网络，旨在为每个人带来不可替代的代币。

时间锁定功能

岩石圈独特的时间锁定功能使您能够从数字资产中提取时间价值

安全

采用MDKM技术分布式管理和控制私钥

可扩展性

解决扩展问题对于比特币和以太坊 v1 等 PoW 区块链来说是一个悬而未决的问题。目前，比特币和以太坊节点处理每笔交易并存储所有状态。由于 Lithosphere 的股权证明可以比工作量证明更快地提交区块，因此由 Lithosphere 的共识支持并在桥接加密上运行的 EVM 区域可以为 PoWblockchains Ethereum、Litecoin 和比特币提供更高的性能。

数字资产

使用 Lithosphere 的 LEP100 协议创建、管理甚至出借您自己的数字资产和 NFT。

跨链游戏资产。

游戏经济，由玩家拥有。
创建永久可用的游戏内资产。在由 Litho 提供支持的 JOT ART 区块链上，让玩家将战利品带到另一款游戏或现实世界，从而为游戏玩家带来持久价值。

岩石圈产品

- Lithosphere 区块链 (PoS) Litho 跨链原生代币 LithoSwap - 支持 NFT
- 交换的跨链 DEX。LEP100 代币 Launchpad - Litho Launchpad
-
- Thanos 多币种、跨链钱包
- JOT NFT 平台（NFT 市场、NFT DEX、用于在任何地方经济高效地分发 NFT、跨链的 SDK） FLEEK - 区块链上的去中心化社
- 区支持的演出平台。
- LAX - 算法稳定币

岩石圈项目治理

理事会成员

被选为在两个主要治理角色中代表被动利益相关者：提议公投和否决危险或恶意的公投。岩石圈创建者乔尔・卡斯尔 (Joel Kasr) 担任理事会委员会主席。

技术委员会

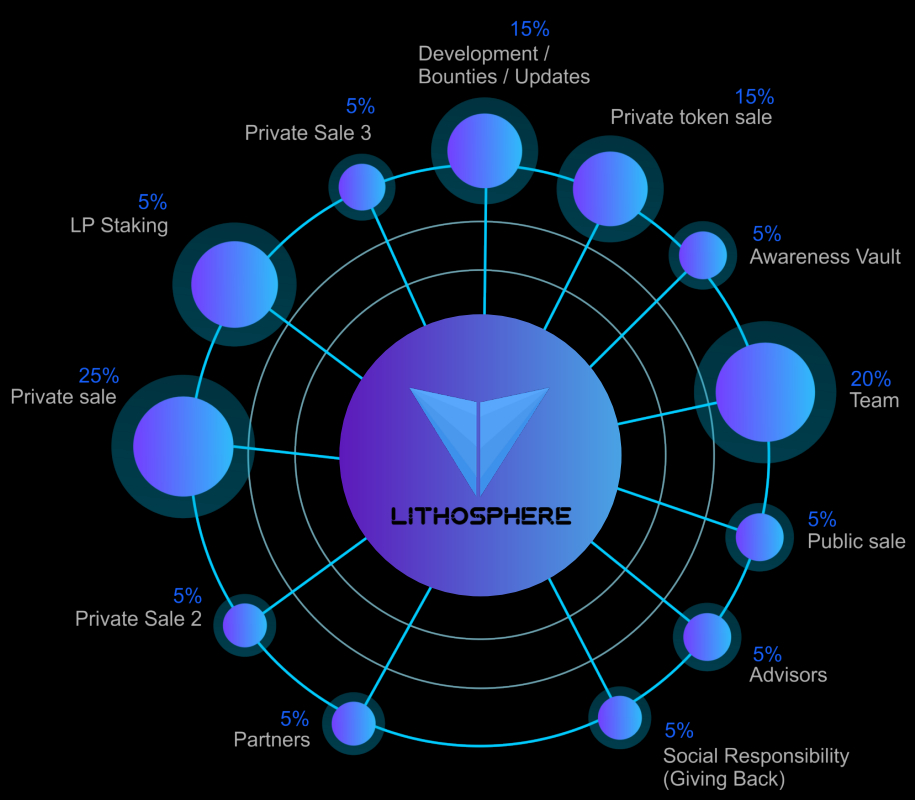
由积极构建 Litho 的核心团队组成。可以与理事会一起提出紧急公投，以进行快速投票和实施。

社区成员

可以就改善岩石圈的提案提出并投票。

代币经济学

总供应量



项目资金：

Kamet（岩石圈网络的第一个版本）上的石版币和验证器的初始分配将分配给岩石圈筹款活动的捐赠者（70%）、主要捐赠者（5%）、KaJ Labs 基金会（10%）、网络意识（ 10%) 和核心团队成员 (10%)。从Kamet 开始，每年Litho 总金额的1/3 将奖励给保税验证人和委托人。

岩石圈中的其中一个金库/胶囊将被设置为持有营销/意识基金。

路线图

2021 年第三季度

完成网络概念

核心开发
团队形成

石斑白
发表的论文

建立密钥
伙伴关系

主要公告

2021 年第四季度

NFT DEX 测试网

媒体存在

引入新令牌
标准 - LEP100

介绍
治理在
岩石圈网
使用原生 Litho
令牌。

Litho 代币预售

2022 年第一季度

推出 Jot NFT 平台
测试网

启动跨链
钱包 - Thanos 钱包

团队扩张

2022 年第二季度

Jot Art NFT 市场主网上线。

实施 DNN
光刻交换

岩石圈核心团队
增强。

建立 Litho
网络测试网

公共代币销售/IEO。

2022 年第三季度

实施 DNN
灭霸钱包。

JOT 代币私募

开始开发
去中心化社区驱动的区块链演出平台 - Fleek

发布 Jot Art SDK

启动 Litho Launchpad

发布区块链
JOT NFT平台上的手机游戏

LAX - 算法稳定币

结论

Lithosphere 项目创建了 BFT 算法、新的代币标准、Litho 货币（LITHO）和密钥分配机制，以实现包容性去中心化平台的目标。原生代币的设计主要由以下五个要素组成：

1.数字。总共有 10 亿个代币可用。这个数量将允许代币以可接受的价格推出，并从那里继续稳步增长。

2.一种用于分发代币的系统。为了实现不通胀的想法，应该限制代币的供应。这使早期成员受益，并使系统从长远来看更加稳定。

3.代币的分配。要实现去中心化的概念，必须适当平衡代币分配。我们授予 Lithosphere 团队 10% 的比例，因为他们不断致力于促进 Lithosphere 在跨链、跨组织和跨数据源计划中的包容性。此外，由于 Lithosphere 的记账节点比普通公链执行更复杂的功能，他们将获得总金额的三分之一左右。其余的将用于环保建筑。

4.环保施工。超过一半的资金将捐给基金会，以帮助项目蓬勃发展，尤其是在跨链、跨组织和跨数据的特性方面。为了在链上传递附加价值并帮助开发新的智能合约应用程序，该项目还需要一个代币交换机制。

5.燃料和矿工 在分布式节点控制系统中，一系列值将进入岩石圈。为了控制代币，链需要大量分散的节点。节点越多，链就越安全，随着链价值的增长，需要的节点也就越多。链必须通过释放代币和收取服务费来补偿矿工，以维持节点数量和算力。

岩石圈应运而生。从 KaJ Labs 成立之初，我们的开发团队就一直分布在世界各地，但我们始终无法有效地工作。我们必须提高我们的整个绩效和流程，以便我们的团队保持分布式。

在参与了众多区块链项目后，我们认识到现有的常用区块链（如以太坊、卡尔达诺等）存在一些效率低下的问题。最严重的问题是这些区块链网络无法连接。在 Lithosphere 之前，您无法使用 BEP20 代币、BTC、DOT 或 BNB 购买 ERC721 NFT。区块链网络必须彼此同步，区块链和 DeFi 才能成长为我们都想要的未来。交易费用/gas费用是以太坊等网络面临的另一个挑战。在以太坊网络上，几乎每项活动都需要花钱。KaJ Labs 团队着手创建一个全球区块链网络，该网络比 Cardano、Polkadot 和 Ethereum 2.0 等现有区块链更快、更便宜且更环保。岩石圈可以被认为是新旧区块链的基础。岩石圈生态系统由本地货币 $LITHO /Litho 提供支持。

免责声明

本岩石圈白皮书仅供参考。KaJ Labs 基金会不保证本白皮书的准确性或得出的结论，本白皮书“按原样”提供。KaJ Labs 基金会不做出并明确否认所有明示、暗示、法定或其他形式的陈述和保证，包括但不限于：(i) 本白皮书的内容没有错误；(ii) 此类内容不会侵犯第三方权利；(iii) 对特定用途、适用性或功能的适用性的保证。KaJ Labs Foundation 及其附属公司对因使用、参考或依赖本白皮书或此处包含的任何内容而导致的任何类型的损害不承担任何责任，即使被告知发生此类损害的可能性。在任何情况下，KaJ Labs 基金会或其附属机构均不对任何个人或实体承担任何类型的损害、损失、责任、成本或费用，无论是直接的或间接的、后果性的、补偿性的、附带的、实际的、惩戒性的、惩罚性的或特别适用于使用、参考或依赖本白皮书或其中包含的任何内容，包括但不限于任何业务损失、收入、利润、数据、使用、商誉或其他无形损失。

词汇表

LEP100： 岩石圈演化提议

白皮书： 关于特定主题及其周围问题的指南。它旨在教育读者并帮助他们理解和解决问题。

区块链： 越来越多的记录列表（称为块）使用密码学链接在一起。

代币： 代币代表一组智能合约中编码的一组规则。每个代币都属于一个区块链地址。它本质上是一种安全存储在区块链上的数字资产。

去中心化： 一种加密货币交换类型，允许直接点对点加密货币交换安全地在线进行，无需中介。

电动汽车： 以太坊虚拟机是一个计算引擎，它的作用就像一个拥有数百万个可执行项目的去中心化计算机。

计分卡： 币安智能链

挂钩硬币： 与外部资产挂钩的 LEP100 代币。

应用程序： 去中心化应用程序是在区块链或点对点计算机网络上运行的数字应用程序，而不是单台计算机。

NFT： 不可替代的代币是存储在称为区块链的数字分类账上的数据单元，用于证明数字资产，因此不可互换。

互操作性： 计算机系统或软件交换和利用信息的能力。

ERC： 以太坊征求意见

烧伤： 数字货币矿工和开发者可以从流通中移除代币或硬币的过程。

牵引力： 在企业中绘制或拉动率。

德菲： 去中心化金融

跨链： 它是两个相对独立的区块链之间的互操作性。

DEX： 去中心化交易所