

IoTeX2.0中文白皮书

IoTeX 2.0 - DePIN for everyone

1.1 版本

IoTeX 团队

摘要

去中心化物理基础设施网络（DePIN）目前是 Web3 中最热门的叙事之一，代表着一种主要的范式转变，可能在不久的将来根本改变物理基础设施网络的构建、运营和管理方式。由于缺乏资金和技术能力，新兴的 DePIN 初创企业在及时将其想法推向市场方面面临着重大挑战。在这份白皮书中，我们介绍了 IoTeX 2.0，这是 IoTeX 网络演进中的一个变革性步骤，旨在解决上述挑战，并帮助 DePIN 社区实现“**人人皆可 DePIN (DePIN for everyone)**”的终极愿景。

IoTeX 2.0 包含以下核心创新：

- 一种新的代币经济设计，广泛探索 IOTX 代币在模块化 DePIN 基础设施中的用途；
- 一种模块化的 DePIN 基础设施，允许 DePIN 初创企业在一个社区拥有的去中心化基础设施上构建他们的应用；
- 一个模块化安全池（MSP），通过重新质押为 DePIN 基础设施模块提供统一的可信层；
- 一个称为 W3bstream 的去中心化多证明者网络，允许 DePIN 构建者利用不同的有效性证明方法实现 DePIN 验证；
- 一个称为 ioID 的统一身份系统，在链上/链下管理和保护机器对机器和机器对人之间的关系；
- 一个称为 ioConnect 的通用嵌入式 SDK，支持设备抽象并促进智能设备在 DePIN 应用中的交互；
- 一个称为 ioDDK 的链 SDK，允许 DePIN 项目同时提供自主应用链并继承 IoTeX L1 的安全性。

目录

第一章 7

DePIN 的今天 5

- 1.1 为什么 DePIN 很重要 7
- 1.2 DePIN 的现状 8
- 1.3 DePIN 技术栈及其挑战 9
- 1.4 我们的 DePIN 哲学 13

第二章 IoTeX 2.0 16

- 2.1 引言 16
- 2.2 我们（未）构建的内容 19
- 2.3 代币经济学 22
- 2.3.1 IoTeX 2.0 中的 IOTX 实用程序 23

2.3.2 通胀质押奖励27

2.3.3 通货紧缩销毁28

2.3.4 增长激励29

2.4 公共产品31

2.5 在整个项目生命周期中支持建设者33

2.6 未来34

第三章 模块化安全池 (MSP) - DePIN 基础设施模块的统一可信层37

3.1 问题37

3.2 开放的安全和信任市场38

3.3 架构39

第四章 W3bstream - 用于 DePIN 验证的去中心化的多重验证网络42

4.1 W3bstream 架构42

4.1.1 四种类型的证明机制43

4.1.2 我们在 ZKP 方面的内部创新47

4.2 W3bstream 工作流程48

4.2.1 验证者加入和管理48

4.2.2 工作流程48

4.3 DePIN 验证和链下 AI 50

4.3.1 DePIN 验证 50

4.3.2 链下 AI 50

第五章 ioID - DePIN 的统一身份系统 52

5.1 链上与链下身份52

5.1.1 链上身份52

5.1.2 链下身份53

5.2 ioID 设计53

5.2.1 设备上的 ioID 生成54

5.2.2 设备上的 ioID 生成55

5.2.3 安全的机器间交互57

5.3 ioID 在 DePIN 项目中的集成57

5.3.1 ioID 的智能合约57

5.3.2 部署设备 NFT 合约58

5.3.3 注册 DePIN 项目58

5.3.4 设置设备 NFT 合约58

5.3.5 申请 ioID59

5.3.6 注册设备59

第六章 ioConnect - 一种抽象 DePIN 设备硬件复杂性的通用嵌入式 SDK 60

6.1 连接选项61

6.1.1 连接到中心化连接层61

6.1.2 连接到去中心化连接层62

6.2 设计通用嵌入式 SDK 的考虑因素63

6.2.1 Arm 的 PSA 认证加密API63

6.2.2 自主身份 (SSI) 64

6.3 实现规范65

6.3.1 ioConnect SDK 核心65

6.3.2 DePIN 设备兼容性66

第七章 ioDDK - 启用自主身份的 DePIN 应用链68

7.1 设计逻辑 68

7.2 共享区块空间和验证者 69

7.3 ioDDK 组件和高级工作流程72

7.3.1 ioDDK 组件72

7.3.2 高级工作流程72

7.4 区块空间租赁市场73

7.5 IoTEx L1 的影响74

第八章 新路线图76

第九章 结论 78

第一章

DePIN 的今天

IoTeX 成立于 2017 年，旨在通过将物联网（IoT）与区块链连接，赋予人们拥有和控制其智能设备及其产生的数据和价值的能力。我们的创立理论是，使用去中心化区块链来协调数十亿智能设备，可以解决现有物联网的主要问题，如信任、安全和主权，并能够让用户拥有的设备网络蓬勃发展。在过去的 6 年里，我们在探索和构建几个核心用例方面取得了开创性的进展：

- 微支付（2017-2018）：使用区块链作为全球数字结算层，促进设备、机器和人之间的自动化、低费率支付。区块链作为一个统一层，使以前不兼容的设备能够通信和交易。
- 溯源和供应链（2018-2020）：利用区块链作为无需信任的会计和所有权分类账，启用智能设备的溯源和去中心化供应链用例（例如，Pebble Tracker [1,2]）。区块链从可信设备收集数据以验证现实世界活动，并触发新的事件和工作流程。
- 数据所有权和隐私（2020-2021）：使用区块链作为去中心化身份层，使人们能够拥有和控制其设备和数据（例如，Ucam [3,6]），并结合了高级加密技术如端到端加密、多方计算和保密计算。与主要企业如 Arm [7,8] 合作开发的去中心化隐私解决方案。
- DePIN（2021-至今）：使用区块链作为去中心化物理基础设施网络（DePIN）的基础，这是一种新的资本形态和人类协作模式，使人们能够为现实世界基础设施网络做出贡献并获得资产权。DePIN 产生的数据和服务也可以为其它类型的项目所用，特别是人工智能（AI）和现实世界资产（RWA）。

2017 年发布的原始 IoTeX 白皮书[5]展示了我们对一个安全、可扩展、多功能和去中心化 Layer 1 的愿景，该愿景结合了隐私保护技术和面向设备的中间件，以连接物理和数字世界。多年来，我们实现了原始白皮书中设定的许多雄心勃勃的目标：

- IoTeX 主网处理了大约 1.2 亿笔交易，且没有任何停机或黑客事件；
- 设计和制造了首批兼容区块链的硬件设备（例如，Ucam、Pebble Tracker），作为开发者的开箱即用硬件开发工具包；
- 各种第三方智能设备已集成到 IoTeX 平台，为如何安全地将现实世界连接到区块链提供了基本概念；
- 在 IoTeX 上推出了整个 DePIN 项目生态系统，包含来自智能设备的现实世界数据；
- 创建了一个由网络验证者、开发者和用户组成的全球社区，这代表了 IoTeX 网络的生命线。

但这只是一个开始。自 2017 年以来，区块链领域呈指数级增长，我们现在对 DePIN 要达到大规模采用所需的条件有了更深的了解。在构建我们初始 IoTeX 愿景的同时，IoTeX 核心开发团队一直在研究和设计新的创新，以将 DePIN 提升到新的水平，例如零知识证明、链下扩展、设备的自主身份和推动整个 DePIN 发展的公共产品。我们在此介绍的 IoTeX 2.0 愿景概述了我们三年计划，以扩展 IoTeX 网络。我们旨在采用新的模块化平台设计，更新我们的代币经济等，以满足 DePIN 领域及更广泛范围内建设者的不断增长的需求。通过这个更新的愿景，我们最终可以实现“**人人皆可 DePIN（DePIN for everyone）**”这一终极目标。

1.1 为什么 DePIN 很重要

在深入探讨 IoTeX 2.0 和 DePIN 未来的愿景之前，我们想首先分享一下 DePIN 是什么以及为什么你应该关注它。今天，世界上许多最重要的行业和公共事业，如电信、能源和计算，都是由中心化公司、政府拥有和控制的垄断和寡头垄断。这些价值数万亿美元的行业在设计时就设定了极高的进入门槛，包括财务和物流；例如，AT&T 每年花费 240 亿美元，需要超过 160,000 名员工来运营他们的电信帝国。由于这些高不可及的准入门槛，人们每天只能选择少数几个商品和服务“提供商”。这意味着竞争有限，创新受到抑制，消费者不得不忍受低于标准的客户服务和过高的价格，因为他们别无选择。在为数百万客户提供服务的同时，企业巨头们还偷偷地从客户那里获取敏感和有价值的数据，以谋取自己的利润。由此产生的问题在新兴市场国家更加突出，进一步加深了贫富差距，限制了普通人的机会。

DePIN 是一个革命性的概念，它将改变现状。建立在开源、去中心化区块链上的 DePIN 可以为服务全球数十亿人的物理基础设施和公共事业带来透明度、信任和创新，而且成本低廉甚至免费。但修复当今世界只是 DePIN 真正潜力的一小部分。真正的机会不是简单地修补当前世界的问题，而是建立一个由普通人拥有、运营和使用的公用事业的新世界。DePIN 将使任何人都可以为现实世界的基础设施网络做出贡献并建立公平性，克服上述的金融和物流准入壁垒。通过利用去中心化金融（DeFi）所推广的新型资本形成方法众包网络资源，DePIN 可以聚合用户贡献的硬件、人力和专业知识，以推动新基础设施网络的建设，并为对这些贡献者提供生态激励。最终，DePIN 可以利用区块链上不可变的智能合约来验证和协调贡献者的行为，以实现对网络的最佳利益。

DePIN 不仅提供了改善当前世界的道路，也提供了设计更美好世界的机会。我们正处于新工业革命的边缘，数十年历史的基础设施，如化石燃料和有线互联网，将被创新的基础设施，如可再生能源和无线取代。有了 DePIN，每个人都可以成为我们全球基础设施现代化的贡献者，并获得这些基础设施所代表的数万亿美元价值的公平份额。一个由人民创造、为人民服务的新世界——这是 DePIN 的承诺。DePIN，属于我们每个人！

1.2 DePIN 的现状

DePIN 是全球数百个项目的共同努力，旨在实现物理基础设施的去中心化和改进。

虽然 DePIN 一词是在 2023 年才提出，但这一概念早已活跃，自 2017 年以来，IoTeX、Helium 和 Filecoin 等项目一直是该领域的先驱。如今，DePIN 格局多种多样，包括构建 DePIN 特定基础设施的项目以及跨多个垂直领域的 DePIN 应用程序。DePIN 现在是区块链最有前途的用例之一，可以细分为物理资源网络和数字资源网络，它们由网络提供的服务类型指定。物理资源网络产生不可替代的资源（即来自任何设备的数据/服务都是唯一的），这些资源本质上更具像化，通常依赖于位置相关的硬件。另一方面，数字资源网络为可替代资源（即 1GB 的存储空间就是 1GB 的存储空间）提供了市场，这些资源本质上更加虚拟，并且依赖于与位置无关的硬件。DePIN 分类还包括促进该类别增长并为 DePIN 应用程序提供现成功能的基础设施和工具。图 1.1 显示了全面的 DePIN 格局。



APR 2024 Decentralized Physical Infrastructure Network

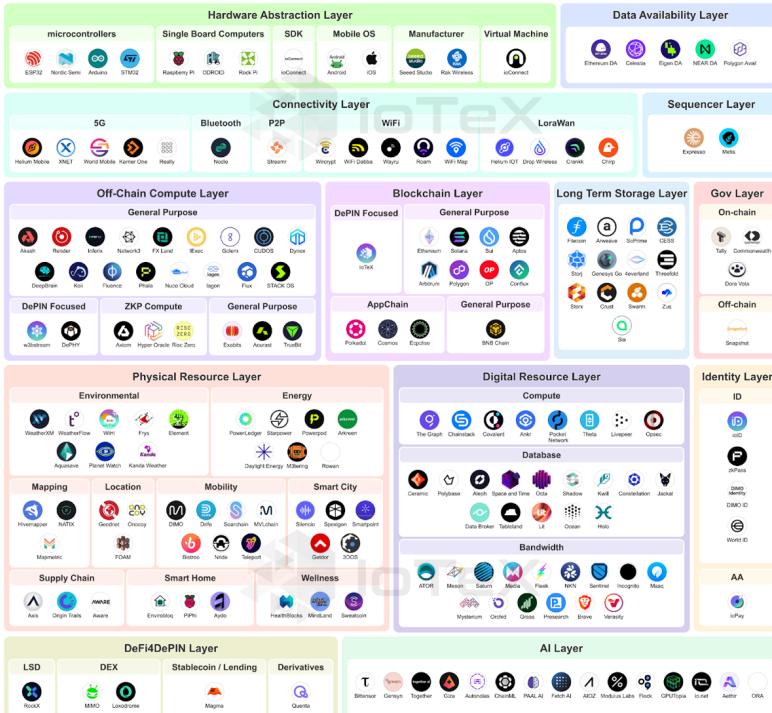


图 1.1: DePIN 全景图

1.3 DePIN 技术栈及其挑战

无论 DePIN 专注于物理资源还是数字资源，也无论他们瞄准哪个特定的垂直领域，都需要一个将现实世界与区块链世界连接起来的端到端技术堆栈。不同于促进 NFT 等数字资产和稳定币等金融资产交换的区块链用例，DePIN 必须与产生大量数据的现实世界智能设备交互。区块链作为一种不可变的账本，是记录现实世界中发生的事情的完美基础；然而，在将“现实世界活动的证明”从设备永久写入区块链之前，必须完成一系列步骤来验证现实世界的活动是否确实发生以及数据是否可信。设备必须在链上注册，必须收集、解析和存储原始数据，并且必须以可验证的方式对数据进行计算，然后才能将任何“现实世界活动的证明”结算到区块链上。参考架构 [9]

如图 1.2 所示，介绍了 DePIN 项目需要考虑的九个基本技术层。

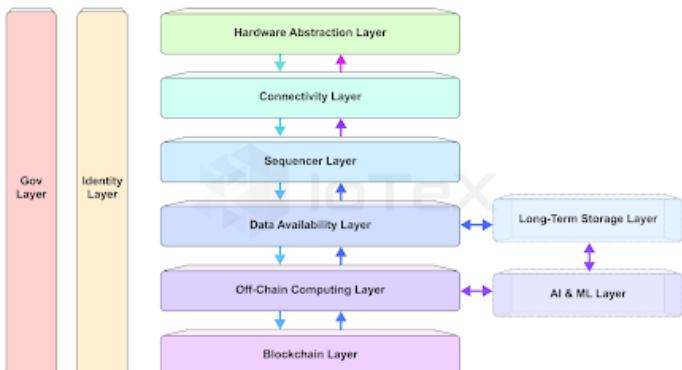


图 1.2: DePIN 技术堆栈

- 硬件抽象层：促进不同规模、型号的智能设备安全地与连接层中的实体连接；
- 连接层：将智能设备生成的数据可靠地中继到序列层；
- 序列层：在将智能设备的数据包发送到数据可用性层之前对其进行排序；
- 数据可用性层：临时存储数据以供立即使用，与链下计算层共享对数据的访问权限，以从原始数据中生成见解；
- 长期存储层：存档供将来使用的原始数据和见解，第三方可以通过 API 访问这些数据以实现合规性、分析、AI 支持等；
- 链下计算层：将业务逻辑应用于存储在数据可用性层中的数据，以生成与现实世界活动相关的见解和证明；
- 区块链层：充当设备身份和数据的信任锚，验证链下计算的有效性并向 DePIN 利益相关者分发通证奖励；
- 身份层：管理所有相关实体（例如智能设备、用户、服务器、制造商、验证器）的链上和/或链下身份；
- 治理层：以去中心化的方式执行网络政策和程序（例如激励措施），通常通过社区投票流程。

DePIN 技术堆栈的大量扩展层对于单个团队来说可能难以以整体方式进行开发。这种复杂性为建设者在 DePIN 中尝试创新想法设置了很高的进入门槛。在过去几年中，资金充足的项目通过筹集大量风险资本并开发自己的整体技术堆栈克服了这些挑战。然而，要让 DePIN 真正蓬勃发展并覆盖世界每个角落（如拉丁美洲、非洲和东南亚），庞大的技术堆栈和高技术复杂性带来了额外的挑战：

- 发布速度：由于硬件限制和前期资本支出要求，DePIN 达到最低供应门槛以推动初始需求的速度有限；
- 需求侧增长：由于启动供应的漫长历程以及难以在用户体验、可靠性和成本方面与现有解决方案相提并论，DePIN 难以建立需求；
- 代币流动性：DePIN 使用通证激励来推动网络增长和资助基础设施运营，但在经济飞轮的持续性和建立链上流动性方面却举步维艰；
- 认知度：DePIN 通常专注于特定行业，其中项目的目的和成功指标并不总是显而易见，尤其是对于那些尚未直接参与该行业的人来说。

由于这些挑战，DePIN 仍处于起步阶段，在市场价值和采用方面尚未超越 DeFi 和其他加密行业。DeFi 和 DePIN 在许多方面都很相似，最显著的是它们都以人们（“供应方”）众包资源来创造其他人想要和使用的产品（“需求方”）。然而，DeFi 和 DePIN 之间获取和维持供需的途径截然不同。从高层次来看，DeFi 的供需更容易引导但持续性较弱，而 DePIN 的供需更难引导但更能经受住时间的考验。此外，DePIN 通常必须聚集大量资源来创造初始需求，而 DeFi 不同，少量聚集的资金可能会有即时需求。将 DePIN 和 DeFi 与上述挑战并排比较，我们可以看到以下详细区别，如图 1.3 所示。

	DeFi	DePIN	Challenges for DePIN	Partial Solutions
Tech Stack	Simple and digital-only: e.g., Solidity + JS mostly, easy to fork-to-launch	Complicated and touches the physical world: C/C++ + Golang/Python/Rust + Solidity + JS + optional Swift, hard to fork.	Challenge 1: DePIN projects are harder to build and require more capital to launch due to their hardware component. Launch is slow and expensive.	<ul style="list-style-type: none"> Launch projects in a centralized way to "test" the market and speed decision-making The lack of decentralization and trustlessness may dissuade contributors and investors
Launch Velocity	Fast: e.g., launch dApp globally; a few "miners" with large capital set up the supply-side quickly	Slow: e.g., ship and deploy project-specific hardware, threshold-scale of supply at which the network can serve demand may be high	Challenge 2: DePIN projects are slow to launch (establish the supply side) due to their hardware constraints, which can create a mismatch with crypto cycles.	<ul style="list-style-type: none"> Working with an existing Web2 partner, e.g., T-Mobile, to reach threshold-scale faster Does not apply to innovative DePIN networks where a Web2 partner does not exist
Demand-side Growth	Easy to attract users if designed properly, e.g., yield farming, but usually short-lasting	Slow to bootstrap, e.g., onboarding cellular plan customers, but can be more impactful over the long-term	Challenge 3: Crypto can provide an unnecessarily complex UX, slowing demand-side adoption	<ul style="list-style-type: none"> Using tokens to incentivize everyday people to adopt and use a DePIN Most people are not crypto-native and don't understand tokens, wallets, etc.
Token Liquidity	Token liquidity is easy to acquire and a natural by-product of a financial application	Token liquidity is often difficult to achieve because founders and contributors have more hardware and Web2 experience than financial experience	Challenge 4: Token liquidity is important for any crypto project, but especially for DePINs that power network growth with token incentives	<ul style="list-style-type: none"> DePIN teams can work with CEXes and market makers to attain token liquidity This can be an expensive and lengthy process
Sharing network growth	Metrica for success are clear e.g., TVL, and easy to pull and display	Metrica for success are project-specific and must be pulled from physical devices	Challenge 5: DePIN teams must spend valuable time and effort building dashboards to display their project metrics	<ul style="list-style-type: none"> On-chain data can be somewhat easily pulled and displayed with tools like Dune However many DePINs start quite centralized and don't have much on-chain data to show

图1.3：关于DePIN和DeFi的特性对比

1.4 我们的 DePIN 哲学

我们坚信 DePIN 应该像 DeFi 一样不断发展，适合每个人：每个建设者、每个贡献者和每个用户。这一信念强调：

- 开放的小团队应该能够构建有影响力的 DePIN 产品，为当地社区和地区服务。
- DePIN 项目应该快速迭代，无需高昂的前期成本即可识别真正的创新。
- DePIN 下的项目应该在功能（例如，为个人汇总来自戒指、汽车、电话的数据）和区域（例如 Uber 的城市模型）方面都是可组合的。
- 为网络提供价值或效用的贡献者应该具有较低的准入门槛，并以稳定、长期的方式获得经济回报。
- 用户应该能够以最低成本或完全免费享受这些 DePIN 网络中的公共和创新效用。

这种信念不仅仅是一厢情愿的想法。它可以实际转化为一种技术设计，称为 IoTeX 2.0，如下所示。

第二章

IoTeX 2.0

2.1 引言

IoTeX 2.0 定义了 IoTeX 网络未来几年的宏大愿景和路线图，扩展了我们使命——为每个人实现“人人皆可 DePIN (DePIN for everyone)”——这是基于我们多年来作为 DePIN 行业先驱的经验。我们的目标不仅是解决当前 DePIN 项目面临的技术和非技术挑战，还要通过使 IoTeX 成为全球最大的 DePIN 生态系统来实现 DePIN 的全部潜力。为了实现这一目标，我们很高兴推出 IoTeX 2.0，结合了新的哲学、

技术、代币经济、公共产品和倡议，以使普通人能够参与和建设 DePIN，并赋予建设者真正将现实世界与区块链世界桥接的能力。

通过 IoTeX 2.0，IoTeX 网络将从仅仅是一个 L1 区块链演变为开放的 DePIN 基础设施，Dapp 和 L2 将通过 IOTX 代币锚定。这将大大增加 IoTeX 网络的参与者和贡献者的数量和类型，从而最终推动 IoTeX 和 DePIN 到新的发展阶段。DePIN 应该是为所有构建的，这就是为什么 IoTeX 2.0 优先考虑在生命周期的每个阶段都包括建设者和用户。无论您是希望扩展到自己的 L2 链的已建立的 Dapp，还是寻求实施基于 DePIN 的业务模型的传统公司，或者只是一个有着伟大想法的小团队，IoTeX 2.0 都提供了适用于所有 DePIN 建设者的完整解决方案。

我们的核心方法论是模块化基础设施：DePIN 项目可以通过选择一系列技术模块来构建适合其特定阶段和要求的技术堆栈。这些提供包括由 IoTeX 核心开发团队构建的内部产品和来自顶级合作伙伴的产品。我们的模块化方案集成了先进的技术，例如链下扩展、零知识证明和人工智能，为 DePIN 行业带来独特的创新。这些模块不仅由 IoTeX 核心开发团队构建，还由专门的基础设施建设者利用 IoTeX 网络进行构建，以确保其安全性和可信。这种方法为最大的 DePIN 团队提供了全面的解决方案，同时为较小的团队提供了专门构建的解决方案，以便他们可以快速而安全地创建新的 DePIN 项目。

从架构的角度来看，IoTeX 2.0 突出了以下几个视角（见图2.1）：

- 模块化安全池（MSP）：模块化的基础是一个统一的、可信任的层，由 IoTeX 和其他主流资产支持，我们称之为 MSP。这些是部署在 IoTeX L1 上的一组智能合约。IoTeX L1 和 MSP 共同作为 DePIN 基础设施模块（DIM）层和 Dapp/L2 层内所有活动的信任锚和不可更改的账本。广义上讲，MSP 允许 IoTeX L1 将其权益证明安全性贷给跨越 DePIN 技术堆栈各部分的 DIM。DIM 提供者将抵押 IOTX 和其他主流资产加入 MSP。此外，从 MSP 获取安全性和信任的 DIM 将定期将其状态锚定到 IoTeX L1，为 DApp 构建者基于可信的实际活动创新开辟可能性。
- DePIN 基础设施模块（DIM）：IoTeX 2.0 中新增的 DIM 层提供了一组模块化功能，涵盖整个 DePIN 技术堆栈。除了 IoTeX 核心开发团队提供的内部实现外，额外的 DIM 如 AI 推理、存储、隐私保护计算、数据分析、RPC 和域名系统将由合作伙伴和开发者提供，他们将向 MSP 抵押 IOTX。每个 DIM 如有必要可拥有自己的代币。
- 公共产品：IoTeX 的目标是将 DePIN 引入全新的阶段，这需要任何人都能信任并自由使用的公共产品。我们的目标是通过创建一套开源资源来引领 DePIN 运动，这些资源能够帮开发者无缝集成，并供给他们的用户以驱动开放参与。这些公共产品包括用户界面工具（例如浏览器、钱包、桥接器）、面向开发者的工具（例如集成开发环境），以及网络范围的资源（例如治理、资金）。
- 评价机制的经济学：IoTeX 网络新增层次将带来新的利益相关者，他们将跨不同领域贡献专业知识。我们刷新的经济模型目标不仅在于扩展 IOTX 代币的实用性，而是通过评价机制的方式，根据利益相关者的贡献重要性分配奖励。IoTeX 网络的扩展范围将为 IOTX 代币带来新的实用性，使其成为 DePIN 领域的基础货币。
- DePIN Dapp 和 DePIN L2：技术堆栈顶层将是一个基于 IoTeX 2.0 DIM 的生态系统，这些 Dapp 和 L2 能够利用 IoTeX L1 上的原生代币并利用所有 DIM 提供的功能。尽管许多 Dapp 选择在 IoTeX L1 上启动其原生代币并利用所有 DIM 提供的功能，但有些 Dapp 可能只选择利用一个或多个 DIM。IoTeX 2.0 的模块化重点使得 Dapp 能够根据其当前状态需求利用不同模块，同时为未来需求提供新的能力。

此外，DIM 层的一个新组件是ioDDK，这是一个 L2 链 SDK，使项目能够在 IoTeX L1 之上启动他们自己的 L2。这将使 DePIN 能够创建自己的主权代币经济体并托管自己的 Dapp，同时受益于 DIM 层的广泛能力，并从 IoTeX L1 获得安全性和信任。

2.2 我们（未）构建的内容

如第 1.3 节所述，构建 DePIN 需要多层次的技术堆栈（见图 2.2），包括了非常多的不同实用性。新引入的IoTeX 2.0 新引入的 DIM 层为这些技术堆栈中的每个元素提供了解决方案。该 DIM 层是完全开放的，任何基础设施构建者都可以实现。这为 DePIN 项目提供了大量创建自定义技术栈的选择。

除了 IoTeX 内部开发的核心模块外，还将从区块链领域的领先项目中获得大量模块建设支持，这些模块具有各自专业的能力。例如，数据可用性层是 Celestia 和 NEX 等项目的主要关注点，而长期存储层则是Filecoin 和 Arweave 等项目的核心重点。由于 IoTeX 2.0 强调模块化和可组合性，我们邀请所有项目整合到 DIM 层。因此，DePIN 项目可以根据自己的偏好设计技术堆栈。

虽然我们公开欢迎提供 DIM 层的任何部分，但 IoTeX 的核心开发为几个关键模块研究并开发了最先进的解决方案，这些模块主要集中在 DIM 的统一可信层、硬件、身份识别、离链计算、L2 SDK 和公共产品。我们将在下文中总结这些内容，并在接下来的章节中详细探讨。

- MSP (DIM 统一可信层)：这是 IoTeX L1 上由一组智能合约组成的统一可信层。它接收质押的 IOTX 和其他主流资产，并将其安全性出租给其他 DIM。
 - W3bstream (链下计算 DIM)：世界上第一个利用可验证计算技术的去中心化链下计算网络，例如零知识证明 (ZKP)、全同态加密 (FHE)、可信执行环境 (TEE) 和多方计算 (MPC)，供不同供应商（包括我们自己）实时生成“现实世界活动的证明”，并将这些证明结算到区块链以奖励设备所有者。
-

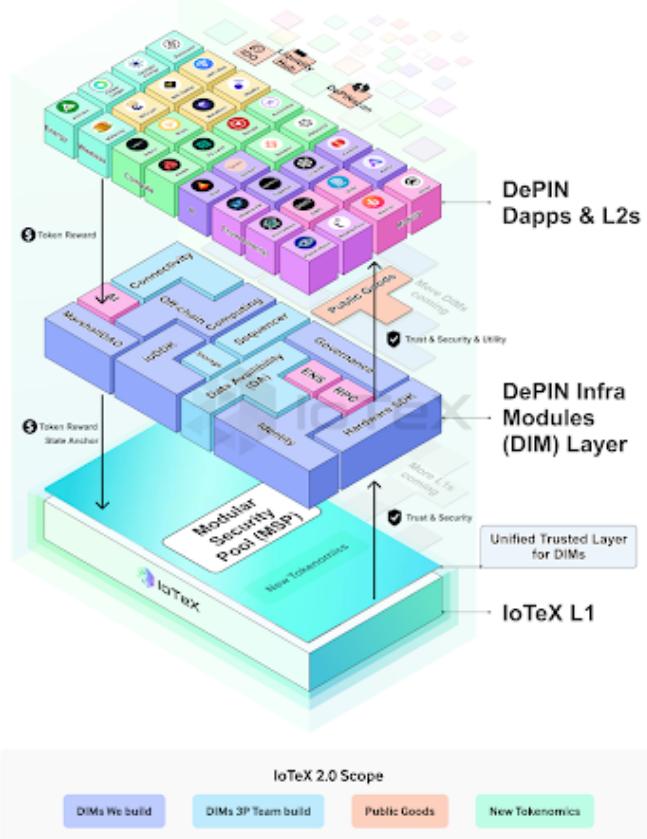


图 2.1: IoTeX 2.0 的整体视角

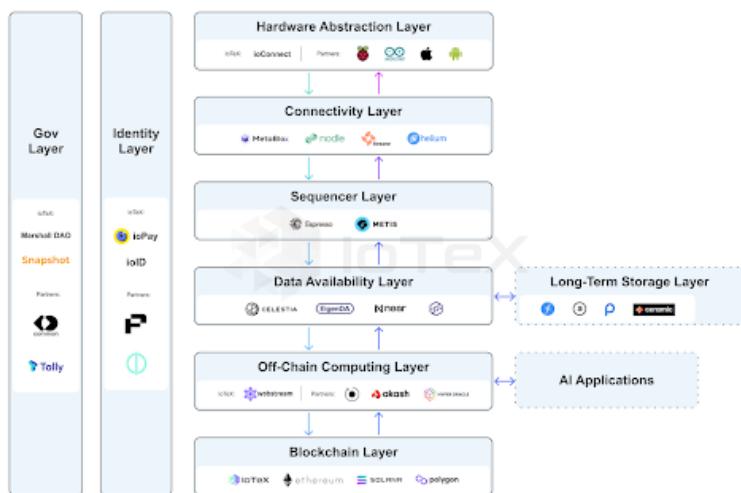


图 2.2: DePIN 基础设施模块 (DIM)

- **ioID (Identity DIM)**：一套链上和链下的自主主权数字身份，使人和机器能够建立丰富的数字关系并相互交互，而无需依赖中心化身份提供者。

- ioConnect（硬件抽象DIM）：一种 SDK，使各种硬件能够与 W3bstream 和各种 L1/L2 连接。它充当硬件抽象层，可在 Raspberry Pi、ESP32 和 Arduino 等主流硬件平台上无缝运行，简化处理硬件的复杂性。换句话说，由 ioConnect 提供支持的设备可以轻松集成到各种 DePIN 应用程序中，充当多重矿工。
- ioDDK（L2 SDK DIM）：一种链 SDK，使 DePIN 构建者能够无缝启动自己的主权区块链，同时享受 IoTeX L1 的安全性。它原生支持 IoTeX 模块，例如 W3bstream、ioID 和 DePINscan。
- IoTeX L1：IoTeX L1 区块链与 EVM 兼容，并运行我们内部的 Roll-DPoS 共识机制，以实现 1,000+ TPS。IoTeX L1 的范围和实用性将在 IoTeX 2.0 中得到扩展：ioID 将注册到 IoTeX L1，MSP 将作为智能合约部署在 IoTeX L1 上，ioDDK 将把 L2 链锚定到 IoTeX L1。
- 公共产品：我们将继续发展我们现有的公共产品，例如 DePINScan [23] 和 DePIN Liquidity Hub [21]，并为 DePIN 构建者构建公共产品

2.3 代币经济学

IOTX 代币于 2019 年推出，作为 IoTeX L1 的基础货币。自主网推出以来，IOTX 代币有效地平衡了验证者（或“代表”）、Dapp 构建者和用户之间的激励措施。作为网络共识的一部分，质押 IOTX 并验证区块链交易的代表将获得 IOTX 奖励，而由 Dapp、代币持有者等组成的开发者和用户则向 IOTX 支付费用以发送交易并与智能合约交互。各种类型的代币持有者也在质押 IOTX 代币以参与全网治理。

随着 IoTeX 从简单的 L1 扩展到互联基础设施的模块化平台，与 IOTX 代币相关的代币经济学也将得到扩展以适应我们对 IoTeX 2.0 的愿景。这包括 IOTX 代币的新形式的实用性，这些实用性将被纳入 IoTeX 2.0 的新技术产品中。此外，IoTeX 2.0 代币经济学的另一个重要目标是平衡通胀质押奖励、基于平台使用情况的通货紧缩销毁代币，并激励 DePIN Dapps 和 L2 使用我们的模块化基础设施。这意味着我们升级后的代币经济学不仅会通过将 IOTX 代币链接到 W3bstream、ioID、ioDDK 和其他 DIM 为其带来新的效用和价值，而且还会通过平衡通胀和通货紧缩机制来维持稳定的代币供应。随着 IoTeX 模块化基础设施产品的采用率不断提高，IOTX 代币将作为 IoTeX 2.0 网络的货币积累新的价值。

2.3.1 IoTeX 2.0 中的 IOTX 实用程序

IOTX 代币将在整个 IoTeX 2.0 基础设施和生态系统中使用，可以从不同角度查看，如图 2.3 和 2.4 所示。

- 从 IoTeX L1 角度来看：节点将质押 IOTX 以获得验证网络交易和参与共识的资格，并将获得 IOTX 代币作为其服务的奖励。代币持有者还可以质押 IOTX 来投票给节点并获得 IOTX 奖励。IOTX 代币将继续作为 IoTeX 2.0 中 IoTeX L1 区块链的原生代币，其中想要在 IoTeX L1 区块链上部署智能合约和处理交易的 Dapps 将使用 IOTX 作为 gas 费用。除了质押 IOTX 参与治理之外，用户还可以使用 IOTX 作为 gas 费来处理 IoTeX L1 上的交易，并通过贡献资本和资源与 Dapps 互动以获得奖励。在 IoTeX 2.0 中，设备所有者还可以销毁 IOTX，将其设备注册到 IoTeX L1 并接收 ioID，从而为参与 DePIN 提供可信的锚点。最后，为了创建飞轮，IoTeX L1 将采用 DAO 治理，代币持有者可以投票决定如何将网络激励分配给各种计划，旨在为新设备、DePIN、Dapps 和用户提供动力。加入的设备、DePIN、Dapps 和用户越多，IOTX 在 IoTeX L1 上通过销毁、质押和使用 IOTX 的效用就越大。

The DePIN Flywheel

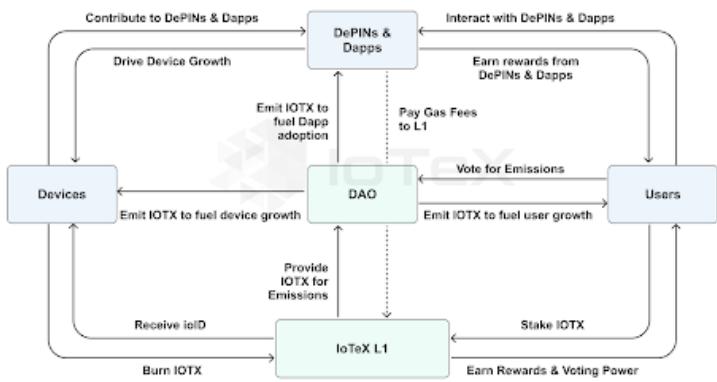


图 2.3: DePIN 飞轮和 IOTX 代币的效用

- 从模块化安全池 (MSP) 角度来看：IoTeX 2.0 将使用户能够通过将其质押或再质押到模块化安全池 (MSP) 来重新利用其质押的 IOTX，该池旨在将 IoTeX L1 区块链的安全性扩展到将其产品集成到 IoTeX 2.0 的 DIM。使用 MSP，DIM 构建者可以激励 IOTX 质押者分配其再质押的 IOTX 来为他们的解决方案提供安全性。这引入了一种结合质押 IOTX 的新经济，其中 MSP 将有效地将安全性和信任“租赁”给 DIM，而 DIM 将是质押 IOTX 所必需的。这也为 IOTX 质押者提供了新的受益机会，他们将获得基本 IOTX 质押奖励以及额外的奖励用于再质押其质押的 IOTX 代币，以及来自 DIM 项目的潜在贿赂。

MSP & DIMs

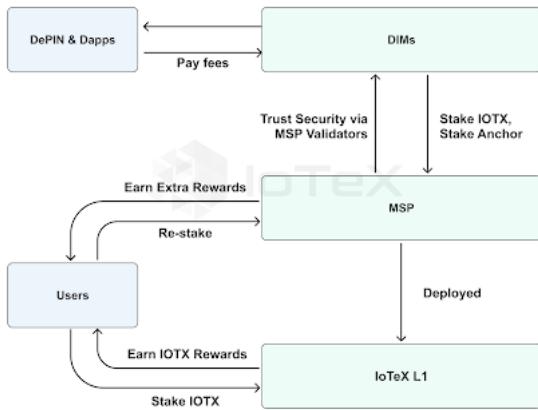


图 2.4: IOTX 代币在 MSP 和 DIM 中的效用

- 从 DePIN 基础设施模块 (DIM) 的角度来看：DIM 需要质押 IOTX 才能加入模块化安全池 (MSP)，从而在再质押的资产池中获得安全性，并以可验证的方式向 Dapp、L2 和用户提供服务。DIM 还可以选择使用 IOTX 作为利用其服务的 Dapp 的付款，或者他们可以使用自己的代币。例如，像 Filecoin 这样的长期存储提供商或像 NEAR 这样的数据可用性提供商会质押 IOTX 以 DIM 的身份加入 IoTeX 2.0，之后他们可以用自己的代币向 Dapp 收取数据服务费用。对于 IoTeX 团队内部构建的几个 IoTeX 2.0 DIM，例如 ioID 和 ioConnect，这些服务的付款将以 IOTX 代币计价。
- 从 DePIN Dapps 和 DePIN L2s 的角度来看：在 IoTeX 2.0 技术栈上启动的 Dapps 和 L2s 将向 IOTX 支付费用以处理交易并与智能合约交互。此外，Dapps 和 L2 链可以选择自己的模块化技术栈，并使

用 DIM 的代币向一个或多个 DIM 支付服务费用，例如连接、数据存储、链下计算等。为了完成这个循环，大多数 Dapps 都有自己的代币，用户可以获取这些代币并使用这些代币来访问 Dapps 服务。

除了上述 IOTX 代币的实用性之外，IoTeX 2.0 还采用了新的设计，包括如何根据基础设施使用情况销毁 IOTX 代币、如何通过激励计划与 Dapps 和构建者共享 IOTX，以及如何向质押者发放新的 IOTX，如图 2.5 所示。我们将在以下小节中探讨这些新设计。

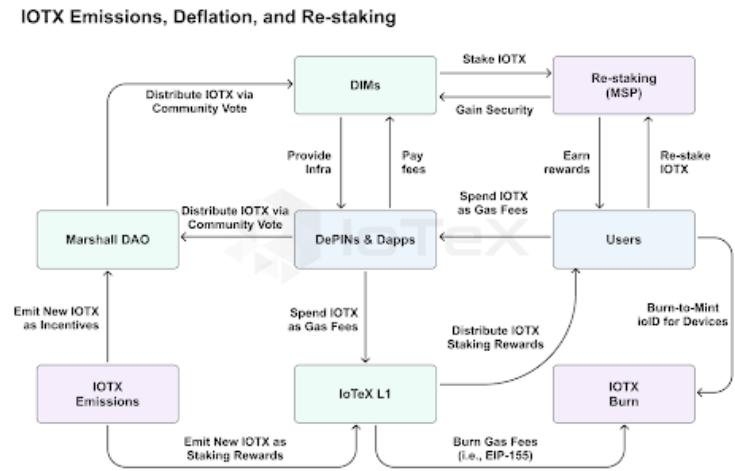


图 2.5：IoTeX 2.0 中 IOTX 代币的发行、通缩和再质押

2.3.2 通胀质押奖励

2019 年 IoTeX 主网启动时，IOTX 总供应量的 12%（即 12 亿 IOTX）被分配给节点质押奖励。代币持有者质押 IOTX 以投票给节点，节点与其选民分享部分质押奖励。自 2019 年以来，每年约有 2 亿 IOTX 以区块奖励和 epoch 奖励的形式分发给节点和选民。每生成一个新区块，就会向共识节点（即有资格生成区块的前 36 名投票节点）提供区块奖励，而 epoch 奖励则在每个 epoch（即每小时）按比例分配给前 100 名投票节点。在主网上线 4 年多后，最初分配给质押奖励的 IOTX 供应量已接近完全分配。因此，通胀质押奖励将作为 IoTeX 2.0 的一部分引入，以激励节点继续验证网络交易并保护网络。

通胀质押奖励指的是将新 IOTX 添加到代币供应中，并交付给参与共识的节点和质押 IOTX 的代币持有者。本质上，这意味着只有那些质押 IOTX 代币的人才能收到新铸造的 IOTX 代币，从而提高 IOTX 的质押率并提高 IoTeX 网络整体的安全性。通胀质押奖励的分配将遵循与之前分配给质押奖励的 IOTX 分配相同的结构，其中产生区块的共识节点将获得区块奖励，前 100 名节点将按比例分配区块奖励。

虽然这对于 IoTeX 网络来说是一个新概念，但几乎所有 L1 都内置了通胀质押奖励，包括以太坊、Solana、Cosmos 等。例如，Solana 最初的通胀率为 8%，每年降低 15%；截至 2024 年第一季度，Solana 网络的通胀率为约 5.5%。虽然 IoTeX 网络的实际年度通胀百分比将由全网治理决定，但目标是引入温和的通胀，为 IoTeX L1 节点提供与其他区块链生态系统相比具有竞争力的质押奖励 APR，并激励 DIM 和 DePIN 应用程序增长，同时在考虑通缩销毁代币时保持稳定的代币供应，这将在下面的部分中详细介绍。

2.3.3 通货紧缩销毁

为了平衡加密网络中必要的通货膨胀，通常会实施基于网络使用情况的通货紧缩销毁代币，以维持稳定的代币供应（销毁和铸造平衡就是这样一种设计模式）。例如，以太坊网络每天向验证者发行约

1,700 个新的 ETH，但通过通货紧缩销毁 gas 费（即 EIP-1559）来平衡这种通货膨胀，以保持整体稳定或通货紧缩的 ETH 代币供应。自 2020 年以来，IoTeX 网络利用 Burn-Drop 计划根据注册到网络的新设备数量来推动 IOTX 的通货紧缩销毁，迄今为止已销毁了约 4% 的总供应量或 4 亿 IOTX。随着 IoTeX 2.0 的推出和 Burn-Drop 计划的结束，根据我们模块化基础设施的使用情况，在协议级别将向 IoTeX 网络添加新的通货紧缩销毁来源。

- 在 L1，IoTeX 2.0 将引入类似于以太坊 EIP-1559 的 gas 费用销毁。这将根据 IoTeX L1 的使用增加来激励和重新分配 IOTX 代币持有者的价值。质押 IOTX 参与治理和投票给节点的操作将保持不变，质押资产将继续在减少 IOTX 代币流通速度方面发挥作用。
- 对于 ioID，为设备创建新的链上身份将需要销毁一定数量的 IOTX，其中销毁率将根据注册到 IoTeX 网络的设备总数而动态变化。此外，ioID 的设计将包含一个额外的通货紧缩销毁机制，以获得 DID 的可验证凭证 (VC)。打个比方，ioID 类似于空护照，而 VC 类似于护照上的印章，使人们能够进入各个国家。

在 IoTeX 2.0 中，ioID 将注册到 IoTeX L1，并且将通过销毁 IOTX 代币来访问 W3bstream 等 DIM，从而获得一个或多个设备的 VC。此设计将根据 IoTeX 网络中“部署”设备数量的增长，将价值重新分配给 IOTX 代币持有者，类似于 Burn-Drop，但经过重新设计，以更好地与 IoTeX 2.0 的模块化设计保持一致。

- 对于 W3bstream、ioConnect 和 ioDDK，由于设备需要与各个 DIM 直接交互，Dapps 和公司对这些模块化产品的增长和采用所推动的网络效应将推动 IOTX 的通货紧缩销毁。此外，可能会根据 IoTeX 社区定义的采用阈值定期销毁 IOTX 代币，以将价值重新分配给代币持有者。

IoTeX 2.0 代币经济学旨在通过推动 IOTX 代币的通货紧缩销毁来奖励 IoTeX 平台各种模块化组件的增加使用。最初，这种通货紧缩销毁将抵消上述通胀质押奖励，以保持净稳定的总代币供应量，并且在未来 IoTeX 平台的大规模采用时可以推动总 IOTX 代币供应量实现净通货紧缩。为了推动实现这一目标所需的大规模采用，IoTeX 2.0 代币经济学将通过下面描述的增长激励计划将 IOTX 代币分配给各种建设者。

2.3.4 增长激励

IoTeX 2.0 的一个重要支柱是 Marshall DAO (IIP-23) [10]，这是一个去中心化自治组织 (DAO)，它将使 IoTeX 利益相关者能够就如何分配 IOTX 激励来发展 IoTeX 生态系统提出建议，包括加入信誉良好的 DePIN 项目和资助全网计划。这创造了一个透明的、精英化的系统，确保最好的创新得到 IOTX 的资助。Marshall DAO 最初将由 5 亿多 IOTX 资助，这些 IOTX 是从 Burn-Drop 分配中重新利用的，这是 IoTeX 社区在 2024 年第一季度通过全网投票决定的。未来，可能会通过进一步的全网投票为 Marshall DAO 增加额外资金，以将新铸造的 IOTX 添加到池中。

如图 2.6 所示，Marshall DAO 采用投票托管链上治理模式，这意味着在 DAO 中质押的 IOTX 越多，用户的投票权就越大。这确保了资助项目和计划的决策是由那些对 IoTeX 的长期成功支持最多的人做出的。质押至少 91 天的代币持有者将获得 velOTX，这是一种不可转让的链上代币，可用于通过节点特定提案的指标来提案和投票决定资金分配。这意味着长期质押者可以使用他们的 velOTX 投票来决定 DAO 中的 IOTX 如何资助各种项目，包括但不限于提高 IoTeX 上 DEX 交易对的流动性、通过

Launchpad赞助早期 DePIN 项目、通过双重挖矿加速 DePIN 项目、为公共产品和网络范围的工具发放补助金等等。

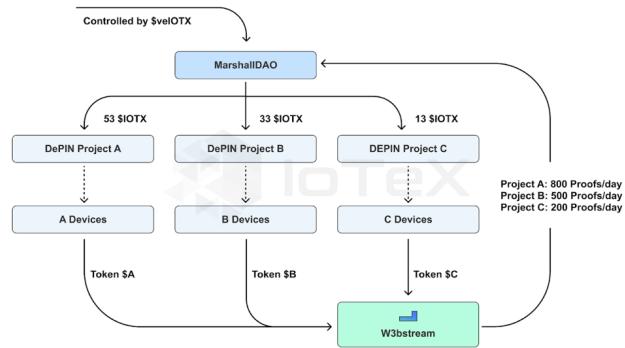


图 2.6: Marshall DAO 治理模型

2.4 公共产品

除了 IoTeX 区块链和 DIM 提供的功能外，解决 DePIN 项目许多近期和中期挑战的公共产品也是 IoTeX 2.0 的重要组成部分。这些公共产品通过简单的集成成为 DePIN 项目提供知名度、可用性和流动性，并为 IoTeX 社区提供了一种监控更广泛的 DePIN 行业以及深入研究特定项目的方法。

- DePINScan [23] 是 DePIN 领域的行业探索者（见图 2.7）。它旨在使 DePIN 的用户、矿工和投资者能够监控 DePIN 项目的增长并发现早期项目。它提供实时设备数量和项目简介，作为发现项目和获取 DePIN 资产的实时价格、数量和市值的一种方式。

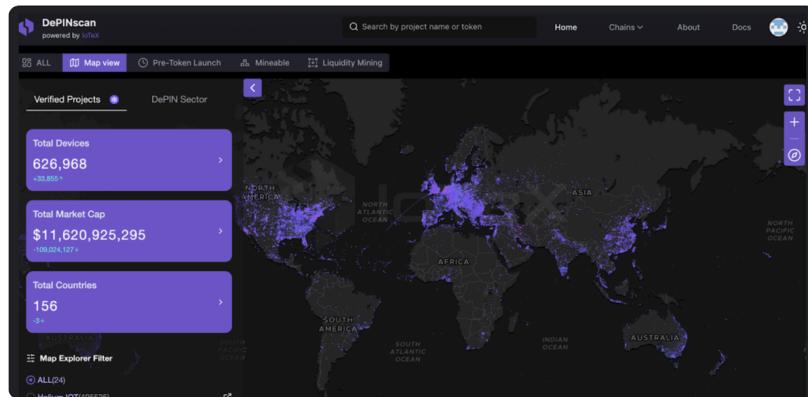


图 2.7: DePINScan Explorer

- DePIN 流动性中心 [21] 是一个用于交易 DePIN 代币的 DEX（见图 2.8）。代币流动性对于任何加密项目都非常重要，尤其是 DePIN，因为他们大量使用代币作为激励机制来发展他们的网络。不幸的是，许多早期的 DePIN 都难以创造和维持健康的链上流动性水平。为了支持新项目，IoTeX 推出了 DePIN 流动性中心 [24]，以增加 DePIN 项目的代币流动性，这些项目可以将其代币从任何其他 L1 链桥接到 IoTeX L1，在各种去中心化交易所 (DEX) 上创建双边流动性池，并开展流动性挖矿活动，以激励投资者引导他们的链上流动性。

Name	Symbol	Liquidity ↓	Volume (24hrs)	Price	Price Change (24hrs)
1 Wrapped IOTX	WITX	\$13,948,780	\$95,531	\$0.0463	+4.34%
2 WEN	WEN	\$1,473,287	\$5,274	\$1.03	+2.86%
3 DIMO	DIMO	\$146,790	\$1,812	\$0.47	+4.00%
4 WiFi Map	WIFI	\$6,501	\$3,569	\$0.13	+24.59%
5 Geodnet	GEOD	\$39,699	\$5,038	\$0.0953	-1.88%
6 Wicrypt Network...	WNT	\$35,731	\$1,005	\$0.31	+1.52%
7 CRUST	CRU	\$20,337	\$0	\$1.59	+4.34%
8 Drop Wireless I...	DWIN	\$19,132	\$142.07	\$0.0722	+7.81%
9 XNet Mobile	XNET	\$18,363	\$302.29	\$0.0366	-2.77%
10 DRFE	DRF	\$12,050	\$1,229	\$0.0024	-3.81%

图 2.8: DePIN 流动性中心

除了上述已经可供建设者使用的公共产品外，还有其他产品将由 IoTeX 团队以及全球建设者在 IoTeX 2.0 的整个开发过程中构建。这些示例包括 DePIN 项目的 launchpad，用于将其项目带给热情的投资者，设备市场用于向矿工展示以 DePIN 为中心的硬件，以及治理工具用于为 DePIN 项目实现去中心化投票。有了可供建设者随时使用的公共产品，IoTeX 2.0 将为项目提供全套功能，使启动和发展 DePIN 项目变得比以往任何时候都更加容易。

2.5 在整个项目生命周期中支持建设者

IoTeX 2.0 提供全方位的基础设施、工具和公共资源，所有这些都由精英代币经济学管理。这些旨在帮助 DePIN 建设者在其项目生命周期的每个阶段，如图 2.9 所示。

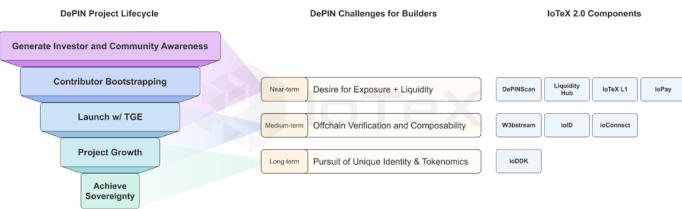


图 2.9: 在整个 DePIN 项目生命周期中支持建设者

- 在初始阶段，DePIN 项目主要专注于开发他们的技术堆栈并提高其项目的知名度。为了促进这一点，IoTeX 2.0 提供了 DePINscan 和 Liquidity Hub 等公共资源来吸引注意力、流动性和用户。
- 随着项目的进展，对更先进、适应性更强的基础设施的需求也在增加，尤其是当项目分散其技术堆栈并追求更高的可扩展性时。为了满足这些需求，IoTeX 2.0 提供了 W3bstream、ioID 和 ioConnect 等基础设施，为 DePIN 构建者提供尖端技术。
- 从长远来看，DePIN 项目需要建立和扩展自己的主权供需网络。IoTeX 2.0 继续支持这些项目，即使在后期阶段，也允许他们通过 ioDDK 启动自己的 L2。

2.6 未来

借助 IoTeX 2.0，我们将踏上新的征程，为全球设备配备实现自主控制所需的所有工具，汇编现实世界的智能以支持创新的 Dapp，并允许用户从其设备中获利。人工智能、区块链和智能设备的持续融合正

在引发一场技术革命，这场革命将从根本上改变我们世界的运作方式。尽管这些技术随着时间的推移而独立发展，但它们正变得越来越交织在一起，并打包成一种新的生产资产：由可信的和用户拥有的设备组成的 DePIN 网络。

智能设备将提供服务并生成数据。区块链将为这些数据和服务增加信任和可验证性。最后，人工智能将从数据中提取价值并自动化这些服务。几年前看似科幻的东西现在正在成为现实。在不久的将来，新兴的机器经济将由这种技术三位一体驱动，成为世界上最有价值的行业。借助区块链，我们将能够使用值得信赖的技术对这种新的机器经济进行编程，这不仅有益于社会，而且还为普通人提供价值和公平。可能性是无穷无尽的，但其中一些最令人兴奋的机会是：

- 集体智慧和人工智能：IoTeX 将成为最大的设备中心，从而成为聚合实时信息的真实世界数据中心。通过从设备捕获数据流并在链上验证真实世界事件，我们可以众包大众的集体智慧，以彻底改变连接、智慧城市和可再生能源等个别行业。更大的机会在于利用人工智能来分析跨行业关系并提取关联洞察，从而发展我们对世界的理解。IoTeX 2.0 将成为一个去中心化的平台，通过我们的智能设备的眼睛记录现实世界的历史，使我们能够了解我们的过去，从而优化我们的未来。
- 自主机器经济：除了生成有价值的数据外，智能设备现在还在不断发展，为人们提供值得信赖和有价值的服务。自动驾驶出租车正在提供首批无人驾驶服务，卫星正在为世界各地的人们提供连接，仓库正在使用比人类更灵活的机器人，下一代可再生能源设备正在生产太阳能和风能。这些服务提供设备的编排最好的方案是通过区块链和智能人工智能来实现。我们设想未来 IoTeX 可以让人工智能系统以前所未有的精度和完全信任的方式监控和管理地球资源。
- 数字资源市场：虽然一些 DePIN 专注于来自定位相关硬件的数据和服务，但其他 DePIN 则从与定位无关的硬件中聚合数字资源。这些可能包括数字存储、通过 CPU 和 GPU 计算、带宽以及传统上由云集团提供的其他数字资源。在“数据是新黄金”和“计算是新石油”的时代，IoTeX 2.0 将使有价值的数字资源能够众包到市场中，任何人都可以以点对点的方式与世界各地的其他人进行交换。
- 去中心化治理与决策：通过将现实世界数据安全透明地集成到区块链中，IoTeX 2.0 可以帮助利用现实世界事件的可验证事实为去中心化决策奠定基础。通过去中心化治理，人类共同定义流程，我们可以利用不可变的智能合约和安全设备以可信的方式运营社会的主要方面。IoTeX 2.0 为任何人提供了贡献专业知识并参与新世界开放治理的途径。

第 3 章

模块化安全池 (MSP) - DePIN 基础设施模块的统一可信层

3.1 问题

DePIN 具有复杂的技术堆栈，包括链上组件（例如场景特定的 DePIN L2）和链下组件（例如数据流、流程、存储和自动化）。这不可避免地意味着需要更多的模块和构建者从头开始建立自己的去中心化信任架构。这些任务可能涉及设计质押代币、创造流动性、吸引质押者、招募验证者和获得市场采用。这导致安全性和去中心化的碎片化。

为了以去中心化的方式建立端到端和统一的信任，至关重要的是确保每个部分尽可能安全和去中心化，这是木桶原理所体现的。因此，在全球构建者不断开发 DIM 的同时，我们必须确保安全性和去中心化既不受到损害也不分散。这样，DIM 就可以迅速集成到现有的技术堆栈中并被 DePIN 项目使用。

模块化安全池 (MSP) 是一个统一的可信层，支持 DePIN 基础设施模块 (DIM)。它从各种已建立的 L1/L2 收集质押安全性，并可能将其安全性借出以换取新 DIM 的补偿。这种方法允许新的基础设施模块利用底层 L1/L2 的安全性，而无需从头开始创建自己的安全基础设施。例如，新的 DIM 可以通过治理提案加入 MSP。如果获得批准，DIM 将继承 L1/L2 的安全性和去中心化。通过将质押指向 MSP 来支持某个 DIM 的质押者可能会获得 DIM 网络代币的补偿。

3.2 开放的安全和信任市场

MSP 自信地提出了一种开放的市场机制，巧妙地管理了质押者和 DIM 对其集合安全的供应和消费。MSP 将在所有 DIM 中整合以 DePIN 为中心的安全性，而不是在众多 DIM 之间分散安全性。具体来说，MSP 中有三种类型的参与者：

- **DIM 构建者**构建 DIM，例如场景特定的 DePIN L2、链下服务，例如数据流、进程处理（如通用进程、基于 ZKP、基于 TEE 等）、数据存储、自动化（如自动支付、价格反馈）以及身份和身份验证模块。DIM 构建者必须激励质押者将其资产分配给他们的模块。MSP 将提供贿赂机制，以确保质押者从 DIM 获得足够的激励。
- **质押者**是网络参与者，他们将资产从完善的区块链委托给一个或多个验证者。他们为网络安全做出贡献，而无需自己运行节点。作为委托的回报，他们将获得网络费用和奖励的一部分。战略分配决定了值得额外池子安全性的模块，并考虑到更多削减的潜力。Stakers 选择允许 MSP 对其资产施加额外的削减条件，从而增强经济安全性。

需要注意的是，我们正在构建的 MSP 基础设施是开源的，将能够利用所有主要区块链的安全性，包括比特币、以太坊和 IoTeX。虽然这个想法还处于早期阶段，但我们可以与 Eigenlayer 或 Babylon 等协议合作，以促进这种跨链互操作性。

- **验证者**为 DIM 构建者提供了一组始终运行的节点，这些节点将直接为 DePIN 项目提供服务。

MSP 的实施应纳入以下关键原则：

- **开放进入和退出：**Stakers 和 DIM 应该可以自由进入和离开市场，而不受任何限制。这确保了有竞争力的定价，反映了服务的真正价值。
- **网络效应：**随着参与者数量的增加，每个参与者都发现市场更有价值。这种正反馈循环可以吸引更多买家和卖家进入市场。
- **去中心化：**市场不受中央权威机构控制。相反，它根据供求规律运作。

3.3 架构

如图 3.1 所示，模块化安全池 (MSP) 的架构旨在为构建新网络（特别是 DePIN 和 DIM）提供简化且安全的流程，该流程基于从成熟的 L1 区块链上的现有质押系统继承的安全性。以下是 MSP 运作方式的详细细分：

1. 质押者委托资产：质押者是比特币、以太坊和 IoTeX 等成熟 L1 的参与者，他们将资产委托给 MSP。通过这样做，他们为 MSP 驱动的网络的安全性做出了贡献。

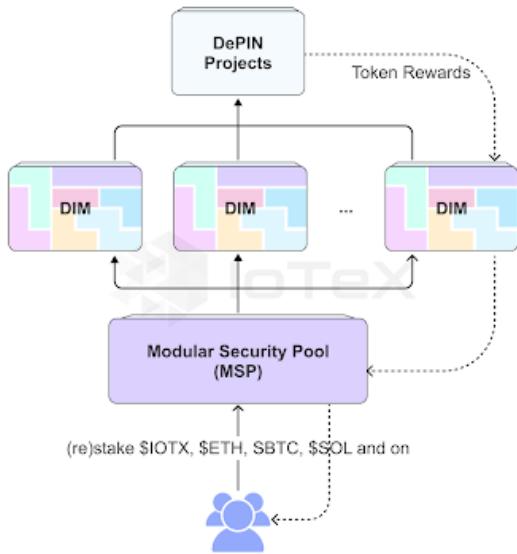


图 3.1：模块化安全池 (MSP) 的架构

2. 质押者有者选择验证者：在 MSP 网络中，质押者可以灵活地从他们所关联的 DIM 网络提供的选项池中选择验证者。验证者负责运行节点以保护网络并验证交易。
 3. 验证者运行节点：一旦被质押者选中，验证者就会在 MSP 网络中运行节点。这些节点在确保整个网络交易的完整性和安全性方面发挥着至关重要的作用。
 4. DIM 构建者建立网络：与此同时，DIM 构建者致力于开发各自的网络。
 5. 激励质押者：DIM 构建者激励质押者将其资产分配给 MSP 网络中的模块。这种激励可以采取多种形式，例如奖励、网络代币或其他福利。MSP 通过贿赂机制等机制确保质押者有足够的积极性来鼓励参与。
 6. 权益质押安全性的分配：MSP 在向新 DIM 分配权益质押安全性方面发挥着关键作用。通过利用从现有 L1/L2 收集的池化安全性以及质押者和验证者的参与，MSP 为这些新网络的安全性和去中心化提供服务。
- 总体而言，这种架构有助于更高效、更安全地启动新 DIM。通过利用现有 L1/L2 的安全性并整合质押者、验证者和构建者等各种利益相关者，MSP 培育了一个强大的生态系统，有利于去中心化信任架构的创新和增长。这种方法不仅为新网络开发人员节省了时间和资源，还增强了 DePIN 生态系统的整体安全性和弹性。

第 4 章

W3bstream - 用于 DePIN 验证的去中心化的多重验证网络

DePIN 应用程序通常包含专用的数据处理场景（例如，计算分数、定位设备、检测欺诈设备等），该场景能够根据 DePIN 设备从现实世界收集的数据提取见解。然后，这些见解用于触发与代币相关的操作的智能合约。由于机器数据量巨大，在链上处理和存储数据是令人望而却步且效率低下的。因此，链下计算已成为解决 DePIN 可扩展性挑战的有希望的解决方案。

4.1 W3bstream 架构

W3bstream 是由 IoTex 开发的区块链协调多重验证网络，旨在利用全球规模异构证明机制的力量来增强新兴的 DePIN 应用程序。简而言之，W3bstream 是一个去中心化的链下计算网络，由执行可验证计算的异构节点组成，如图 4.1 所示。W3bstream 生成的证明通过链上验证器进行验证，然后由 DePIN dApp 使用。

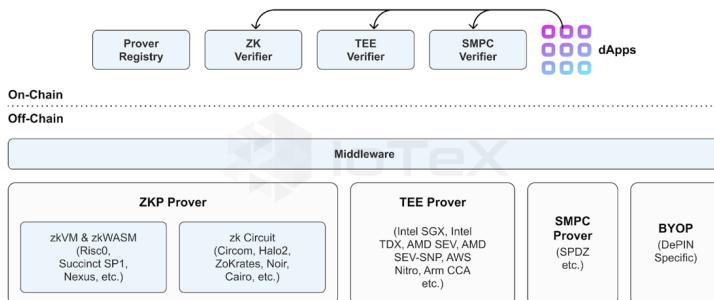


图4.1：Web3stream概览

4.1.1 四种类型的证明机制

过去已经开发了许多技术来证明数据处理的完整性并允许公开验证，包括零知识证明 (ZKP)、可信执行环境 (TEE)、安全多方计算 (SMPC)。这些技术依赖于各种安全假设，在实践中具有不同的含义。

W3bstream 能够通过精心设计的中间件层容纳四类证明机制来实现 DePIN 应用的可验证计算，即零知识证明 (ZKP) 证明、可信执行环境 (TEE) 证明、安全多方计算 (SMPC) 证明机制和自带证明 (BYOP)。

- ZKP 证明机制：ZKP 允许一方（即验证者）向另一方（即验证者）证明给定的陈述是真实的，而不会泄露除了该陈述是真实的事之外的其他信息。ZKP 需要满足完整性、健全性和零知识的正式要求，从而使我们能够构建无需信任的应用程序。实际上，ZKP 证明机制可以使用通用零知识虚拟机 (zkVM) 或定制约束系统（即电路）来实现。基于 zkVM（或定制电路）构建的基于 SNARK 的应用程序的典型系统架构如图 4.2 和 4.3 所示。

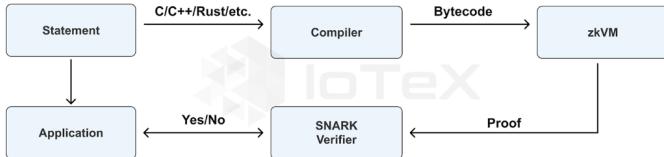


图 4.2：基于 zkVM 构建的基于 SNARK 的应用程序的系统架构

虽然基于 zkVM 的通用证明机制封装了生成 ZKP 的复杂性，并允许开发人员使用 C/C++、Rust 等高级编程语言编写其业务逻辑，但构建具有定制电路的 ZKP 证明机制需要更深入地了解 ZKP 生成工作流程以及领域特定语言 (DSL)。然而，与基于 zkVM 的证明机制相比，具有定制电路的 ZKP 证明机制通常可以实现更好的性能。ZKP 证明机制使 DePIN 开发人员能够利用强大的 ZKP 技术进行无需信任的链下计算。W3bstream 将逐步支持领先的 zkVM/zkWASM 项目（例如 Risc0 [28]、Succinct SP1 [29]、Nexus [30]、zkWASM [31] 等）以及流行的 DSL（例如 Circom [32]、Halo2 [33]、ZoKrates [34]、Noir [35]、Cairo [36] 等）以构建定制的 zk 电路。

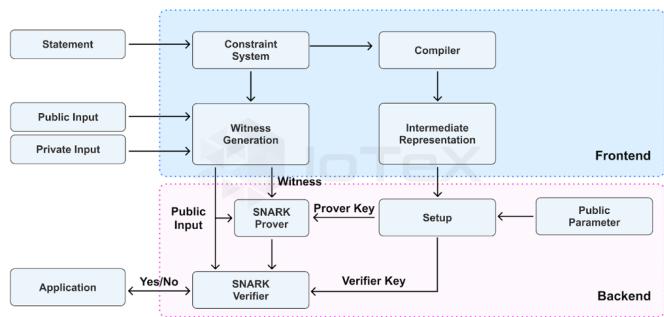


图 4.3：基于定制电路构建的基于 SNARK 的应用程序的系统架构

- TEE 证明机制：根据机密计算联盟 (CCC) 的定义，可信执行环境 (TEE) 是一个专用的硬件（和软件）环境，可提供以下三个属性的一定程度的保证：1) 数据机密性：未经授权的实体无法在 TEE 中使用数据时查看数据；2) 数据完整性：未经授权的实体无法在 TEE 中使用数据时添加、删除或更改数据；3) 代码完整性：未经授权的实体无法添加、删除或更改在 TEE 中执行的代码。这些显著的安全属性确保了数据和程序的机密性和完整性，从而允许远程方信任支持 TEE 的硬件平台（例如 Intel SGX、AMD-SEV、Arm CCA、AWS Nitro、NVIDIA H100 等）上的计算结果。基于 TEE 的系统将其安全性植根于硬件，用户必须相信硬件没有被篡改或以不可检测的方式被破坏。

基于 TEE 的应用程序的典型系统架构如图 4.4 所示，它依赖于基于 TEE 的硬件平台的远程认证机制。远程认证是一个过程，通过该过程，一方（即验证者）评估可能不受信任的远程对等方（即验证者）的可信度。认证的目标是通过获得关于验证者的软件和数据状态的真实、准确和及时的报告，让验证者对验证者的可信度充满信心。借助认证服务，可以获得包含执行环境（即硬件、软件、自定义数据等）的加密测量的认证报告。

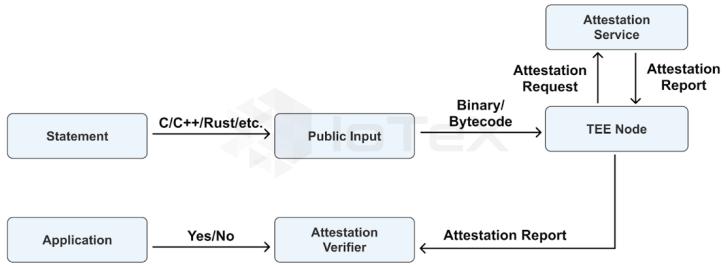


图 4.4: 基于 TEE 的应用程序的系统架构

可以按照某个 TEE 提供商的一般开发流程来实现 TEE 证明机制。TEE 证明机制有助于 DePIN 开发人员利用最先进的机密计算技术进行隐私保护的链下计算。W3bstream 将逐步支持领先的基于 TEE 的硬件平台的开发流程，例如 Intel SGX [37]、Intel TDX [38]、AMD SEV [39]、AMD SEV-SNP [40]、AWS Nitro [41]、Arm CCA [42] 等。

- SMPC 证明机制：MPC 代表了一组用于分布式数据隐私保护协作计算的技术，只显示计算结果。鉴于各种安全假设和威胁模型（例如，可能欺诈对手、恶意对手、隐蔽对手），SMPC 协议至少应满足三个属性，即输入隐私、正确性和输入独立性。基于预处理模型构建的基于 SMPC 的应用程序的典型系统架构如图 4.5 所示。

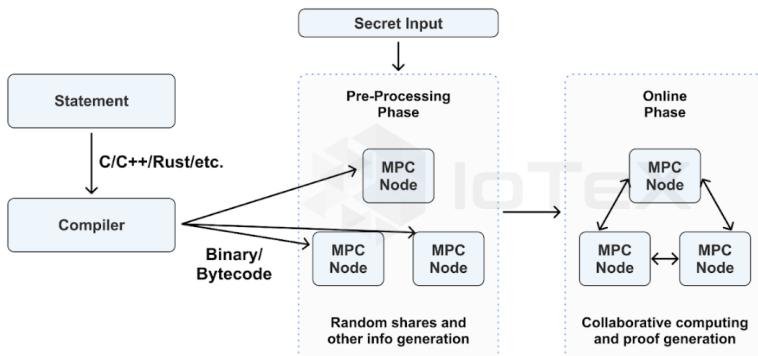


图 4.5: 基于 SMPC 的应用程序的系统架构

SMPC 证明机制可以通过遵循特定 SMPC 协议（例如，SPDZ）的一般开发流程来实现。然而，以有效的方式实现公开可验证性仍然是一个持续的研究方向。

- 自带证明机制 (BYOP)：BYOP 为 DePIN 开发人员提供了极大的灵活性，他们可以部署针对特定 DePIN 项目量身定制的优化证明机制，或在 DePIN 环境中探索新的高效可验证计算技术。

4.1.2 我们在 ZKP 方面的内部创新

多标量乘法 (MSM) 是许多零知识证明系统的核心组件之一，也是这些方案中证明生成的主要性能瓶颈。加速 MSM 的一个主要策略是利用预算计算。在这个方向上已经提出了几种算法（例如，Pippenger [11,12] 和 BGMW [13]）及其变体。在我们最近的研究 [15] 中，我们重新审视了 Luo、Fu 和 Gong 在 CHES 2023 [14] 上提出的最新基于预算计算的 MSM 计算方法，并概括了他们的方法。特别是，我们提出了一种最佳存储桶的通用构造。这一改进带来了约 15% - 40% 的性能提升，这已通过理论分析和实验得到验证。我们还引入了一种桶适应记录，使用 $j = 0$ 椭圆曲线上的快速内射映射将存储需求除以 3，与我们已经优化的 LFG 算法相比，几乎没有性能损失。

4.2 W3bstream 工作流程

4.2.1 验证者加入和管理

验证者加入基于 ioID，并遵循第 5.2.2 节 - ioID 注册和绑定中描述的过程。链上队列管理合约负责安排任务并跟踪所有验证者节点的生命周期。每个验证者节点都可以处于“忙碌”、“空闲”或“离线”状态，并且节点状态将在车队管理合约中不断更新。W3bstream 浏览器可用于检查所有验证者节点的状态。

4.2.2 工作流程

在模块化 DePIN 基础设施中，W3bstream 是链下计算层 (OCCL) 的实现，具有第 4.1 节中描述的多个验证者。Webstream 是一个去中心化的异构证明池，能够对存储在数据可用性层 (DAL) 中的数据执行项目特定的业务逻辑，并生成执行计算的有效性证明（例如，零知识证明、证明报告等）。

W3bstream 作为模块化 DePIN 基础架构中的无状态计算组件工作，并遵循高级 OCCL 工作流程，如下图 4.6 所示。

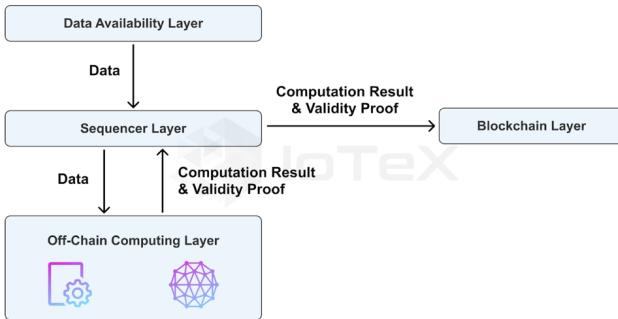


图 4.6：链下计算层的高级工作流程

1. 序列层节点根据 DePIN 项目的配置从数据可用性层检索数据；
2. 序列层节点将数据提供给链下计算层中的空闲节点或选定的一组空闲节点；
3. 链下计算层节点执行 DePIN 项目指定的计算并生成计算结果和相应的有效性证明；
4. 将计算结果和有效性证明返回给序列层节点；
5. 序列层节点将计算结果和有效性证明发送到智能合约进行进一步处理。

一旦有效性证明在链上成功验证，计算结果就可以被 DePIN 项目的 dApp 信任和使用。

4.3 DePIN 验证和链下 AI

W3bstream 中提供的全面证明机制套件允许开发人员向 L1 层区块链证明各种 DePIN 应用程序的链下计算的完整性。特别是，开发人员可以为特定应用程序选择最合适的可验证计算技术。

4.3.1 DePIN 验证

正如 a16z 的 Guy Woullet 所指出的 [43]，DePIN 的成功取决于解决一个关键挑战：确保在不需要中央权威的情况下对地理上分散的服务节点进行可信验证。当前的 DePIN 验证技术大致可分为三类 [44]，

即基于可信硬件的方法、统计方法和基于有效性证明的方法。每种验证方法都有自己的优缺点，在实践中可能需要多种方法的组合。W3bstream 促进各种 DePIN 项目在平台上部署并随后更新其验证算法。这些验证算法可以用 Rust、Golang、C++ 等高级编程语言编写。通过使用 W3bstream 中提供的证明机制之一，可以保证 DePIN 验证算法的可信度。

4.3.2 链下 AI

DePIN 应用为不同行业的 AI 训练和推理开辟了新的机会。一方面，DePIN 应用能够以可信的方式将大量现实世界数据带入 Web3，从而显著提高 AI 模型的准确性。另一方面，DePIN 应用可以在全球范围内有效地组织 AI 训练和推理的计算和存储资源。然而，AI 应用通常是计算密集型的，对链上部署提出了重大挑战。

W3bstream 允许开发人员进行链下 AI 计算，并同时确保计算过程的可信度。虽然零知识证明能够为链下计算提供强大的集成保护，但与不可验证的 AI 计算相比，将零知识证明应用于 AI（例如 ZKML）可能会轻易产生 10,000 倍到 100,000 倍的开销 [45]。开发人员可以不使用 ZKP 证明机制，而是改用更高效的 TEE 证明机制来进行 W3bstream 中的链下 AI 计算。我们基于 Arm 的 Veracruz 框架和 AWS 的 Nitro enclave 进行的初步工作 [7,8] 已经显示出一些非常有希望的结果。

第 5 章

ioID - DePIN 的统一身份系统

DePIN 应用涉及系统参与者之间的大量链上（如质押、资产转移、借贷等）和链下（如人机和机器间通信）交互。模块化 DePIN 基础设施中的身份层是管理各种实体关系并确保其之间安全交互的重要组成部分。因此，设计一个能够满足链上和链下交互需求的统一身份层对于 DePIN 应用来说是非常必要的。

5.1 链上与链下身份

5.1.1 链上身份

链上身份的主要目标是证明加密资产的所有权，并执行各种与加密资产相关的操作，如转移、质押、借贷等。根据 ERC-4337 规范，外部账户（EOA）或智能合约钱包（SCW）的区块链地址能够很好地满足这一目的。特别是，支持任意验证逻辑的 SCW 可以抽象区块链交易的复杂性（如签名验证、随机数增加、Gas 费用支付、链兼容性等），使最终用户与区块链的交互更加直观。通过非同质化代币（NFTs）或灵魂绑定代币（SBTs），可以将额外的属性（如事件参与、提案投票等）与链上身份（即区块链地址）关联起来。这些属性可能是某些去中心化应用（dApps）所需的（例如，代币空投）。

5.1.2 链下身份

在 DePIN 应用中，链下身份用于建立可信的人机和机器间关系。虽然数字证书（如 X.509）通过将身份绑定到公钥来广泛用于集中式系统中以实现信任，但自我主权身份（SSI）为去中心化环境中的实体之间安全通信提供了有前途的身份解决方案。正如图 5.1 所示，SSI 由去中心化标识符（DIDs）、可验证凭证（VCs）和 DIDComm 消息传递三大支柱组成。一旦去中心化系统中的每个参与者（即人或机器）在可验证的数据注册表（如区块链）上注册了其 DID，两实体可以通过交换 DIDComm 消息建立安全的通信渠道并相互认证。当需要由特定实体（即 VC 发行者）验证的额外身份属性时，VCs 将派上用场。

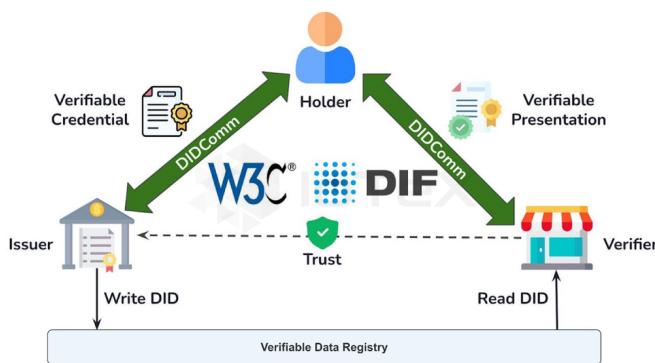


图5.1: SSI的三大支柱

5.2 ioID 设计

ioID 利用区块链钱包地址（外部账户（EOA）或账户抽象（AA）钱包）作为链上身份，并使用 DIDs 作为链下身份，是 IoTeX 设计的一个统一身份系统，用于处理 DePIN 应用参与者之间的链上和链下数字关系。作为一个通用身份系统，我们设想 ioID 可以在 DePIN 模块化基础设施的不同层次中使用，如图 5.2 所示。

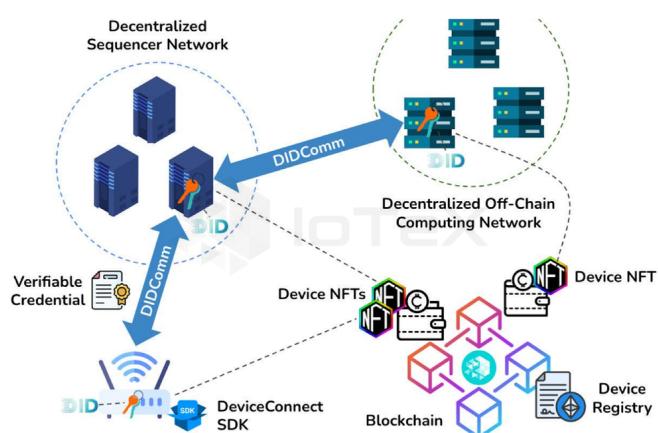


图5.2: ioID身份系统

5.2.1 设备上的 ioID 生成

DePIN 设备可以通过集成 IoTEx 的 ioConnect SDK 在设备上即时生成 DID 及其对应的 DID 文档。对于部署在模块化 DePIN 堆栈中的某个集中式或去中心化层中以支持操作的 DePIN 节点，节点操作员可以使用命令行界面（CLI）生成 DID 及其对应的 DID 文档。对于嵌入式 DePIN 设备，制造商可以将 ioConnect SDK 集成到设备固件中，并允许用户通过串口从设备中读取 DID 和 DID 文档。

5.2.2 设备上的 ioid 生成

DePIN 设备所有者可以通过网络平台（如 IoTEx 的 MachineFi Portal）注册设备。注册过程如下图 5.3 所示：

1. 设备所有者首先使用 Metamask 登录网络平台；
2. 设备所有者在网络平台上存入最低的代币（如 10 IOTX 代币）。这些代币用于支付设备注册过程中的 Gas 费用；
3. 设备所有者获得 DePIN 设备的 DID 和 DID 文档：
 - 对于 DePIN 节点，设备所有者（即节点操作员）需要本地或远程登录节点，并使用 CLI 生成 DID 和相应的 DID 文档；
 - 对于嵌入式 DePIN 设备，设备所有者需要：
 - 通过 USB 将设备连接到 PC；
 - 点击网络门户上的“读取设备 DID 和 DID 文档”按钮，通过串口检索设备的 DID 和 DID 文档；
4. 设备所有者选择集中式或去中心化存储层提供商（如 AWS S3、IPFS 等），存储 DID 文档，使其公开访问，并获取其 URI；
5. 设备所有者调用设备注册合约，提供设备的 DID、DID 文档的哈希值和 DID 文档的 URI。

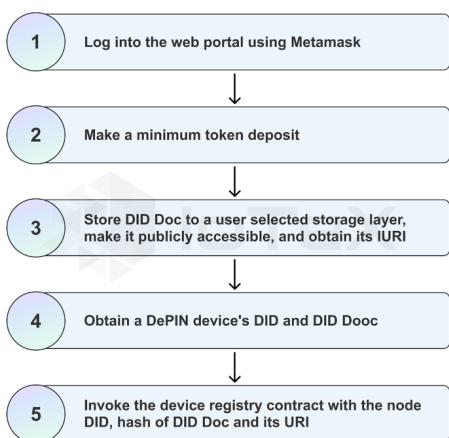


图5.3: 矿工为DePIN设备进行接入的流程

在成功完成设备注册过程后，DePIN 设备所有者可以在其区块链钱包中看到一个设备 NFT，代表 DePIN 设备的链上所有权。

5.2.3 安全的机器间交互

在设备注册过程中注册了 DePIN 设备的 DID 后，它能够基于标准化的 DIDComm 消息协议与网络中的其他实体进行安全的链下通信。

5.3 ioID 在 DePIN 项目中的集成

在使用 ioID 模块之前，DePIN 项目需要完成若干设置。

5.3.1 ioID 的智能合约

ioID 的一套智能合约为 IoTeX 区块链上的去中心化身份管理提供了强力支持。这些合约共同为 IoTeX 生态系统内的身份管理和交互提供了一个强大的框架。

- DePIN 项目注册：DePIN 项目注册是一个基于 NFT 的注册管理系统，用于管理所有 DePIN 项目。它确保每个项目在网络中都具有唯一的身份和认证。
- ioID NFT 合约：ioID NFT 合约是 IoTeX 区块链上去中心化身份管理框架的核心部分。它由项目注册直接管理，负责为设备创建和分配唯一的 ioID 代币。这涉及根据 ERC6551 标准将设备链接到项目 ID 和所有者，并生成相关的钱包地址。
- ioID Store：ioID Store 负责管理所有项目中的 ioID 的申请和激活。它处理身份管理应用的生命周期，确保身份被正确设置和维护。
- ioID Registry：ioID Registry 合约用于在链上注册设备并激活其 ioID。它还充当 DID 解析器，为跨项目验证设备身份提供可靠的手段。

5.3.2 部署设备 NFT 合约

为了将 DePIN 项目与 IoTeX ioID 模块集成，项目所有者首先需要部署一个“设备 NFT”合约，以将其项目中的每个设备进行代币化。拥有 DePIN 项目设备 NFT 的用户有权为物理设备注册一个新的 ioID 身份，并将其绑定到他们的区块链钱包。当设备注册了新的 ioID 后，会向所有者的钱包中铸造一个 ioID NFT，并将相应的设备 NFT 转移到 ioID 的 ERC-6551 钱包中。这一过程有效地“激活”了 ioID，将物理设备与其数字身份及其在区块链上的所有者绑定起来。

5.3.3 注册 DePIN 项目

任何希望使用 ioID 身份的 DePIN 项目必须通过支付所需的费用申请一定数量的 ioID。只有在 IoTeX 区块链上注册的 DePIN 项目才能申请 ioID。项目所有者可以直接调用智能合约或使用 IoTeX 命令行接口（如 ioctl）来注册 DePIN 项目。一旦交易完成，您将收到一个带有特定 Token ID 的项目 NFT，代表您在 IoTeX 区块链上的 DePIN 项目 ID。

5.3.4 设置设备 NFT 合约

在注册 DePIN 项目后，下一步是为该项目在 ioID Store 中设置设备 NFT 合约。必须在设备尝试为您的项目注册 ioID 之前设置该合约。项目所有者可以直接调用智能合约或使用 IoTeX 命令行接口（如 ioctl）来完成此步骤。

5.3.5 申请 ioID

项目所有者需要通过支付所需数量的 IOTX 代币来申请 ioID。所需数量取决于申请的 ioID 数量。项目所有者可以直接调用智能合约或使用 IoTeX 命令行接口（如 ioctl）来申请 ioID。交易完成后，请求的 ioID 数量将与 DePIN 项目关联。

5.3.6 注册设备

在为 DePIN 项目设置设备 NFT 合约并申请一定数量的 ioID 后，物理设备现在可以通过在 ioIDRegistry 合约中注册来激活。这一过程由设备所有者执行，将一个新的 ioID NFT 铸造到设备所有者的账户中，并将其绑定到设备

第六章

ioConnect - 一种抽象DePIN设备硬件复杂性的通用嵌入式SDK

DePIN 应用涉及多种具有不同能力和功能的硬件设备。模块化 DePIN 基础设施中硬件抽象层（HAL）的主要目标是抽象各种智能设备（无论大小）的复杂性和异质性，并使它们能够以安全的方式连接到集中式或去中心化的连接层（CL），如图6.1所示。一个具有挑战性的问题是设计一个通用的嵌入式 SDK，使设备制造商能够轻松地将他们的设备连接到 DePIN 后端。在实践中，ioConnect SDK 旨在支持流行的微控制器系列（例如 ESP32、Arduino、STM32 等）、单板计算机（例如 Raspberry Pi、ODROID、Rock Pi 等）和智能手机（例如 Android 和 iOS），这是非常理想的。

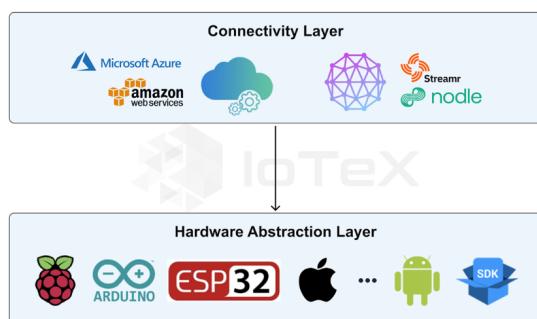


图6.1: HAL与CL之间的安全连接

6.1 连接选项

6.1.1 连接到集中式连接层

将智能设备连接到集中式连接层（例如基于云的物联网网关）在传统物联网行业中得到了广泛研究，并且由于其技术成熟度，已被一些早期阶段的DePIN项目采用。数字证书（例如X.509）通常用于确保智能设备与集中式连接层之间的安全通信。以基于云的物联网网关（例如AWS IoT Core）为例（见图6.2），用户可以首先在云中创建一个数字孪生并生成一个设备证书。一旦证书安装在智能设备中，它就可以与基于云的物联网网关建立安全的TLS连接。数字孪生随后代表智能设备与云中的其他服务进行交互。

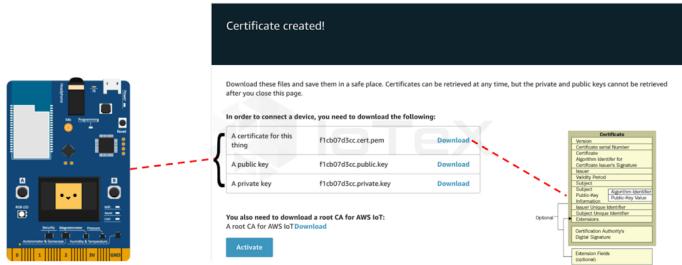


图6.2: 使用AWS IoT Core进行设备接入

虽然集中式连接层简化了设备的连接和管理，但在DePIN应用中它代表了单点故障，未来的DePIN项目应认真考虑采用去中心化的连接层。

6.1.2 连接到去中心化连接层

虽然去中心化连接层为DePIN应用提供了更强大的网络连接，但将智能设备连接到它引入了一些技术挑战：

- 如何使智能设备在不依赖集中式证书颁发机构（CA）和数字证书的情况下，与去中心化连接层中的节点安全连接？
- 如何使智能设备与去中心化连接层中的节点进行双向认证？
- 如何使智能设备与去中心化连接层中的节点建立安全通道？

为了应对上述技术挑战，DePIN设备应实现可在这种去中心化环境中使用的新技术和协议。

6.2 设计通用嵌入式SDK的考虑因素

将各种智能设备连接到去中心化连接层的潜在挑战导致了以下设计要求，以开发适用于DePIN设备的通用嵌入式SDK：

- SDK应兼容流行的硬件芯片组和平台（例如微控制器、单板计算机、智能手机等）；
- SDK应易于DePIN设备制造商集成到其设备中；
- SDK应允许DePIN设备使用高级安全功能（例如安全元件、加密加速器等）；
- SDK应使DePIN设备能够在去中心化环境中与其他实体（即人或机器）建立可信关系。

这些设计要求促使我们探索新兴技术，例如Arm的PSA认证加密API和自主身份（SSI），以及分层的SDK设计方法。

6.2.1 Arm的PSA认证加密API

Arm的PSA认证加密API [47]定义了在各种硬件平台上访问加密操作和密钥管理服务的标准化和统一接口。通过加载目标硬件平台上可用的加密软件/硬件驱动程序，开发者可以通过PSA加密API轻松访问所有与安全相关的功能，如图6.3所示。

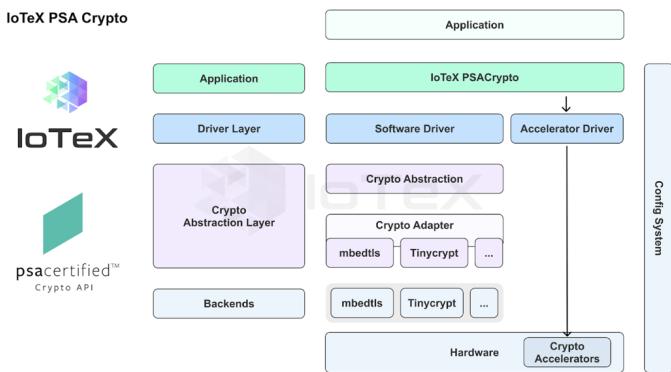


图6.3: IoTeX的PSACrypto库在DePIN设备中的应用

将Arm的PSA认证加密API集成到DePIN设备中，可以显著增强DePIN设备的安全性，从而有效地减轻DePIN应用中日益增加的欺诈风险。

6.2.2 自主身份 (SSI)

自主身份 (SSI) [48]技术，如去中心化标识符 (DIDs) [49]、可验证凭证 (VCs) [51]和DIDComm消息[50]，将数字身份的控制权从传统身份提供者转移到个人手中，为人、组织和物体形成丰富的数字关系奠定了基础。在去中心化环境中，SSI为建立可信的人机和设备间关系提供了一个有前途的解决方案，而无需依赖第三方集中式或联合身份提供者，如图6.4所示。

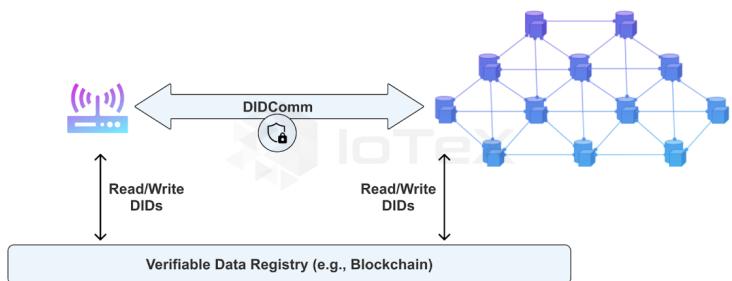


图6.4: 去中心化环境下基于SSI的通信

6.3 实现规范

ioConnect [16]是由IoTeX专门设计的通用嵌入式SDK，用于支持DePIN设备。为了支持各种智能设备和应用需求，该SDK采用了SDK核心和平台适配层（PAL）的架构。

6.3.1 ioConnect SDK核心

ioConnect核心由四层组成，如图6.5所示。底部两层实现了Arm的PSA加密API规范v1.1，而顶部两层则实现了SSI的三个关键支柱（即DIDs、VCs和DIDComm）。所有在SSI中所需的加密操作都通过PSA加密API调用完成。

请注意，ioConnect SDK核心与硬件平台无关，不绑定到DePIN设备上的特定组件/资源。

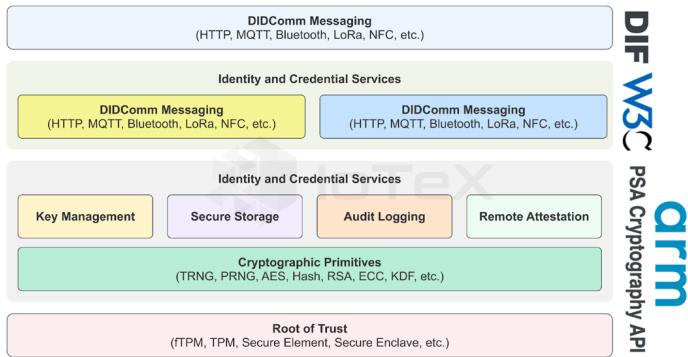


图6.5: ioConnect SDK核心

6.3.2 DePIN设备兼容性

为了适应各种DePIN设备，整个ioConnect SDK采用了如图6.6所示的分层设计方法。一方面，核心包含硬件无关的规范实现（例如SSI、PSA加密API等），另一方面，平台适配层（PAL）处理不同嵌入式系统和平台之间的差异（例如编译规则、编码约定、框架设计等）。

PAL的引入使开发者能够通过开发另一个仅有300到500行代码的PAL组件，轻松添加新硬件支持，从而有效解决DePIN设备兼容性问题，并显著降低DePIN设备制造商的集成复杂性。

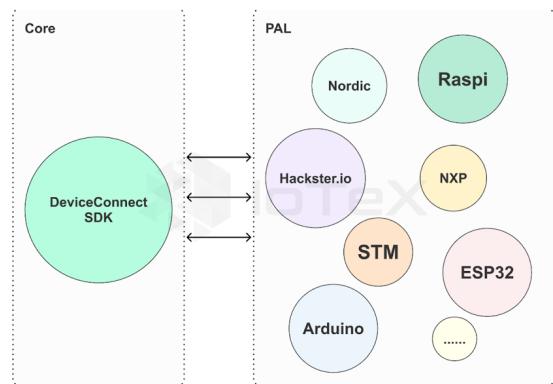


图6.6: ioConnect SDK的分层架构

ioDDK - 启用自主身份的DePIN应用链

7.1 设计逻辑

在IoTeX L1上为DePIN项目启用特定应用的L2的理由是由几个令人信服的因素驱动的。

- 首先，特定应用的L2对DePIN项目至关重要，因为它们允许引入独特的代币经济学、定制的用户体验（例如钱包和浏览器）以及定制的治理结构。这种定制对于优化区块链以满足每个DePIN应用在可扩展性方面的特定需求和场景至关重要，确保每个项目都能充分发挥其潜力。
- 此外，许多DePIN项目缺乏构建和维护自己的区块链基础设施所需的专业知识和财务资源。

截至目前，IoTeX L1通过我们内部的随机委托权益证明（Roll-DPoS）共识协议，由一个由120多个全球分布的代表（即验证者）组成的池来确保安全。通过利用IoTeX L1的安全区块空间，这些DePIN项目可以无缝地启动其特定应用的L2，而无需与区块链开发相关的繁重工作。

ioDDK是一个链SDK，它允许DePIN项目同时提供自主应用链并继承IoTeX L1的安全性，如图7.1所示。在验证和提议IoTeX L1区块的同时，验证者还对来自DePIN应用链的交易达成共识。通过租赁区块空间，IoTeX L1可以为DePIN项目提供必要的资源，以高效部署其定制解决方案，而无需大量前期投资或技术专长，从而促进一个更加充满活力和创新的生态系统。

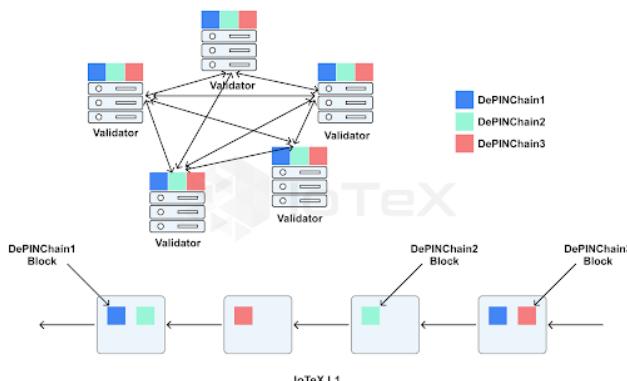


图7.1: 由IoTeX L1保护的自主身份DePIN应用链

7.2 共享区块空间和验证者

为了最小化开发复杂性，所有自主身份的DePIN链可以与IoTeX L1共享区块空间和验证者。实践中可以考虑三种实施选项，如图7.2所示。

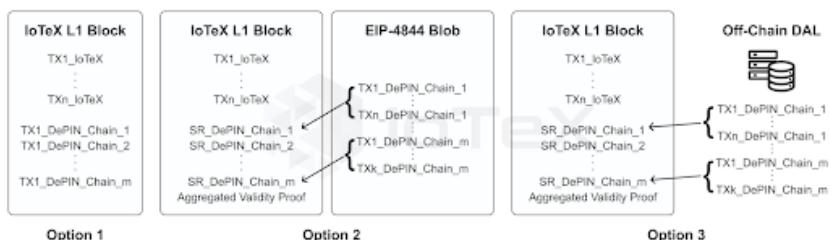


图7.2: 用于共享区块空间和验证者的三种实现方案

选项1 - 将所有交易存储在IoTeX L1上 在此选项中，自主身份的DePIN链的交易与IoTeX L1上的交易共享同一区块空间，并且所有交易都需要通过IoTeX L1的共识过程。这种方法确保所有自主身份的DePIN

链实现与IoTeX L1相同的安全性。然而，由于区块大小的限制，只能支持一定数量的DePIN项目。可能需要一个去中心化治理流程来确定哪些DePIN项目有资格采用这种方法。

选项2 - 使用EIP-4844存储DePIN链交易 在此选项中，自主身份的DePIN链的交易暂时存储在IoTeX L1上，使用EIP-4844的blob。状态根连同所有自主身份的DePIN链状态转换的聚合有效性证明与IoTeX L1的交易共享同一区块空间。在IoTeX L1上验证聚合有效性证明以完成自主身份的DePIN链上的所有交易。这种基于Rollup的方法可以有效提升系统的可扩展性，并允许所有自主身份的DePIN链同时继承IoTeX L1的安全性。注意，W3bstream网络中的一个验证者应该被利用来实现这种方法。

选项3 - 使用离链DAL存储DePIN链交易 在此选项中，自主身份的DePIN链可以选择一个离链数据可用性层（DAL）来存储它们的交易。类似于选项2，状态根连同所有自主身份的DePIN链状态转换的聚合有效性证明与IoTeX L1的交易共享同一区块空间。在此方法中，状态根应由DAL提交到IoTeX L1。虽然这种基于validum的方法也可以提高系统的可扩展性，但安全性取决于特定DAL实施的安全性。注意，W3bstream网络中的一个验证者应该被利用来实现这种方法。

三种方案的比较

表7.1对上述三种实现方案在DePIN链事务存储、可扩展性、W3bstream需求和安全性等方面进行了比较。

表7.1: 三种实现方案的比较

	DePIN链事务存储	扩展性	是否需要 W3bstream	安全性
选项1	链上区块	低	否	高
选项2	链上blob	强	是	高
选项3	链下DAL	强	是	低/中

7.3 ioDDK组件和高级工作流程

7.3.1 ioDDK组件

ioDDK使DePIN项目能够利用IoTeX L1中现有的代表（即验证者）和区块空间来托管自主身份的DePIN链，包括以下组件：

- 链配置**：链配置组件允许开发者配置DePIN链的特定参数（例如开始高度、交易类型、区块空间需求等）；
- 链部署**：链部署组件允许开发者管理将DePIN链的部署过程分布到IoTeX L1的所有代表中；
- 链浏览器**：链浏览器组件允许DePIN项目及外部方监控DePIN链的状态和关键指标（如区块高度、TPS、交易详情等）；

- **链指挥官**: 链指挥官是一个命令行工具，提供一系列命令来简化DePIN链的开发和管理。

7.3.2 高级工作流程

一旦DePIN项目通过去中心化治理流程批准使用IoTeX L1的共享区块空间和验证者来配置自主身份链，项目可以如下使用ioDDK:

- 开发者使用ioDDK中的“链配置”功能指定一些DePIN链特定的参数：
 - **chainID**: 自动生成的链标识符，代表自主身份的DePIN链；
 - **Transaction type**: 交易中的不同字段；
 - **Maximum transaction numbers**: 在IoTeX L1区块中处理的DePIN链交易的最大数量；
 - **W3bstream prover**: 选择一个W3bstream验证者。
- 开发者准备DePIN链交易处理逻辑的docker镜像，并使用ioDDK中的“链部署”功能将docker镜像部署到IoTeX L1的所有代表中。

一旦DePIN链特定的交易处理逻辑部署到IoTeX L1的代表中，DePIN链交易将会相应地进行处理。开发者可以使用ioDDK中的“区块链浏览器”检查配置的DePIN链的状态。此外，开发者还可以使用“链指挥官”使用多个支持命令来管理DePIN链。

7.4 区块空间租赁市场

我们计划实施一个区块空间市场，使开发者能够交易为其使用ioDDK构建的特定DePIN L2定制的区块空间。这种面向市场的策略确保资源分配适应实时需求，从而优化网络的整体效率。可交易区块空间的引入还影响了IOTX代币的用途和流动性。例如，开发者可以质押或销毁IOTX以获得一定数量的区块空间。通过交易产生的收入可以通过多种方式分配，包括为金库提供资金或通过销毁来调节代币供应。

7.5 对IoTeX L1的影响

向IoTeX L1引入共享区块空间带来了许多旨在满足DePIN L2项目不断增长需求的功能：

- 快速区块时间和最终确定性：DePIN L2的主要要求之一是快速的区块时间和快速的最终确定性，以优化用户体验。目前，IoTeX L1的区块时间为5秒。然而，为了满足高性能DePIN项目的需求，我们计划将这一区块时间减少到2秒。这一减少将显著提高L2应用的响应能力和效率，确保更流畅和更友好的用户体验。
- 增加吞吐量和去中心化：DePIN L2的总吞吐量本质上受到IoTeX L1网络中所有验证者计算能力的限制。为了解决这个问题，增加验证者的数量和提高网络的整体去中心化程度是至关重要的。通过扩展验证者池，IoTeX L1可以支持更高的交易量并提供更强的安全性。这一增强还将促进一个更加去中心化和弹性的网络，这对于维护不断增长的生态系统中的信任和稳定性至关重要。

为了满足上述要求，计划引入提议者-构建者分离（PBS）。PBS是由以太坊研究人员最初提出的一个概念，旨在增强区块链网络的抗审查性和整体性能。它将区块提议者和区块构建者的角色分离，以优化区块生成并确保验证过程中的公平性。

- 区块提议者：负责根据区块链的当前状态和网络规则提议新区块。他们收集交易并创建一个区块提议，该提议将由网络验证。这一角色很可能由当前的共识代表承担。
- 区块构建者：专注于通过从交易池中选择最有价值的交易、优化区块空间使用和潜在提高吞吐量来构建区块的专业实体。他们将构建的区块提交给提议者，提议者然后将这些区块提交给网络进行验证。这将是引入IoTeX L1网络的新角色，专门处理包括来自DePIN L2的交易包。

这些角色的分离有助于通过将职责分散到不同的实体来降低集中控制和审查的风险。这提高了网络容量并减少了交易处理时间，即允许更高效的区块生产，因为构建者可以专注于交易选择、优化甚至分片，而提议者处理共识和区块最终确定过程。这种方法将确保基于IoTeX L1提供的共享区块空间的DePIN L2能够高效和安全地运行，满足其特定应用场景的需求。

第八章

新路线图

IoTeX 2.0是我们计划从现在到2026年建设的众多组成部分的集合。路线图如图8.1所示。请注意，列出的许多组件依赖于治理提案和投票，因此可能会有所变化。

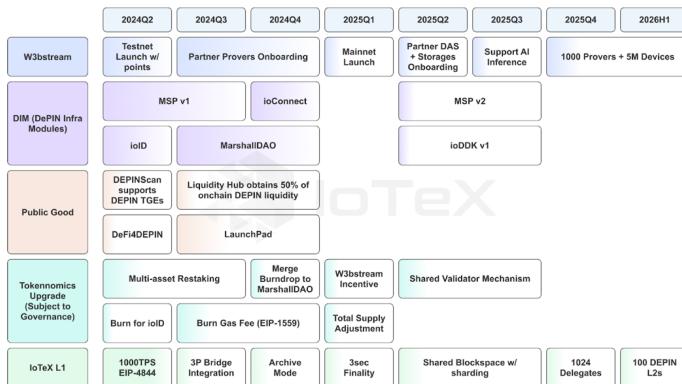


图8.1: IoTeX 2.0 Roadmap

第九章

结论

IoTeX 2.0为IoTeX网络提供了一个新的愿景，同时保留了引发其创立的核心原则。从一开始，IoTeX就设想了一个未来，在这个未来中，个人可以拥有和控制他们的设备及其产生的数据和价值。IoTeX旨在成为现实世界和实时数据的中心，驱动超级智能AI网络。这个网络不仅将超越人类智能，还将利用反映物理环境真实动态的精确可靠数据。这种转变改变了数据的价值和使用方式，影响着文明的未来。最重要的是，IoTeX所赋能的一切将由人民拥有和运营，为人民服务。

感谢IoTeX社区对我们持续的贡献、支持和反馈。在我们踏上这个新的雄心勃勃的旅程时，我们知道IoTeX和我们的全球社区将实现真正的变革，并将DePIN带给世界上的每个国家。现在是建设的时候了！

免责声明

本白皮书是IoTeX核心开发团队与IoTeX社区成员的共同努力成果。它概述了IoTeX网络的一个建议方向。然而，本文的内容并不构成任何作者或其各自组织的承诺。IoTeX社区负责调整和采纳本文中提出的措施。任何提案的成功最终取决于更广泛社区和在IoTeX网络内建设的努力。

本文提供的信息仅供参考。任何PARTIES或其任何附属公司、董事、官员、管理者、雇员或代表对本文中包含的任何材料或信息，无论是明示的还是隐含的，均不作任何声明或保证。此外，PARTIES或任何此类个人对您或您的附属公司、您或您的附属公司的任何董事、官员、管理者、雇员或代表因使用本文中包含的信息和材料而产生的责任或义务均不承担或具有。

提供此处信息是基于相信的信息，但不保证其准确或完整。本文中的信息不应被视为投资建议、金融建议、交易建议或任何其他形式的建议。建议您在做出任何投资决策之前进行自己的尽职调查，并咨询您的财务顾问。

致谢

我们向以下个人和风险投资公司（即来自 Escape Velocity (EV3) 的 Vinayak Kurup，来自 1kx 的 Robert Koschig，6th Man Ventures (6MV)，SNZ Capital，Future Money Group (FMG)，来自 Borderless Capital 的 Álvaro Gracia，Lattice，Summer Capital，Pantera Capital，BlueYard Capital，Spartan Capital，Lemniscap，NGC Ventures，Stanford Blockchain Accelerator，Foresight Venture 和 Samsung NEXT），Web3 项目（即 NEAR Foundation，RISC0，Helium Foundation，The Graph Foundation，Filecoin Foundation 和 Textile），以及加密研究公司（即 IntoTheBlock (ITB) 和 Messari）表示衷心的感谢。你们的宝贵反馈和不懈支持对于我们这份白皮书的形成起到了至关重要的作用。你们的专业知识、洞察力和承诺大大提升了我们工作的深度和质量。我们深深感谢你们投入的时间和资源，你们的贡献对于推动 IoTeX 2.0 使命的前进至关重要。

参考文献

- [1] Pebble Tracker. <https://docs.iotex.io/dev-toolkit/web3-smart-devices/pebble-tracker>.

- [2] X. Fan, Q. Chai, Z. Li, and T. Pan, "Decentralized iot data authorization with pebble tracker," in 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 2020, pp. 1-2.
- [3] Ucam. <https://ucam.iotex.io/>.
- [4] DePIN DevKit - SenseCAP Indicator D1. <https://www.seeedstudio.com/SenseCAP-Indicator-D1-p-5643.html>
- [5] IoTeX - A Decentralized Network for Internet of Things Powered by a Privacy-Centric Blockchain, The IoTeX Team, https://github.com/iotexproject/files/blob/main/publications/IoTeX_Whitepaper_1.5_EN.pdf, July 12, 2018.
- [6] X. Fan, Z. Zhong, Q. Chai, and D. Guo, "Ucam: A User-Centric, Blockchain- Based and End-to-End Secure Home IP Camera System," in Security and Privacy in Communication Networks, N. Park, K. Sun, S. Foresti, K. Butler, and N. Saxena, Eds., Cham: Springer International Publishing, 2020, pp. 311â323.
- [7] M. Brossard, G. Bryant, X. Fan, A. Ferreira, E. Grimley-Evans, C. Haster, D. Miller, D. P. Mulligan, H. J. M. Vincent, S. Xiong, and L. Xu, "Privacy- Preserving Object Detection with Veracruz", PerCom Workshops 2023, pp. 322- 324, 2023.
- [8] M. Brossard, G. Bryant, B. El Gaabouri, X. Fan, A. Ferreira, E. Grimley-Evans, C. Haster, E. Johnson, D. Miller, F. Mo, D. P. Mulligan, N. Spinale, E. Van Hensbergen, H. J. M. Vincent, and S. Xiong, "Private Delegated Computations Using Strong Isolation," IEEE Trans. Emerg. Top. Comput, 12(1): 386-398, 2024.
- [9] IoTeX Foundation, The Building Blocks of DePIN, <https://iotex.io/blog/the-building-blocks-of-depin/>.
- [10] IIP-23: The Marshall DAO, <https://community.iotex.io/t/iip-23-the-marshall-dao/11172>.
- [11] N. Pippenger, "On the evaluation of powers and related problems," In 17th Annual Symposium on Foundations of Computer Science (sfcs 1976), pp. 258â263. IEEE Computer Society, 1976.
- [12] D. J. Bernstein, J. Doumen, T. Lange, and J.-J. Oosterwijk, "Faster batch forgery identification," In International Conference on Cryptology in India, pp. 454â473. Springer, 2012.
- [13] E. F. Brickell, D. M. Gordon, K. S. McCurley, and D. B. Wilson, "Fast exponentiation with precomputation: Algorithms and lower bounds," preprint, 1995.
- [14] G. Luo, S. Fu, G. Gong, "Speeding up multi-scalar multiplication over fixed points towards efficient zkSNARKs," IACR Trans. Cryptogr. Hardw. Embed. Syst. 2023(2), pp. 358â380, 2023.
- [15] X. Fan, V. Kuchta, F. Sica, and L. Xu, "Speeding Up Multi-Scalar Multiplications for Pairing-Based zkSNARKs," Cryptology ePrint Archive, Paper 2024/750, 2024, <https://eprint.iacr.org/2024/750>.

[16] ioConnect - A Universal Embedded SDK for Connecting Smart Devices to Web3.
<https://github.com/machinefi/ioConnect>.

[17] W3bstream. <https://w3bstream.com/>.

[18] D. Patrick, DePIN Supercharged â Introducing the Worldâs First DePIN Ac- celerator.
<https://iotex.io/blog/depin-accelerator/>.

[19] ioTube - A Decentralized Multi-Asset Cross-Chain Bridge. <https://bridge.iotex.io/>.

[20] ioPay - A DePIN Wallet. <https://iopay.me/>.

[21] DePIN Liquidity Hub. <https://iotex.io/depin-liquidity>.

[22] mimo - A Decentralized Exchange for Everyone. <https://mimo.finance/>.

[23] DePINscan. <https://depinscan.io/>.

[24] A. Basi, DePIN Liquidity Hub - Join the Fastest Growing Sector in Crypto,
<https://iotex.io/blog/depin-liquidity-hub/>.

[25] V. Buterin, Y. Weiss, D. Tirosh, S. Nacson, A. Forshatt, K. Gazso, and T. Hess, ERC-4337: Account Abstraction Using Alt Mempool, Ethereum Improvement Proposals, 2021.

[26] W. Entriken, D. Shirley, J. Evans, and N. Sachs, ERC-721: Non-Fungible Token Standard, Ethereum Improvement Proposals, 2018.

[27] T. Daubenschütz and Anders, ERC-5192: Minimal Soulbound NFTs, Ethereum Improvement Proposals, 2022.

[28] Risc0. <https://www.risczero.com/>.

[29] Succinct Processor 1 (SP1). <https://succinctlabs.github.io/sp1/>. [30] Nexus.
<https://www.nexus.xyz/>.

[31] zkWasm. <https://delphinuslab.com/zk-wasm/>.

[32] Circom 2. <https://docs.circom.io/>.

[33] Halo 2. <https://zcash.github.io/halo2/>.

[34] ZoKrates. <https://zokrates.github.io/>.

[35] Noir. <https://noir-lang.org/>.

[36] Cairo. <https://www.cairo-lang.org/>.

[37] Intel Software Guard Extensions (SGX). <https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html>.

[38] Intel Trust Domain Extensions (TDX). <https://www.intel.com/content/www/us/en/developer/tools/trust-domain-extensions/overview.html>.

[39] AMD Secure Encrypted Virtualization (SEV). <https://www.amd.com/en/developer/sev.html>.

- [40] AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More. <https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/solution-briefs/amd-secure-encrypted-virtualization-solution-brief.pdf>.
- [41] AWS Nitro System. <https://aws.amazon.com/ec2/nitro/>.
- [42] Arm Confidential Compute Architecture. <https://www.arm.com/architecture/security-features/arm-confidential-compute-architecture>.
- [43] G. Wuollet, Introducing the Nakamoto Challenge: Addressing the Toughest Problems in Crypto. <https://a16zcrypto.com/posts/article/introducing-the-nakamoto-challenge-addressing-the-toughest-problems-in-crypto>.
- [44] IoTeX Foundation, Decentralized Verification in DePIN. <https://iotex.io/blog/decentralized-verification-in-depin/>.
- [45] Modulus Labs, The Cost of Intelligence: Proving Machine Learning Inference with Zero-Knowledge. https://github.com/Modulus-Labs/Papers/blob/master/Cost_Of_Intelligence.pdf.
- [46] AWS IoT Core. <https://aws.amazon.com/iot-core/>.
- [47] Arm PSA Certified APIs. <https://arm-software.github.io/psa-api/crypto/>.
- [48] Self-Sovereign Identity. https://en.wikipedia.org/wiki/Self-sovereign_identity.
- [49] Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations. W3C Recommendation, 19 July 2022. <https://www.w3.org/TR/did-core/>.
- [50] DIDComm Messaging. DIF Ratified Specification. <https://identity.foundation/didcomm-messaging/spec/>.
- [51] Verifiable Credentials Data Model v1.1. W3C Recommendation, 03 March 2022. <https://www.w3.org/TR/vc-data-model/>.
- [52] IoTeX Research, <https://iotex.io/research>.