Messari详解CKB：原生比特币L2架构与RGB++资产发行协议

### 摘要

自 RGB++ 协议在 CKB 主网推出以来，CKB 网络的交易活动重新活跃起来，4月份新增了近40万个地址，环比3月增长了181%。

将支付通道网络集成到闪电网络的工作正在进行中，这将使 CKB 更具可扩展性，并适用于各种区块链应用。

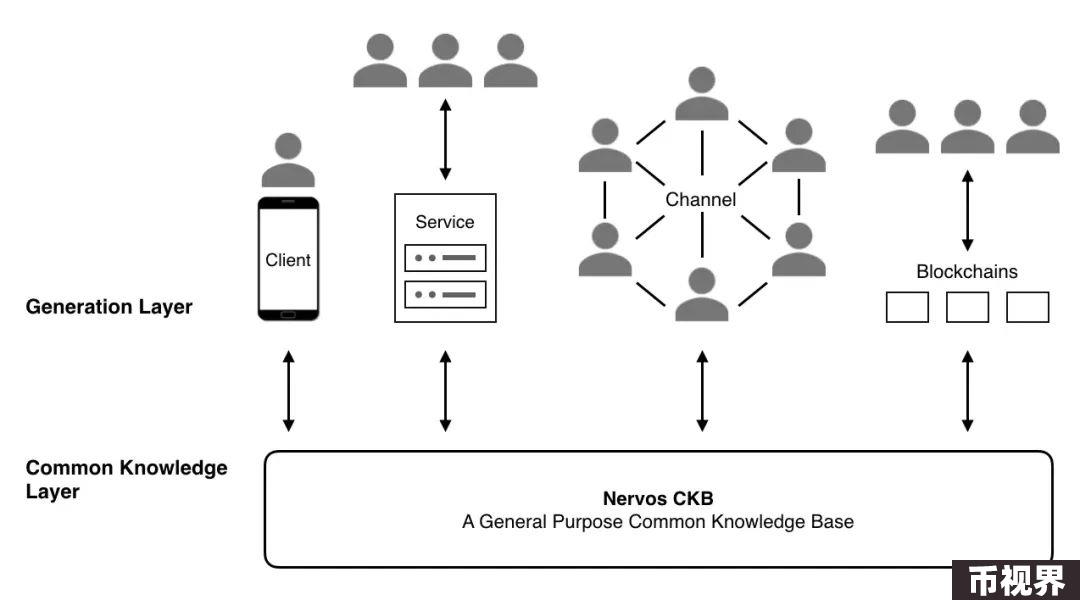
### 背景

作为最大的加密货币，比特币不断获得采用和认可。然而，它的成功也暴露出一些限制和挑战，特别是在可扩展性方面。例如，比特币区块链在 Segwit 升级之后，将区块大小限制在 4 MB 以内，这限制了在给定时间内能处理的交易数量。随着网络的增长，这种限制导致了更长的确认时间和更高的交易费用，使得比特币在处理大规模交易量时效率下降。与其他区块链相比，除了价值转移，比特币的脚本语言目前还缺乏开发复杂智能合约所需的灵活性和表现力。

为了解决这些限制，人们提出了多种Layer 2(L2) 解决方案，如支付通道、侧链和 Rollup。它们大多旨在通过在链下处理交易来扩展比特币，试图在不影响基础层安全性的情况下提高交易吞吐量。例如，闪电网络创建了一个二层支付通道网络，允许近乎即时的小额支付。另一种方法是侧链— — 与比特币主链相连的独立区块链，拥有更大的脚本可能性和更快的交易。然而，这些解决方案往往有所取舍，如增加了复杂性、信任假设和潜在的安全漏洞。

Nervos Network是比特币可扩展性解决方案之一，它采用了更原生的方式，修改了支撑比特币的UTXO 模型。它改进了RGB 协议，在无需跨链桥的情况下为比特币提供图灵完备的合约能力。Nervos Network 由 Terry Tai、Kevin Wang、Cipher Wang 和 Daniel Lv 于 2018 年第一季度立项，是一个旨在提高可扩展性的 Layer 1 区块链。为了推动网络的开发，项目团队从种子轮、私募轮和公募中筹集了超过 1 亿美元的资金。2019 年 11 月，Nervos Network 的 Layer 1 区块链 — — Common Knowledge Base（共同知识库，简称 CKB）上线。2024 年 2 月，由 Nervos 联合创始人 Cipher Wang 领导的CELL Studio推出了比特币一层资产发行协议 RGB++。受 RGB 协议的启发，RGB++ 协议使用 CKB 作为数据可用性和执行层，为比特币实现了智能合约能力和资产发行。自 2024 年 4 月 RGB++上线主网以来，利用 RGB++ 在比特币上发行资产的项目数量不断增加。截至 2024 年 6 月，现有的 15+ 个生态项目使 CKB 的链上活动重新活跃起来。

### 技术



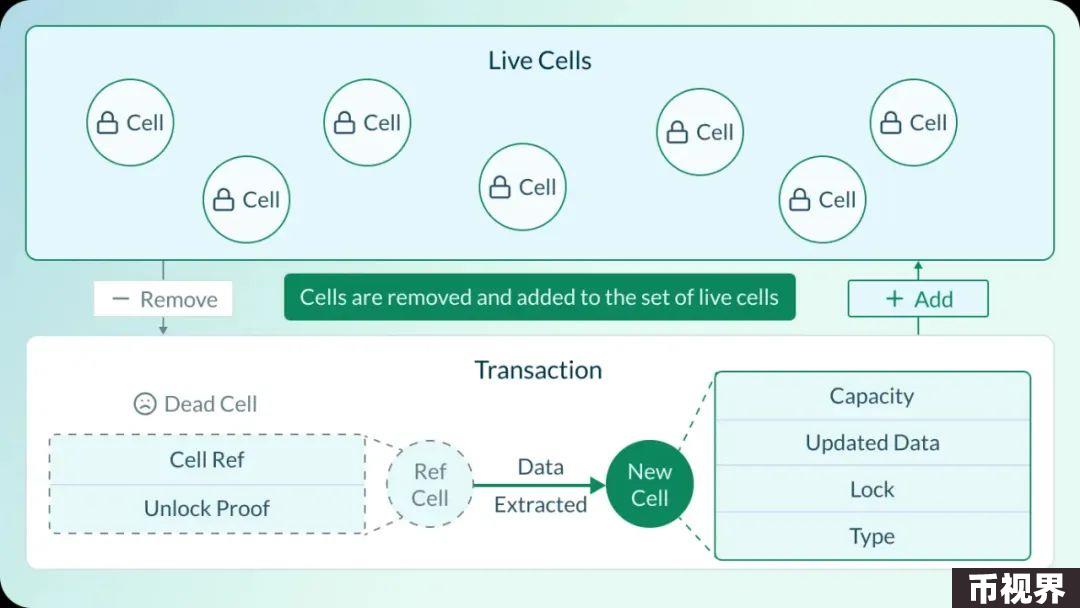
Nervos Network 采用分层架构，包括一个可通过支付通道和RGB++进行扩展的L1 区块链（Common Knowledge Base，简称 CKB）。Cell 模型是比特币 UTXO 记账模型的改进版，CKB-VM 是一种定制虚拟机，它们支持了网络的分层设计。CKB-VM为在网络上发起交易或构建应用提供了灵活的执行环境。这种设计可以让网络通过在每一层运行专用组件来进行垂直扩展，类似于模块化区块链。

#### Common Knowledge Base

CKB是 Nervos Network 的底层 L1 区块链，其运行方式与比特币类似，采用工作量证明（PoW）共识机制。它使用比特币算法的升级版NC-MAX，通过加快交易确认时间和降低孤块率来提高网络效率和响应速度。比特币以 10 分钟的区块间隔为目标，大约每两周调整一次挖矿难度。而 CKB 会根据网络活动的变化动态调整区块间隔（大约每四小时一次），从而优化性能。

CKB 使用了Eaglesong函数来确保网络的安全，这是一种 ASIC 中立的定制型哈希函数，可替代广泛使用的 SHA256 哈希函数。Eaglesong 是一种海绵函数，对多个加密元素进行了优化，可提供与其他工作量证明（PoW）哈希函数同等级别的安全性，同时专门为 Nervos Network 量身定制。

#### Cell 模型



Cell 模型是 CKB 数据结构的核心，可以在链上存储和验证任何数据。比特币原始的脚本语言和 UTXO 模型限制了其执行智能合约所需的复杂计算的能力。相比之下，CKB 对 UTXO 模型进行了一般化处理，允许更灵活的数据存储和验证。与使用单一脚本验证交易的比特币不同，CKB 在其 Cell 模型中引入了双脚本：

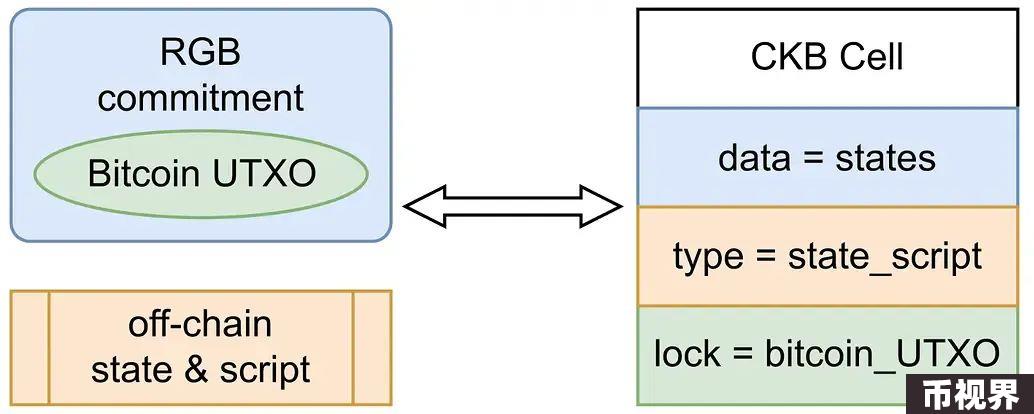
与比特币的有限选项相比，这一系统使 CKB 能够支持更多的功能，使其更适合各种应用。CKB 中的每个 Cell 都是一个可编程 Cell ，可以保存不同的数据类型，如代币、智能合约和特定的应用状态。它还可以运行复杂的类似于图灵完备语言中的脚本。Cell 独立运行，这意味着它们可以在不影响区块链其他部分的情况下进行更新或引用，通过并行的方式提高可扩展性。

#### CKB-VM

CKB-VM是 CKB 的执行引擎，用于运行智能合约和去中心化应用程序。该虚拟机使用 RISC-V 指令集，这是一种灵活、简单的开源硬件架构集（ISA），支持多种编程语言，包括 C 和 Rust 等流行语言。这种广泛的兼容性使 CKB-VM 有别于通常仅限于特定语言的其他区块链的虚拟机，向更广泛的开发者社区开放。CKB 网络还支持 JavaScript、Rust、Go 和 Java 等主流语言的 SDK，方便开发者使用熟悉的工具进行开发。这使得开发人员更容易使用熟悉的编程语言创建复杂的去中心化应用。

此外，CKB-VM 的架构提供了可预测的 gas 费用、安全的执行以及与 Cell 模型的高效集成，有助于有效管理状态和验证交易。可预测的 gas 费用模型避免了意外费用，提升了用户体验，并简化了合约开发。

#### RGB++ 协议



CKB 利用RGB++协议扩展比特币，该协议是一种资产发行标准，可在 CKB 上扩展比特币的功能。RGB++ 协议可实现复杂的智能合约和资产管理操作，而这在比特币网络上通常是不可能实现的。最初的RGB 协议是一个 L2 解决方案，目的是在不改变比特币主网的情况下，为比特币实现智能合约和资产发行。它通过将资产绑定到特定的比特币 UTXO，使这些资产可以随着 UTXO 本身的转移而转移。RGB 协议主要依赖客户端验证，交易在链下处理和验证，从而减少了比特币网络的负载。然而，这种方法也有局限性，比如数据可用性方面的潜在问题 — — 由于数据不存储在链上，因此在需要时可能无法随时访问。此外，对客户端验证的依赖增加了复杂性，可能会影响用户体验。

Nervos Network 通过RGB++协议解决了这些限制，该协议通过使用 CKB 作为比特币的数据可用性和执行层，扩展并增强了原始 RGB 协议背后的原理。RGB++ 通过同构绑定技术，将比特币 UTXO 映射到 CKB 的 Cell 上，实现了与 CKB 图灵完备智能合约的无缝集成。这是通过利用 CKB 的分层架构和 Cell 模型实现的，允许比特币资产与 CKB 上的 dApp 进行交互。通过使用 RGB++，CKB 可以为比特币执行更复杂的智能合约，而这在最初的 RGB 协议中是不可能实现的。RGB++ 还引入了关键交易元素的链上验证，提高了安全性和数据可用性。此外，RGB++ 协议还能实现交易折叠、共享状态的无主合约以及非交互式转账，且无需跨链桥即可实现比特币的跨链转移。

#### 支付通道

作为底层公链，CKB 可以通过支付通道进行扩展，比如Polycrypt开发的支付通道框架Perun。通过在链下处理交易和链上结算，这些支付通道可以支持从小额支付到支付网关等多种应用，从而提高 CKB 的性能。Perun 利用了 CKB 的 Cell 模型，其中 Cell 携带了 capacity、Lock Script、Type Script 和数据来管理通道的状态。通道的其中一个实现（PerunLockScript）可以管理通道实时 Cell 的访问权限，而另一个实现（PerunTypeScript）可以处理状态转换的验证逻辑。从通道获得资金到关闭，这些转换都是自动管理的。截至发稿时，Perun 仍在测试中，尚未在 CKB 主网上线。Nervos 核心开发人员还在努力将 CKB 连接到比特币的闪电网络，使用户能够在不依赖第三方的情况下交换 BTC 和 CKB。

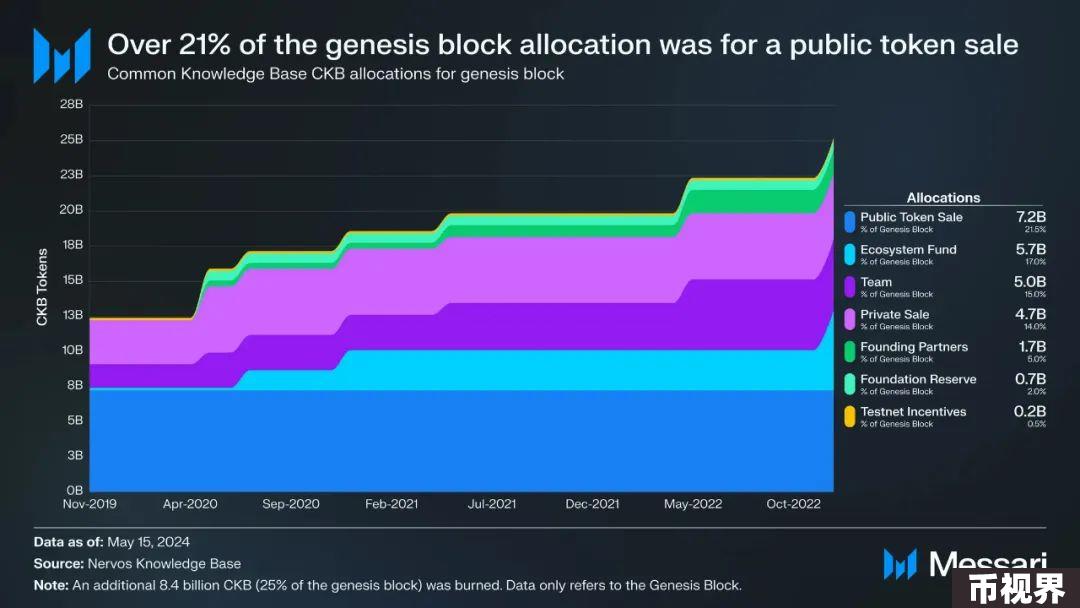
### 代币经济学

Nervos Network 的原生代币CKByte（CKB）在维护网络安全和激励有效存储方面发挥着重要作用。CKB在网络中的主要作用包括：

此外，CKB 代币有三个来源：（1）创世区块；（2）基础发行；（3）二级发行。

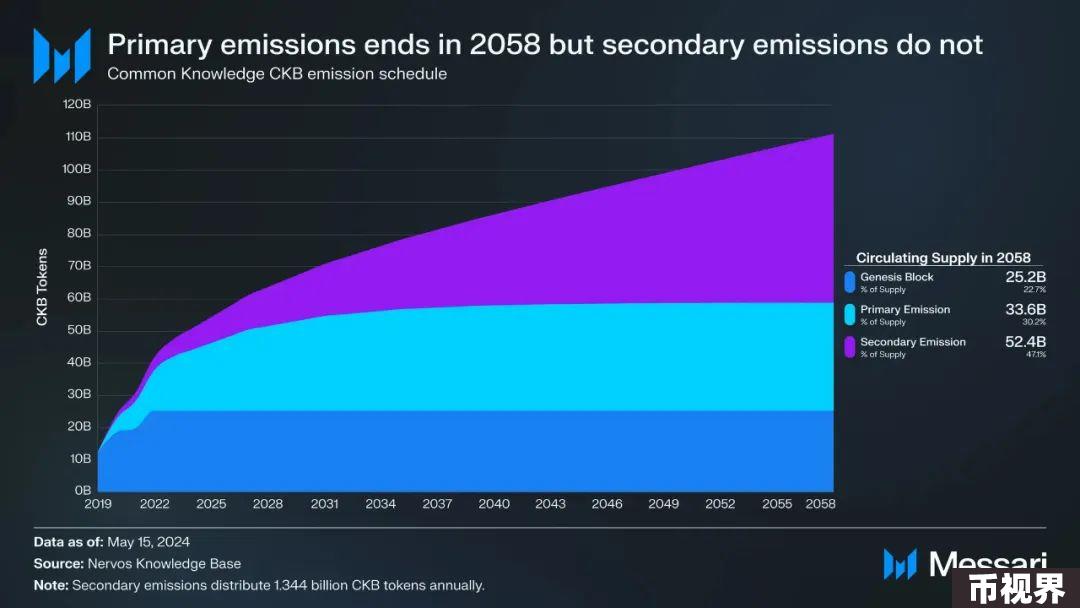
#### 创世区块

2019 年 11 月主网启动时，创世区块铸造了 336 亿枚 CKB 代币，其中 84 亿枚 CKB 代币（占初始发行的 25%）被立即销毁。在销毁的这84 亿枚 CKB 中，50.4 亿枚代币被用于链上存储（”占用链上空间”），剩余的 33.6 亿枚代币处于流动状态（”流动性”）。对这些被销毁的代币进行相应的状态分配，目的是为了让矿工在最初时至少能获得二级发行的 15%，而国库基金至少能获得 10%。值得注意的是，目前分配给的国库基金的 CKB 代币全部被销毁，只有通过网络硬分叉才能更改此设定。



创世区块中的 CKB分配如下：

#### 基础发行



CKB基础发行（一级发行）的目标是在网络的早期发展阶段提升网络的安全性。每个 Epoch 的 CKB 基础发行量固定，全部奖励给矿工，奖励他们处理网络上的交易。基础发行的上限为 336 亿枚 CKB 代币，并遵循与比特币类似的通胀时间表，即每四年减半一次，直至达到供应量的上限。2023 年 11 月，CKB 经历了首次减半事件，基础发行的年发行量从 42 亿枚 CKB 降至 21 亿枚。

#### 二级发行

CKB 通过两种方法管理状态爆炸。首先，要在链上存储数据，用户必须锁定 CKB 代币。CKB 并不直接向锁定 CKB 代币的用户收取费用来支付状态租金，而是通过一种称为二级发行的通胀机制间接收取费用。每年，13.44 亿枚 CKB 代币通过二级发行被铸造出来，并分配给矿工、Nervos DAO 储户以及国库基金。因此，二级发行针对存储数据的用户引入了通货膨胀，因为锁定的 CKB 代币会自动面临价值稀释，这是支付状态租金的一种间接方式。截至写文，已有超过 6 亿枚 CKB 代币作为状态租金分配给了矿工，约 11.5 亿枚 CKB 代币奖励给 Nervos DAO 储户，分配给国库基金的超过 42.7 亿枚 CKB 代币被直接销毁。

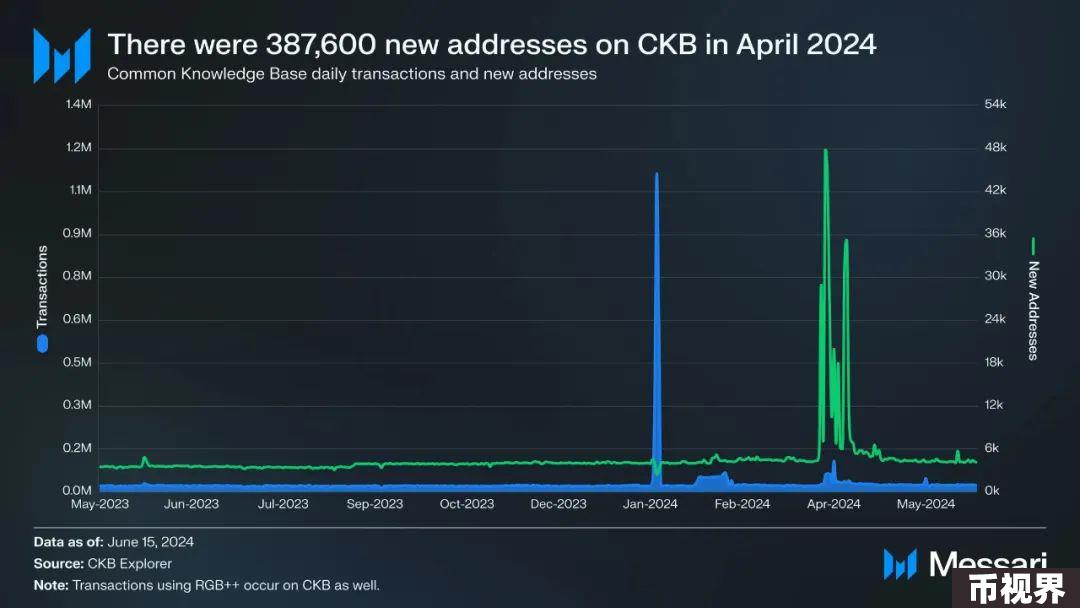
#### Nervos DAO

通过 Nervos DAO，CKB 代币持有者可以原生地避免被二级发行所稀释。通过将持有的 CKB 代币锁定到 Nervos DAO 智能合约中，用户可以从二级发行中获得代币奖励，确保其持有的代币免受通货膨胀的影响。Nervos DAO 储户获得的收益率与二级发行的通胀率相同，随着总供应量的增加，APR 也会继续下降。用户可以随时往 Nervos DAO 存款，最低金额为 102 CKB，但取款只能在30 天存款周期结束后才能进行。



截至写文，已有 92 亿枚 CKB 代币存入 Nervos DAO。CKB 的存入流通比为 20.84%，在过去两年中一直呈下降趋势。这种下降趋势可能是因为 CKB 上的未花费 Cell 数量不断增加。

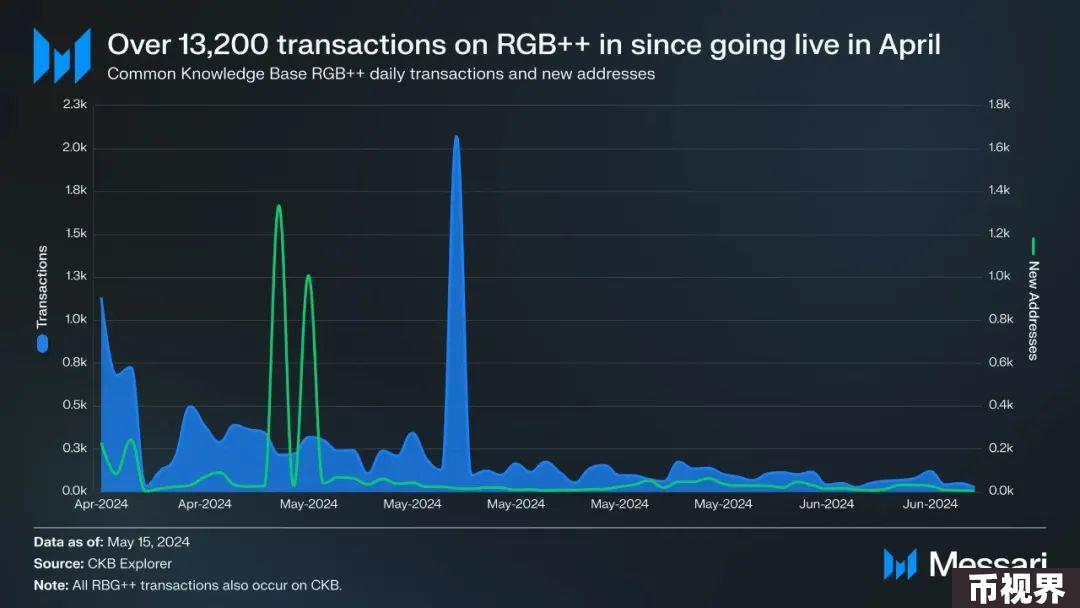
### 网络活动



在过去的一年里，CKB 网络持续活跃。截至目前，CKB 的日均交易量为 43,600 笔。与 2023 年第四季度的日均 20,800 笔相比，增长了 110%。在新增地址方面，4 月份的链上活动明显增加。4 月份创建了 387,600 个新地址，与 3 月份相比，环比增长了 181%。



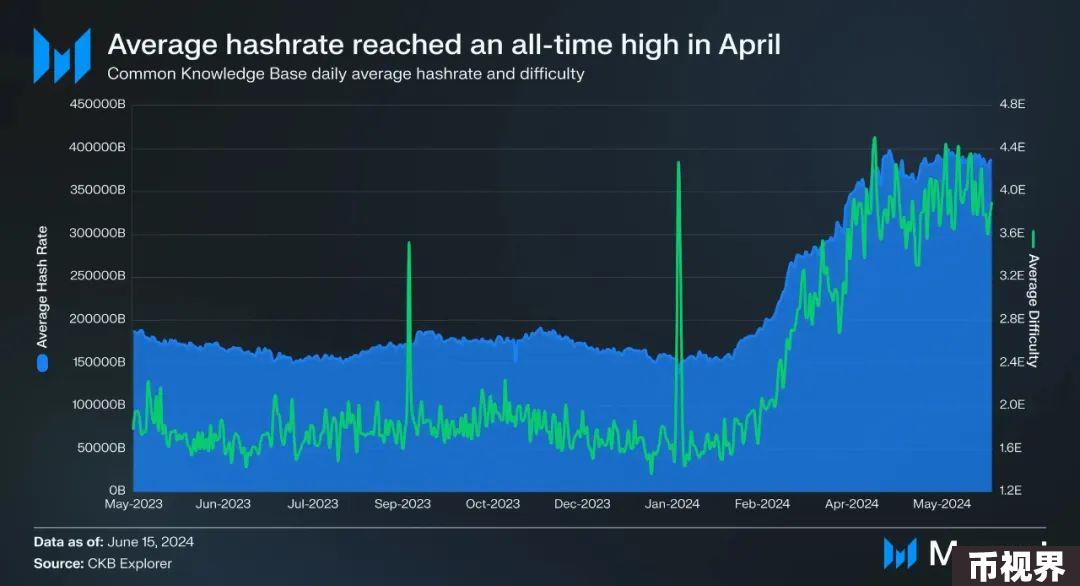
自 4 月份以来，CKB 上的 Cell 活动一直在稳步增加，部分原因是 RGB++ 协议的推出。Cell 活动分为未花费 Cell 和已花费 Cell。未花费 Cell 可用于未来的交易、智能合约执行和数据存储，反映了网络活动和采用率的提高。已花费 Cell 虽然不再用作交易输入，但仍包含可访问和引用的有价值数据，有助于区块链的历史和数据可追溯性。截至 2024 年 5 月 15 日，共有 170 万个未花费 Cell ，与第一季度末相比增长了 13%。至于已花费 Cell ，截至发稿时，CKB 上共有 5760 万个已花费 Cell 。



自 RGB++ 协议于 2024 年 4 月 3 日上线以来，已有超过 13,200 笔交易和 4,400 个独立地址使用该协议。整个 5 月和 6 月的网络活动呈下降趋势，但利用 RGB++ 的更多生态项目应该有助于扭转这一趋势。

### 安全性与去中心化

作为 PoW 网络，矿工通过解决加密难题来验证交易并向区块链添加新区块，从而确保 CKB 的安全。每挖出一个区块，矿工就能获得该区块的全部 “基础发行” 奖励和部分 “二级发行” 奖励。矿工还可以从处理网络交易的交易费中获得提案奖励或提交奖励。为了在不降低性能的情况下管理网络活动的变化，CKB 定制的 NC-MAX 共识协议大约每四个小时根据网络的孤块率调整一次挖矿难度。这样，网络可以优化出块时间，同时降低区块重组的可能性，因为区块重组可能会破坏网络的稳定性。



算力是对 PoW 区块链矿工基础计算能力的衡量标准。因此，算力代表着 CKB 网络的安全性。2024 年，CKB 全网算力不断刷新历史新高。4 月 27 日，CKB 的全网算力达到 397.5 PH/s，是 CKB 网络有史以来的最高算力值。算力上升的部分原因是 Binance 于 2024 年 4 月 18 日开启了 CKB 矿池。与算力类似，2024 年的平均挖矿难度也创下了历史新高（4 月 21 日该值为 3.96E）。

### 生态系统

Nervos Network 继续通过资金、基础设施和工具支持来促进生态系统的发展。在 2019 年 11 月主网上线时，约 57 亿 CKB（占创世区块 CKB 分配额的 17% — 写文时为 6240 万美元）被预留用于生态基金。多年来，生态基金已为多个生态发展计划提供了种子资金，以推动网络的发展计划。其中之一是CKB Eco Fund（前身为 InNervation），该生态基金专注于孵化和投资使用 RGB++ 连接 CKB 和比特币的早期和种子轮项目。CKB Eco Fund 支持生态项目建设关键的基础设施和跨领域的去中心化应用，包括 DeFi、游戏、工具、NFT 市场等。2024 年 1 月，CKB Eco Fund 推出了 BTCKB 计划，旨在通过 PoW 共识机制和 UTXO 模型加强比特币和 CKB 区块链之间的集成。BTCKB 计划引入新的智能合约功能，将 BTC、Taproot Assets和 RGB++ 资产纳入到 CKB 区块链中，从而增强比特币区块链的功能。作为该计划的一部分，CKB Eco Fund 还孵化了CELL Studio，这是一家由 Nervos 联合创始人 Cipher Wang 领导的区块链软件公司，也是 BTCKB 计划的牵头者。CELL Studio 开发基础设施和应用程序，以增强和扩展 Nervos 生态系统，它与 ConsenSys 为以太坊开发Infura和MetaMask等基础工具的方式类似。截至目前，CELL studio 开发的知名生态系统工具包括：

自 2024 年 4 月 RGB++主网上线以来，已经有超过 15 个现有生态项目利用该协议进行资产发行。值得重视的生态项目包括：

CELL Studio 发布的 RGB++开发路线图强调了 2024 年内要完成的重要计划包括：

作为 BTCKB 计划的一部分，CKB Eco Fund 还打算推出连接 BTC 和 CKB 的跨链桥和基于 UTXO 的 DEX。此外，还会利用 RGB++ 协议为 CKB 开发了一个支付通道网络，相关的概念验证已完成。该支付通道网络将连接到闪电网络，使 CKB 更具可扩展性，适合各种区块链应用。

### 竞品分析

作为比特币 L2，Nervos Network 扩展比特币的方法主要是通过 RGB++ 协议来增强比特币的功能。像Stacks这样的竞品提供了定制的执行环境和编程语言，而Rootstock则对两条链之间的交易进行挂钩。相比之下，Nervos 的目标是在不增加复杂性或损害去中心化的情况下增强原生的比特币体验。借助 RGB++ 协议，CKB 可以为比特币提供与比特币原始 UTXO 模型紧密结合的智能合约执行环境。这种设计可能会为 Nervos Network 带来优势，吸引那些对偏离比特币核心理念 ——去中心化和安全性 — — 的解决方案持怀疑态度的用户

与闪电网络这样的扩展解决方案相比，CKB 的智能合约提供了更广泛的功能，可为开发者在比特币上构建更复杂的应用程序提供服务。虽然闪电网络能有效促进快速、低成本的交易，但它并不支持复杂的去中心化应用。与此同时，Liquid Network、Merlin Chain和Bouncebit等平台需要信任半中心化的联盟来管理侧链与比特币主网之间的跨链桥。CKB 使用链下计算和链上结算的方法，避免了这种程度的中心化。

尽管如此，Nervos 利用 RGB++ 协议扩展比特币的方法并非没有局限性。在数据可用性和资产发行方面对外部网络（特别是 CKB 区块链）的依赖，为比特币带来了额外的复杂性和潜在的延迟。此外，由于缺乏全面的开发工具和多方交互解决方案，限制了该协议有效支持去中心化应用的能力。最后，CKB 区块链上交易的透明性损害了 RGB 协议最初提供的隐私优势。

### 总结

随着人们对比特币原有功能之外的可扩展性和功能的需求不断增长，比特币 L2 市场也在持续发展。各种 L2 解决方案，如闪电网络、侧链和 Rollup，旨在通过将交易移出主链来解决这些问题，从而在不影响安全性的情况下提高比特币的吞吐量。然而，这些解决方案往往会带来新的复杂性和安全挑战。Nervos 的与众不同之处在于通过 RGB++ 扩展了 RGB 协议。RGB++ 为比特币提供了原生扩展，集成了与比特币 UTXO 模型直接相关的更深层次的智能合约功能。这些功能反过来又促进了比特币实用性更加无感、更加安全的扩展。此外，将支付通道网络与闪电网络连接在一起的工作正在进行中，这将使 CKB 更具可扩展性，适用于许多区块链应用。

最终，Nervos 的目标是通过简化用户和开发者体验来加强其在比特币 L2 领域的地位。此外，Nervos 还可以优先为更广泛的资产类型和复杂应用提供 RGB++ 支持，从而提高其在比特币生态系统中的实用性。通过这样做，Nervos 可以在比特币作为去中心化应用和智能合约平台的更广泛采用和功能性方面发挥关键作用。