

NERVOS

Nervos CKB


加密经济模型提案

2019.03.08

Copyright © 2019 Nervos Foundation

Supported by Nervos Community

目录

1. 代币经济学的设计目标
 2. 比特币的加密经济模型
 3. 可保值和交易的智能合约平台
 4. 资产存储
 5. 去中心化与状态限制的需求
 6. Nervos CKB 的经济模型
 7. 用于保存价值的经济模型
 8. 代币经济学的应用
 9. 附件 1：交易成本分析
 10. 联系 Nervos
- 

1. 代币经济学的设计目标

公有非许可链是开放给所有人自由参与的分布式系统。一个精心设计的加密经济模型，可以将各方参与者的利益与协议的整体利益对齐，使其在追求自身经济利益的同时也能对整个区块链网络做出贡献。

更具体地说，加密经济系统的设计必须回答以下问题：

- 经济模型如何保障协议的安全性？
- 经济模式如何维护协议的可持续性？
- 经济模型如何将不同参与者的经济目标与提高整个网络价值的目标对齐？

2. 比特币的加密经济模型

比特币协议使用原生代币激励矿工验证交易和挖矿。Nakamoto 共识遵循最长链原则，以此激励矿工在挖出新块后立即广播，在收到新块后立即验证，以达成全网共识。

比特币的原生代币既是功能代币，也是储值资产。当比特币作为功能代币时，可用于支付交易费用，当作为储值资产时，可用来保存价值。通常我们用术语 MoE (Medium of Exchange, 交易媒介) 和 SoV (Store of Value, 价值存储) 分别指代这两种用例。两者并不冲突，它们对比特币网络的正常运行都发挥着重要的作用。然而，研究这两种用例背后不同的经济动机，对分析比特币网络的可持续性具有重要的指导意义。

比特币协议中对区块大小的限制制约了整个网络的交易处理能力，因此用户需要通过类似拍卖的机制竞争有限的交易处理资源。拍卖价格也就是交易费由实际的交易需求决定，当交易需求增加时，为了击败竞拍对手，交易费的价格也会水涨船高。

2.1 比特币作为交易媒介网络

MoE 用户将比特币网络看作一个点对点的价值传输网络，他们不通过持有比特币获益，而是利用比特币网络的点对点交易功能受益。事实上，已经有专业的比特币支付服务商提供这种资金流动性服务，用户不需要持有加密货币也可以将比特币作为价值载体完成交易。MoE 用户并不关心加密货币的价格和价格波动，他们只关心交易费用换算成法币后的价格。

比特币要成为一个 MoE 主导的网络是很有挑战性的。如果协议限制了出块时间和区块大小，那么网络的交易处理能力会非常受限，因此网络的繁荣必然会导致交易成本增加，而这将反过来降低比特币网络与其他类似的区块链协议甚至是与比特币分叉链之间的竞争力。如果协议致力于维持较低的交易成本，通过设置更快的出块时间或更大的区块大小来提高交易处理能力，这会导致更频繁的分叉或者更高的参与共识成本，实际上这相当于在去中心化与安全性上做了妥协。

2.2 比特币作为价值存储的网络

而 SoV 用户则将比特币网络看作一种为原生代币提供安全保障的协议，他们相信原生代币可以长期保值，而 MoE 是一种不可或缺的功能。SoV 用户，特别是长期持币者，并不在乎交易成本，因为交易成本会随着持有时间的累积被分摊。SoV 用户关注

的是比特币本身的价值，而这依赖于网络的安全性和去中心化程度 - 如果网络变得不够安全、易受攻击，那么价值将无法被储存，比特币也将一文不值；如果网络算力过于集中，比特币作为一种资产不再具有独立价值，并将面临保管方风险。

如果比特币要成为一个 SoV 主导的网络，其必须继续坚持当前的货币政策，维护网络的安全性以及保持一定程度的去中心化。然而，比特币的发行总量有限，当所有的比特币被开采一空后，给矿工的激励只剩下交易费。这种模式是否可持续仍然是一个问号，特别是在一个 SoV 主导的网络里往往不会产生许多交易。

2.3 谁能长期补贴矿工？

安全性和去中心化是区块链网络的两个基本属性，维护这两个属性需要付出很高的成本，因此支付给网络维护者(主要是矿工)的奖励必须能够覆盖这些成本。根据比特币当前的模型，当代币开采完毕后，如果矿工仍可赚取足够的交易费，那么比特币网络依然保有安全性。然而，MoE 用户需要承受网络安全风险的时间非常有限，因此他们不愿意为此付费。而虽然 SoV 用户愿意支付高额交易费，因为他们暴露于网络安全风险的时间更长，但问题是他们很久才产生一次交易。

比特币的共识机制激励矿工去识别并验证最长的链以当作全网的最新状态。矿工持续投入的算力不只为最新的区块提供了安全性，也维护了之前所有区块的不可篡改性。仅靠 SoV 用户的一次性付款让矿工持续提供安全保障非长久之策。

而在 SoV 网络中，如果依靠通胀来为网络安全提供资金对矿工的激励更持久，对用户也更友好。基于通胀的区块奖励暗含用户间接地向安全提供者支付费用，并且费用多少与其享受安全服务的时间成正比。

3. 可保值和交易的智能合约平台

像以太坊这样的智能合约平台具有图灵完备的可编程性，可以支持更多的应用场景。原生代币通常用于为去中心化的计算服务定价和费用支付。与比特币网络一样，智能合约平台也具有资产保值和交易媒介的双重功能。它们与纯支付网络的不同之处在于，它们保存的价值不仅仅是它们自己的原生代币，还包括去中心化应用的内部状态，例如在 ERC20 智能合约里的加密资产。

另一个与支付网络的重大区别是智能合约平台上的交易更加「便携」。利用智能合约平台更高级的脚本优势来开发交互协议，能够更容易的将交易转移到更具成本效益的「交易为主」子链上，并安全地将数据安置回「纪录为主」主链。

智能合约平台的经济模型面临着类似支付网络的两极化趋势 - 由于其良好的交互能力，智能合约平台要么偏向「交易平台」，要么偏向「保值平台」。在经济上，这种分歧源自这样的事实：这两种「平台」具有不同的系统资源利用方式，处理交易消耗的计算和带宽是瞬时的，而且这两种资源是可再生的，但是保值却需

要长期占用全球共识状态。所以，为其中一个方向而设计优化的经济模型不太可能适用于另一个方向。

有竞争力的交易平台需要优先考虑降低交易成本。MoE 用户可以接受不太理想的安全性，因为他们只在有限的时间内暴露在危险之中。他们可以接受交易审查的可能性，大不了去其他地方进行交易。致力于提高安全性或抗审查性的交易平台将付出更高的交易成本，这将导致更高的交易费或者在“stake for access”模型中付出更高的资金成本，这都会使得这个交易网络的竞争力下降。

尤其是在设计良好的跨链协议可以允许无信任的状态转移与抗交易作恶时，这样的状况就更明显。我们已经可以看到很多的例子反映了 MoE 用户会优先考虑低成本的手续费而不是更高的安全性，他们往往选择在中心化的交易所和没那么去中心化的区块链上交易。而由于交易效率的原因，尽管它们缺点重重但仍然很受欢迎。

但是，有竞争力的保值平台需要具有可持续的安全性和抗审查性。因此需要设计一种不是基于即时交易而是基于对世界状态的占用而设计的经济模型，并且让用户为网络基础设施的关键资源的消耗付费。

4. 资产存储

智能合约平台最重要的用例之一是发行代币来代表资产的所有权。这些加密资产可以拥有自己的社区和市场，其价值与平台代币的价值是独立的。在另一方面，这些资产依赖于平台来处理交易并提供安全性。像比特币这样的支付网络可以被视为单一资产平台，而智能合约平台则是多资产平台。与比特币背景下的「价值存储 (SoV)」概念类似，我们称智能合约平台的功能是可以保留其加密资产「资产存储 (SoA)」的价值。

以保存资产为重点的智能合约平台，必须具有「资产存储」的代币经济设计。平台安全级别必须与平台上加密资产的价值一起增长。否则随着平台上加密资产价值的增长，因为攻击的利益也会增长，平台本身遭到「双花攻击」的可能性会大大增加。

目前的智能合约平台都不是为了「资产存储」平台而设计的。这些平台的代币经济学旨在促进交易（例如，以太坊的原生代币用于支付去中心化计算的费用）或满足权益证明的要求。在任何一种情况下，资产价值的增长并不一定会提高矿工的收入，而事实

是只有确保矿工的持续高收入才能激励矿工持续投入，从而使得平台获得更多的安全保障。

每个多资产平台都是独立的生态系统。平台的安全性可被视为有益于所有项目的「公用物品」。为了从安全的角度使得生态系统可持续发展，必须有一个明确的机制，即该平台需要能够捕捉到平台上生态系统的成功，以同时提高其自身的安全级别。换句话说，「资产存储」平台必须能将对加密资产的需求转化为其矿工的收入，通常是通过提高对矿工的补偿，让其获得额外的原生代币。

否则，平台的安全级别会成为加密资产价值的上限。当资产价值上升，平台不再能够充分保护在平台上典型的交易时，流动性就会枯竭，对资产的需求也会减少。

去中心化的多资产智能合约平台必须持续的做好「资产存储」的功能。

5. 去中心化与状态限制的需求

与其他长期价值存储的系统一样，「资产存储」平台必须保持中立，并且确保没有审查和充公的风险。这些条件使得黄金成为世界上数千年来最受欢迎的价值存储。对于完全开放无须许可的区块链网络，抗审查的能力主要来自于最广泛的全球共识，并且让全节点参与的门槛足够的低。与支付网络相比，智能合约平台运行全节点需要更密集的资源，因此，「资产存储」平台必须采取措施来保持全节点的运营成本，以保持网络有足够的去中心化。

比特币和以太坊都限制了交易吞吐量以确保参与方不仅只有「超级计算机」 - 比特币限制带宽，以太网限制计算能力。然而，他们没有采取有效的方式，来容纳共识参与和交易验证所需的不断增长的全局状态。尤其是整个智能合约平台有着高度集中的需求，全局状态的增长速度只会更快。

在比特币中，全局状态是 UTXO 的集合。比特币不会直接控制 UTXO 大小的增长，但每个新增的 UTXO 都会增加交易费用，使交易成本变得更高。

在以太坊中，全局状态由 EVM 的状态树来表示，该状态是包含所有帐户的余额和内部状态的数据结构。创建新帐户或新的智能合约值时，全局状态的大小就会增加。以太坊收取固定的 Gas 费用用于存入新的数据，并在移除数据时提供固定数量的 Gas 作为交易退款。以太坊的方法是朝着正确方向迈出的一步，但仍有几个问题：

- 全局状态的增长不受任何限制，并且可以无限增长，因此全节点的参与成本并不确定；
- 该系统为扩大状态存储提高了一次性收费，但矿工和全节点必须承担长期存储费用；
- 没有充分的理由说明为什么扩展存储的成本应该以固定数量的 Gas 定价（Gas 用于计算一个单位的计算费用）
- 「一次性支付，永远占用」的状态存储模型的激励很小，很难让用户自愿清除状态并减少全局状态的占用。

以太坊社区正在积极解决这个问题，主要的解决方案是收取智能合约的「状态租金」 - 合约必须根据其状态占用的大小来定期支付费用。如果没有支付租金，合同将会进入「休眠状态」，并且在支付租金之前无法访问。可以看出，这种方案也有几个难以解决的问题：

- 许多合约，特别是流行的 ERC20 合约，代表了去中心化的社区，并代表了许多用户的资产所有权。协调所有用户以公平并且有效率的方式支付租金是一个很难的问题；
- 即使一个合约的租金是已支付的状态，它仍然可能无法运作顺利，因为其他需要调用的合约可能会拖欠租金；
- 使用状态租赁合约的用户体验并不理想。

我们认为，一个精心设计的状态存储机制必须能够实现以下目标：

- 必须限制全局状态的增长，以便为参与全节点提供可预测性。理想情况下，成本能控制在非专业参与者可以负担的范围内，以保持网络最大程度的去中心化与抗审查；
- 随着全局状态的有限增长，价格的上升与降低将由市场决定。特别是当状态存储空间快满的时后，需要将状态存储的成本提高，而当它大部分为空时，需要降低成本，这是非常吸引人的；
- 系统需要能够不断收取其状态用户的租金，以支付矿工提供这种资源。这有助于平衡矿工的经济收入，同时激励用户尽早清除不必要的状态。

就像比特币如何限制带宽，以及以太坊限制计算的定价，来保持区块链网络长期去中心化和可持续，我们必须提出一种对于全局

状态的约束与定价方法。对于以保护资产为重点的「资产存储」平台来说，这是特别重要的，因为这种平台关心的不是大部分将发生在链下的交易，而是持续占用全局状态的存储成本。

6. Nervos CKB 的经济模型

Nervos Common Knowledge Base (简称 Nervos CKB) 是一个以保存价值为重点的「资产存储」区块链。在架构上, 是为了要最好地支持链上的状态和链外计算。在经济上, 是为了要提供可持续的安全性和去中心化。 Nervos CKB 是整个网络的基础层。

6.1 原生代币

Nervos CKB 的原生代币是「Common Knowledge Byte」, 简称「CK Byte」。CK Byte 代表 Cell 空间, 它们让拥有者能够占用区块链的全局状态。例如, 如果 Alice 拥有 1000 个 CK Bytes, 她可以创建一个空间为 1000 Bytes 的 Cell, 或者空间合计最多为 1000 Bytes 的多个 Cell。她可以使用 1000 个 Bytes 来存储资产、应用程序状态或是其他类型的数据资料。

一个 Cell 中已占用的空间可以等于或者小于这个空间被指定的大小。比如说, 一个空间为 1000 Bytes 的 Cell, 4 个 Bytes 用于表示它所能使用的容量, 64 个 Bytes 用于锁定脚本, 128

个 Bytes 用于存储状态。也就是说，这个 Cell 目前已被占用的容量是 196 个 Bytes，但它还有足够的空间，最多可以使用到 1000 个 Bytes。

6.2 代币发行政策

有两种类型的原生代币发行政策。「基础发行」的总供给量有限，发行时间表与比特币类似 - 基础发行数量大约每 4 年减半一次，直到所有「基础发行」的代币被挖出来。所有「基础发行」代币都会奖励给矿工，作为保护网络的激励措施。

「二级发行」的设计则是为了收取状态租金，每年的发行数量是不变的。「基础发行」停止后，「二级发行」仍会继续。

6.3 收取二级发行的状态租金和 NervosDAO 设计

由于原生代币代表了占用全局状态的权利，所以代币发行政策会限制状态的增长。由于状态存储受限制并且成为了稀缺资源，就好比比特币的带宽和以太坊的计算吞吐量，它们可以在市场上被定价和交易。状态租金在状态占用的费用结构上，增加了必要的时间维度。我们采用两个步骤作为「目标通胀」框架来收取这笔租金，而不是强制定期收取租金：

- 在「基础发行」的基础上，我们添加了「二级发行」，可以将其视为对所有代币持有者的「通胀税」。对于使用 CK Byte 存储状态的用户，这种定期的通胀税是他们向矿工支付状态租金的方式。
- 然而，由于我们对于那些没有使用 CK Byte 存储状态的所有者也收取了租金，所以我们需要将租金归还。我们允许这些用户将他们的原生代币存入并锁定到一个特殊合约中，我们称它为 NervosDAO。NervosDAO 将接受部分「二级发行」的补偿，以弥补因为不公平造成的稀释。

假设在「二级发行」时，所有 CK Byte 的 60% 用于存储状态，所有 CK Byte 的 35% 被存放并锁定在 NervosDAO 的合约中，剩下的 CK Byte 中的 5% 保持流动性。那每次进行「二级发行」出块奖励的时候，60% 的「二级发行」会奖励给矿工，35% 的会进入 NervosDAO 按比例分配给锁定的代币（用户），最后剩下的 5% 既没有占用也没有锁币的部分，将交由社群订定的治理机制处理；在社群未达到机制的共识之前，这部分的「二级发行」将会烧毁。

对于长期代币的持有者，只要他们将代币锁定在 NervosDAO 合约中，「二级发行」的通胀效应只是名义上的。对他们而言，

就像「二级发行」不存在一样，他们持有的代币，就会像比特币这样有硬顶的设计。

6.4 矿工补贴

矿工会获得两种出块奖励和交易手续费。他们将会收到所有的「基础发行」，以及部分的「二级发行」。长期来看，当「基础发行」停止后，矿工仍然可以获得状态租赁的收入。

6.5 交易手续费支付

去中心化区块链网络的交易吞吐量是有限的，其资源是受到限制的。交易手续费有两个目的，一个是为了有限的交易吞吐量建立一个市场，另一个则是防止恶意大量攻击。在比特币中，交易手续费表现在输出和输入之间的差异，而在以太坊中，处理交易需要矿工执行无法有效估算的计算，因此交易手续费表现为计算的单位成本或「gas price」。以太坊交易包括 gas price 和 gas limit 的属性，实际交易费用是 gasPrice 乘以使用的 gas 量，但不会超过上限的 gasLimit。

为了确保去中心化，Nervos CKB 限制了计算和带宽的吞吐量，当用户要使用这些系统资源时，它可以有效地成为一个拍卖市场。

当用户提交交易时，提交的总输入需超过总输出的 Cell，将其差值作为以原生代币来支付的交易费用，支付给打包交易的出块矿工。

计算的单位数量(计算循环数)也需要作为交易的一部分来提交。Nervos CKB 是一种「链下计算，链上验证」的平台，因此提交交易的客户端知道计算循环数。在出块时，矿工根据交易费用和交易验证所需的计算循环来排序每笔交易，以在有限的计算和带宽吞吐量下，最大化每一个计算循环数的收入。

在 Nervos CKB 中，手续费的支付可以透过原生代币、「用户自定义代币」，或是两者结合使用。

6.6 使用「用户自定义代币 UDT」支付交易手续费

用户还可以自由地发行其他代币，例如稳定币，用来支付交易费用，这个概念是一种「经济抽象」。即使没有明确的协议支持，用户总是可以与矿工自行安排使用在协议之外的代币支付交易手续费。这通常被许多平台视为一种威胁 - 如果平台的原生代币纯粹是为了促进交易，这将剥夺其系统的内在价值，并进一步导致崩溃。

通过 Nervos CKB, 我们拥抱经济抽象以及其带来的好处。由于原生代币的内在价值不是基于支付手续费的, 因此经济抽象不会让我们的经济模型造成威胁。然而, 我们确实希望原生代币将成为绝大多数用户和应用的的首选支付方式 - 原生代币将会成为 Nervos 生态系统中最广泛持有的代币, 因为每个拥有资产的人都必须拥有 Nervos 的原生代币, 原生代币对应的是状态的存储空间, 因为资产本身也占有了一定的存储空间。

更多的手续费分析详见附件 1。

7. 用于保存价值的经济模型

Nervos CKB 的经济模型专门设计用于保存资产以及各种类型通用知识数据的价值。让我们回顾 3 个重要的经济模型设计目标，并在此背景下检查我们的设计：

- 经济模型如何确保协议的安全性？
- 经济模式如何确保协议的长期可持续性？
- 经济模型如何让不同参与者拥有共同的目标，以促进整个网络的价值？

7.1 协议的安全性和可持续性

为了确保 Nervos CKB 成为「资产存储」协议，并且保障协议的安全性，我们选择的主要设计是：

- 我们的原生代币代表相应状态存储空间的主张权。这意味着，如果想在平台上通过状态空间持有资产，必须拥有对应状态空间的原生代币。因此，在平台上持有资产，直接创造了原生代币的需求。通过对资产的价值保存，原生代币打造

出有效的价值捕获机制。正是这种机制，「资产存储」平台可以随着时间的推移持续增加安全预算，而不是基于投机和利他主义。

- 二级发行可以保证矿工的补偿是可预测的，并且是基于价值保存的需求，而不是交易的需求。同时，二级发行也消除如中本聪协议的共识节点在出块奖励停止后，潜在的激励矛盾问题。对于「二级发行」造成的通胀效应，NervosDAO提供对应的反制力量，确保代币长期持有者的代币价值不会因为「二级发行」而被稀释。

为了保持网络的去中心化和抗审查能力，我们认为降低参与共识以及成为主节点所需要的资源门槛是非常重要的。我们通过调节计算和带宽的吞吐量来保护节点的运营成本，类似于比特币和以太坊的实现方式。甚至，我们透过「总量管制」的定价框架，与基于存储用户成本模型的机会成本这两种方式的结合，进行了状态存储的管制。

7.2 让网络中每一类参与者的利益一致

在传统的智能合约平台中，网络参与者有着不同的意图 - 用户希望更加低廉的交易手续费，开发者希望自己的应用可以得到广泛使用，矿工们希望获取更高额的收入，持有者希望持有的代币

可以增值。每一类参与者的利益并不是完全一致的，甚至，各自的利益诉求可能发生冲突 - 例如，广泛的应用使用不可能让交易变得低廉（相反，随着区块链的使用需求增加，交易应该更加昂贵）；更加低廉的交易也不会给矿工增加收入；高涨的代币价格对于交易的成本也没有任何帮助（倘若用户不调整其本地交易费用的设置，则可能发生相反的情况）。去中心化计算平台通过处理交易提供价值，基于这类平台的代币价格并不会实质性地改变整个网络的内在价值。例如，以太币（Ether）的价格翻倍并不会增加或减少以太坊（Ethereum）作为去中心化计算平台的内在价值。假设 gasPrice 没有发生变化，用户在整个网络上可以用同样的成本完成相同的任务。如此一来，以太坊的代币持有者仅仅扮演了投资者的角色，而不是积极的贡献者。

在 Nervos CKB 中，存储资产的用户希望其资产安全；开发者希望(其产品)得到更多地使用，并与之相应，保存更多的资产价值；矿工们希望获得更高的收入，而代币持有者希望他们的代币价格升值。更高的代币价格支撑着每个人的利益 - 网络变得更加安全，矿工得到更高额的收入，代币持有者得到更丰厚的回报。梳理齐整所有参与者的激励，将使得全网可以最好地利用网络效应来增强其内在价值。此外，这也会培养出一个更具凝聚力的社区，使得整个 Nervos 系统面临更少的治理挑战。

7.3 引导网络效应和网络增长

随着网络的发展，更多资产和通用知识的价值得到安全地保障，相应地，更多对应存储空间的 Nervos CKB 原生代币将被占用。这样，原生代币的流通量和供应量将被减少，同时，其市场价格会获得有效地支撑，进而，CKB 的价值得到增加。更高的代币价格和二级发行增加的收益份额，可以激励矿工扩大规模，并确保网络更加安全，同时，也增加整个网络和原生代币的内在价值，吸引更多丰富和更高价值的资产存储使用场景。

网络对顺向循环的使用以及其内在的价值，为其本身提供了强大的增长引擎。随着网络通过各种方式积累原生代币的价值，并由长期持有者获取对应的价值，网络中的原生代币会成为价值存储的绝佳候选者。与比特币作为货币存储价值相比，Nervos CKB 同样设计为安全且长期去中心化的。我们相信 Nervos CKB 拥有比比特币更加平衡和可持续的经济模型，并且具有保护加密资产及通用知识价值的本质功能。

7.4 开发者在「一级资产」平台中的成本

在以太坊中，顶层的抽象是账户。智能合约账户拥有资产所代表的状态。在 Nervos CKB 中，资产是 Cell 顶层的抽象，其所

有权由交易输出的锁定脚本来表示, 这个概念称为「第一级资产」。换句话说, 就像比特币一样, CKB 中的资产由用户直接拥有, 而不是在智能合约中被保管。

「第一级资产」的设计允许开发者可以不用拥有资产, 以及负担状态存储的成本, 而是由具体独立的用户承担。举例而言, 开发人员使用 400 CK Bytes 的代码, 创建了一个用户自定义代币的验证规则, 每个资产所有权的记录都将占用 64 个字节。即使资产拥有 10,000 个所有者, 开发人员仍然只需要使用 400 CK Bytes。

对于开发者而言, 我们预计即使在原生代币价格上升幅度较大的情况下, 在 CKB 上构建项目的成本也是适中的。对于用户来说, 即使平台在被大幅度采用的假设下, 64 CK Bytes 在 Nervos CKB 上的拥有成本也很低。

在未来这些开发成本或拥有成本变得非常昂贵的情况下, 开发者仍然可以依靠租赁来启动他们的项目, 用户可以在愿意采取取舍的情况下, 将 CKB 上面的资产转移到 Nervos Network 中的其他交易型区块链。相关信息请参考「7.6 Nervos Network」部分。

7.5 租赁

实际上 Nervos CKB 也将支持原生代币的租赁，以改善 CK Bytes 的流动性，这归功于 CKB-VM 和 Cell 模型提供的编程能力。由于原生代币的功能是通过空间占用而不是交易来实现的，因此，可以在已知的一定时间内锁定 CK Bytes 进行无风险的无担保借贷。开发者可以在 6 个月这样的时间内，以较低的资金成本借入他们需要的 CK Bytes 来完成产品原型并证明他们的商业模式。长期的代币持有者也可以出租他们的代币来赚取额外收入。

租赁的实际利率由市场供求决定，但代币的占用状况也有著重要的影响。如果全局状态利用率高，代表可用于贷款的代币就更少了。这将使得租赁利率更高，在 NervosDAO 合约中释放状态，锁定代币以获得收入，变得更具吸引力。这有助于减少全局状态。而较低的全局状态利用率代表着有更多的代币可以出租。这将使得贷款利率降低以鼓励使用。

7.6 Nervos Network

Nervos CKB 是 Nervos Network 的基础层，具有最高级别的安全性，去中心化，交易成本和状态存储成本。正如比特币和以

以太坊可以通过 lightning network 和 plasma 方案来进行链下扩容，Nervos CKB 同样拥有链下扩容解决方案，并允许用户在链下保存和交易资产。当使用链下解决方案时，用户和开发者可以在成本、安全性、延迟和活跃度之间做出权衡。

在 Nervos CKB 上持有资产和交易资产需要最高的资本和交易成本，但这也是最安全的。这最适合于高价值资产和长期资产的存储用途。第 2 层解决方案可以为交易吞吐量和状态存储提供扩展，但它们会带有相对较弱的安全性证明，或者会要求额外的强制步骤，而且通常会要求参与者在一定的时间范围内在线。如果这两者都可以接受（可能用于短期持有和交易低价值资产），Nervos CKB 可以被用作其他交易型区块链的安全之锚，以有效地放大其交易量和状态存储空间。

假如交易型区块链的系统不希望引入额外的安全性证明，它们可以要求在 CKB 上发行高价值的资产，而在交易型区块链上面发行低价值的资产。然后，他们可以在 CKB 上使用 CK Bytes 来存储周期性的区块提交，带着交易型区块链的挑战和证明 - 这是链下交易安全的关键常识。如果交易型链不介意使用基于委员会的共识协议，引入额外的安全性证明层，他们也可以让他们的验证节点在 CKB 上绑定 CK Bytes 以明确地调整安全性的参数。

8. 代币经济学的应用

Nervos CKB 的经济模型提供 App 开发者可以直接使用的构建模块，作为开发者特有经济模型的一部分。下面，我们列举订阅模型和流动性收入模型两个可能的构建模块。

8.1 订阅模型

在很长时间内，定期性支付或订阅是区块链提供服务的典型经济模型。相关的例子如，第 2 层解决方案经常需要的链下交易监控服务。基于 Nervos CKB 的订阅模型，一定时间内服务的提供商可以要求其用户在 NervosDAO 中锁定一定数量的原生代币，并将服务提供商指定为 NervosDAO 生成的利息收入受益者。再者，通过从 NervosDAO 撤回代币，用户也可以停止使用相应的服务。

实际上，占用全局状态的资产存储用户可以视为根据其状态的存储规模，支付持续订阅的费用，当然，受益人是提供安全服务的矿工。

8.2 流动性收入模型

在类似于 Plasma 的第 2 层解决方案中,典型的模式是用户在第 1 层区块链的智能合约中抵押原生代币,换取第 2 层上的交易代币。对于信誉足够的第 2 层运营商,他们可以接受用户提交的固定时限内的资产抵押,然后使用这些抵押的资产进行贷款,为借贷市场提供流动性和赚取收入。这样,第 2 层解决方案的运营商除了在第 2 层收取的费用之外,也拥有额外的收入方式。

9. 附件 1：交易成本分析

Nervos CKB 采用的是基于中本聪共识的工作量证明 (PoW) 共识机制，这一点上类似于比特币。欲了解更多关于 Nervos CKB 共识机制的细节，请参阅“Nervos Consensus Paper”。

达成共识的经济学设计，不仅旨在激励所有参与达成共识过程的节点，而且，也向节点提供用来确认交易优先级的衡量标准。设计的核心，在于帮助共识节点回答一个问题：“如果有机会生产下一个区块，这笔交易值不值得加入这个区块？”

为了回答这个问题，出块节点可以进行一个成本/收益分析。在下一个区块中加入一笔交易能够获得的收益，就是该笔交易的转账手续费。而把这笔交易加入区块中，需要付出的成本主要包含以下三个部分：

- **手续费估算成本 (FEC)**：节点在将待定交易加入下一个区块的过程中，评估具体打包哪一笔待定交易可以获得最大收入对应的估算成本。

- 交易验证成本 (TVC): 包含无效交易的区块, 将会被共识处理过程拒绝, 因此, 出块节点在将待定交易加入新块之前, 必须验证每笔交易。
- 状态转换成本 (STC) : 在一个新块生成后, 出块节点必须根据该区块包含的所有交易内容, 通过状态机完成本地状态转换。

特别的, 在转账验证中, TVC 可能包含以下两个步骤:

- V_{auth} : 授权验证成本
- V_{st} : 状态转换验证成本

我们采用 CPC 和 EVC 来表示完整处理成本和估算验证成本:

- **CPC**: 完整处理成本
$$CPC = EVC + STC$$
- **EVC**: 估算及验证成本
$$EVC = FEC + TVC$$

9.1 比特币的交易成本分析

比特币通过 Bitcoin Script (比特币脚本) 完成灵活的授权验证。用户在构建交易时, 可以通过 scriptPubKey 编写授权规则, 创建智能合约。比特币拥有固定的状态转换语句, 亦即基于通常所说的 UTXO 模型, 实现状态转换的花费和创建新 UTXO 语句。在比特币中, 状态转换的结果已经被包含在交易里, 因此, 状态转换成本 (STC) 为 0。

比特币通过输入和输出之间的金额差异来表示该笔交易的交易手续费。因此, 手续费估算成本记为 $O(N_{IO})$, 其中 N_{IO} 是输入和输出的总数量。

比特币的授权验证要求运行所有输入的脚本。由于比特币脚本禁止跳转和循环, 所以, 计算复杂度可以通过输入脚本的总长度 $O(N_I \cdot L_{script})$ 进行估算, 其中 N_I 是输入的数量, L_{script} 是每个输入的平均脚本长度。因此, 总的授权验证成本 V_{auth} 可以粗略地通过全部交易的大小 $O(N_I \cdot L_{script})$ 进行估算。

比特币的状态转换规则十分简单, 节点仅仅需要验证输入的总数与输出的总数是否相等即可。因此, 比特币的状态转换验证成本 V_{st} 和 **FEC** 一样, 约等于 $O(N_{IO})$ 。

综上, 比特币处理交易的总成本可以通过交易的大小进行粗略计算:

$$\begin{aligned}CPC_{btc} &= EVC_{btc} = FEC_{btc} + V_{auth} + V_{st} \\ &= O(N_{IO}) + O(N_I \cdot L_{script}) + O(N_{IO}) \approx O(L_{tx})\end{aligned}$$

9.2 以太坊的交易成本分析

以太坊具有图灵完备的脚本语言，允许用户灵活地通过智能合约自定义状态转换规则。以太坊的转账交易包含 Gas Limit 和 Gas Price，交易手续费由这两者的乘积计算得出。因此， $O(FEC_{eth})$ 等于 $O(1)$ 。

与比特币不同，以太坊的转账交易只包括状态转换的计算命令，而不包含状态转换的结果。因此，以太坊的交易验证仅限于授权验证，而没有状态转换验证。以太坊的授权验证规则如下：

- 验证 Secp256k1 签名的有效性，计算复杂度为 $O(L_{tx})$ ；
- 验证开启交易的账户和交易之间的 nonce 是否一致，计算复杂度为 $O(1)$ ；
- 验证开启交易的账户是否有足够的余额支付转账手续费和转账金额。这需要访问账户的当前余额。忽略全局状态大小对账户访问的影响，我们可以假定这个步骤的复杂度也是 $O(1)$ 。

综上所述，以太坊总的授权验证复杂度为 $O(L_{tx})$ 。

由于交易数据的每个字节都有成本($G_{txdata*}$), L_{tx} 越大, 需要的 gas 越多, 但是最多不能超过给定的 Gas Limit(G_{limit}), 因此:

$$G_{txdata*} \cdot L_{tx} \leq G_{limit}$$

以太坊拥有图灵完备的虚拟机, 其状态结果的计算可以包括任何复杂逻辑。以太坊交易中的 Gas Limit 是进行计算的上限, 因此 $STC_{eth} = O(G_{limit})$ 。综上所述:

$$TVC_{eth} = O(L_{tx}) + 0 = O(L_{tx})$$

$$EVC_{eth} = O(1) + O(L_{tx}) \approx O(L_{tx})$$

$$CPC_{eth} = O(1) + O\left(\frac{G_{limit}}{G_{txdata*}}\right) + O(G_{limit}) \approx O(G_{limit})$$

不同于比特币, 以太坊节点的 **EVC** 小于 **CPC**。这是因为, 以太坊节点只在交易被包含进入区块之后, 才会计算状态结果。另外, 这也是以太坊中交易结果可能无效的原因 (比如出现合约调用异常或者计算超出 Gas Limit), 而比特币区块链则只会包含成功执行的交易以及有效的结果。

9.3 Nervos CKB 的交易成本分析

Nervos CKB 交易亦是由输入和输出组成, 类似于比特币。因此, Nervos CKB 的 **FEC** 和 **STC** 与比特币相同:

$$FEC_{ckb} = O(N_{IO})$$

$$STC_{ckb} = 0$$

因为在 Nervos CKB 交易的输出中包含交易结果，因此：

$$EVC_{ckb} = CPC_{ckb} = FEC_{ckb} + TVC_{ckb}$$

9.4 Cycles 作为计算复杂度的度量单位

我们引入 cycles 作为 CKB 中计算复杂度的衡量单位，类似于以太坊中“Gas”的概念。Nervos CKB 的虚拟机是 RISC-V CPU 模拟器，因此，这里的 cycles 其实就是虚拟机中实际 CPU 工作的计算循环。执行一个指令所需的 cycles 数量，就是该指令的相对计算成本。在 Nervos CKB 中的交易，要求发送方指定验证该笔交易需要的 cycles 数量。节点可以选择和设置接受 cycles 数量的上限 $cyclemax$ ，进而只处理需要较少 cycles 数量的交易。此外，我们在区块中引入 cycles，其值等于所有指定交易的 cycles 总和。区块中的 cycles 值不能超过 $blockcyclemax$ 的值。这些值会进行初始化设置，并且由系统进行自动调整。

网络中各个节点可以将其 $cyclemax$ 设定为不同的值。 $cyclemax$ 影响的是一个「出块节点」如何接受新的「待定交易」，而非影响一个节点如何接受新块中已包含的交易，因此，它并不会导致区块验证的不一致。有效的区块要求有效的工作量证明，正因如

此，出块节点不大可能接受一个具有很高 cycles 值，但却是无效的转帐交易。

下表显示了比特币、以太坊和 Nervos CKB 在运行时的差异：

	Authorization (V_{auth})	State Validation (V_{st})	State Transition (ST)
Bitcoin	Generalized	Fixed	None
Ethereum	Fixed	None	Generalized
CKB	Generalized	Generalized	None

下表是比特币、以太坊和 Nervos CKB 在达成共识过程中不同部分的计算复杂性总结 (C_{limit} 指 cycles 上限)

	FEC	TCV	RSC	EVC	CPC
Bitcoin	$O(N_{IO})$	$O(L_{tx})$	0	$O(L_{tx})$	$O(L_{tx})$
Ethereum	$O(1)$	$O(L_{tx})$	$O(G_{limit})$	$O(L_{tx})$	$O(G_{limit})$
CKB	$O(N_{IO})$	$O(C_{limit})$	0	$O(C_{limit})$	$O(C_{limit})$

10. 联系 Nervos



Website: <https://www.nervos.org>



Github: <https://github.com/nervosnetwork>



Blogs: <https://medium.com/nervosnetwork>



Twitter: <https://twitter.com/nervosnetwork>



Telegram: <http://t.me/nervosnetwork>



Forum: <https://talk.nervos.org>



Reddit: <https://www.reddit.com/r/NervosNetwork>