Neo (N3)
Neo Legacy
站点地图
Neo 介绍
Neo 白皮书
Neo 技术
Neo 节点
Neo 网络
智能合约开发
DApp 开发
Neo工具开发
交易所对接指南
开发参考

Improve this Doc
Send feedback

In this article

Neo 的设计目标：智能经济
数字资产
数字身份
智能合约
应用与生态
Neo 的管理模式
经济模型
分发机制
治理机制
Neo 的技术实现
共识机制：DBFT
智能合约体系：NeoContract
跨链互操作协议：NeoX
分布式存储协议：NeoFS
抗量子密码学机制：NeoQS
总结

Neo 白皮书

一种智能经济分布式网络

Neo 的设计目标：智能经济

Neo 是利用区块链技术和数字身份进行资产数字化，利用智能合约对数字资产进行自动化管理，实现 “智能经济” 的一种分布式网络。

数字资产

数字资产是以电子数据的形式存在的可编程控制的资产。用区块链技术实现资产数字化有去中心、去中介、免信任、可追溯、高度透明等特点。Neo 在底层支持多数字资产，用户可在 Neo 上自行注册登记资产，自由交易和流转，并且通过数字身份解决与实体资产的映射关系。用户通过合规的数字身份所注册登记的资产受到法律的保护。

Neo 中有两种形式的数字资产：全局资产和合约资产。全局资产能够被记录在系统空间，可以被所有智能合约和客户端所识别；合约资产被记录在智能合约的私有存储区中，需要兼容该智能合约的客户端才能识别。合约资产可以参照某种约定的标准，从而实现与多数客户端的兼容。

数字身份

数字身份是指以电子数据形式存在的个人、组织、事物的身份信息。目前较为成熟的数字身份体系是基于 PKI（Public Key Infrastructure）的 X.509 标准。在 Neo 中，我们将实现一套兼容 X.509 的数字身份标准。这套数字身份标准，除了兼容 X.509 的层级式的证书签发模式，还将支持 Web Of Trust 式的点对点的证书签发模式。并通过人脸、指纹、语音、短信等多因素认证实现签发阶段和使用阶段的真实身份比对。同时，还将使用区块链取代 OCSP 协议来管理、记录 X.509 的吊销证书列表 CRL。

智能合约

智能合约是 1994 年由密码学家尼克萨博（Nick Szabo）最先提出的理念，几乎与互联网同龄。根据 Nick Szabo 的定义：当一个预先编好的条件被触发时，智能合约执行相应的合同条款。区块链技术给我们带来了一个去中心化的，不可篡改的，高可靠性的系统，在这种环境下，智能合约才大有用武之地。Neo 具备独立的智能合约体系：NeoContract。

NeoContract 智能合约体系的最大特点是无缝对接现有的开发者生态。开发者无需学习新的编程语言，就能用 C#、Python、Java 等主流编程语言在熟悉的 IDE 环境（Visual Studio、Eclipse 等）中进行智能合约的开发、调试、编译。Neo 的通用轻量级虚拟机 NeoVM 具有高确定性、高并发性、高扩展性等优点。NeoContract 智能合约体系让全球百万级的开发者能够快速进行智能合约的开发。

应用与生态

生态是开源社区项目的生命力所在。为了实现智能经济网络的目标，Neo 将致力于发展开发者生态，提供成熟的开发工具，完善的开发文档，组织教育培训活动，提供资金支持。我们计划对以下基于 Neo 的应用与生态进行支持，并对完善与提升体验的设计给予奖励：

◆ **节点程序**

- 完整功能的 PC 全节点程序
- 更好体验的 PC 轻节点程序
- 提供不需要同步区块链的 Web / Android / iOS 客户端
- 硬件钱包

◆ **区块链浏览器**

◆ **SDK 开发工具包**

- 支持 Java / Kotlin、.NET C# / VB、JavaScript / Typescript、Python、Go

◆ **智能合约编译器与 IDE 插件**

- C# / VB.Net / F#，Visual Studio
- Java / Kotlin，Eclipse
- C / C++ / GO
- JavaScript / TypeScript
- Python / Ruby

◆ **去中心化应用**

- 智能基金
- AI 辅助的法律智能合约
- 网络社交
- 自动化代币流动性提供者
- 去中心化交易所
- 安全通讯协议
- 数据交易市场
- IP 交易市场
- 预测市场
- 广告市场
- 算力市场
- GAS 市场

Neo 的管理模式

经济模型

Neo 中内置两种原生代币，NEO（缩写符号 NEO）和 GAS（缩写符号 GAS）。

NEO 是管理代币，总量 1 亿份，用于实现对 Neo 网络的管理权。管理权包括投票进行共识节点选举，Neo 网络参数更改等。NEO 的最小单位为 1，不可再分割。

GAS 是燃料代币，最大总量上限为 1 亿，用于实现对 Neo 网络使用时的资源控制。Neo 网络对代币转账和智能合约的运行和存储进行收费，从而实现对共识节点的经济激励和防止资源滥用。GAS 的最小单位为 0.00000001。

在 Neo 网络的创世块里，1 亿份 NEO 已经生成，而 GAS 尚未生成，数量为零。1 亿份 NEO 所对应的 1 亿份 GAS，将通过一个衰减的算法在约 22 年的时间内逐步生成至 NEO 管理代币的地址中。NEO 管理代币转入新的地址后，之后的 GAS 也将在新的地址生成。

Neo 网络将通过投票设置一个阈值，对一定量的转账交易和智能合约运行存储免收 GAS，以提升使用体验。当发生大量垃圾交易时，可以通过 NeoID 来优先处理具有合格身份的交易和智能合约。没有合格数字身份的交易和智能合约可以通过支付 GAS 来获得优先处理。

分发机制

NEO 的分发：

NEO 的 1 亿管理代币分为两部分，第一部分 5000 万份 NEO 用于按轮次和比例分发给 Neo 开发经费众筹的支持者，该部分已经分发完毕。

第二部分 5000 万份由 Neo 理事会管理，用于支持 Neo 网络的长期开发、运维和生态发展。该部分的 NEO 处于锁定期，在 2017 年 10 月 16 日 Neo 网络运行达 1 年时方可解锁被使用。这部分 NEO 不会进入交易所交易，仅用于长期支持 Neo 项目，计划按如下比例分配使用：

◆ 1000 万份（总量 10%）用于激励 Neo 开发者和 Neo 理事会成员

◆ 1000 万份（总量 10%）用于激励 Neo 周边生态开发者

◆ 1500 万份（总量 15%）用于交叉投资其他区块链项目，所获得代币归属于 Neo 理事会，并仅用于 Neo 项目

◆ 1500 万份（总量 15%）机动使用

◆ 每年使用的 NEO 原则上不得超过 1500 万份

GAS 的分发：

GAS 伴随着每个新区块的生成而产生。GAS 初期总量为零，伴随着新区块的生成逐渐增多，直至约 22 年后达到总量上限 1 亿。Neo 每个区块的间隔时间约为 15-20 秒，200 万个区块约合 1 年时间。

第一年（实际为 0-200 万个区块），每个区块新生成 8 个 GAS；第二年（实际为第 200-400 万个区块），每个区块新生成 7 个 GAS；以此类推，每年递减 1 个 GAS，直至第 8 年递减至每个区块新生成 1 个 GAS；自此保持每个区块新生成 1 个 GAS 直至约 22 年后的第 4400 万个区块，GAS 总量到达 1 亿，则停止伴随新区块生成 GAS。

按照这样的发行曲线，第 1 年会有 16% 的 GAS 被创造，前 4 年会有 52% 的 GAS 被创造，前 12 年 80% 的 GAS 被创造。这些 GAS 都会按照 NEO 的持有比例，记录在对应的地址上。NEO 持有人可以在任意时间进行发起一笔认领交易，将这些 GAS 认领到 NEO 的地址上。

治理机制

链上治理：NEO 管理代币的持有人是 Neo 网络的所有者和管理者，通过在 Neo 网络上构造投票交易来实现管理权，通过获得 NEO 管理代币所对应的 GAS 代币来实现 Neo 网络的使用权。Neo 管理代币可以被转让。

链下治理：Neo 理事会是 Neo 项目的创始人组织成立的常务管理机构，下设管理委员会、技术委员会和秘书处，分别负责战略决策、技术决策和具体执行。Neo 理事会向 Neo 社区负责，以推广和发展 Neo 生态为首要工作目标。

Neo 的技术实现

共识机制：DBFT

DBFT 全称为 Delegated Byzantine Fault Tolerant，是一种通过代理投票来实现大规模节点参与共识的拜占庭容错型共识机制。NEO 管理代币的持有者通过投票，可以选出其所支持的共识节点。随后由被选出的共识节点通过 BFT 算法，来达成共识并生成新的区块。投票在 Neo 网络持续实时进行，而非按照固定任期。

DBFT 对由 n 个共识节点组成的共识系统，提供 $f=\lfloor (n-1)/3 \rfloor$ 的容错能力，这种容错能力同时包含安全性和可用性，可以抵抗一般性故障和拜占庭故障，并适用于任何网络环境。DBFT 具有良好的最终性，一个确认即最终确认，区块无法被分叉，交易也不会发生撤销或回滚。

在 Neo 的 DBFT 共识机制下，每 15~20 秒生成一个区块，交易吞吐量实测可达到约 1000 tps，在公有链中性能优秀。通过适当优化，有能力到达 10000 tps，可以支持大规模的商业化应用。

DBFT 结合数字身份技术，使得共识节点可以是实名的个人或机构。从而使得冻结、撤销、继承、找回、司法判决过户等非常规操作成为可能。这有利于合规性金融资产在 Neo 网络中的登记发行。Neo 网络计划在必要的时候支持此类操作。

智能合约体系：NeoContract

Neo 的智能合约体系由三部分组成：

NeoVM - 通用区块链虚拟机：

NeoVM 是一个轻量级的通用型虚拟机，其架构与 JVM 和 .NET Runtime 非常接近，类似于一个虚拟 CPU，负责读取并按顺序执行合约中的指令，根据指令的功能进行流程控制、算数运算、逻辑运算等。它具有良好的启动速度和通用性，非常适合应用于智能合约这种小程序，也可以被移植到非区块链的场景中，或者与 IDE 集成从而提供良好的开发体验。可以对 NeoVM 的功能进行扩展，引入 JIT（即时编译器）机制，从而提高指令的执行效率。

InteropService - 互操作服务：

用于加载区块链账本、数字资产、数字身份、持久化存储区等底层服务。它们就像是为虚拟机提供的虚拟设备，使得智能合约可以在运行时访问这些服务，从而实现一些高级功能。通过这种低耦合的设计， **NeoVM 可以被移植到任意区块链甚至非区块链系统中使用，使得智能合约的适用领域大大扩宽。**

DevPack - 编译器和 IDE 插件：

DevPack 包含高级语言编译器和 IDE 插件。由于 NeoVM 的架构与 JVM、.NET Runtime 等高度相似，这些 DevPack 里的编译器可以将 Java byte code 和 .NET MSIL 这类中间语言编译成 NeoVM 的指令集。Java / Kotlin、C#等主流语言的开发者不需要学习新的语言，在 VS、Eclipse 等熟悉的 IDE 环境中就能立即着手编写智能合约。 **这使得智能合约的学习成本大大降低，可以建立丰富的 NeoContract 智能合约生态。**

NeoContract 可以在运行智能合约之前，就通过静态分析来建立智能合约的调用树。通过确定性的调用树， **Neo 节点可以对智能合约进行动态分片，实现理论上无限的扩展** ，克服了其他区块链系统的静态分片导致的 “闹市拥堵效应”。

跨链互操作协议：NeoX

NeoX 是实现跨链互操作的协议。NeoX 分为两个部分：“跨链资产交换协议” 和 “跨链分布式事务协议”。

跨链资产交换协议：

NeoX 在已有的双链原子资产交换协议上进行了扩展，可以让多个参与者在不同的区块链上进行资产交换，并保证整个交易过程中的所有步骤全都成功或全都失败。为了实现这个功能，我们需要利用 NeoContract 的功能，为每一个参与者创建一个合约账户。对于其它的区块链，如果它不兼容 NeoContract，但是只要能够提供简单的智能合约功能，也能够与 NeoX 相兼容。

跨链分布式事务协议：

跨链分布式事务是指，事务的多个步骤分散在不同的区块链上执行，且保证整个事务的一致性。这是对跨链资产交换的一种扩展，将资产交换的行为扩展成任意行为。通俗的说，NeoX 使得跨链智能合约成为了可能，一个智能合约可以在多个不同的区块链上执行不同的部分，要么全部执行完毕，要么全部退回执行前的状态。这赋予了跨链协作极大的想象力，我们正在探索跨链智能合约的应用场景。

分布式存储协议：NeoFS

NeoFS 是一套利用了 Distributed Hash Table 技术的分布式存储协议。NeoFS 通过文件内容（Hash）而非文件路径（URI）来对数据进行索引。大文件将被分割为固定大小的数据块分布式地存储在众多节点中。

该类系统的主要问题是需要在冗余度和可靠性之间寻找平衡点。NeoFS 计划通过代币激励机制和建立骨干节点的方式来解决这一矛盾。用户可以选择文件的可靠性要求，低可靠性的文件可以免费或几乎免费的被存储和访问，高可靠性的文件将由骨干节点提供稳定可靠的服务。

NeoFS 将作为 NeoContract 体系下的 InteropService 互操作服务之一，使得智能合约可以在区块链上存放大型文件，并为这些文件设定访问权限。此外，NeoFS 可以与数字身份相结合，使记录数字身份的数字证书可以点对点签发、传送、吊销，而无需中心化服务器来管理。未来可以将陈旧的区块数据存放在 NeoFS 中，使得大部分的全节点可以释放旧数据，获得更高的扩展性，并保证历史数据的完整性。

抗量子密码学机制：NeoQS

量子计算机的出现将对基于 RSA 和 ECC 的密码学机制产生重大挑战。量子计算机能够在极短的时间内解决 RSA 所依赖的大数分解问题和 ECC 所依赖的椭圆曲线离散对数问题。NeoQS 是一种基于格的密码学机制，QS 是 Quantum Safe 的缩写。目前，量子计算机尚无快速解决最短向量问题（SVP）和最近向量问题（CVP）的能力，格密码学被认为是抵御量子计算机的最可靠算法。

总结

Neo 是一种结合数字资产、数字身份和智能合约的分布式网络。Neo 系统还将使用 DBFT、NeoX、NeoFS、NeoQS 等多项原创技术，成为未来智能经济的基础架构。

← Preveous 站点地图
Next NeoVM →