Neo N3 小程序平台

技术白皮书

版本 1.0
2025 年 12 月

基于 *Neo N3* 区块链构建安全、可扩展
去中心化小程序的综合基础设施

摘要

Neo N3 小程序平台代表了去中心化应用开发的范式转变，提供了一个综合基础设施，弥合了传统 Web2 用户体验与区块链技术安全保障之间的鸿沟。本白皮书介绍了该平台的技术架构、安全模型和运营框架，旨在使开发者能够在安全的沙箱环境中构建、部署和运营轻量级去中心化应用——即小程序（MiniApps）。通过利用基于 Intel SGX 技术的可信执行环境（TEE）和 MarbleRun 编排框架，平台确保密钥管理、交易签名和随机数生成等敏感操作在硬件保护的飞地中执行。平台强制执行严格的资产分离，规定所有支付操作使用 GAS 代币，治理活动使用 bNEO（Burger NEO）代币，从而确保合规性和利益相关者的一致性。凭借七个基础智能合约、六个基于 TEE 的服务，以及涵盖游戏、去中心化金融、社交互动和治理领域的二十三个生产就绪的内置应用，Neo N3 小程序平台为安全且易于访问的区块链应用开发树立了新标准。

Neo R3E Network
WhitePaper

目录

1 引言

1.1 去中心化应用的演进

自智能合约平台问世以来，区块链行业经历了显著增长，去中心化应用（dApps）已成为分布式账本技术的主要用例。然而，尽管技术取得了重大进步，区块链应用的普及仍受到用户体验、安全性和开发者可访问性等根本性挑战的制约。传统的 dApp 架构要求用户管理加密密钥、理解 Gas 机制并操作复杂的钱包界面——这些障碍历来将区块链的采用限制在技术精通的用户群体中。

Neo N3 小程序平台通过从根本上重新构想去中心化应用架构来应对这些挑战。平台不再向用户暴露区块链交互的底层复杂性，而是引入了小程序（MiniApps）的概念：在托管环境中运行的轻量级沙箱应用，其中安全性、密钥托管和交易管理由平台基础设施透明处理。

1.2 问题陈述

当代区块链应用开发面临着几个相互关联的挑战，阻碍了主流采用：

- **基础设施复杂性**：开发者不仅需要具备智能合约开发专业知识，还需掌握加密密钥管理、节点运营和分布式系统架构。
- **密钥管理安全漏洞**：用户难以安全地存储和管理私钥，导致整个行业遭受重大财务损失。
- **用户体验不足**：区块链应用的用户体验始终未能达到 Web2 标准，交易确认延迟、Gas 费用复杂性和钱包管理造成的摩擦阻碍了采用。
- **开发者准入门槛高**：需要学习专业编程语言、理解共识机制以及在碎片化的工具生态系统中导航，限制了能够构建区块链应用的人才库。

1.3 小程序范式

在本平台中，小程序被定义为在宿主环境中执行的轻量级沙箱应用，同时利用区块链基础设施进行结算、随机数生成和数据完整性保障。与需要用户直接与区块链原语交互的传统 dApp 不同，小程序将这些复杂性抽象在熟悉的界面之后。用户通过标准的 Web 或移动界面与小程序交互，而平台代表他们管理钱包创建、密钥托管、交易签名和区块链交互。

这种架构方法带来了几个根本性优势：

- **简化用户体验**：用户受益于与传统应用相似的体验，无需理解区块链机制或管理加密密钥。
- **降低开发门槛**：开发者可以访问抽象了区块链复杂性的综合 SDK 和 API，无需专业的区块链知识即可快速开发应用。
- **硬件级安全**：平台通过硬件保护的执行环境确保安全性，将密钥管理的负担从用户和开发者身上移除。
- **即时部署**：小程序无需为前端逻辑部署链上合约即可实现即时部署，大大缩短了新应用的上市时间。

1.4 设计理念

Neo N3 小程序平台建立在四个基础原则之上，这些原则指导所有架构和实现决策：

1. **安全优先**：所有敏感操作——包括密钥生成、交易签名和随机数生成——在受 Intel SGX 硬件保护的可信执行环境中执行。
2. **开发者体验**：具有清晰、文档完善的 API 的综合 TypeScript SDK 使开发者无需区块链专业知识即可构建复杂应用。
3. **可扩展性**：账户池架构维护超过一万个预生成账户，以支持高吞吐量交易处理而不产生瓶颈。
4. **合规性**：强制执行 GAS 实用代币和 bNEO 治理代币之间的严格资产分离，确保平台在监管框架内运营，同时保持清晰的利益相关者激励。

2 平台架构

2.1 架构概述

Neo N3 小程序平台采用精心设计的多层架构，以实现安全性、可扩展性和开发者生产力。该架构由五个不同的层组成，每层服务于特定功能，同时与相邻层保持清晰的接口。跨层的关注点分离使得独立扩展、针对性安全加固和平台能力的模块化演进成为可能。

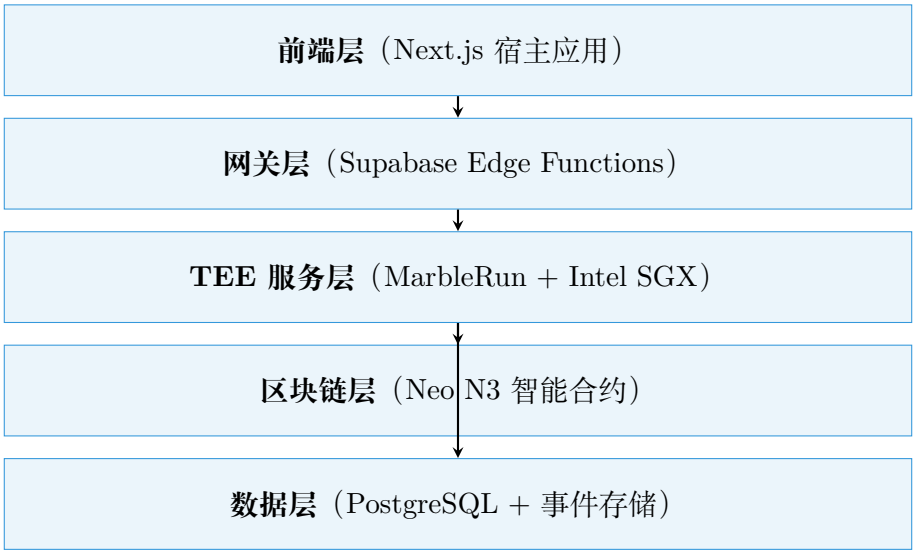

图 1: Neo N3 小程序平台架构

2.2 前端层

前端层作为用户与平台之间的主要接口，实现了一个作为小程序”应用商店”的宿主应用架构。该层基于 Next.js 构建并通过 Vercel 边缘网络部署，提供全球低延迟访问，同时在宿主应用和各个小程序之间保持严格的安全边界。

小程序隔离通过两种互补机制实现：

- **沙箱 iframe**：为了最大程度的安全性，小程序在具有限制性内容安全策略（CSP）的沙箱 iframe 中执行，防止跨域数据访问和脚本注入。
- **Module Federation**：对于需要更紧密集成的性能关键型应用，Webpack Module Federation 在保持逻辑分离的同时实现受控的代码共享。

宿主应用通过 Supabase Auth 管理认证状态，提供基于 OAuth 的用户引导，消除了初始注册时创建区块链特定钱包的需要。

前端层实现了一个桥接协议，使小程序与平台服务之间能够进行安全通信。该桥接器根据小程序声明的清单权限验证所有请求，确保应用不能超出其授权的能力范围。桥接器还管理用户会话的生命周期，处理令牌刷新、会话持久化以及网络连接中断时的优雅降级。

2.3 网关层

网关层作为 Supabase Edge Functions 实现，提供无状态的路由和验证层，调解前端层与后端服务之间的所有通信。该层在网络边缘执行，最小化延迟，同时无论用户地理位置如何都提供一致的安全执行。

认证和授权是网关层的主要职责：

- **JWT 验证**：每个请求都经过 JWT 验证以确认用户身份。
- **速率限制**：防止滥用并确保用户之间的公平资源分配。
- **清单验证**：根据发起小程序的清单验证所有请求，确保请求的操作在声明的权限和资源限制范围内。
- **资产策略执行**：对于支付操作，强制执行平台的 GAS-only 策略，在请求到达后端服务之前拒绝任何处理非 GAS 资产的尝试。

网关层与 TEE 服务之间的通信通过双向 TLS（mTLS）连接进行，确保只有经过认证的网关实例才能调用敏感的后端操作。这种架构防止了从外部网络直接访问 TEE 服务，将网关层确立为所有平台交互的强制安全检查点。

2.4 TEE 服务层

可信执行环境服务层代表了 Neo N3 小程序平台的安全基础，为所有敏感操作提供硬件保护的执行。该层通过 EGo 框架利用 Intel 软件保护扩展（SGX）技术，MarbleRun 提供跨飞地实例的编排、证明和安全密钥分发。

在该层内，六个专业服务处理不同类别的敏感操作：

- **NeoFeeds**：从多个外部来源聚合价格数据，在飞地内计算中位数以防止操纵。
- **NeoVRF**：使用飞地保护的签名密钥生成加密安全的随机数，可选择链上锚定以实现可验证随机性。
- **NeoOracle**：从白名单端点获取外部数据，使用 AES-GCM 加密安全注入密钥。
- **NeoCompute**：在飞地内执行受限的 JavaScript 代码，实现带加密输出的机密计算。
- **NeoFlow**：管理任务调度和自动化触发器，在链上锚定执行证明。
- **TxProxy**：处理交易构建和签名，在向 Neo N3 网络提交交易之前执行策略约束。

TEE 服务层内的密钥材料通过 SGX 密封绑定到特定的飞地测量值，确保即使特权系统软件也无法提取密钥。MarbleRun 的基于清单的配置定义了每个服务的预期测量值，在配置密钥之前启用远程证明以验证飞地完整性。

2.5 区块链层

区块链层由部署在 Neo N3 网络上的七个智能合约组成，提供平台规则的不可变执行，并作为所有金融和治理操作的最终权威。这些合约设计为最小复杂性以减少攻击面，同时为平台操作提供全面功能。

- **PaymentHub**：中央结算机制，处理所有 GAS 支付并在小程序开发者和平台国库之间分配收入。实施严格的资产验证，在合约级别拒绝任何非 GAS 代币。
- **Governance**：管理 bNEO 质押和提案投票，使代币持有者能够参与平台治理决策。

- **PriceFeed**：存储带有 TEE 证明签名的预言机价格数据，为 DeFi 应用提供链上价格参考。
- **RandomnessLog**：锚定由 NeoVRF 服务生成的可验证随机值，使游戏应用中使用的随机性能够在链上验证。
- **AppRegistry**：维护已批准小程序的注册表，存储清单哈希并管理授权应用的白名单。
- **AutomationAnchor**：记录来自 NeoFlow 服务的任务执行证明，为自动化操作提供防重放保护。
- **ServiceLayerGateway**：将链上服务请求路由到适当的 TEE 服务，使智能合约能够调用平台能力。

2.6 数据层

数据层提供持久存储和事件处理能力，支持平台操作和分析。PostgreSQL 通过 Supabase 托管服务作为主要数据存储，行级安全（RLS）策略确保用户和应用之间的数据隔离。

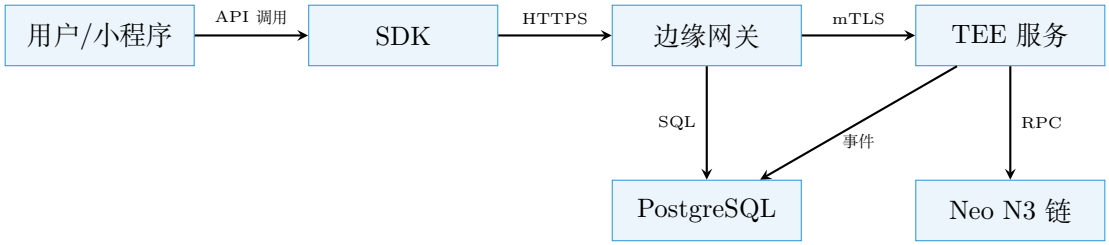

图 2: 平台数据流架构

3 安全模型

3.1 纵深防御架构

Neo N3 小程序平台实施纵深防御安全策略，在多个架构层建立冗余安全控制。这种方法确保任何单一层的妥协都不会导致完全的安全失败，因为后续层会维持独立的安全执行。每一层都实现独立的验证逻辑，确保一层的妥协不会自动传播到其他层。

表 1: 纵深防御安全层

层级	位置	主要功能	信任级别
第一层	客户端 SDK	输入验证、类型检查	不可信
第二层	边缘网关	认证、限流、模式验证	可信
第三层	TEE 服务	加密操作、业务逻辑	硬件保护
第四层	智能合约	不可变规则执行	区块链保护

3.2 资产分离与合规

平台强制执行 GAS 实用代币和 bNEO 治理代币之间的严格分离，这种分离在所有架构层得到执行：

- **支付操作**：专门使用 GAS 代币，PaymentHub 合约在合约级别拒绝任何非 GAS 资产。
- **治理活动**：需要 bNEO 代币，Governance 合约验证所有质押和投票操作仅涉及 bNEO。
- **多层执行**：SDK、网关和 TEE 服务都在请求到达区块链之前验证资产类型。

这种分离简化了监管合规，同时为利益相关者提供了关于平台处理资产的清晰保证。

3.3 可信执行环境安全

TEE 服务层利用 Intel SGX 技术提供硬件级安全保证：

- **密钥密封**：飞地内的密钥材料通过 SGX 密封绑定到特定的飞地测量值，确保即使特权系统软件也无法提取密钥。
- **远程证明**：MarbleRun 的基于清单的配置定义了每个服务的预期测量值，在配置密钥之前启用远程证明以验证飞地完整性。
- **侧信道防护**：在整个 TEE 服务中实施侧信道攻击缓解措施，包括常量时间操作和内存访问模式混淆。

3.4 账户池安全

账户池架构维护超过一万个预生成的 Neo N3 账户，实现高吞吐量交易处理：

- **密钥生成**：所有账户密钥在 TEE 飞地内生成，从不暴露给飞地外的任何软件。
- **账户锁定**：并发控制机制防止同一账户被多个操作同时使用。
- **密钥轮换**：定期密钥轮换确保长期安全性，旧密钥在轮换后安全销毁。

4 核心服务

表 2: TEE 服务概览

服务	功能	描述
NeoFeeds	价格数据	多源聚合，中位数计算，链上锚定
NeoVRF	随机数	可验证随机函数，签名证明
NeoOracle	外部数据	白名单端点，密钥注入
NeoCompute	机密计算	受限脚本执行，加密输出
NeoFlow	自动化	任务调度，事件触发
TxProxy	交易代理	签名广播，策略执行

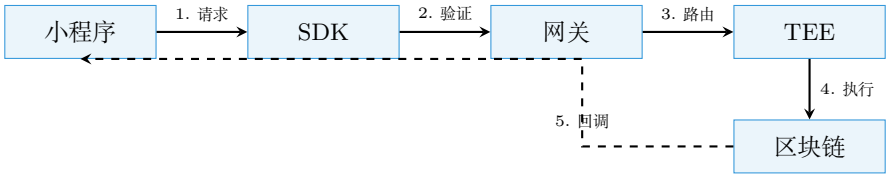

图 3: 服务请求工作流

4.1 NeoFeeds：实时价格数据聚合

NeoFeeds 服务解决了去中心化金融应用对可靠、抗操纵价格数据的关键需求。传统预言机解决方案面临单点故障、恶意来源的数据操纵以及价格更新延迟等挑战。NeoFeeds 通过在可信执行环境内进行多源聚合来缓解这些风险。

该服务持续从多个独立来源轮询价格数据，包括中心化交易所、去中心化交易所和专业数据提供商。在 SGX 飞地内，服务计算跨来源的中位数值，有效过滤异常值并防止任何单一来源操纵报告的价格。可配置的偏差阈值（默认为 0.1%）决定何时价格更新需要链上锚定，在数据新鲜度和交易成本之间取得平衡。

价格数据通过 PriceFeed 智能合约锚定在链上，附带 TEE 证明签名，使消费者能够验证数据真实性。这种架构确保即使外部数据源被攻破，飞地内的聚合逻辑也能提供抗操纵的弹性，而链上锚定则创建了历史价格的不可变记录。

4.2 NeoVRF：可验证随机函数服务

随机性是游戏、彩票和公平选择应用的基本原语，然而在确定性区块链环境中生成真正不可预测的随机值面临重大挑战。NeoVRF 服务通过在 TEE 内执行的可验证随机函数实现提供加密安全的随机性。

该服务使用飞地保护的签名密钥生成随机值，产生的输出在生成前不可预测，在生成后可验证。每个随机值都附带一个证明，使任何方都能验证输出是从输入种子和服务的公钥正确派生的，而不会泄露生成中使用的私钥。

对于需要链上可验证性的应用，NeoVRF 支持通过 RandomnessLog 合约进行可选锚定。这种锚定创建了生成随机值的不可变记录，使智能合约能够验证游戏结果或彩票抽奖中使用的随机性。每个随机值附带的证明哈希提供了该值在有效 TEE 实例内生成的加密证明。

4.3 NeoOracle：机密外部数据访问

许多区块链应用需要访问外部数据源,从参数保险的天气信息到预测市场的体育比分。NeoOracle 服务使安全获取外部数据成为可能，同时保护敏感凭证和 API 密钥不被暴露。

该服务维护一个已批准 HTTP 端点的白名单，防止可能被利用于恶意目的的任意网络访问。在获取数据时，服务可以使用 AES-GCM 加密注入密钥（如 API 密钥或认证令牌），确保凭证永远不会暴露在飞地之外。每个密钥的权限执行确保每个小程序只能访问明确授予它的密钥。

通过 NeoOracle 获取的数据在返回给请求应用之前在飞地内处理。这种处理可以包括解析、验证和转换，确保应用接收到干净、结构化的数据。飞地的隔离保证即使特权系统管理员也无法提取敏感凭证。

4.4 NeoCompute：机密代码执行

某些应用逻辑需要通过链上执行无法实现的机密性保证，因为链上所有计算都是公开可见的。NeoCompute 服务使在 TEE 内执行受限 JavaScript 代码成为可能，为敏感业务逻辑提供机密计算能力。

该服务接受 JavaScript 代码和输入参数，在飞地内的沙箱环境中执行代码。可配置的超时和资源限制防止通过资源耗尽进行的拒绝服务攻击。执行环境提供对加密原语和实用函数的访问，同时限制网络访问和文件系统操作。

计算输出使用从请求应用身份派生的密钥加密，确保结果只能由授权方解密。每个输出都包含来自飞地证明密钥的签名，使验证计算发生在有效 TEE 实例内成为可能。这种架构使应用能够实现机密业务逻辑——如密封投标拍卖或私有匹配算法——同时保持可验证性。

4.5 NeoFlow：工作流自动化与调度

区块链应用通常需要自动执行重复任务或对外部事件的触发响应。NeoFlow 服务提供工作流自动化能力，使小程序能够调度任务和定义触发器，而无需维护专用基础设施。

该服务支持基于 cron 的重复任务调度，使应用能够执行周期性操作，如每日结算、每周分配或每小时数据更新。基于价格的触发器实现响应式自动化，当资产价格越过定义的阈值时执行指定操作。所有计划执行都通过 AutomationAnchor 合约锚定在链上，提供防重放保护并创建自动化操作的可审计记录。

任务定义存储在 TEE 内，确保自动化逻辑不能被外部方观察或操纵。服务管理任务生命周期，包括创建、修改、暂停和删除，所有操作都根据请求应用的身份进行认证。

4.6 TxProxy：交易构建与签名

TxProxy 服务作为平台服务与 Neo N3 区块链之间的网关，处理交易构建、签名和提交。该服务实现平台的交易策略，确保所有区块链交互符合定义的约束。

在构建任何交易之前，TxProxy 根据多个策略层验证请求：

- **合约白名单**：确保交易只能与已批准的智能合约交互。
- **方法限制**：限制可以调用的合约方法。
- **金额限制**：限制单笔交易可以转移的价值。
- **意图门控**：对高价值或敏感操作要求明确的用户确认。

交易签名使用账户池中的密钥进行，密钥选择基于请求服务和操作类型。服务管理交易生命周期，包括 nonce 管理、费用估算、提交和确认监控。失败的交易会自动使用调整后的参数重试，而持续失败会报告给请求服务以进行适当处理。

5 智能合约基础设施

Neo N3 小程序平台的区块链层由七个精心设计的智能合约组成，提供平台规则的不可变执行，并作为所有金融和治理操作的权威真相来源。这些合约使用 Neo N3 智能合约框架以 C# 实现，利用平台对复杂数据结构和高效执行的原生支持。

表 3: 平台智能合约

合约	资产策略	主要功能
PaymentHub	仅 GAS	支付结算和收益分配
Governance	仅 bNEO	质押、提案和投票
PriceFeed	无	带 TEE 证明的预言机价格数据
RandomnessLog	无	VRF 随机数锚定
AppRegistry	无	小程序注册和白名单
AutomationAnchor	无	任务执行证明
ServiceLayerGateway	GAS（费用）	链上服务请求路由

表 4: 平台合约地址（Neo N3 测试网）

合约	脚本哈希
PaymentHub	`0x0bb8f09e6d3611bc5c8adbd79ff8af1e34f73193`
Governance	`0xc8f3bbe1c205c932aab00b28f7df99f9bc788a05`
PriceFeed	`0xc5d9117d255054489d1cf59b2c1d188c01bc9954`
RandomnessLog	`0x76dfee17f2f4b9fa8f32bd3f4da6406319ab7b39`
AppRegistry	`0x79d16bee03122e992bb80c478ad4ed405f33bc7f`
AutomationAnchor	`0x1c888d699ce76b0824028af310d90c3c18adeab5`
ServiceLayerGateway	`0x27b79cf631eff4b520dd9d95cd1425ec33025a53`

5.1 PaymentHub：中央结算机制

PaymentHub 合约作为所有 GAS 支付操作的中央结算机制：

- **支付处理**：处理用户向小程序的支付、小程序之间的结算。
- **收益分配**：70% 流向开发者，20% 归入国库，10% 分配给质押者。
- **资产验证**：在合约级别拒绝任何非 GAS 代币。
- **限额管理**：强制执行每笔交易和每日限额。

5.2 Governance：利益相关者参与

Governance 合约使用 bNEO 代币实现平台治理：

- **质押机制**：用户质押 bNEO 获得投票权。

- **提案系统**：支持参数调整、应用审批、资金分配等提案类型。
- **投票流程**：讨论期 → 投票期 → 时间锁 → 执行。
- **法定人数**：提案需达到法定人数和超级多数才能通过。

5.3 AppRegistry：应用管理

AppRegistry 合约管理小程序的注册、状态和元数据：

- **清单存储**：存储每个应用的清单哈希，确保配置不可变。
- **状态管理**：管理应用的审核状态（待审核、已批准、已暂停）。
- **白名单**：维护授权合约和 MRSIGNER 的白名单。

6 内置小程序

Neo N3 小程序平台包含二十三个生产就绪的应用，涵盖游戏、去中心化金融、社交互动和治理四个主要类别。这些应用展示了平台能力，同时为用户提供即时效用，并作为第三方开发者的参考实现。

表 5: 内置小程序分类

类别	应用	描述
游戏	CoinFlip	硬币翻转游戏
	DiceGame	骰子游戏
	ScratchCard	刮刮卡
	Lottery	彩票
	MegaMillions	大型彩票
	GasSpin	转盘游戏
DeFi	FlashLoan	闪电贷
	GridBot	网格交易机器人
	TurboOptions	期权交易
	PricePredict	价格预测
	ILGuard	无常损失保护
	AITrader	AI 交易
社交	RedEnvelope	微信式随机红包（手气最佳）
	SecretVote	秘密投票
	FogChess	战争迷雾象棋
	SecretPoker	秘密扑克
	NFTEvolve	NFT 进化
治理	GovBooster	治理加速器
	PredictionMarket	预测市场
	MicroPredict	微型预测
	GasCircle	GAS 互助圈

表 6: 小程序合约地址 - 游戏类（Neo N3 测试网）

类别	合约	脚本哈希
游戏	MiniAppLottery	0x3e330b4c396b40aa08d49912c0179319831b3a6e
	MiniAppCoinFlip	0xbd4c9203495048900e34cd9c4618c05994e86cc0
	MiniAppDiceGame	0xfacff9abd201dca86e6a63acfb5d60da278da8ea
	MiniAppScratchCard	0x2674ef3b4d8c006201d1e7e473316592f6cde5f2
	MiniAppGasSpin	0x19bcb0a50ddf5bf7cefbb47044cdb3ce4cb9e4cd
	MiniAppSecretPoker	0xa27348cc0a79c776699a028244250b4f3d6bbe0c
	MiniAppFogChess	0x23a44ca6643c104fbaa97daab65d5e53b3662b4a

表 7: 小程序合约地址 - DeFi 类（Neo N3 测试网）

合约	脚本哈希
MiniAppPredictionMarket	0x64118096bd004a2bcb010f4371aba45121eca790
MiniAppFlashLoan	0xee51e5b399f7727267b7d296ff34ec6bb9283131
MiniAppPriceTicker	0x838bd5dd3d257a844fadddb5af2b9dac45e1d320
MiniAppPricePredict	0x6317f97029b39f9211193085fe20dcf6500ec59d
MiniAppMicroPredict	0x73264e59d8215e28485420bb33ba841ff6fb45f8
MiniAppTurboOptions	0xbbe5a4d4272618b23b983c40e22d4b072e20f4bc
MiniAppILGuard	0xd3557ccbb2ced2254f5862fbc784cd97cf746872
MiniAppAITrader	0xc3356f394897e36b3903ea81d87717da8db98809
MiniAppGridBot	0x0d9cfc40ac2ab58de449950725af9637e0884b28

6.1 游戏应用

游戏类别包含七个应用，利用平台的可验证随机性和支付基础设施提供可证明公平的游戏体验。这些应用展示了如何使用区块链支持的公平性保证来实现传统游戏机制。

Neo Lottery 应用实现了基于票据的彩票系统，用户使用 GAS 代币购买彩票，通过可验证随机数生成选出获胜者。每轮彩票从票据销售中累积奖池，NeoVRF 服务在每轮结束时生成中奖票号。随机值的链上锚定使任何参与者都能验证获胜者选择是公平且未被操纵的。

CoinFlip 应用提供简单的双倍或零游戏，用户对虚拟硬币翻转的结果下注 GAS。该应用展示了平台提供即时游戏体验的能力，随机数生成和支付处理在几秒内完成。50/50 的赔率可通过 VRF 证明机制进行数学验证。

DiceGame 应用扩展了乘数概念，允许用户对骰子结果下注，支付高达六倍的投注金额。基于所选数字范围的可变赔率展示了平台如何在保持可证明公平性的同时支持复杂的支付结构。

其他游戏应用包括：ScratchCard 提供即时中奖体验，GasSpin 提供转盘机制，SecretPoker 提供 TEE 保护的德州扑克（隐藏牌由可信执行环境保护），FogChess 提供信息不对称的战略游戏体验。

6.2 DeFi 应用

DeFi 类别包含九个应用，展示了平台在金融应用方面的能力，从简单的价格查询到复杂的交易策略。这些应用利用 NeoFeeds 价格预言机和支付基础设施，在平台的安全模型内提供金融服务。

PredictionMarket 应用使用户能够对支持的资产对的未来价格走势进行投注。用户在指定时间范围内对价格上涨或下跌进行押注，结果由 NeoFeeds 预言机的价格数据决定。该应用展示了如何将外部数据安全地纳入链上结算逻辑。

FlashLoan 应用实现即时借贷机制，使用户能够获取流动性用于套利或其他在单笔交易内完成的操作。该应用强制在同一交易内还款，消除违约风险，同时实现资本高效运营。

PriceTicker 应用为支持的资产对提供实时价格数据，展示 NeoFeeds 预言机集成。用户可以查询当前价格并订阅价格更新通知，基于可靠的市场数据做出明智的交易决策。

表 8: 小程序合约地址 - 社交与治理类（Neo N3 测试网）

类别	合约	脚本哈希
社交	MiniAppRedEnvelope	0xf2649c2b6312d8c7b4982c0c597c9772a2595b1e
	MiniAppGasCircle	0x7736c8d1ff918f94d26adc688dac4d4bc084bd39
	MiniAppSecretVote	0x7763ce957515f6acef6d093376977ac6c1cbc47d
	MiniAppNFTEvolve	0xadd18a719d14d59c064244833cd2c812c79d6015
治理	MiniAppGovBooster	0xebabd9712f985afc0e5a4e24ed2fc4acb874796f
	MiniAppBridgeGuardian	0x2d03f3e4ff10e14ea94081e0c21e79e79c33f9e3
	MiniAppGuardianPolicy	0x893a774957244b83a0efed1d42771fe1e424cfec
工具	MiniAppServiceConsumer	0x8894b8d122cbc49c19439f680a4b5dbb2093b426

其他 DeFi 应用包括：PricePredict 和 MicroPredict 提供不同时间框架的二元期权交易，TurboOptions 提供超快速交易，ILGuard 提供无常损失保护，AITrader 提供自主交易策略，GridBot 提供自动化网格交易。

6.3 社交与治理应用

社交和治理类别包含七个应用，促进社区互动和平台治理。这些应用展示了区块链技术如何增强社会协调和民主决策。

RedEnvelope 应用实现微信式随机红包功能，使用户能够创建装有 GAS 的红包供收件人领取随机金额。与平均分配不同，每位收件人获得不同的 VRF 生成的随机金额，让用户在发现自己运气时充满期待。该应用跟踪所有抢红包者及其金额，防止同一用户重复领取。当所有红包被领完时，获得最高金额的人将被加冕为" 手气最佳"，平台通知会向所有参与者宣布获胜者。智能合约已部署在 Neo N3 测试网，地址为 `0xf2649c2b6312d8c7b4982c0c597c9772a2595b1e`。

GasCircle 应用创建每日储蓄圈，参与者向共享池贡献 GAS，每个周期由一名成员获得累积资金。该应用展示了如何使用区块链支持的透明度和执行来实现传统的轮转储蓄机制。

SecretVote 应用为社区决策提供隐私保护投票，利用 TEE 确保个人投票保持机密，同时产生可验证的汇总结果。该应用展示了平台的机密计算能力如何在治理场景中保护投票者隐私。

GovBooster 应用提供 bNEO 治理优化工具，帮助代币持有者最大化其在 Neo 网络治理中的参与度。其他应用包括：NFTEvolve 提供动态 NFT 机制，BridgeGuardian 提供跨链资产转移，GuardianPolicy 提供 TEE 强制的交易安全策略。

7 开发者指南

Neo N3 小程序平台提供全面的工具和文档，使开发者能够高效地构建、测试和部署小程序。本节概述了开发工作流程、SDK 能力以及管理小程序行为的清单规范。

7.1 开发环境

开发者首先安装平台 SDK，该 SDK 为所有平台服务提供 TypeScript 绑定。SDK 通过 npm 分发，可以通过单个命令安装。安装后，开发者可以访问支付、随机数、价格数据、治理和其他平台能力的类型化接口。

SDK 实现自动环境检测，根据初始化参数配置为测试网或主网。在开发过程中，应用可以针对本地模拟环境运行，该环境模拟平台行为而无需区块链交易，从而实现快速迭代和测试。

开发者可以使用以下工具进行本地开发和测试：

- **neo-express**：本地 Neo N3 私有链，用于合约测试。

- **Supabase 本地**：本地数据库和认证服务。
- **TEE 仿真**：EGo 仿真模式，无需 SGX 硬件即可测试。
- **SDK Mock**：模拟平台 SDK 响应，加速前端开发。

7.2 SDK 架构

SDK 通过模块化架构暴露平台能力，不同服务类别使用独立的命名空间。payments 命名空间提供发起 GAS 转账、查询余额和订阅支付事件的方法。rng 命名空间支持请求可验证随机值，并提供可配置的锚定选项。datafeed 命名空间提供对价格预言机数据的访问，支持历史查询和实时订阅。

TypeScript SDK 通过 `window.MiniAppSDK` 全局对象提供访问：

表 9: SDK 命名空间概览

命名空间	功能
`wallet`	地址获取、余额查询
`payments`	GAS 支付、交易历史
`governance`	bNEO 质押、投票
`rng`	随机数请求、验证
`datafeed`	价格订阅、历史数据
`stats`	使用统计、分析

SDK 使用示例：

```
// 获取用户地址
const address = await window.MiniAppSDK.wallet.getAddress();

// 发起 GAS 支付
await window.MiniAppSDK.payments.payGAS(appId, "1.5", "entry fee");

// 请求随机数
const { randomness, reportHash } =
    await window.MiniAppSDK.rng.requestRandom(appId);

// 获取价格数据
const price = await window.MiniAppSDK.datafeed.getPrice("BTC-USD");
```

7.3 清单规范

每个小程序必须通过清单文件声明其能力和约束，这是一个 JSON 文档，指定应用的身份、权限和资源限制。清单作为应用与平台之间的契约，定义应用可以执行的操作和可以消耗的资源。

清单包含几个必需字段。应用标识符必须全局唯一，遵循反向域名表示法约定。入口 URL 指定应用前端代码的托管位置，必须通过 HTTPS 从批准的内容分发网络提供服务。版本字段支持应用更新跟踪和回滚功能。

权限部分声明应用需要访问的平台服务。应用必须明确请求支付、随机数、价格数据、治理操作和其他能力的权限。平台在运行时强制执行这些权限，拒绝清单中未声明的任何操作。

表 10: 清单字段规范

字段	类型	描述
`app_id`	string	唯一应用标识符
`entry_url`	string	前端 HTTPS URL
`permissions`	object	请求的 SDK 权限
`assets_allowed`	array	允许的支付资产（仅 GAS）
`limits`	object	交易和使用限制

资源限制约束应用对平台资源的消耗。最大交易金额防止应用处理意外的大额支付。每日上限限制每个用户的累计资源消耗。速率限制防止应用通过过多请求压垮平台服务。

8 代币经济学

Neo N3 小程序平台在 Neo N3 代币生态系统内运营，使用 GAS 作为所有支付操作的实用代币，使用 bNEO（Burger NEO）作为平台决策的治理代币。这种双代币模型与更广泛的 Neo 生态系统保持一致，同时在实用功能和治理功能之间提供清晰的分离。使用 bNEO 而非原生 NEO 可以实现更灵活的 DeFi 集成和与其他 Neo N3 协议的可组合性。

表 11: 代币对比：GAS vs bNEO

属性	GAS	bNEO
用途	支付/结算	治理/质押
获取方式	交易所/持有 NEO	Burger NEO
平台角色	唯一支付代币	唯一治理代币

8.1 GAS：实用代币

GAS 作为平台内所有支付操作的唯一交换媒介。用户使用 GAS 代币支付小程序服务、游戏投注和平台费用。这种单一资产方法简化了用户体验，消除了多代币管理的复杂性，并确保所有平台服务的定价一致。

平台的 GAS-only 策略在架构的每一层都得到执行，从客户端 SDK 验证到链上智能合约验证。这种全面的执行确保该策略无法通过任何攻击向量被绕过，为用户和监管机构提供关于平台处理资产的强有力保证。

通过平台操作收取的 GAS 按照透明的收益分享模式分配。70% 的收取费用流向小程序开发者，激励高质量应用的创建。20% 归入平台国库，资助持续开发和运营。10% 分配给 bNEO 质押者作为治理奖励，使治理参与者的利益与平台成功保持一致。

8.2 bNEO：治理代币

bNEO（Burger NEO）代币赋予平台内的治理权利，使持有者能够参与塑造平台演进的决策过程。治理参与需要质押 bNEO 代币，投票权与质押数量成正比。用户可以通过官方 bNEO 合约包装其原生 NEO 代币来获取 bNEO，从而在保持流动性选项的同时无缝参与平台治理。

治理决策涵盖几类平台变更。协议参数，包括费用结构、速率限制和资源分配，可以通过治理提案进行修改。新小程序的批准需要治理审查，确保社区对平台准入应用的监督。国库分配用于开发资助、营销计划和生态系统投资，通过治理投票决定。

治理流程遵循结构化的生命周期，旨在确保深思熟虑的审议。提案进入讨论期，社区成员可以提供反馈和建议修改。讨论结束后，提案进入投票期，bNEO 质押者投票表决。达到法定人数和超级多数批准的提案在时间锁定期后排队执行，以便为变更做好准备。

9 平台愿景

Neo N3 小程序平台设计为可扩展的基础设施，以满足去中心化应用开发中不断涌现的需求。本节概述了平台在四个关键能力层的战略方向。

表 12: 平台能力层

层级	能力
基础层	7 个智能合约、TEE 服务、账户池（10K+ 账户）
应用层	23 个内置小程序，涵盖游戏、DeFi、社交、治理
生态层	开发者 SDK、文档、审批流程、分析仪表板
扩展层	跨链互操作、移动 SDK、企业部署选项

9.1 基础层

基础层提供小程序运行所需的核心平台基础设施。七个平台智能合约提供平台规则的链上执行，包括支付结算、治理投票和应用注册管理。基于 MarbleRun 和 Intel SGX 构建的 TEE 服务层为敏感操作建立安全基础，包括密钥管理和交易签名。账户池架构支持超过一万个预生成账户，实现高吞吐量交易处理而不产生瓶颈。

9.2 应用层

应用层通过生产就绪的小程序展示平台能力。二十三个内置应用涵盖游戏、DeFi、社交和治理类别，为用户提供即时效用，同时作为开发者的参考实现。TypeScript SDK 提供全面的文档和示例代码，支持新应用的快速开发。从用户交互到区块链结算的端到端工作流程得到完全支持。

9.3 生态层

生态层支持第三方开发并扩大平台采用。全面的开发者文档和教程降低了新开发者的准入门槛。简化的小程序审批流程在保持安全标准的同时加速第三方应用的上线。增强的分析和监控能力为开发者提供关于应用性能和用户参与度的可操作洞察。

9.4 扩展层

扩展层将平台能力扩展到更广泛的用例和更大的用户群。跨链桥接集成实现 Neo N3 与其他区块链网络之间的资产转移。移动 SDK 支持 iOS 和 Android 平台的原生移动应用开发。企业功能包括专用基础设施、自定义 SLA 和合规工具。

10 结论

Neo N3 小程序平台代表了去中心化应用开发在可访问性和安全性方面的重大进步。通过将硬件保护的执行环境与综合开发者工具和精心设计的智能合约基础设施相结合，平台解决了历

来限制区块链采用的根本性挑战。

10.1 技术成就

平台的纵深防御安全架构确保敏感操作在每一层都受到保护，从客户端验证到链上执行。通过 MarbleRun 框架使用 Intel SGX 技术提供了软件攻击无法绕过的硬件级保证，而多层验证方法确保了对新型攻击向量的弹性。

GAS 实用代币和 bNEO 治理代币之间的严格分离建立了清晰的边界，简化了监管合规，同时协调了利益相关者的激励。这种分离在所有平台层得到全面执行，为用户和监管机构提供关于平台处理资产的强有力保证。

账户池架构实现高吞吐量交易处理，而不会出现通常限制区块链应用的瓶颈。凭借超过一万个预生成账户和 TEE 保护的密钥管理，平台可以支持大规模用户群，同时保持安全保证。

10.2 生态系统价值

二十三个内置小程序展示了平台能力，同时为用户提供即时效用。这些应用作为第三方开发者的模板和参考实现，通过提供常见用例的经过验证的模式来加速新应用的开发。

全面的 TypeScript SDK 抽象了区块链复杂性，使没有专业区块链知识的开发者也能构建复杂的去中心化应用。这种可访问性扩大了能够为生态系统做出贡献的人才库，加速创新和应用多样性。

10.3 未来方向

平台的模块化架构使其能够持续演进而不中断现有应用。可以添加新的 TEE 服务以支持新兴用例。智能合约升级可以引入新功能同时保持向后兼容性。治理框架确保平台演进反映社区优先事项。

随着区块链行业的成熟，成功平衡安全性、可用性和开发者体验的平台将获得越来越多的市场份额。Neo N3 小程序平台定位于服务这个不断增长的市场，为下一代去中心化应用提供所需的基础设施。

如需技术文档、SDK 参考和开发者资源，
请访问 Neo N3 小程序平台文档门户。