PHAROS
RESEARCH

公链真的安全吗，谁在定义公链的生存标准？

目录

01 / 公链安全演进的必然性

早期公链的安全，很大程度上依赖于合约中心主义，将安全焦点高度集中在智能合约代码的审计上，普遍认为只要合约本身无懈可击，安全防线便固若金汤。然而，一系列代价高昂的安全事件无情地揭示了这种观念的局限性。2023 年，黑客攻破了 ZKSync 代币空投分发合约相关的私钥控制权，数百万美元的资产被转移；2022 年 6 月，Loopring 遭受的 DDoS 攻击，云基础设施的瘫痪使网络服务中断长达十数小时；同年 3 月，朝鲜黑客针对生态合作伙伴 Ronin 桥的漏洞发起攻击，侵入员工的 IT 基础设施，成功控制了 4 个属于验证器节点，直接击穿了整条防线，成为区块链史上损失最严重的攻击之一。我们可以越来越清晰看到，区块链攻击面已不再局限于智能合约或虚拟机层面，而是迅速扩展至密钥管理、运维基础设施、第三方依赖，乃至针对内部人员的社会工程攻击。区块链系统的安全，深度依赖部署在复杂、多层、由人和组织构成的现实技术栈之上。

这与国际货币基金组织（IMF）、国际清算银行（BIS）等全球核心金融监管机构的战略重点不谋而合。IMF 在其 2024 年的多次发言与报告中明确指出，随着加密资产与主流金融体系的融合，监管的重点已不再局限于市场波动，而必须扩展到更深层的结构与运营维度，其中操作风险与治理风险被视为代币化金融演进过程中的关键脆弱环节。BIS 则在其提交给 G20 的多份报告中进一步强调，健全的治理安排是有效风险管理的基石，且这种风险管理必须是全面且贯穿始终的，必须无死角地覆盖包括操作风险（特别是网络韧性）和治理风险在内的所有领域。这些来自顶层设计的共识传递出一个清晰的信号，当区块链技术开始承载与传统金融市场等量齐观、甚至更具流动性的真实资产时，其安全标准必须向顶级金融机构看齐并实现无缝对齐。这意味着，区块链安全不再是仅由开发团队在代码层面负责的单一环节，而必须进化为一种系统性工程，需要渗透到技术架构的设计、日常运营的流程、组织文化的塑造以及合作伙伴管理的每一个细微环节之中。

在如此背景下，行业需要有能力承载未来数字金融资产的安全模式，这样的公链必须具备三重能力：回答监管的质询，承载机构的信任，并在持续不断的真实攻击中，证明自己配得上被托付的万亿价值。**Pharos 公链的出现，恰逢其时地定义了安全公链的标杆。它率先将 IMF、BIS 的监管框架工程化为可运行、可验证的链上链下协同体系，志在成为服务万亿级实体资产的安全公链。**

02 / 公链安全的风险矩阵与多维架构

2.1 Pharos 公链的安全架构

Pharos 是旨在服务金融机构与高价值真实世界资产（RWA）的公链，其安全架构超越常见的公有链社区自治模式，构建涵盖技术、运营、法律与金融等完整的保障体系。具体而言，其安全架构彻底覆盖以下六个核心维度，以实现公链安全的确定性。

第一，物理与硬件安全维度。对于金融公链而言，验证者节点、密钥管理设施乃至数据中心的物理访问控制，必须达到银行金库或同等数据中心的安全等级。更重要的是，广泛采用经认证的硬件安全模块（HSM）来生成、存储和处理核心密钥，确保私钥材料在任何情况下均不可被软件提取，从物理根源杜绝私钥泄露的可能。

第二，密钥管理与访问控制维度。在机构场景中，密钥不仅代表控制权，更对应法律上的所有权与责任。因此，金融公链必须设计一套精细化的企业级密钥管理体系，包括支持多签、门限签名（TSS）等复杂的签名方案，以匹配企业内部的分权制衡要求；实现密钥的合规托管与恢复流程，避免因个人失能导致资产永久损失；提供基于角色的、可审计的细粒度访问控制策略。该维度的目标是将区块链私钥即一切的原始模型，安全地适配到金融机构严密的内部治理与合规框架之中。

第三，网络与通信安全维度。 公链网络本身是一个公开的 P2P 系统，金融级应用更要求其通信具备机密性、完整性与高可用性。这需要通过实施零信任网络架构、对所有节点间及客户端与节点间的通信进行强制加密（如使用 TLS 1.3 或更强协议）来实现。同时，必须部署企业级的 DDoS 缓解方案，以抵御旨在瘫痪交易或清算流程的流量攻击。该维度确保了交易指令、区块数据等关键信息在传输过程中不可被窃听、篡改或阻断。

第四，智能合约与协议安全维度。 智能合约安全是区块链安全的传统焦点，对金融公链的要求更为严苛。它要求核心协议与智能合约（尤其是处理资产发行、结算、赎回的合约）需经过形式化验证，以数学证明其代码行为完全符合设计规范，杜绝重入、溢出等漏洞。此外，必须建立一套受控的、具有明确回滚与紧急暂停机制的合约升级治理流程，以应对极端情况。对于 RWA 资产，合约逻辑必须与链下法律文件中的权利、义务及违约处置条款实现精准且不可篡改的映射。

第五，合规、监控与审计维度。 金融机构运营于高度监管的环境中，因此金融公链必须内置合规可审计性。这包括提供完整的、不可篡改的链上活动审计线索，并能够与链下的监控、审计和风险管理系统（如 SIEM）集成。实时监控需覆盖异常交易模式、智能合约风险指标、节点健康状况及预言机数据源等多个层面，使机构能够主动发现威胁、满足监管报告要求，并为事后取证提供不可抵赖的证据。

第六，治理、应急与生态安全维度。 终极的安全考验在于面对未知冲击时的系统韧性。金融公链必须预设清晰的链上治理与链下应急响应相结合机制，具体包括：针对严重漏洞或市场极端波动的紧急响应预案；验证者集及关键服务商（如跨链桥、预言机）的严格准入、持续评估与退出机制；以及对生

态合作伙伴（如资产发行方、托管方）的安全标准传导与协同防御能力。该维度表明，安全并非静态状态，而是一个动态、协同、能够内外联动抵御系统性风险的持续过程。

总结如下：

图1：Pharos公链的安全架构

安全维度	核心要求	关键技术/措施
1. 物理与硬件安全	物理访问控制达银行金库级；硬件安全模块保护私钥	HSM，防软件提取
2. 密钥管理与访问控制	企业级密钥体系，多签/TSS，合规托管与恢复，基于角色的访问控制	多签，门限签名，角色权限审计
3. 网络与通信安全	零信任，强制加密，DDoS防护	TLS 1.3，DDoS缓解
4. 智能合约与协议安全	形式化验证，合约升级治理，法律映射	形式化验证，紧急暂停，法律代码映射
5. 合规、监控与审计	审计线索，实时监控，SIEM集成	不可篡改日志，异常检测，监管报告
6. 治理、应急与生态安全	链上+链下应急，准入退出，生态协同	紧急响应，验证者评估，协同防御

资料来源：Pharos Research

Pharos 所代表的安全架构清晰表明，金融级公链的安全架构是从物理硬件的信任根基出发，穿透密钥、网络、合约、监控直至治理与生态的每一层，构建起一个立体、纵深且闭环的保障体系。其最终目的，是将区块链技术固有的不确定性，转化为金融机构可理解、可计量、可信任的确定性服务，从而为万亿美元级别的传统资产安全上链铺平道路。

2.2 差异化战略与实践框架

风险矩阵中的六大维度，没有任何一种单一技术方案或运营策略能够覆盖全部威胁。 成熟的公链安全战略必然呈现差异化与纵深防御的双重特征。差异化的本质，是公链根据自身定位在安全、性能与去中心化之间做出明确取舍；而纵深防御，则是通过多层、互补的控制措施将单点失效的冲击控制在有限范围内。目前，主流公链在安全保护上，逐步形成兼具差异化定位与纵深防御特征的战略性框架，既为头部公链的安全路径提供了可拆解的分析维度，也为新兴公链的安全成熟度评估设立了可对标的参照基准。

技术战略

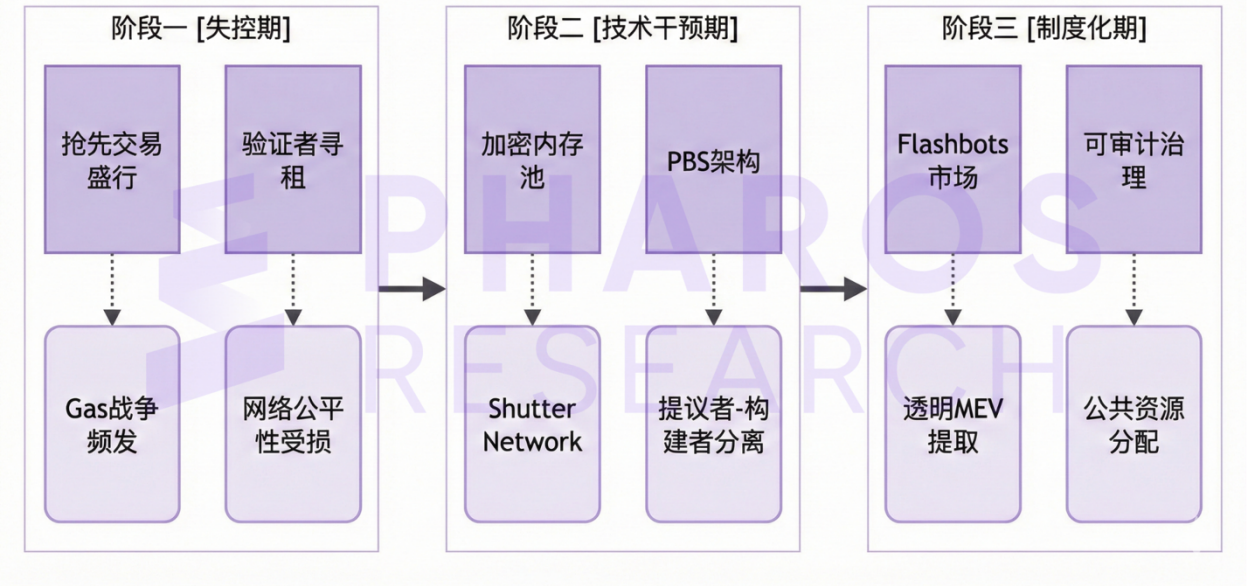
- 共识层是公链安全基座的第一道分水岭。Solana 选择 PoH（历史证明）+ PBFT 组合，以高硬件门槛换取轻量级出块速度，其安全假设锚定于节点算力的持续领先。2025 年 9 月，Solana 通过 Alpenglow 升级引入 Votor/Rotor 新共识机制，取代原有 PoH/TowerBFT，将交易最终性时间从约 13 秒大幅压缩至 100-150 毫秒，峰值吞吐量突破 10 万 TPS，并获得超过 98%验证者支持[1]。以太坊则采用 CasperFFG + LMD-GHOST 的混合 PoS 机制，目前活跃验证者数量已超过 90 万，全球分布实现较高去中心化水平，最终性时间约 12 分钟（两个 epoch）[2]。比特币的 PoW 则将安全锚定于物理世界的能源与专用芯片，年耗电量约 175.87 TWh[3]，形成一套截然不同的算力即信任模式。共识选择的背后，是公链对安全与效率根本性权衡的差异化回答。
- 头部公链已普遍启动后量子密码学的迁移准备，并对零知识证明技术进行深度集成。IACR 2025 年研究指出，采用 EdDSA 及 SLIP-0010 密钥派生标准的区块链（如 Sui、Solana、Near、Aptos）具备结构性的后量子迁移优势——可通过后量子零知识证明证明种子所有权，在不改变地址的前提下实现量子安全签名，而基于 BIP32 的 ECDSA 钱包（如 Bitcoin、以太坊现有账户）则无法实现向后兼容的平滑迁移[4]。以太坊 Layer 2 生态通过 ZK-Rollups 与 ZK-STARKs，将交易的隐私性与可验证性压缩至链上，使验证成本与数据可用性解耦。这不仅是扩容手段，更是一种安全前置——将复杂计算移出主网，同时用数学证明确保其结果无法被篡改。
- 模块化架构的风险隔离价值。Celestia 引领的"执行层—结算层—共识层—数据可用性层"分离架构，正在成为模块化公链的安全范本。其核心贡献在于：单一组件的漏洞不再直接蔓延至全系统。以太坊 Danksharding 的演进路线同样遵循这一逻辑，通过将数据可用性与共识解耦，降低单点故障对网络最终性的冲击。Immunefi 2025 年披露的 Movement Labs 攻击 athon 报告指出[5]，若 Celestia 节点错误使用 blob.GetAll 而非 blob.Get 数检索数据可用性 blob，攻击者可注入恶意区块导致全节点分叉——这一漏洞的发现恰恰印证了模块化架构中组件边界定义的重要性。以太坊 Danksharding 的演进路线同样遵循这一逻辑，通过将数据可用性与共识解耦，降低单点故障对网络最终性的冲击。

经济与博弈战略

- 质押与罚没的动态均衡。PoS 公链普遍引入罚没（Slashing） 机制，对双重签名、长期离线等行为实施经济惩罚。但罚没的有效性取决于惩罚力度与网络价值的动态匹配：过轻无法形成威慑，过重则会抑制小型验证者的参与意愿。以太坊将罚没条件嵌入信标链与同步委员会的复合约束中，形成一套兼顾安全性与去中心化的参考模型。
- MEV 从失控到民主化。MEV 的恶性竞争曾是以太坊主网公平性的重大威胁。行业应对策略已从早期的被动放任转向主动引导与权力分散：Shutter Network 等加密内存池防止抢先交易；提议者—构建者分离（PBS） 通过拍卖机制将区块构建权与提议权拆解，遏制验证者寻租；Flashbots Auction 则为 MEV 提取建立了透明市场。这些机制共同在效率与公平之间寻

求再平衡，使 MEV 从"暗黑森林"转向可审计、可治理的公共资源。MEV 治理的三个阶段演进如下图所示：

图 2：MEV 治理三阶段演进



资料来源：Pharos Research

生态与治理战略

- 去中心化治理的路线图与混合模式。几乎没有公链在创世阶段即实现完全去中心化治理。关键在于设定清晰、可预期的权力下放路线图。以太坊由基金会引导早期研发，逐步过渡至 EIP（以太坊改进提案）流程与全社区共识；Polkadot 则直接采用链上治理与国库系统，允许代币持有者对财政支出与协议升级进行投票。实践中，链上治理（高效但易受投票贿赂攻击）与链下社会共识（慢速但抗女巫攻击）的混合模式已成为主流公链规避治理攻击的标准配置。
- 开发者激励与审计透明化。头部公链普遍设立专项安全基金与漏洞赏金计划。Immunefi 平台累计发放赏金已超 1.6 亿美元[6]，覆盖项目超 900 个，注册白帽黑客超 9 万名，单个严重漏洞最高奖励达 1000 万美元，将白帽黑客转变为安全生态的职业共建者。同时，头部 DeFi 协议已形成多审计机构交叉验证的行业惯例，并将完整审计报告链上公开，前 50 大 TVL 协议中超过 80%采用至少两家审计机构交叉审计，并将完整审计报告通过 Dune Analytics 或 GitHub 链上公开，使安全透明度成为市场竞争力的直接来源。
- 运营与响应战略
- 客户端与基础设施的多样性。2023 年以太坊主网因 Geth 客户端内存池漏洞导致近 80%节点同步异常的事件，是客户端单一化风险的标志性案例。此后，主流公链开始主动激励多客户端生态——以太坊扶持 Nethermind、Besu 等替代客户端，Solana 引入 Firedancer 重构节点

软件。同时，节点部署层面亦从“单一云厂商”向多云/混合云架构迁移，以降低云服务商单点故障对网络可用性的系统性影响。

- 链上监控与应急响应制度化。建立实时链上监控仪表盘正成为行业标配。关键指标包括：区块重组深度、验证者质押集中度、跨链桥流量异常、稳定币脱钩前兆等。以太坊在主网合并前夕设立的警戒委员会（由核心开发者、客户端团队与独立安全专家组成）为行业提供了应急协调机制的参考范式——在协议级风险爆发时，能够在不牺牲去中心化原则的前提下实现有限、透明的临时干预。2023 年全球跨链桥攻击事件数量同比下降 35%[7]，部分归因于实时监控与响应机制的普及。
- 用户安全教育的基础设施化。生态层面的安全标准正在从“可选项”变为应用层的默认基础设施。WalletConnect 的会话验证规范有效降低了钓鱼签名的成功率；SIM 卡互换攻击防范指南已在多家主流钱包的交互流程中内置提醒；硬件钱包签名可视化使交易意图在物理设备上清晰呈现。这些实践将安全认知从用户责任转移为平台责任，是公链生态迈向主流采纳的必要台阶。
- 这一框架清晰地表明，公链安全是一套贯穿共识机制、经济博弈、治理规则与运营纪律的动态策略系统，差异化的价值不在于评判孰优孰劣，而在于明确每条公链在安全光谱中的坐标；纵深防御的意义，则是在承认“绝对安全不存在”的前提下，为未知威胁预留足够的缓冲与纠错空间。

2.3 公链安全风险对比

市场不同参与者的安全选择，实质上反映了其业务定位与价值主张的差异。

图3：主流公链架构类型与安全风控特征对比表

类型	机构级公链	高灵活公链	战略型融合链
头部公链	Pharos / 摩根大通 Onyx	Solana / BSC / Base	蚂蚁数科Jovay / OKX Chain
核心安全目标差异	零差错金融分帐合规平台	持续保障高性能网络不间断	建立合规互通性的国际通道
技术及运营风险的天然劣势点	自研/定制化代码的复杂性	生态项目智能合约质量参差不齐（风险分散但规模大）	跨链和桥接协议合约的安全性（攻击面复杂，牵一发动全身）
相对安全基础设施的成熟对标与主要优点	对标：全球系统重要性银行(G-SIB)的IT风控体系 优点：银行级的网络隔离、硬件安全模块(HSM)密钥管理、7x24监控与异地灾备，抗大规模定向攻击能力强。	对标：大型互联网云服务商（如AWS） 优点：弹性伸缩能力强、全球节点分散、开源社区反应迅速，防御大规模流量攻击和快速漏洞修复能力高。	对标：跨国企业的全球合规与风控平台 优点：在技术可控的基础上，平衡东西方监管要求，能实现生态风险的分担与隔离。
最佳适配场景	跨境支付，跨境结算、RWA、国债类高合规强信用的金融资产	DeFi、NFT、高频交易、Meme文化驱动的个人市场	大型跨链资产互通、贸易金融、多法币稳定币结算网络
资料来源：Pharos Research			

Pharos 对安全的责任，超越了链上代码，覆盖了从物理服务器到私钥存储间，再到第三方合作伙伴的整个价值链。这种将自身安全边界不断外延的重资产模式，提供一个确定性最高、变量最少的运行环境。通过构建业内最苛刻、最透明的安全体系，保障对对安全有极致要求的高净值资产与机构。选择 Pharos，在某种意义上，是选择将其深厚的安全基础设施，变为自身业务的护城河。

03 / 可持续性验证：价值清算下的安全经济学

安全本质上是一种需要持续投入资源（包括研发、审计、监控与基础设施）进行维护与升级的公共服务，而非一次性工程。任何安全战略的长期有效性，必须建立在可持续的经济模型之上。如果一条公链无法通过自身经济活动产生足够收入来覆盖这些成本，那么其安全承诺便如同空头支票，长期来看必然失效。市场正通过链上现金流进行残酷的价值清算与差异化验证。

安全战略的可持续性，终究要接受经济模型的检验。透过链上现金流这一最诚实的度量衡，当前公链的安全路径已呈现出三种截然不同的经济范式，其可持续能力也随之分化。

以 Base、Hyperliquid 为代表的生态公链路径，其核心是构建一个现金流驱动的增长飞轮。在这类模型中，安全投入是直接的运营成本，但其目标明确服务于能够产生即时收入的核心业务，例如高频交易与链上应用。用户活动所产生的持续手续费收入，为安全与开发提供了直接的资金来源，从而形成一个正向循环，安全与体验提升吸引更多用户与开发者，进而产生更多收入，收入再反哺于更高级别的安全建设。因此，评估此类公链健康度的关键指标在于其协议收入与费用市值比，其商业本质是一个依靠规模与流量盈利的交易平台。

以 Pharos 为代表金融路径的公链，则遵循一种准入与信任驱动的资产托管逻辑。在这里，巨额的安全与合规投入是其核心产品的价值本身。它的目标客户是银行、资产管理公司与 RWA 发行方，这些机构对安全确定性的需求优先级远高于交易成本。因此，其经济模型类似于传统金融中的托管或服务提供商，前期需要极高的资本支出构建金融级础设施，长期收入则依赖于托管资产的总规模以及向机构客户收取的服务费、节点许可费等。其成功的关键验证指标是托管资产总值与机构客户的质量，安全成本在此被视为获取并服务高净值客户的必要入场费。

与之形成鲜明对比的，是陷入僵尸链困境的公链。它们缺乏可行的经济模型，链上经济活动稀疏，收入与市值严重倒挂。安全投入因无现金流支撑而难以为继，导致网络陷入“不活跃→无收入→更不安全→更不活跃”的死亡螺旋，最终在市场的价值清算中经历坍缩。

综上所述，安全不仅
是技术问题，更是经济问题，是选择成为靠流量规模盈利的平台，还是成为靠提供极致信任服务盈利的提供商。市场最终只奖励能创造真实、可持续现金流的模型，链上收入成为检验真实效用与安全可持续性最残酷的标尺。

Pharos 的选择，是一个能让机构安心托付亿万资产、能让机器经济在严密防护下自主运行的安全世界。在这场漫长的价值互联网建设中，Pharos 所代表的，不是最快的链，而是最值得托付的基石。

参考来源

[1] PANews. 内地向左，香港向右：中资券商公链布局的“双城记”丨下篇[EB/OL]. (2025-12-12)[2026-02-26]. https://www.panewslab.com/zh/articles/c8c76715-289b-454d-9da9-29e58af6ccea

[2] PANews. 2025 年公链市场的残酷清算：繁荣的赌场、虚假的鬼城与 VC 的收割局[EB/OL]. (2025-12-18)[2026-02-26]. https://www.panewslab.com/zh/articles/7a9f1125-701d-473c-b7f3-eace0cee8e28

[3] PANews. 9 大公链新观察：公链之王即将易主？Solana 退潮与 BSC 的强势崛起[EB/OL]. (2025-09-26)[2026-02-26]. https://www.panewslab.com/zh/articles/f00a6d40-65b9-4ae1-8b90-d745fe9113bd

[4] PANews. OKX 最强公链“朋友圈”：拆解 OP、Base、Unichain 等 7 大链的 2025 实战成绩单[EB/OL]. [2026-02-26]. https://www.panewslab.com/zh/articles/43643932-83bb-4449-b1fe-e63d96d6aabb

[5] PANews. AI 能成为老牌公链的新叙事吗？盘点 7 个公链与 AI 的结合[EB/OL]. [2026-02-26]. https://www.panewslab.com/zh/articles/rh070jrd

[6] PANews. 四大顶级公链代表齐聚，畅谈公链技术创新之路[EB/OL]. [2026-02-26]. https://www.panewslab.com/zh/articles/D77724764

[7] PANews. ‘新公链们频频宕机，公链稳定性的未来在哪里？[EB/OL]. [2026-02-26]. https://www.panewslab.com/zh/articles/D94993654

[8] Odaily. 日活为 8？Solana 与 Starknet 舆论战下的数据真相[EB/OL]. [2026-02-26]. http://www.odaily.news/zh-CN/post/5208784

核心贡献

作者：Huijie Tang (𝕏@web3sensen)

审校：Colin Su、Grace Gui、NingNing 、Owen Chen

设计：Alita Li

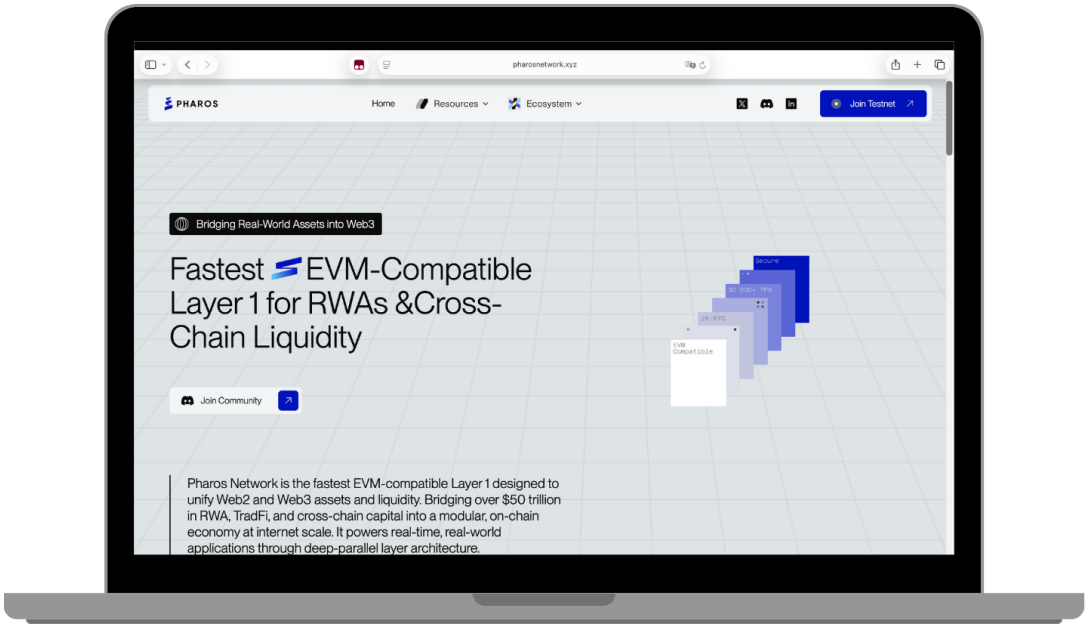
免责声明

本材料由 Pharos Research 编制，旨在提供一般性信息，不构成且不应被视为投资、法律、会计或税务建议，也不构成对任何证券、加密资产或策略的要约、邀请或推荐。所载信息与观点可能来源于自有或第三方渠道，力求可靠但不保证准确、完整或及时，任何据此作出的决策与风险由读者自行承担；历史表现不代表未来结果。内容可能包含前瞻性陈述（包括预测与情景），存在不确定性且不保证实现；加密资产波动性高，可能发生全部损失，并受流动性、技术、智能合约、对手方及合规等风险影响。法律许可范围内，本研究院及/或关联方或研究人员可能持有相关资产头寸或与相关主体存在业务关系，或影响观点客观性。本文并非面向受限制司法辖区之人士，阅读、关注或订阅不构成客户关系。除非书面许可，任何机构或个人不得转载、复制、修改或分发本文，引用须客观完整并注明来源“Pharos Research”。

联系我们

Pharos Network 是面向真实世界资产（RWA）与稳定币的下一代公链，专注于资产通证化与链上流通。我们连接传统机构与 Web3 生态，丰富链上资产类型，拓展收益来源，满足更广泛投资者的配置需求，同时以定制化方案帮助传统企业在链上释放可持续价值。团队兼具深厚的专业能力与一流技术实力，构建安全、高效、可扩展的基础设施，为机构提供将资产上链的全方位去中心化生态。我们欢迎与具备长期视角的战略伙伴共建开放、合规与可持续的 RWA 生态。如果希望与我们开展行业交流，请联系：chris@pharoslabs.xyz

Pharos 官网: https://www.pharosnetwork.xyz/



微信公众号：Pharos Research

微信搜一搜

Pharos Research

PHAROS
RESEARCH

From RWA to On-Chain Finance.

Mapping Real-World Value.