

Arc：一条为稳定币金融量身打造的开放式第一层区块链

Gordon Y. Liao

gordon.liao@circle.com

Rachel Mayer

rachel.mayer@circle.com

Adrian Soghoian

adrian.soghoian@circle.com

Sanket Jain

sanket.jain@circle.com

Erik Tierney

erik.tierney@circle.com

2025 年 8 月

摘要

Arc 是一条为稳定币金融和代币化而打造的、兼容 EVM 的第一层区块链。其特性包括以 USDC 作为原生 Gas、确定性的结算最终性、可选择开启的隐私，以及稳定的交易费率架构。Arc 针对稳定币原生用例（如全球支付、外汇与资本市场）进行优化，致力于成为互联网可编程货币的基础结算层。

1 引言

全球金融体系虽然是现代商业的基石，但其基础设施依旧沿用传统范式，与互联网所强调的速度、开放性与可编程性根本不相容。尽管消费级与企业级软件已历经数十年的创新，金融可得性、金融包容与实时资本流动性依然受到严重制约，尤其体现在跨境与新兴市场。跨境支付缓慢、信息不透明且成本高昂；财资运营被割裂在不同法域、不同中介以及相互不兼容的金融轨道之上；资本市场受到人工流程与多层中间机构的拖累而高度封闭与割裂。这些结构性低效带来经济成本，并引入系统性的对手方与操作风险 [Committee on Payments and Market Infrastructures, 2020]。

区块链技术的出现曾承诺为金融与商业带来新范式，提供可编程性、透明性与抗审查性。然而，现有公链存在根本性限制，阻碍了机构与企业级应用的采用。在许多链上，使用高度波动的原生代币支付 Gas 费用会引入不可预测的运营成本与会计复杂性；缺乏清晰的结算最终性也增加了金融风险；交易隐私的缺失则成为敏感商业活动难以落地的关键阻碍。完全开放且透明的交易提交还催生了最大可提取价值（MEV）等现象，特权参与者通过交易排序攫取利润，损害市场完整性 [Daian et al., 2019]。此外，稳定币流动性与应用在多条区块链上的碎片化进一步增加了用户与开发者的摩擦。

为弥补这些关键缺口，本文提出 Arc——一条面向稳定币金融的开放式第一层区块链。我们的基本信念是，金

融与商业的未来并非对旧体系的全面替代，而是对旧要素的融合：智能合约的可编程性与法律的可执行性（例如 GENIUS 法案）；区块链的效率与法币支持货币的稳定性；公共账本的透明度与商业交易所需的隐私性。作为一条兼容 EVM 的网络，Arc 为可编程性提供熟悉的开发环境；其采用的高性能拜占庭容错（BFT）共识——基于 Tendermint 的 Malachite——为受监管的金融服务在互联网规模的运行提供了机构级基础设施。该设计依赖经许可的验证者集合，亦与新兴监管框架保持一致，例如巴塞尔银行监管委员会对加密资产的审慎监管处理办法提出，在具备稳健控制的网络上运行的稳定币，有望被归类为对银行更为友好的“第一组（Group 1）”资产，从而获得更有利的资本计提待遇 [Basel Committee on Banking Supervision, 2022]。

从本质上看，Arc 重新定义了数字价值的流转与安全保障。它引入三项关键创新：

- 稳定费用与 USDC 作为原生 Gas：**通过以 USDC 作为交易费用的原生产资产，显著降低费率波动与会计复杂性；同时通过专用的付费代理（paymaster）集成，亦支持其他本地稳定币与代币化货币作为 Gas。
- 确定性的结算最终性：**在不到一秒内提供清晰而确定的最终结算，符合金融市场基础设施原则（PFMI）[Committee on Payment and Market Infrastructures and International Organization of Securities Commissions, 2012]。
- 可选择开启的隐私：**集成隐私保护技术以实现选择性透明，满足敏感金融流程所需的保密性，同时有助于机构履行自身的合规义务。

Arc 提供支撑互联网规模金融所需的基础设施。Circle Internet Group（下称 Circle）凭借其在运营 USDC、跨境构建金融原语以及与机构、监管者和开发者社区的紧密合作方面的经验，具备独特优势来引领这项工作。通

过聚焦稳定币驱动的金融的独特需求，Arc 致力于成为可编程货币的基础结算层与流动性枢纽。

2 Arc 的核心架构

Arc 的架构自底向上为金融服务与应用在稳定币与代币化资产之上构建提供坚实、机构级的基础。它旨在克服现有区块链的关键限制，打造安全、高性能并适配受监管金融与真实世界商业需求的平台。如图 1 所示，网络核心是运行 Malachite 共识引擎的经许可验证者集合，为性能与安全提供基石。该架构建立在三个基础支柱之上，分别满足主流金融采用的关键需求。

其一，网络**稳定币原生**，使用 USDC 作为 Gas，以消除费用波动并简化运营；其二，通过高性能共识引擎实现确定性的亚秒级**结算最终性**，为高价值结算提供所需的确定性；其三，将**可选隐私**纳入路线图，通过对余额与交易的选择性透明来保护敏感金融信息，同时保留可审计性。这些核心特性旨在支撑稳定币原生应用（如可编程外汇、支付与机构交易），并通过 Circle 的平台与日益壮大的稳定币合作伙伴生态，与更广泛的链上与链下金融系统无缝衔接。本节将详细阐述这三大核心架构支柱，它们共同确立了 Arc 作为互联网原生经济可信结算层的地位。

2.1 USDC 作为原生 Gas 与稳定费率机制

Arc 的一项基础性设计原则是将 USDC 用作所有交易费用（Gas）的原生资产。此外，Arc 还将通过专用付费代理（paymaster）集成，支持其他本地稳定币与代币化法币作为 Gas。将 Gas 与法币价值锚定，解决了企业采用区块链技术的一项关键障碍：使用投机性原生代币作为运营成本带来的波动与会计复杂性。通过以稳定的计价单位计费，Arc 为用户与开发者提供可预测、可审计且精简的财务运营。这使得价值转移的计价单位与交易成本的计价单位保持一致。

为说明这一点，考虑从用户视角出发的交易成本 C_{USD} 的简单模型。在使用波动性原生资产（如 ETH）的网络中，以美元计的成本是三个变量的乘积：消耗的 Gas 单位数 g 、协议以原生资产计价的每单位 Gas 的基础费率 b_{native} ，以及该资产的市场价格 P_{native} 。于是 $C_{USD} = g \times b_{native} \times P_{native}$ 。该成本包含两类不同来源的波动性：协议层面 b_{native} 的波动（来自区块空间需求）与市场层面 P_{native} 的波动（来自投机）。类似 EIP-1559 的费率稳定机制只能影响 b_{native} ，而无法消除 Gas 代币价格 P_{native} 的波动，且后者往往是主导因素。这使得协议无法在美元单位上提供可预测的交易成本。

相比之下，在 Arc 上，成本可近似表示为 $C_{USD} \approx g \times b_{USDC}$ ，因为 USDC 的价格稳定在 1。市场驱动的价格波动被有效剔除。协议因此可以通过调整 b_{USDC} 直接且有意义地以稳定计价单位管理交易成本。将“双重波动性”转变为仅由协议管理的“单一波动性”，从根本上降低了企业使用区块链的风险，支持可预测的财务规划和稳健的商业模式，从而提升网络在机构与商业用例中的采用潜力。

选择稳定币作为原生 Gas 不仅是为了便利；它还开启了在波动性代币下无法实现的强大费率设计空间。这使得可预测的费率市场、程序化的费率奖励与补贴，以及允许用户以其他货币支付费用的专用付费代理服务成为可能。

在初始阶段，Arc 将实施以稳定与可预测为目标的费率市场，灵感来自以太坊的 EIP-1559 [Buterin et al., 2019]。关键增强在于“费率平滑”机制：协议基础费率不再逐块调整，而是依据区块利用率的指数加权移动平均（EWMA）进行更新。该方法结合有界的基础费率，能够抑制短期波动，确保交易成本持续保持低位。初期收取的费用将归集到链上 Arc 国库（Arc Treasury），以支持网络的长期发展。

2.2 共识与最终性

Arc 的安全模型旨在提供超越常规共识所能实现的更高等级的信任与韧性。其方法是将允许确定性最终性的高性能共识引擎 Malachite，与由受认可机构组成的经许可验证者集合相结合，从而保障网络完整性。

Arc 的目标不是争夺现有的交易量，而是通过提供特定的、高频次的结算保证，来拓展可寻址市场，将下一个数万亿美元的支付与机构资本引入链上。

公有链成为全球金融市场基础设施的一大阻碍，是缺乏对结算最终性的清晰定义。在大多数现有区块链（包括 PoS 与 PoW）上，交易通常会经历一个概率性阶段，并可能遭遇链回滚（“reorg”），逆转最近确认的交易。这种结算不确定性会为高价值金融流程引入风险与资本低效。在极端情况下，完全去许可（permissionless）的 PoS 链也可能遭受“最终性攻击”——若恶意参与者获得质押代币的超级多数，甚至可能逆转一个已宣称“最终”的区块。尽管当前质押代币的价值或许足以覆盖以加密原生为主的用例规模，但若保障数万亿美元规模的代币化金融资产，所需的经济性抵押将达到更高量级。此外，许多链上即便“结算”完成的交易，仍可能被依赖生态治理的社会协调式分叉所逆转。¹ 此外，构建在第一层之上的第二层网络也继承其底层的最终性风险与延

¹关于 DAO 攻击与分叉的讨论，见 Dupont [2018]。

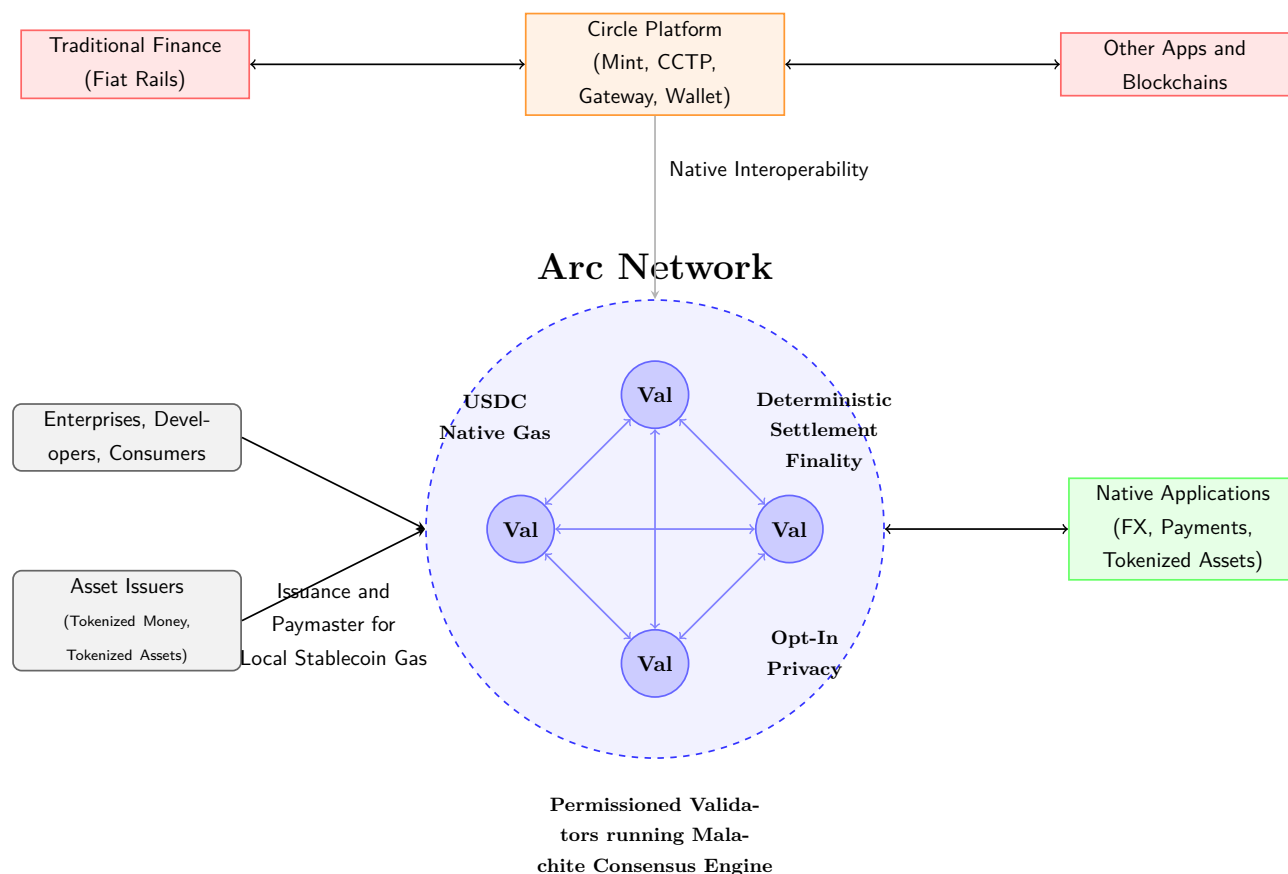


图 1: Arc 的架构，突出其核心组件、原生应用以及与更广泛金融生态的连接。

迟。

Arc 的机构级性能与安全的基础是其共识：基于 Malachite 的 Tendermint BFT 协议的高性能实现。这一选择明确背离了早期链的概率性最终性模型以及较新一代第二层的中心化排序方案。

Arc 将依赖由有限数量、身份已知、资质良好且地理分布广泛的机构组成的经许可权威证明（PoA）验证者集合。² Arc 的愿景是成为受监管资金流动的基础设施，支持全球分布的金融系统。虽然区块链网络中的“去中心化”传统上侧重于技术韧性与抗审查能力，Arc 采取更广义的视角：通过与分布在多个法域且具系统重要性的多元机构开展战略协作，让这些实体参与网络验证，以提供能够支持关键金融运营、并具备合规能力与韧性的基础设施。这些验证者负责出块并确保网络的日常运营完整性与性能。其真实世界身份以及监管义务（如 SOC 2 合规）构成对恶意行为的强有力威慑。

在 Arc 上，交易要么未确认，要么 100% 最终且不可逆转，不存在概率性阶段。一旦超过三分之二的验证者通过多轮投票流程提交某个区块，该区块即刻获得最终性。这与金融市场基础设施原则（PFMI）的第 8

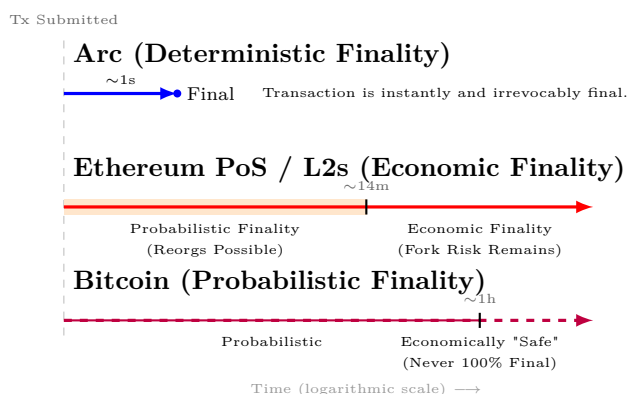


图 2: 不同最终性模型的时间线对比。

²验证者遴选标准包括但不限于：经验证的运营韧性记录、在线率保证、合规性与安全实践等。

条相一致，强调清晰而确定的最终结算 [Committee on Payment and Market Infrastructures and International Organization of Securities Commissions, 2012]。最终性的确定性对金融体系稳定至关重要，因为它为相关方的权利与关系提供明确基础，使其能够更有效地管理风险暴露 [Cheng, 2022]。在 Arc 上，这一过程在不到一秒内即可提供结算保证——这对需要确定性与速度并重的应用至关重要。

2.2.1 性能

Arc 面向机构级性能进行了工程化设计，提供高吞吐与快速最终性，以满足全球金融市场基础设施的严格要求。在 20 个地理分布的验证者场景下，Arc 约可处理每秒 3,000 笔交易 (TPS)，并实现低于 350 毫秒的近乎即时最终性。³ 在 4 个地理分布的验证者场景下，Arc 的吞吐可超过每秒 10,000 笔，最终性低于 100 毫秒。⁴ 这些性能基准基于商用硬件实现，表明在生产级基础设施下仍具有进一步提升的显著潜力。⁵

作为参照，在 20 验证者设置下，Arc 每日可处理的交易数量超过联邦储备 Fedwire 汇款系统的 280 倍。⁶ 这凸显了 Arc 运行规模远超传统实时全额结算系统的能力。⁷

Malachite 共识引擎的规划增强包括引入多提议者 (multi-proposer)，有望将吞吐提升约 10 倍；以及可选的更低容错配置，可将时延降低约 30%。

2.2.2 缓解 MEV 的路线图

Arc 设计哲学的关键方面是缓解最大可提取价值 (MEV)。虽然在许多公链上，MEV 已成为网络拥堵、不稳定以及掠夺性行为的重要来源 [Daian et al., 2019]，Arc 的路线图认识到，并非所有 MEV 都是有害的。在稳定币原生支付的语境下，Arc 将 MEV 大致分为“建设性”与“有害”两类。建设性 MEV 包括跨场所套利，有助于提升稳定币的同质性，并保持链上市场的外汇价格紧密对齐——二者对无缝的支付体验至关重要。例如，使 USDC/EURC 在不同流动性场所间价格趋同的套利，直接支持稳定币在商业中的可靠性。相反，有害

³ 该 20 验证者设置包含 10 个地区，每个地区 2 个验证者。10 个地区为：纽约（两个数据中心）、阿姆斯特丹、法兰克福、伦敦、旧金山、多伦多、新加坡、悉尼与班加罗尔。

⁴ 该 4 验证者设置包含 3 个地区，纽约 2 个验证者，另 2 个分别位于旧金山与多伦多。

⁵ 需注意，这里的时延尚未计入 EVM 执行的额外开销，因为基准测试主要聚焦于共识层。

⁶ 基于 2025 年 6 月 Fedwire Funds Service 数据：平均每日 912,515 笔转账。

⁷ 关于支付稳定币在实时全额结算中的讨论，参见 Liao et al. [2023]。

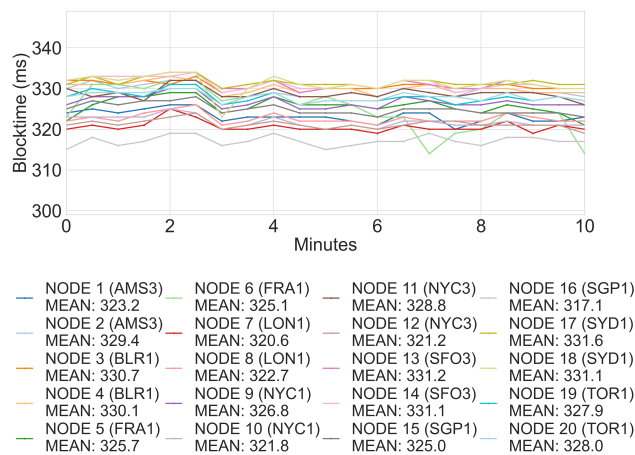


图 3: 20 个地理分布验证者下 Malachite 共识引擎在 10 分钟窗口内的区块时间（毫秒，纵轴，对时间横轴）。

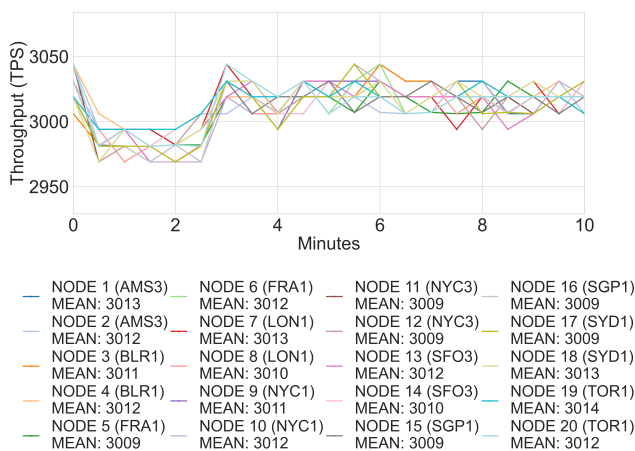


图 4: 20 个地理分布验证者下 Malachite 共识引擎在 10 分钟窗口内的吞吐 (TPS，纵轴，对时间横轴)。

MEV 包括三明治攻击等在支付意图与最终结算之间插入“有毒流”的行为，这些行为降低交易的可预测性并削弱用户信任，尤其是在需要低时延的场景（如 POS 或 B2B 支付）。因此，网络设计将致力于区分并抑制掠夺性抢跑，同时保留有助于价格发现与市场效率的有益跟跑 (back-running) 活动。为此，路线图将引入高级缓解技术，例如加密内存池、批量交易处理与多提议者，以营造公平有序、面向机构级金融结算的市场。

2.3 隐私：面向合规金融的路线图

若要将金融服务迁移到链上，隐私不是选项，而是前提。从工资支付到贸易融资明细，再到企业财资运营，敏感的商业与个人数据无法在完全透明的公共账本上暴露。然而挑战在于：在保留对监管方、审计方与授权第三方的完全可审计性的同时实现隐私，并使机构能够完全履行其监管义务。Arc 通过务实、分阶段的路线图实现这一目标，以可选择开启的隐私为核心，采用模块化与面

向未来的架构。

Arc 的隐私路线图以**保密转账**为起点——该特性在保持链上结算的同时，向公众隐藏交易金额。需要将其与完全匿名（还会隐藏地址）区分开来。在第一阶段，交易双方地址仍在公共账本上可见，但转账金额会被加密。此设计既为敏感商业数据提供机密性，也确保公共账本仍与现有链上分析与监测工具兼容，以支持地址追踪。

鉴于全球金融在受监管环境中运行，Arc 的隐私模型从一开始就支持机构内部的合规程序。可选特性允许通过“查看密钥（view keys）”等机制进行选择披露，为审计或监管等授权第三方提供特定交易数据的只读访问。此外，机构始终对其自身客户所进行的交易拥有完全可见性，包括上下游交易，这对于满足交易监测与旅行规则（Travel Rule）等监管义务至关重要。

上述能力通过模块化架构实现：智能合约可通过专用 EVM 预编译与密码学后端交互。该后端利用可信执行环境（TEE）在加密数据上进行计算。尽管许多隐私方案受制于性能，Arc 依托 TEE 的保密转账可提供快速且可审计的“遮蔽”交易。模块化设计也允许随着新型密码后端的成熟进行集成，使 Arc 能在不牺牲机构对时延与用户体验（UX）预期的前提下，交付“保密金融”。

展望未来，路线图将超越简单转账，迈向**私有状态与保密计算**。更高级的隐私形态将允许复杂金融逻辑（例如私有订单簿的状态、贸易融资协议或自动化财资）以私密方式管理。该分阶段推进基于模块化与面向未来的设计。虽然 TEE 为保密计算提供了成熟且高性能的起点，但 Arc 的架构并不绑定于单一技术。可插拔的后端设计将允许在其成熟可用于生产级金融系统后，集成包括多方安全计算（MPC）、同态加密（FHE）与零知识证明在内的其他先进隐私增强技术。

3 原生应用与用例

Arc 被设计成一套金融操作系统，提供一系列原生应用与服务，使开发者能够构建复杂的金融产品。该一体化方法降低了复杂性，并为创新提供坚实基础。Arc 不仅为 Circle 的产品而建——它也是面向机构、开发者与企业家的开放式邀请，邀请大家在信任、安全与规模化的前提下，共同构建下一代金融创新。

3.1 稳定币、可编程外汇与代币化资产

Arc 的一项关键能力是对多种形式的代币化货币的原生支持。除 Circle 发行的 USDC、EURC 与代币化货币市场基金 USYC 在主网上线即受支持外，Arc 亦是一个开放平台，旨在支持其他代币化货币的发行方——从法币支持稳定币到代币化银行存款与央行货币。这使得创

建锚定美元以外货币的稳定币与代币化工具成为可能，从而促进更具包容性的全球金融体系。结合未来内置的付费代理抽象（paymaster abstraction），用户将能够以本地稳定币支付费用，大幅提升非美元中心化应用的可用性。

Arc 还被设计为代币化、可产生收益的资产的优质场所。主网上线即支持 Circle 的 USYC——一种受监管的、以短久期美国国债为抵押的计息代币。⁸ 这为机构、企业 with 合格 DeFi 协议提供了原生的、链上的低风险收益来源，使其资本在安全与合规环境中发挥效用。像 USYC 这样的资产集成为 Arc 赋能强大的链上财资管理、抵押借贷以及新型资本市场基础设施的创建。

在多货币基础之上，Arc 的路线图包括一套机构级外汇（FX）引擎。该引擎使经过审查的交易对手之间能够在 7x24 小时场景下，实现可编程的货币兑货币（PvP）结算；同时利用链上智能合约进行交易登记、可配置的结算窗口与抵押品管理。它还集成链下的询价（RFQ）执行层，使机构级吃单方能够从做市商网络获取 FX 报价。初期，FX 引擎将以经许可系统运行，以确保合规性、市场完整性与关键通道的深度流动性。长期路线图还包括一套去许可的协议，以便向更广泛的参与者开放机构级 FX 流动性。⁹

最后，Arc 还被设计以支持高质量代币化金融资产的下一阶段发展。除稳定币与代币化现金工具之外，该平台也将支持受监管的现实世界资产（RWA）的发行、结算与可组合性——包括代币化股票、固收产品、私募信贷、私募基金与其他机构级证券。这将与受监管的资产发行方、托管方与基金管理人协作完成，以确保代币化表示具有稳健的法律基础、恰当的抵押与与真实世界金融义务的集成。一旦在 Arc 上发行，这些代币化资产即可与完整的 DeFi 原语进行原生组合——包括借贷协议、交易与兑换场所、质押机制与收益策略。由此，资本配置方、金融科技企业与资产管理人能够构建新一代金融产品，这些产品透明、自动化、全球可达，同时仍锚定于真实世界的合规要求。

通过将链下金融系统迁移至链上，Arc 改变了过去受地理、基础设施或牌照限制的金融工具的可得性。它创建了一个统一环境，使全球投资者能够持续地访问、交易与结算资产，并通过可选隐私控制来满足合规义务。Arc 不仅是数字资产的区块链，更是自底向上重塑资本市场的平台。

这些关于稳定币发行、高质量代币化资产与可编程外汇的能力，使网络成为打造新一代全球金融应用的强大平台：从跨境支付解决方案到自动化对冲、链上资本市场

⁸关于 USYC 可用性的免责声明见文末注释。

⁹关于链上外汇与跨境支付的讨论，参见 Adams et al. [2023]。

以及企业财资的货币风险管理工具。

3.2 跨链流动性与结算枢纽

Arc 被设计为稳定币流动性与应用的枢纽。凭借快速最终性与 USDC 作为 Gas, Arc 将使用户能够通过 Circle 的 CCTP 与 Gateway, 在十余条甚至更多区块链上的任意应用间实现即时访问。通过这些互联能力, 用户可以在不关心底层链的前提下使用 USDC 与应用交互, 将跨链活动简化为统一直观的体验。Arc、USDC 与 Circle 的互操作产品共同构成无摩擦金融生态的基础。

这一能力由一组原生集成的 Circle 产品赋能:

- **Mint:** Circle 客户可从法币银行存款直接在 Arc 上无缝铸造 USDC 与 EURC, 打造从传统金融到链上资本的最快上坡道, 无需依赖授信或预置流动性。
- **CCTP (跨链转移协议)**¹⁰: 作为 USDC 的原生发行链, Arc 借助 CCTP 实现对任意连接区块链的无许可、安全且快速的稳定币流动性转移, 使资本能够迅速流向最需要的地方。
- **Gateway:** Arc 通过 Gateway 支持跨链抽象的 USDC 余额, 使企业可在各链之间即时 (<1 秒) 满足稳定币流动性需求, 无需预先注资或再平衡。应用与数字钱包可在统一余额与跨生态可组合性的基础上, 交付无缝用户体验。

这些产品也将努力扩展至其他稳定币, 以实现跨链流动性愿景。

这一模型的基石是 Arc 的确定性最终性。由于交易在单个区块内即获得最终性 (亚秒级), 因此 Arc 上的流动性可以被销毁并在目标链上几乎瞬时地、可验证地重新铸造。这消除了依赖概率性或经济性最终性的链上所需的长时间等待 (跨链桥必须等待结算保证)。因此, Arc 既是法币到稳定币转换的最快上坡道, 也是将该流动性分发至更广泛区块链版图的最高效分层。

3.3 企业级支付与结算

稳定的计价单位、可预测的费用、快速的结算与机密性相结合, 使 Arc 成为企业级支付与结算的理想平台。网络的原生特性旨在支持企业金融的复杂需求, 不仅仅是简单的价值转移, 还可实现复杂、可编程的支付 workflow。

Arc 为开发者与企业提供一组核心支付模块 (计入 Arc 路线图并逐步交付), 可组合为强大的应用:

- **发票关联支付:** 对交易附加结构化数据 (如发票详

情或消息) 的原生支持。¹¹ 这有助于简化对账并自动化应付/应收流程。

- **退款与争议协议:** 管理退款与解决支付争议的链上机制。它提供了主流采用所必需、但许多现有区块链系统所缺乏的消费者与商户保护水平。
- **智能财资代理:** 可创建自治、面向 AI 的代理来管理企业财资, 执行可编程支出政策, 并实时优化营运资本。这将释放可扩展的、实时化的金融运营, 降低人工开销并提升资本效率。

这些能力将与 Circle Payments Network (CPN) 协同, 提升跨境支付的运营效率, 同时支持从自动化全球供应链金融与版税分发, 到构建完全合规的链上薪酬系统与资本市场基础设施在内的广泛重要用例。通过这些工具作为原生原语提供, Arc 显著降低了企业在区块链上构建与部署安全、高性能且合规金融解决方案的门槛。

4 路线图

Arc 公开测试网预计于 2025 年秋季推出。Arc 的主网测试版将包含核心组件, 例如稳定费率架构、毫秒级的确定性最终性与 FX 引擎路线图。此外, Circle 的平台产品 (CPN、USDC、EURC、USYC、Mint、Wallets、Contracts、CCTP、Gateway、Paymaster 等) 以及第三方生态基础设施支持也将一并可用。

隐私增强将在后续的网络升级中推出, 起步于保密转账, 并逐步演进到完全可编程的隐私功能。除隐私之外, Arc 还将在路线图中探索 MEV 缓解方案, 例如加密内存池、批量交易处理与多提议者, 以营造公平有序、面向机构级金融结算的市场。

最后, Arc 的额外安全保障路线图还包括过渡到一种经许可的权益证明 (PoS) 机制 (在选定验证机构集合内实施)。该升级可在更广泛验证者去中心化与治理灵活性之间取得平衡, 符合 Circle 的长期目标, 确保网络稳健运行。它还确保在初始验证者集合之外, Arc 能够独立于 Circle 运行, 从而带来额外的运营韧性。Malachite 的路线图还包括一种新颖的多提议者设计以提升性能, 并在共识栈上进行多项优化, 例如通过“两阶段 Tendermint”变体减少时延。

5 结论

Arc 从根本上重构了用于金融与商业的区块链基础设施应该是什么样子。它扎根于对在互联网上构建全球化、受监管且高效金融系统的务实理解, 真正满足机构、平

¹⁰关于 CCTP 的细节, 见 Mayerchak et al. [2025]。

¹¹参见 Belenkiy [2025], 关于“Recibo: 用于 ERC-20 交易的加密消息”。

台与企业的现实需求。通过解决围绕费率波动、结算不确定性以及隐私与合规无法兼得的核心限制，Arc 为可编程货币时代提供了量身打造的基础。

本文提出的关键创新——以 USDC 作为 Gas 的稳定币原生架构、高性能且确定性的结算最终性，以及对合规隐私的长期承诺——并非孤立的特性，而是一个一致愿景下的有机整体，共同构建面向现代经济的基础信任层。

Arc 是互联网的速度与开放，与受监管金融的信任与可靠性交汇之处。

从全球支付与跨境汇款，到代币化资本市场与自治的企业财资，应用前景广阔。Arc 旨在成为互联网上构建金融服务与应用的安全、透明与高性能结算层。我们诚邀全球领先的金融机构、企业与创新者，共同以互联网规模构建金融与商业的未来。

参考文献

- Austin Adams, Mary-Catherine Lader, Gordon Y. Liao, David Puth, and Xin Wan. On-chain foreign exchange and cross-border payments. *SSRN Electronic Journal*, 2023. doi: 10.2139/ssrn.4328948. URL <https://ssrn.com/abstract=4328948>. Accessed August 2025.
- Basel Committee on Banking Supervision. Prudential treatment of cryptoasset exposures. Technical report, Bank for International Settlements, December 2022. URL <https://www.bis.org/bcbs/publ/d545.pdf>.
- Mira Belenkiy. Recibo: Encrypted messages for ERC-20 transactions. <https://www.circle.com/blog/recibo-encrypted-messages-for-erc-20-transactions>, January 2025. Accessed July 2025.
- Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, Ian Norden, and Abdelhamid Bakhta. EIP-1559: Fee market change for ETH 1.0 chain. <https://eips.ethereum.org/EIPS/eip-1559>, April 2019. Ethereum Improvement Proposal 1559.
- Juliet M. Cheng. How to build a stablecoin: Certainty, finality, and stability through commercial law principles. *Berkeley Business Law Journal*, 19(1):129–170, 2022. URL <https://scholarship.law.berkeley.edu/bblj/vol19/iss1/5/>.
- Committee on Payment and Market Infrastructures and International Organization of Securities Commissions. Principles for financial market infrastructures. Technical report, Bank for International Settlements, April 2012. URL <https://www.bis.org/cpmi/publ/d101.htm>.
- Committee on Payments and Market Infrastructures. Enhancing cross-border payments: building blocks of a global roadmap - technical background note. Technical report, Bank for International Settlements, July 2020. URL <https://www.bis.org/cpmi/publ/d194.pdf>.
- Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges. *arXiv preprint arXiv:1904.05234*, 2019.
- Quinn Dupont. Experiments in algorithmic governance: A history and ethnography of 'the dao,' a failed decentralized autonomous organization. In Malcolm Campbell-Verduyn, editor, *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, pages 169–187. Routledge, 2018.
- Gordon Y. Liao, Thomas Hadeed, and Ziming Zeng. Beyond speculation: Payment stablecoins for real-time gross settlements. *SSRN Electronic Journal*, June 2023. doi: 10.2139/ssrn.4476859. URL <https://ssrn.com/abstract=4476859>. Accessed August 2025.
- Walker Mayerchak, Mike Grant, Jonathan Lim, Chase McDermott, Elim Poon, Adrian Soghoian, Kaili Wang, and Gordon Y. Liao. Cross-Chain Transfer Protocol (CCTP) V2. https://github.com/circlefin/evm-cctp-contracts/blob/master/whitepaper/CCTPV2_White_Paper.pdf, March 2025. Accessed July 2025.

免责声明 本文仅用于一般信息目的。本文不构成投资建议，亦非购买或出售任何投资的建议或招揽，亦不应用于评估任何投资决策优劣之用。本文不应被依赖作为会计、法律或税务建议，或投资建议。Arc 由 Circle Technology Services, LLC (“CTS”) 提供。CTS 为软件服务提供方，不提供受监管的金融或咨询服务。本文所述所有产品特性可在任何时间、由 CTS 自主决定地进行修改、延期或取消，恕不另行通知。您对向用户提供的服务承担全部责任，包括但不限于获取任何必

要的牌照或审批，并遵守适用法律。本文所述仅反映作者当前观点，并不代表 Circle Internet Group 或其附属机构的立场，也不必然反映与他们相关的个人之观点。本文观点如有变更，恕不另行更新。

USYC 为一种数字资产代币。每个 USYC 代币代表 Hashnote International Short Duration Fund Ltd. (“基金”) 的一股的数字化表示，该基金为开曼群岛注册的互惠基金。基金已委任 Circle International Bermuda Limited (“CIBL”) 作为其代币管理员，负责代表基金管理 USYC。

基金份额与 USYC 仅向《1933 年证券法》(经修订) 项下的非美国人士 (Non-U.S. Persons) 开放。其他资格限制亦可能适用。本文所提供的信息仅用于教育与信息目的，不应被解释为出售要约或购买任何证券、金融工具或其他产品的招揽。