Arc: An open Layer-1 blockchain purpose-built for stablecoin finance

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

August 2025

Abstract

Arc is a purpose-built, EVM-compatible Layer-1 blockchain advancing the frontier of stablecoin finance and tokenization. It features USDC as native gas, deterministic settlement finality, opt-in privacy, and a stable transaction fee architecture. Optimized for stablecoin-native use cases, such as global payments, FX, and capital markets, Arc serves as a foundational settlement layer for programmable money on the internet.

1 Introduction

The global financial system, while foundational to modern commerce, operates on legacy infrastructure that is fundamentally incompatible with the speed, openness, and programmability of the internet. Despite decades of innovation in consumer and enterprise software, financial access, inclusion, and real-time capital mobility remain deeply constrained, particularly across borders and in emerging markets. Cross-border payments are slow, opaque, and expensive. Treasury operations are fragmented across jurisdictions, intermediaries, and incompatible financial rails. Capital markets remain gated, siloed, and burdened by manual processes and layers of middlemen. These structural inefficiencies create economic costs and introduce counterparty and operational risks that are systemic in nature [Committee on Payments and Market Infrastructures, 2020].

The advent of blockchain technology promised a new paradigm for finance and commerce, offering programmability, transparency, and censorship-resistance. However, existing public blockchains present fundamental limitations that impede institutional and enterprise adoption. The use of volatile native tokens for gas fees introduces unpredictable operational costs and accounting complexities. Furthermore, a lack of clear settlement finality on many chains introduces financial risk, while the absence of transaction privacy is a key missing component for sensitive commercial activities. The permissionless and transparent nature of transaction submission also gave rise to phenomena such as Maximal Extractable Value (MEV), where privileged actors exploit transaction ordering for profit, degrading market integrity [Daian et al., 2019]. Finally, fragmentation of stablecoin liquidity and apps across multiple blockchains creates friction for both users and developers.

To address these key gaps, this litepaper introduces Arc, an open Layer-1 blockchain purpose-built for stablecoin finance. It is built on the conviction that the future of finance and commerce is not a wholesale replacement of the old, but a synthesis of the new and the established: the programmability of smart contracts with the enforceability of law (i.e., GENIUS Act); the efficiency of blockchain with the stability of fiat-backed currency; and the transparency of public ledgers with the privacy required for commercial transactions. As an EVM-compatible network, Arc provides a familiar environment for programmability, and its adoption of a high-performance Byzantine Fault Tolerant (BFT) consensus, based on Tendermint (Malachite), provides the institutional-grade infrastructure required for regulated financial services at internet scale. This design, which relies on a permissioned set of validators, aligns with emerging regulatory frameworks, such as the Basel Committee on Banking Supervision's prudential treatment of cryptoassets, which outlines a path for stablecoins on networks with robust controls to be classified as "Group 1" assets with more favorable capital treatment for banks [Basel Committee on Banking Supervision, 2022].

At its core, Arc redefines how digital value is transacted and secured. It introduces three key innovations:

1. **Stable Fee and USDC as Native Gas:** significantly reduces fee volatility and accounting complexity by using USDC as the native asset for transaction fees while also supporting other local stablecoins and tokenized money as gas through a dedicated paymaster integration.
2. **Deterministic Settlement Finality:** provides clear and certain final settlement in less than one second, aligned with the Principles for Financial Market Infrastructures [Committee on Payment and Market Infrastructures and International Organization of Securities Commissions, 2012].
3. **Opt-In Privacy:** integrates privacy-preserving technologies to enable transactions with selective transparency, a prerequisite for many sensitive financial workflows and a feature that would support institutions' own compliance programs.

Arc delivers the infrastructure required for finance at internet scale. Circle Internet Group (hereinafter Circle) is uniquely positioned to lead this effort because of its experience operating USDC, building financial primitives across chains, and working closely with institutions, regulators, and the developer community. By focusing on the unique requirements of stablecoin-based finance, Arc provides a foundational settlement layer and liquidity hub for programmable money.

2 Core Architecture of Arc

The architecture of Arc is designed from the ground up to provide a robust, institutional-grade foundation for financial services and applications to be built using stablecoins and tokenized assets. It aims to overcome the critical limitations of existing blockchains by delivering a platform that is secure, performant, and tailored for regulated financial applications and real-world commerce. As illustrated in Figure 1, the network's core is a permissioned set of validators operating on the Malachite consensus engine, providing the bedrock for its performance and security. This architecture is built on three foundational pillars, each addressing a critical need for mainstream financial adoption.

First, the network is **stablecoin-native**, using USDC for gas to eliminate fee volatility and simplify operations. Second, it delivers deterministic, sub-second **settlement finality** through a high-performance consensus engine, providing the certainty required for high-value settlement. Third, it features **opt-in privacy** on its roadmap, enabling selective transparency on balances and transactions to shield sensitive financial information while preserving auditability. These core features are designed to support stablecoin-native applications like programmable FX, payments, and institutional trading, while seamlessly connecting to the broader onchain and offchain financial systems through Circle's platform and growing stablecoin partner ecosystem. This section will elaborate on these three core architectural pillars, which collectively establish Arc as a trusted settlement layer for the internet-native economy.

2.1 USDC as Native Gas and Stable Fee Mechanism

A foundational design principle of Arc is the use of USDC as the native asset for all transaction fees (gas). Additionally, Arc will support other local stablecoins and tokenized fiat money as gas through a dedicated paymaster integration. The decision to have gas tied to fiat currency values addresses a critical barrier to enterprise adoption of blockchain technology: the volatility and accounting complexity associated with using a speculative native token for operational costs. By denominating fees in a stable unit of account, Arc provides predictable, auditable, and streamlined financial operations for users and developers. This aligns the unit of account for value transfer with the unit of account for transaction cost.

To illustrate this point with a simple model, consider the cost of a transaction, C_{USD}, from a user's perspective. In a network using a volatile native asset (e.g., ETH), the cost in U.S. dollars is a product of three variables: the gas units consumed (g), the protocol's base fee in the native asset per unit gas (b_{native}), and the market price of that asset (P_{native}). Thus, $C_{USD} = g \times b_{native} \times P_{native}$. This cost has two distinct sources of volatility: protocol-driven volatility in b_{native} (from block space demand) and market-driven volatility in P_{native} (from speculation). A fee stability mechanism like EIP-1559 can only influence b_{native}, leaving users fully exposed to the price volatility of the gas token, which is often the dominant factor. This makes it impossible for the protocol to provide predictable, dollar-denominated transaction costs.

By contrast, on Arc, the cost is $C_{USD} \approx g \times b_{USDC}$, since the price of USDC is stable at \$1. Market-driven price volatility is effectively eliminated as a variable. The protocol can therefore directly and meaningfully manage transaction costs in a stable unit of account by adjusting b_{USDC}. This shift from dual volatility to single, protocol-managed volatility fundamentally de-risks the use of the blockchain for enterprises. It enables predictable financial planning and robust business models, thereby enhancing the adoption potential of the network for institutional and commercial use cases.

The choice to use a stablecoin as the native gas asset is not merely for convenience; it unlocks a powerful design space for fee structures that is impossible with a volatile token. It allows for predictable fee markets, programmatic fee rewards and subsidies, and dedicated paymaster services that enable users to pay fees in other currencies.

At launch, Arc will implement a fee market designed for stability and predictability, inspired by Ethereum's EIP-1559 [Buterin et al., 2019]. The primary enhancement is a fee smoothing mechanism: instead of adjusting on a per-block basis, the protocol's base fee is updated using an exponentially-weighted moving average of block utilization. This approach, combined with a bounded base fee, dampens short-term volatility and ensures that transaction costs remain consistently low. The fees at launch are directed to an onchain Arc Treasury to support the network's long-term growth.

2.2 Consensus and Finality

Arc's security model is engineered to provide a higher degree of trust and resilience than what is achievable through conventional consensus alone. It accomplishes this by combining a high-performance consensus engine, Malachite, that allows for deterministic finality with a permissioned set of established validators to guarantee the integrity of the network.

Arc is designed not to compete for existing transaction volume, but to instead expand the total addressable market by providing the specific, high-frequency settlement assurances required to bring the next trillion dollars of payments and institutional capital onchain.

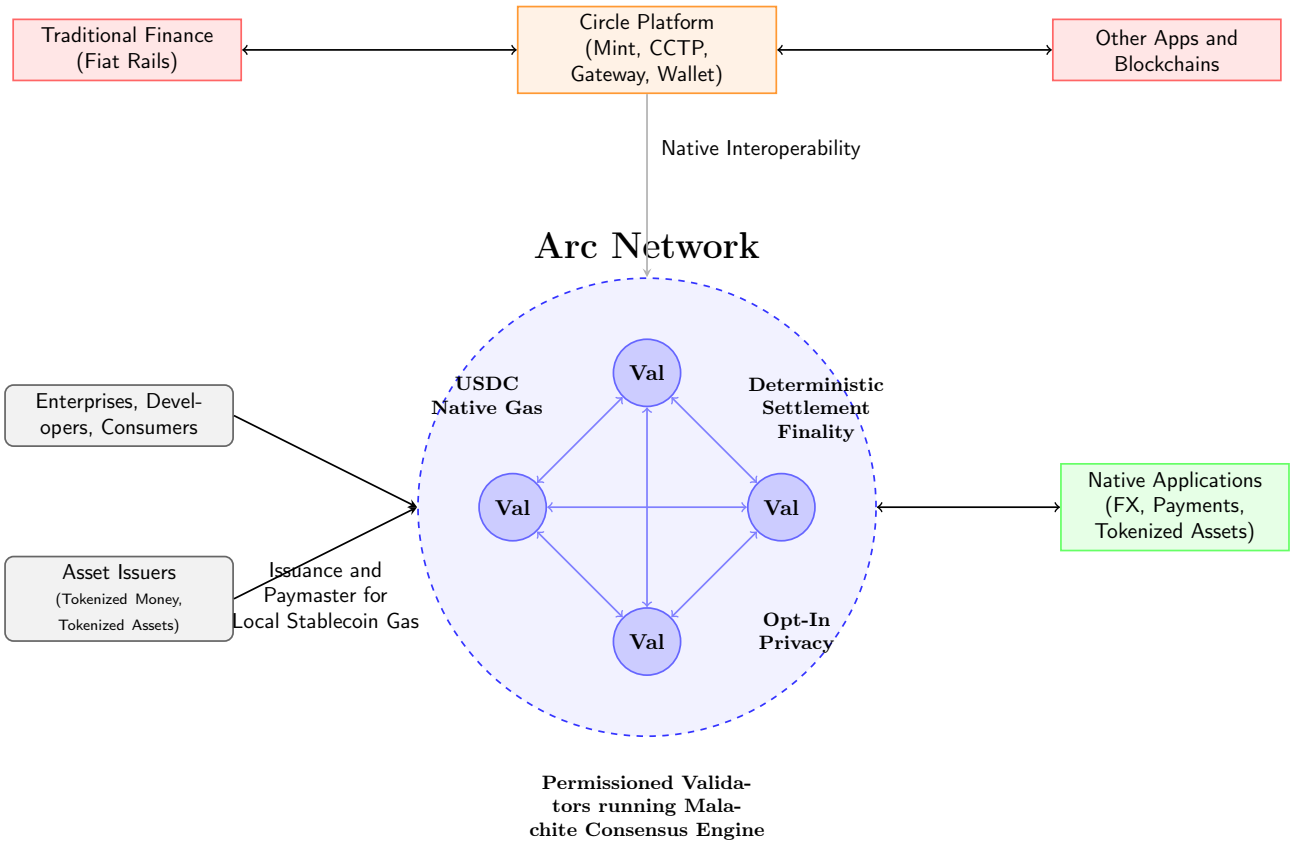

Figure 1: The architecture of Arc, highlighting its core components, native applications, and connectivity to the broader financial ecosystem.

One of the major deterrents to public blockchains becoming global financial market infrastructure is a lack of a clear definition of settlement finality. On most existing blockchains including Proof-of-Stake (PoS) and Proof-of-Work (PoW) chains, transactions often pass through a probabilistic state and are subject to chain reorganizations ("reorgs"), which can reverse recently confirmed transactions. This settlement ambiguity introduces risk and capital inefficiency for high-value financial workflows. In an extreme case, permissionless PoS chains can also suffer from a finality attack that reverses a finalized block if a malicious actor obtains a supermajority of the staked tokens. While the value of staked tokens is typically sufficient for the current scale of crypto-native use cases, securing trillions of dollars in tokenized financial assets would necessitate a far greater magnitude of economic stake. Additionally, even "settled" transactions on many chains can be reversed by a socially-coordinated spin-off that depends on the governance of the ecosystem.[1] Furthermore, Layer-2 networks built on top of Layer 1 inherit the same finality risks and latency from their base layer.

The foundation of Arc's institutional-grade performance and security is its consensus, which is built on Malachite, a high-performance implementation of the Tendermint BFT protocol. This choice represents a deliberate departure from the probabilistic finality models of early-generation blockchains as well as the centralized sequencing of more recent Layer-2s.

Arc will rely on a permissioned, Proof-of-Authority (PoA) validator set composed of a limited number of known, established, and geographically distributed institutions held to high standards of accountability and operational guarantees.[2] Arc aims to establish itself as foundational infrastructure for regulated money movement, supporting a globally distributed financial system. While decentralization in blockchain networks has traditionally been associated with technological resilience and censorship resistance, Arc adopts a broader perspective. Arc envisions a model of decentralization rooted in strategic collaboration with a diverse, globally distributed set of jurisdictions and systemically important institutions. By enabling these entities to participate in network validation, Arc aims to offer a resilient and compliant infrastructure capable of supporting mission-critical financial operations for both sovereigns and enterprises worldwide. These validators are responsible for producing blocks and ensuring the day-to-day operational integrity and performance of the network. Their real-world identities and, often, regulatory obligations and SOC 2 compliance requirements provide a strong deterrent against malicious behavior.

A transaction on Arc is either unconfirmed or it is 100% final and irreversible. There is no probabilistic

[1] See DuPont [2017] for discussion on the DAO hack fork.

[2] Validator selection criteria include but are not limited to: proven history of operational resilience, uptime guarantees, regulatory compliance, and security practices.

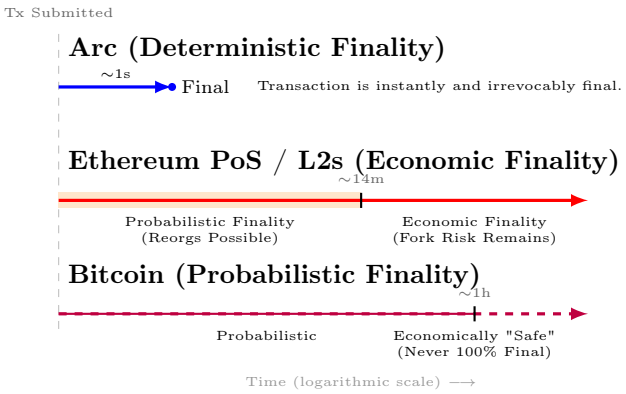

Figure 2: A timeline comparison of finality models.

phase. Once a block is committed by over two-thirds of the validator set through a multi-round voting process, it is instantly final. This aligns with Principle 8 of the Principles for Financial Market Infrastructures (PFMI), which emphasizes clear and certain final settlement [Committee on Payment and Market Infrastructures and International Organization of Securities Commissions, 2012]. The certainty of finality is critical for financial system stability, as it provides a baseline foundation of clarity and certainty regarding the rights and relationships between parties, allowing them to manage their risk exposure more effectively [Cheng, 2020]. This process provides settlement guarantees in less than one second—a critical feature for applications where certainty and speed are paramount.

2.2.1 Performance

Arc is engineered for institutional-grade performance, delivering high throughput and rapid finality to meet the rigorous demands of global financial market infrastructure. Arc is capable of processing approximately 3,000 transactions per second (TPS) with near-instantaneous finality of less than 350 milliseconds, with a geographically distributed set of 20 validators.[3] With four geographically distributed validators, Arc's throughput can exceed 10,000 TPS with finality of less than 100 milliseconds.[4] These performance benchmarks were achieved using commodity hardware, indicating significant potential for even greater throughput with production-grade infrastructure.[5]

To put this into perspective, with 20 validators, Arc can process over 280 times the number of daily transactions of the Fedwire Funds Service.[6] This performance underscores Arc's capability to operate at a scale far beyond traditional real-time gross settlement systems.[7]

Planned enhancements to the Malachite consensus engine include multi-proposer support, which could increase throughput by roughly 10x, and optional lower fault-tolerance configurations that can reduce latency by about 30%.

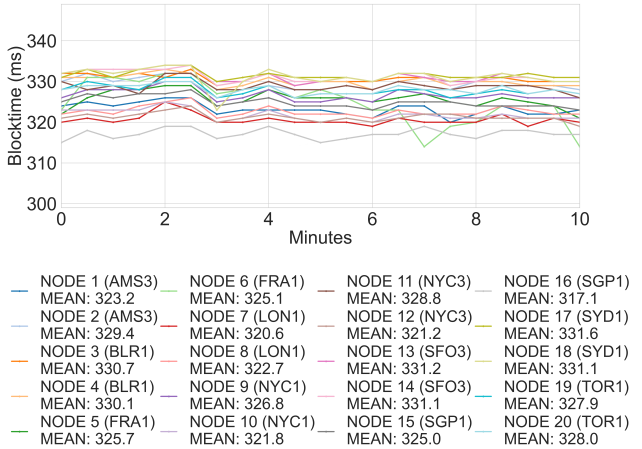

Figure 3: Blocktime in milliseconds (y-axis) for Malachite Consensus Engine with 20 geographically distributed validating nodes over 10 minutes (x-axis)

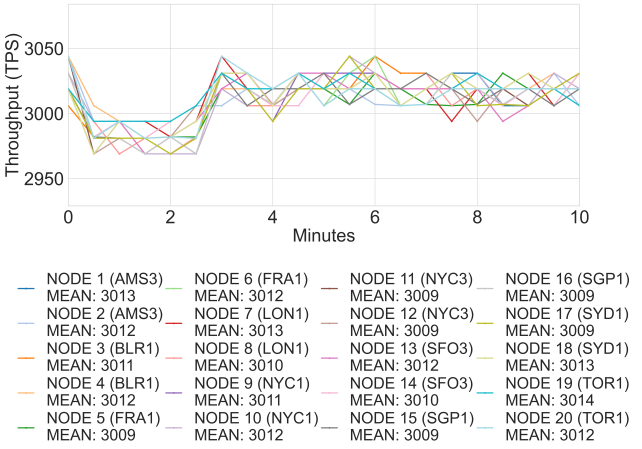

Figure 4: Throughput in Transactions per Second (y-axis) for Malachite Consensus Engine with 20 geographically distributed validating nodes over 10 minutes (x-axis)

2.2.2 Roadmap to Mitigate MEV

A crucial aspect of Arc's design philosophy is its approach to mitigating Maximal Extractable Value (MEV). While MEV has become a significant source of network congestion, instability, and predatory behavior on many public blockchains [Daian et al., 2019], Arc's roadmap acknowledges that not all forms of MEV are detrimental. In the context of stablecoin-native payments, Arc classifies MEV into two broad categories:

[3] The 20-validator setup has 10 regions, with 2 validators in each region. The 10 regions are: New York (two data centers), Amsterdam, Frankfurt, London, San Francisco, Toronto, Singapore, Sydney, and Bangalore.

[4] The 4-validator setup has 3 regions, with 2 validators in New York and the other two validators in San Francisco and Toronto, respectively.

[5] It is also important to note that this latency does not yet account for the additional overhead of EVM execution as the benchmarks were focused on consensus.

[6] Based on Fedwire Funds Service data for June 2025, which showed 912,515 average daily transfers.

[7] See Liao et al. [2023] for discussions of payment stablecoins for real-time gross settlements.

constructive and harmful. Constructive MEV includes cross-venue arbitrage that enhances stablecoin fungibility and keeps FX rates tightly aligned across onchain markets—both of which are essential for a seamless payments experience. For example, arbitrage that equalizes USDC/EURC prices across liquidity venues directly supports stablecoin reliability in commerce. Conversely, harmful MEV includes sandwich attacks and other behaviors that insert toxic flow between payment intent and final settlement, degrading transaction predictability and undermining user trust—particularly in low-latency use cases like point-of-sale or B2B payments. The network's design will therefore aim to distinguish between and discourage predatory front-running while preserving beneficial arbitrage activities, such as back-running between decentralized exchanges, that contribute to price discovery and market efficiency. To this end, the roadmap includes implementing advanced mitigation techniques, such as encrypted mempools, batch transaction processing, and multi-proposers, to foster a fair and orderly market optimized for institutional-grade financial settlement.

2.3 Privacy: A Roadmap for Compliant Finance

For financial services to migrate onchain, privacy is not an option; it is a requirement. Sensitive commercial and personal data, from salary payments to trade finance details, and corporate treasury operations, cannot be exposed on a fully transparent public ledger. The challenge, however, is to enable privacy while preserving full auditability for regulators, auditors, and authorized parties, and enabling institutions to fully comply with their own regulatory obligations. Arc addresses this through a pragmatic, phased roadmap designed to deliver **opt-in privacy** via a modular, future-proof architecture.

Arc's privacy roadmap begins with **confidential transfers**, a feature that shields transaction amounts from public view while maintaining onchain settlement. It is crucial to distinguish this from full anonymity that additionally shields addresses. In this first step, the addresses of the parties involved in a transaction remain visible on the public ledger, but the value of the transfer is encrypted. This design provides confidentiality for sensitive commercial data while ensuring that the public ledger remains compatible with existing blockchain analytics and monitoring tools for address tracing.

Recognizing that global finance operates within a regulated environment, Arc's privacy model is built to support institutional compliance programs. The opt-in features allow for selective disclosure through mechanisms like "view keys", which grant authorized third parties, such as auditors or regulators, read-only access to specific transaction data. Furthermore, an institution always retains full visibility into the transactions conducted by its own customers, including up and downstream transactions, which is essential for regulatory obligations like transaction monitoring and the Travel Rule.

This is enabled through a modular architecture where smart contracts can interact with a cryptographic backend via a dedicated EVM precompile. This backend leverages technologies like Trusted Execution Environments (TEEs) to perform computations on encrypted data. While many privacy solutions suffer from performance constraints, Arc's use of TEEs for confidential transfers provides fast, auditable shielded transactions. This modular design also allows for the integration of new cryptographic backends as they mature, positioning Arc to deliver confidential finance without compromising the latency and UX expectations of institutions.

Looking ahead, the roadmap extends beyond simple transfers to enable **private state and confidential computation**. This more advanced form of privacy will allow complex financial logic—such as the state of a private order book, a trade finance agreement, or an automated treasury—to be managed privately. This phased rollout is underpinned by a modular and future-proof design. While TEEs offer a mature and performant starting point for confidential computation, Arc's architecture is not tied to a single technology. The pluggable backend design will allow for the future integration of other advanced privacy-enhancing technologies, including Multi-Party Computation (MPC), Fully Homomorphic Encryption (FHE), and zero-knowledge proofs, as they become ready for production-scale financial systems.

3 Native Applications and Use Cases

Arc is designed as a financial operating system with a suite of native applications and services that enable developers to build sophisticated financial products. This integrated approach reduces complexity and provides a robust foundation for innovation. Arc is not just built for Circle products — it is an open invitation to institutions, developers, and entrepreneurs to build the next wave of financial innovation with trust, security, and scale.

3.1 Stablecoins, Programmable FX and Tokenized Assets

A key capability of Arc is its native support for the issuance of multiple forms of tokenized money. While Circle-issued stablecoins like USDC and EURC and tokenized money market fund USYC will be supported at launch, Arc is an open platform designed to also support other issuers of tokenized money—from fiat-backed stablecoins to tokenized bank deposits and central bank money. This allows for the creation of stablecoins and tokenized instruments pegged to currencies beyond the U.S. dollar, enabling a more inclusive global financial system. Combined with future embedded paymaster abstraction, users will be able to pay fees in local stablecoins, dramatically improving usability for non-USD-centric applications.

Arc is also designed to be a premier venue for tokenized, yield-bearing assets. At launch, the network will support Circle's USYC, a regulated, interest-bearing token

collateralized by short-duration U.S. Treasury securities.[8] This provides a native, onchain source of low-risk yield, enabling institutions, enterprises, and qualified DeFi protocols to put their capital to productive use in a secure and compliant environment. The integration of assets like USYC transforms Arc into a powerful platform for onchain treasury management, collateral for lending, and the creation of new capital markets infrastructure.

Building on the multi-currency foundation, Arc's roadmap includes an institutional-grade foreign exchange (FX) engine. This engine enables 24/7, programmable, payment-versus-payment (PvP) settlement between vetted counterparties, leveraging onchain smart contracts for trade registration, configurable settlement windows, and collateral management. It also integrates an offchain Request-for-Quote (RFQ) execution layer, enabling institutional takers to source FX pricing from a network of market makers. Initially, the FX engine will operate as a permissioned system to ensure regulatory compliance, market integrity, and deep liquidity in key corridors. The long-term roadmap also includes a permissionless protocol that democratizes access to institutional FX liquidity.[9]

Finally, Arc is also designed to support the next evolution of high-quality, tokenized financial assets. Beyond stablecoins and tokenized cash instruments, the platform enables the issuance, settlement, and composability of regulated real-world assets (RWAs)—including tokenized equities, fixed income, private credit, private funds, and other institutional-grade securities. This will be achieved in partnership with regulated asset issuers, custodians, and fund administrators, ensuring that tokenized representations are legally robust, properly collateralized, and integrated with real-world financial obligations. Once issued on Arc, these tokenized assets can be composed natively with the full suite of DeFi primitives—including borrow and lend protocols, trade and swap venues, staking mechanisms, and yield strategies. This allows capital allocators, fintechs, and asset managers to build next-generation financial products that are transparent, automated, and globally accessible, while still anchored in real-world compliance.

By bringing the offchain financial system onchain, Arc transforms access to financial instruments that have historically been restricted by geography, infrastructure, or licensing. It creates a unified environment where investors around the world can access, trade, and settle assets continuously, with opt-in privacy controls to meet compliance obligations built into the protocol layer. Arc is more than a blockchain for digital assets; it is a platform for rebuilding capital markets from the ground up.

These capabilities for stablecoin issuance, high quality tokenized assets, and programmable FX transform the network into a powerful platform for building a new generation of global financial applications, from cross-border payment solutions to automated hedging, onchain capital markets, and currency risk management tools for enterprise treasuries.

3.2 A Crosschain Liquidity and Settlement Hub

Arc is designed to serve as the hub for stablecoin liquidity and applications. With fast finality and USDC as the gas token, Arc will enable users to instantly access any application across more than dozens of blockchains through Circle's CCTP and Gateway. Through these connectivities, users can use USDC with applications regardless of their underlying chain, simplifying crosschain activity into a unified, intuitive experience. Arc, USDC, and Circle's interoperability products together form the foundation for a frictionless financial ecosystem.

This capability is enabled by a suite of natively integrated Circle products:

- **Mint:** Circle customers can seamlessly mint USDC and EURC directly onto Arc from fiat bank deposits, creating the fastest possible onramp from traditional finance to onchain capital without credit reliance or liquidity prepositioning.
- **CCTP (Cross-Chain Transfer Protocol)[10]:** As a native issuance chain for USDC, Arc leverages CCTP to enable permissionless, secure, and rapid transfers of stablecoin liquidity to any connected blockchain. This allows capital to flow to where it is most needed without delays.
- **Gateway:** Arc supports chain-abstracted USDC balances via Gateway, enabling businesses to meet demand for stablecoin liquidity instantly (<1 second) across chains without prefunding or rebalancing. Apps and digital wallets can deliver seamless user experiences with unified USDC balances and composability across ecosystems.

These products will also aim to expand their utility for other stablecoins to enable this promise of crosschain liquidity.

The cornerstone of this model is Arc's deterministic finality. Because a transaction is final within a single block (sub-second), liquidity on Arc can be burned and then verifiably minted on a destination chain almost instantaneously. This eliminates the long waiting periods associated with chains that rely on probabilistic or economic finality, where crosschain bridges must wait for settlement assurance. Consequently, Arc functions as both the fastest chain to onramp for fiat-to-stablecoin conversion and the most efficient distribution layer for deploying that liquidity across the broader blockchain landscape.

[8] See endnote for disclaimer on USYC availability.

[9] See Adams et al. [2023] for discussion of on-chain FX and cross-border payments.

[10] See Mayerchak et al. [2025] for details on CCTP.

3.3 Enterprise-Grade Payments and Settlement

The combination of a stable unit of account, predictable fees, rapid settlement, and confidentiality makes Arc an ideal platform for enterprise-grade payments and settlement. The network's native features are designed to support the complex requirements of enterprise finance, moving beyond simple value transfer to enable sophisticated, programmable payment workflows.

Arc provides developers and enterprises with a suite of core payment modules that can be composed into powerful applications, accounted for on the Arc roadmap and including:

- **Invoice-linked Payments:** Native support for attaching structured data to transactions, such as invoice details or messages.[11] This simplifies reconciliation and automates accounts payable and receivable processes.
- **Refund and Dispute Protocols:** Onchain mechanisms for managing refunds and resolving payment disputes. This provides a level of consumer and merchant protection that is essential for mainstream adoption but often lacking in existing blockchain systems.
- **Smart Treasury Agents:** The ability to create autonomous, AI-native agents that can manage corporate treasuries, execute programmable spending policies, and optimize working capital in real-time. This unlocks scalable, real-time financial operations that reduce manual overhead and improve capital efficiency.

These capabilities will be leveraged with Circle Payments Network (CPN) to enhance the operational efficiency of cross-border payments, while also enabling a wide range of other important use cases, from automating global supply chain finance and royalty payments to building fully compliant, onchain payroll systems and capital markets infrastructure. By providing these tools as native primitives, Arc significantly lowers the barrier for enterprises to build and deploy secure, performant, and compliant financial solutions on a blockchain.

4 Roadmap

Arc's public testnet is expected in the Fall of 2025. The mainnet beta launch of Arc will contain core components such as stable gas fee architecture, sub-second deterministic finality, and the FX engine roadmap. Additionally, Circle's platform products (CPN, USDC, EURC, USYC, Mint, Wallets, Contracts, CCTP, Gateway, Paymaster and more) alongside third-party ecosystem infrastructure support will be available.

Privacy enhancements will come in a follow-on upgrade of the network, starting with confidential transfers and evolving into fully programmable privacy. In addition to privacy, MEV mitigation will also be explored on the roadmap such as encrypted mempools, batch transaction processing, and multi-proposers, to foster a fair and orderly market optimized for institutional-grade financial settlement.

Finally, the roadmap for additional security guarantees of Arc also includes a transition to a Proof-of-Stake (PoS) mechanism, which will be permissioned within the set of selected validating institutions. This upgrade enables broader validator decentralization and governance flexibility aligned with Circle's long-term desire to ensure the network is robust. It also ensures that Arc can function independently of Circle beyond the initial validator set, providing added operational resilience. The Malachite roadmap will also include a novel multi-proposer design to increase performance, alongside optimizations across the consensus stack such as reducing latency with a two-phase Tendermint variant.

5 Conclusion

Arc represents a fundamental rethinking of what blockchain infrastructure for finance and commerce should be. It is grounded in a pragmatic understanding of what is required to build a global, regulated, and efficient financial system on the internet, one that meets the real-world demands of institutions, platforms, and enterprises. By solving core limitations around fee volatility, settlement uncertainty, and the simultaneous lack of privacy and regulatory compliance, Arc delivers a purpose-built foundation for the era of programmable money.

The key innovations presented in this paper: a stablecoin-native architecture with USDC as gas, performant and deterministic settlement finality, and a commitment to compliant privacy—are not isolated features. They are the integrated components of a cohesive vision to create a foundational trust layer for the modern economy.

> Arc is where the speed and openness of the internet meet the trust and reliability of regulated finance.

From global payments and remittances to tokenized capital markets and autonomous corporate treasuries, the potential applications are vast. Arc is engineered to be the secure, transparent, and performant settlement layer upon which the types of financial services and applications on the internet will be built. It is an invitation to the world's leading financial institutions, enterprises, and innovators to build the future of finance and commerce, at internet scale.

References

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.

[11] See Belenkiy [2025] for "Recibo: Encrypted Messages for ERC-20 Transactions"

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.

Jess Cheng. How to build a stablecoin: Certainty, finality, and stability through commercial law principles. *Berkeley Business Law Journal*, 17(2), 2020. doi: 10.2139/ssrn.3698410. URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3698410.

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 *Bitcoin and beyond*, pages 157–177. Routledge, 2017.

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.