

Arc: una blockchain de capa 1 abierta, diseñada para las finanzas con stablecoins

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

Agosto de 2025

Resumen

Arc es una blockchain de capa 1 abierta y compatible con EVM, diseñada para avanzar la frontera de las finanzas con stablecoins y la tokenización. Presenta USDC como gas nativo, finalidad de liquidación determinista, privacidad opcional (opt-in) y una arquitectura de comisiones estable. Optimizada para casos de uso nativos de stablecoins —como pagos globales, FX y mercados de capitales— Arc sirve como una capa de liquidación fundamental para el dinero programable en internet.

1. Introducción

El sistema financiero global, a pesar de ser la base del comercio moderno, opera sobre una infraestructura heredada que es fundamentalmente incompatible con la velocidad, la apertura y la programabilidad de internet. Aun con décadas de innovación en software de consumo y empresarial, el acceso financiero, la inclusión y la movilidad de capital en tiempo real siguen profundamente limitados, especialmente a través de fronteras y en mercados emergentes. Los pagos transfronterizos son lentos, opacos y costosos. Las operaciones de tesorería están fragmentadas entre jurisdicciones, intermediarios y rieles financieros incompatibles. Los mercados de capitales continúan cerrados, aislados y cargados de procesos manuales y capas de intermediación. Estas ineficiencias estructurales generan costos económicos e introducen riesgos de contraparte y operacionales de naturaleza sistémica [Committee on Payments and Market Infrastructures, 2020].

El advenimiento de la tecnología blockchain prometió un nuevo paradigma para las finanzas y el comercio, ofreciendo programabilidad, transparencia y resistencia a la censura. Sin embargo, las blockchains públicas existentes presentan limitaciones fundamentales que obstaculizan la adopción institucional y empresarial. El uso de tokens nativos volátiles para las comisiones de gas introduce costos operativos impredecibles y complejidades contables. Además, la falta de una finalidad de liquidación clara en muchas cadenas introduce riesgo financiero, mientras que la ausencia de privacidad transaccional es un elemento faltante clave para actividades comerciales sensibles. La naturaleza sin permisos y

transparente de la presentación de transacciones también dio lugar al fenómeno del Valor Máximo Extraíble (MEV), donde actores privilegiados explotan el ordenamiento de transacciones para obtener ganancias, degradando la integridad del mercado [Daian et al., 2019]. Finalmente, la fragmentación de la liquidez de stablecoins y las aplicaciones a través de múltiples blockchains crea fricción tanto para usuarios como para desarrolladores.

Para abordar estas brechas clave, este documento presenta Arc, una blockchain de capa 1 abierta diseñada específicamente para las finanzas con stablecoins. Se construye sobre la convicción de que el futuro de las finanzas y el comercio no es el reemplazo total de lo anterior, sino la síntesis de lo nuevo y lo establecido: la programabilidad de los contratos inteligentes con la ejecutabilidad de la ley (p. ej., la ley GENIUS); la eficiencia de la blockchain con la estabilidad de la moneda respaldada por dinero fiat; y la transparencia de los registros públicos con la privacidad necesaria para transacciones comerciales. Como red compatible con EVM, Arc ofrece un entorno familiar para la programabilidad, y su adopción de un motor de consenso tolerante a fallas bizantinas (BFT) de alto rendimiento, basado en Tendermint (Malachite), proporciona la infraestructura de grado institucional necesaria para servicios financieros regulados a escala de internet. Este diseño, que depende de un conjunto de validadores autorizados, se alinea con marcos regulatorios emergentes, como el tratamiento prudencial de criptoactivos del Comité de Supervisión Bancaria de Basilea, que traza una vía para que las stablecoins en redes con controles robustos sean clasificadas como activos de "Grupo 1" con un tratamiento de capital más favorable para los bancos [Basel Committee on Banking Supervision, 2022].

En esencia, Arc redefine cómo se transfiere y asegura el valor digital. Introduce tres innovaciones clave:

1. **Comisiones estables y USDC como gas nativo:** reduce significativamente la volatilidad de comisiones y la complejidad contable al utilizar USDC como el activo nativo para comisiones de transacción, al tiempo que admite otras stablecoins locales y dinero tokenizado como gas mediante una integración dedicada de paymaster.

2. **Finalidad de liquidación determinista:** proporciona liquidación final clara y cierta en menos de un segundo, alineada con los Principios para las Infraestructuras del Mercado Financiero [Committee on Payment and Market Infrastructures and International Organization of Securities Commissions, 2012].
3. **Privacidad opcional (opt-in):** integra tecnologías de preservación de la privacidad para habilitar transparencia selectiva, un requisito para flujos financieros sensibles y que respalda los programas de cumplimiento de las instituciones.

Arc proporciona la infraestructura necesaria para las finanzas a escala de internet. Circle Internet Group (en adelante, Circle) está en una posición única para liderar este esfuerzo gracias a su experiencia operando USDC, construyendo primitivas financieras a través de cadenas y colaborando estrechamente con instituciones, reguladores y la comunidad de desarrolladores. Al enfocarse en los requisitos únicos de las finanzas basadas en stablecoins, Arc ofrece una capa de liquidación fundamental y un centro de liquidez para el dinero programable.

2. Arquitectura principal de Arc

La arquitectura de Arc está diseñada desde cero para ofrecer una base robusta y de grado institucional para que los servicios y aplicaciones financieras se construyan sobre stablecoins y activos tokenizados. Busca superar las limitaciones críticas de las blockchains existentes para ofrecer una plataforma segura, de alto rendimiento y adaptada a aplicaciones financieras reguladas y al comercio del mundo real. Como se ilustra en la Figura 1, el núcleo de la red es un conjunto de validadores autorizados que operan sobre el motor de consenso Malachite, que proporciona la base de su rendimiento y seguridad. Esta arquitectura se apoya en tres pilares fundacionales, cada uno de los cuales aborda una necesidad crítica para la adopción financiera generalizada.

Primero, la red es **nativa de stablecoins**, utiliza USDC como gas para eliminar la volatilidad de las comisiones y simplificar las operaciones. Segundo, ofrece **finalidad de liquidación** determinista y sub-segundo mediante un motor de consenso de alto rendimiento, proporcionando la certeza necesaria para la liquidación de alto valor. Tercero, incluye **privacidad opcional** en su hoja de ruta, habilitando transparencia selectiva sobre saldos y transacciones para proteger información financiera sensible, preservando a la vez la auditabilidad. Estas características centrales están diseñadas para sustentar aplicaciones nativas de stablecoins como FX programable, pagos y trading institucional, a la vez que se conectan sin problemas con los sistemas financieros dentro y fuera de cadena a través de la plataforma de Circle y un ecosistema creciente de socios de stablecoins. Esta sección detalla estos tres pilares arquitectónicos, que en conjunto establecen a Arc como una capa de liquidación confiable para la economía nativa de internet.

2.1. USDC como gas nativo y mecanismo de comisiones estables

Un principio de diseño fundamental de Arc es el uso de USDC como el activo nativo para todas las comisiones de transacción (gas). Además, Arc admitirá otras stablecoins locales y dinero fiat tokenizado como gas a través de una integración dedicada de paymaster. Vincular el gas a valores en moneda fiat aborda una barrera crítica para la adopción empresarial de la tecnología blockchain: la volatilidad y la complejidad contable asociadas con el uso de un token nativo especulativo para costos operativos. Al denominar las comisiones en una unidad de cuenta estable, Arc brinda operaciones financieras predecibles, auditables y simplificadas para usuarios y desarrolladores. Esto alinea la unidad de cuenta para la transferencia de valor con la unidad de cuenta para el costo de transacción.

Para ilustrarlo con un modelo simple, considere el costo de una transacción, C_{USD} , desde la perspectiva del usuario. En una red que usa un activo nativo volátil (p. ej., ETH), el costo en dólares es el producto de tres variables: las unidades de gas consumidas (g), la comisión base del protocolo en el activo nativo por unidad de gas (b_{native}) y el precio de mercado de ese activo (P_{native}). Así, $C_{USD} = g \times b_{native} \times P_{native}$. Este costo tiene dos fuentes distintas de volatilidad: la volatilidad impulsada por el protocolo en b_{native} (por la demanda de espacio en bloques) y la volatilidad impulsada por el mercado en P_{native} (por la especulación). Un mecanismo de estabilidad de comisiones como EIP-1559 solo puede influir en b_{native} , dejando a los usuarios expuestos a la volatilidad del precio del token de gas P_{native} , a menudo el factor dominante. Esto hace imposible que el protocolo proporcione costos de transacción predecibles denominados en dólares.

Por el contrario, en Arc, el costo es $C_{USD} \approx g \times b_{USDC}$, puesto que el precio de USDC es estable en 1. La volatilidad de precios impulsada por el mercado queda efectivamente eliminada como variable. Por lo tanto, el protocolo puede gestionar de manera directa y significativa los costos de transacción en una unidad de cuenta estable ajustando b_{USDC} . Este cambio —de una doble volatilidad a una única volatilidad gestionada por el protocolo— reduce fundamentalmente el riesgo para las empresas al utilizar blockchain. Permite una planificación financiera predecible y modelos de negocio robustos, aumentando el potencial de adopción de la red para casos de uso institucionales y comerciales.

La elección de una stablecoin como activo nativo para el gas no es solo por conveniencia; desbloquea un potente espacio de diseño para las comisiones, imposible con un token volátil. Permite mercados de comisiones predecibles, recompensas y subsidios programables, y servicios dedicados de paymaster que habilitan a los usuarios a pagar comisiones en otras monedas.

En el lanzamiento, Arc implementará un mercado de comisiones diseñado para la estabilidad y la previsibilidad, inspirado en EIP-1559 de Ethereum [Buterin et al., 2019]. La mejora principal es un mecanismo de suaviza-

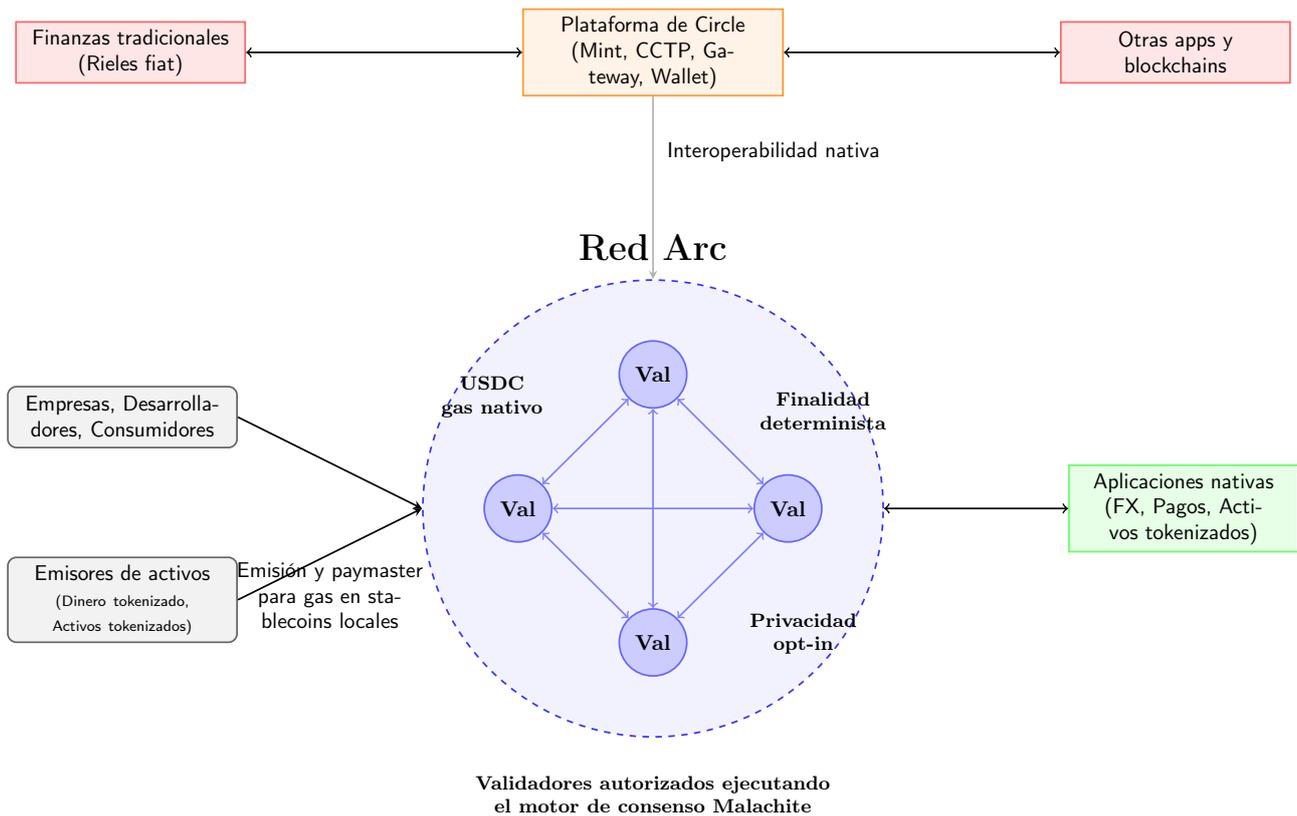


Figura 1: La arquitectura de Arc, destacando sus componentes principales, aplicaciones nativas y conectividad con el ecosistema financiero más amplio.

do de comisiones: en lugar de ajustarse por bloque, la comisión base del protocolo se actualiza utilizando una media móvil exponencialmente ponderada (EWMA) de la utilización de los bloques. Este enfoque, combinado con una comisión base acotada, amortigua la volatilidad de corto plazo y asegura que los costos de transacción se mantengan consistentemente bajos. Las comisiones en el lanzamiento se dirigirán a un Tesoro de Arc en cadena para apoyar el crecimiento a largo plazo de la red.

2.2. Consenso y finalidad

El modelo de seguridad de Arc está diseñado para proporcionar un grado de confianza y resiliencia superior al alcanzable solo mediante consenso convencional. Lo hace combinando un motor de consenso de alto rendimiento, Malachite, que permite finalidad determinista, con un conjunto autorizado de validadores establecidos para garantizar la integridad de la red.

Arc no busca competir por el volumen de transacciones existente, sino ampliar el mercado direccionable total ofreciendo las garantías de liquidación de alta frecuencia necesarias para traer el próximo billón de dólares en pagos y capital institucional a la cadena.

Uno de los principales disuasivos para que las blockchains públicas se conviertan en infraestructuras de mercado financiero global es la falta de una definición clara de finalidad de liquidación. En la mayoría de las blockchains existentes, incluidas PoS y PoW, las tran-

sacciones suelen atravesar un estado probabilístico y están sujetas a reorganizaciones de cadena ("reorgs"), que pueden revertir transacciones recientemente confirmadas. Esta ambigüedad en la liquidación introduce riesgo e ineficiencia de capital para flujos financieros de alto valor. En un caso extremo, las cadenas PoS sin permisos también pueden sufrir un ataque a la finalidad que revierta un bloque finalizado si un actor malicioso obtiene una supermayoría de los tokens en staking. Aunque el valor de los tokens en staking puede ser suficiente para la escala actual de casos cripto-nativos, asegurar billones de dólares en activos financieros tokenizados requeriría una magnitud mucho mayor de garantía económica. Además, incluso las transacciones "liquidadas" en muchas cadenas pueden revertirse mediante una escisión coordinada socialmente que depende de la gobernanza del ecosistema.¹ Asimismo, las redes de capa 2 construidas sobre una capa 1 heredan los mismos riesgos y latencias de finalidad de su capa base.

El fundamento del rendimiento y la seguridad de grado institucional de Arc es su consenso, construido sobre Malachite, una implementación de alto rendimiento del protocolo BFT de Tendermint. Esta elección representa una desviación deliberada de los modelos de finalidad probabilística de las primeras blockchains, así como del secuenciamiento centralizado de las capas 2 más recientes.

Arc dependerá de un conjunto de validadores con Prue-

¹Véase Dupont [2018] para la discusión sobre la bifurcación del hackeo de The DAO.

ba de Autoridad (PoA) compuesto por un número limitado de instituciones conocidas, establecidas y geográficamente distribuidas, sujetas a altos estándares de responsabilidad y garantías operativas.² Arc aspira a establecerse como infraestructura fundamental para el movimiento de dinero regulado, apoyando un sistema financiero globalmente distribuido. Si bien la descentralización en redes blockchain se ha asociado tradicionalmente con resiliencia tecnológica y resistencia a la censura, Arc adopta una perspectiva más amplia. Arc concibe un modelo de descentralización arraigado en la colaboración estratégica con un conjunto diverso y globalmente distribuido de jurisdicciones e instituciones sistémicamente importantes. Al permitir que estas entidades participen en la validación de la red, Arc busca ofrecer una infraestructura resiliente y conforme capaz de sustentar operaciones financieras críticas para soberanos y empresas en todo el mundo. Estos validadores son responsables de producir bloques y garantizar la integridad operativa y el rendimiento diarios de la red. Sus identidades en el mundo real y, a menudo, sus obligaciones regulatorias y requisitos de cumplimiento (p. ej., SOC 2) ofrecen un fuerte disuasivo contra el comportamiento malicioso.

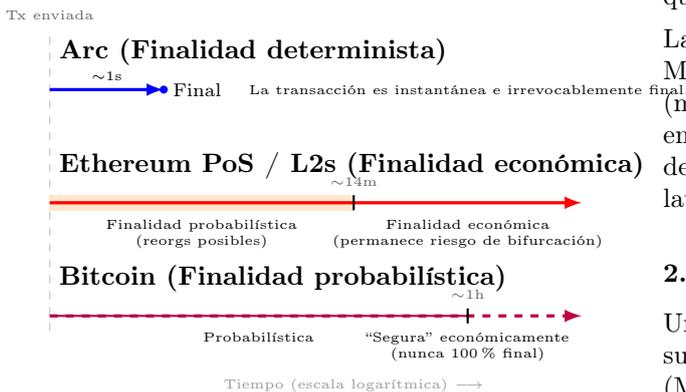


Figura 2: Comparación temporal de modelos de finalidad.

Una transacción en Arc está sin confirmar o es 100% final e irreversible. No hay fase probabilística. Una vez que un bloque es comprometido por más de dos tercios del conjunto de validadores a través de un proceso de votación de múltiples rondas, es instantáneamente final. Esto se alinea con el Principio 8 de los Principios para las Infraestructuras del Mercado Financiero (PFMI), que enfatiza una liquidación final clara y cierta [Committee on Payment and Market Infrastructures and International Organization of Securities Commissions, 2012]. La certeza de la finalidad es crítica para la estabilidad del sistema financiero, ya que proporciona una base clara de derechos y relaciones entre las partes, permitiéndoles gestionar su exposición al riesgo de manera más efectiva [Cheng, 2022]. Este proceso proporciona garantías de liquidación en menos de un segun-

²Los criterios de selección de validadores incluyen, entre otros: historial comprobado de resiliencia operativa, garantías de tiempo de actividad, cumplimiento normativo y prácticas de seguridad.

do, una característica crucial para aplicaciones donde la certeza y la velocidad son primordiales.

2.2.1. Rendimiento

Arc está diseñada para un rendimiento de grado institucional, ofreciendo alto throughput y finalidad rápida para satisfacer las exigencias rigurosas de la infraestructura de los mercados financieros globales. Arc es capaz de procesar aproximadamente 3.000 transacciones por segundo (TPS) con finalidad casi instantánea inferior a 350 milisegundos, con un conjunto de 20 validadores geográficamente distribuidos.³ Con cuatro validadores distribuidos geográficamente, el throughput de Arc puede superar las 10.000 TPS con una finalidad inferior a 100 milisegundos.⁴ Estos indicadores de rendimiento se lograron usando hardware de consumo, lo que indica un potencial significativo para un throughput aún mayor con infraestructura de producción.⁵

Para ponerlo en perspectiva, con 20 validadores, Arc puede procesar más de 280 veces el número de transacciones diarias del servicio Fedwire Funds.⁶ Este rendimiento subraya la capacidad de Arc para operar a una escala muy superior a los sistemas tradicionales de liquidación bruta en tiempo real.⁷

Las mejoras planificadas para el motor de consenso Malachite incluyen soporte para múltiples proponentes (multi-proposer), lo que podría aumentar el throughput en aproximadamente 10x, y configuraciones opcionales de tolerancia a fallas más baja que pueden reducir la latencia alrededor de un 30%.

2.2.2. Hoja de ruta para mitigar MEV

Un aspecto crucial de la filosofía de diseño de Arc es su enfoque para mitigar el Valor Máximo Extraíble (MEV). Si bien el MEV se ha convertido en una fuente importante de congestión, inestabilidad y comportamiento depredador en muchas blockchains públicas [Daian et al., 2019], la hoja de ruta de Arc reconoce que no todas las formas de MEV son perjudiciales. En el contexto de pagos nativos de stablecoins, Arc clasifica el MEV en dos categorías generales: constructivo y dañino. El MEV constructivo incluye el arbitraje entre venues que mejora la fungibilidad de stablecoins y mantiene ajustados los tipos de cambio entre mercados en cadena, ambos esenciales para una experiencia de pagos fluida. Por ejemplo, el arbitraje que iguala los precios USDC/EURC entre lugares de liquidez respalda direc-

³La configuración de 20 validadores tiene 10 regiones, con 2 validadores en cada región. Las 10 regiones son: Nueva York (dos centros de datos), Ámsterdam, Fráncfort, Londres, San Francisco, Toronto, Singapur, Sidney y Bangalore.

⁴La configuración de 4 validadores tiene 3 regiones, con 2 validadores en Nueva York y los otros dos en San Francisco y Toronto, respectivamente.

⁵También es importante señalar que esta latencia aún no tiene en cuenta la sobrecarga adicional de la ejecución EVM, ya que los benchmarks se centraron en el consenso.

⁶Basado en datos de Fedwire Funds Service de junio de 2025, que mostraron 912.515 transferencias diarias promedio.

⁷Véase Liao et al. [2023] para la discusión sobre stablecoins de pago para liquidaciones brutas en tiempo real.

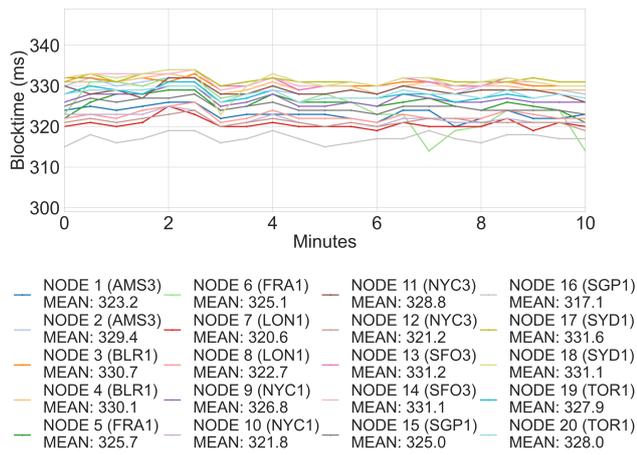


Figura 3: Tiempo de bloque en milisegundos (eje y) para el motor de consenso Malachite con 20 nodos validadores distribuidos geográficamente durante 10 minutos (eje x).

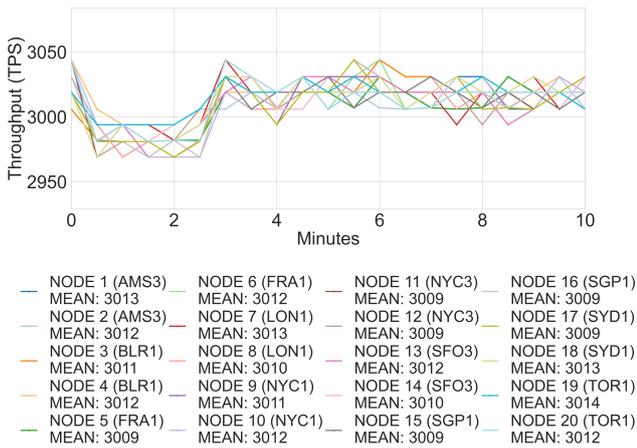


Figura 4: Throughput en transacciones por segundo (eje y) para el motor de consenso Malachite con 20 nodos validadores distribuidos geográficamente durante 10 minutos (eje x).

tamente la fiabilidad de las stablecoins en el comercio. Por el contrario, el MEV dañino incluye ataques sándwich y otros comportamientos que insertan flujo tóxico entre la intención de pago y la liquidación final, degradando la previsibilidad de la transacción y socavando la confianza del usuario, particularmente en casos de baja latencia como punto de venta o pagos B2B. El diseño de la red, por tanto, buscará distinguir y desalentar el front-running depredador, preservando actividades beneficiosas de back-running que contribuyen al descubrimiento de precios y a la eficiencia del mercado. Con este fin, la hoja de ruta incluye técnicas avanzadas de mitigación, como mempools cifrados, procesamiento por lotes de transacciones y múltiples proponentes, para fomentar un mercado justo y ordenado optimizado para la liquidación financiera de grado institucional.

2.3. Privacidad: una hoja de ruta para finanzas conformes

Para que los servicios financieros migren a la cadena, la privacidad no es opcional; es un requisito. Los datos comerciales y personales sensibles —desde pagos de nómina hasta detalles de financiación del comercio y tesorería corporativa— no pueden exponerse en un registro público totalmente transparente. El desafío es habilitar la privacidad preservando la auditabilidad completa para reguladores, auditores y terceros autorizados, habilitando a las instituciones a cumplir plenamente con sus obligaciones regulatorias. Arc aborda esto mediante una hoja de ruta pragmática y por fases, diseñada para ofrecer **privacidad opcional** a través de una arquitectura modular y preparada para el futuro.

La hoja de ruta de privacidad de Arc comienza con **transferencias confidenciales**, una función que oculta los importes de las transacciones de la vista pública manteniendo la liquidación en cadena. Es crucial distinguir esto del anonimato total, que además oculta direcciones. En este primer paso, las direcciones de las partes de la transacción permanecen visibles en el registro público, pero el valor de la transferencia se cifra. Este diseño proporciona confidencialidad para datos comerciales sensibles a la vez que garantiza que el registro público siga siendo compatible con las herramientas actuales de analítica y monitoreo de blockchain para el rastreo de direcciones.

Reconociendo que las finanzas globales operan en un entorno regulado, el modelo de privacidad de Arc está construido para apoyar programas de cumplimiento institucional. Las funciones opt-in permiten la divulgación selectiva a través de mecanismos como “claves de visualización” (view keys), que conceden a terceros autorizados, como auditores o reguladores, acceso de solo lectura a datos específicos de transacciones. Además, una institución siempre conserva visibilidad completa sobre las transacciones realizadas por sus propios clientes, incluidas las transacciones aguas arriba y aguas abajo, lo cual es esencial para obligaciones regulatorias como el monitoreo de transacciones y la Travel Rule.

Esto se habilita mediante una arquitectura modular donde los contratos inteligentes pueden interactuar con un backend criptográfico a través de un precompile dedicado de EVM. Este backend aprovecha tecnologías como los Entornos de Ejecución Confiable (TEE) para realizar cálculos sobre datos cifrados. Si bien muchas soluciones de privacidad sufren restricciones de rendimiento, el uso de TEE por parte de Arc para transferencias confidenciales proporciona transacciones protegidas rápidas y auditables. Este diseño modular también permite la integración de nuevos backends criptográficos a medida que maduran, posicionando a Arc para ofrecer finanzas confidenciales sin comprometer la latencia y la experiencia de usuario esperadas por las instituciones.

De cara al futuro, la hoja de ruta va más allá de las transferencias simples para habilitar **estado privado y cómputo confidencial**. Esta forma más avanzada de privacidad permitirá gestionar de forma privada ló-

gica financiera compleja —como el estado de un libro de órdenes privado, un acuerdo de financiación del comercio o una tesorería automatizada—. Este despliegue por fases se sustenta en un diseño modular y preparado para el futuro. Si bien los TEE ofrecen un punto de partida maduro y de alto rendimiento para el cómputo confidencial, la arquitectura de Arc no está atada a una sola tecnología. El diseño de backend enchufable permitirá la integración futura de otras tecnologías avanzadas de mejora de la privacidad, incluidas la Computación Multipartita (MPC), el Cifrado Homomórfico Completo (FHE) y las pruebas de conocimiento cero, a medida que estén listas para sistemas financieros de escala de producción.

3. Aplicaciones nativas y casos de uso

Arc está diseñada como un sistema operativo financiero con un conjunto de aplicaciones y servicios nativos que permiten a los desarrolladores construir productos financieros sofisticados. Este enfoque integrado reduce la complejidad y proporciona una base robusta para la innovación. Arc no está construida solo para los productos de Circle: es una invitación abierta a instituciones, desarrolladores y emprendedores para construir la próxima ola de innovación financiera con confianza, seguridad y escala.

3.1. Stablecoins, FX programable y activos tokenizados

Una capacidad clave de Arc es su soporte nativo para la emisión de múltiples formas de dinero tokenizado. Si bien las stablecoins emitidas por Circle como USDC y EURC y el fondo tokenizado del mercado monetario USYC serán compatibles en el lanzamiento, Arc es una plataforma abierta diseñada también para admitir a otros emisores de dinero tokenizado: desde stablecoins respaldadas por fiat hasta depósitos bancarios tokenizados y dinero de bancos centrales. Esto permite crear stablecoins e instrumentos tokenizados anclados a monedas más allá del dólar estadounidense, posibilitando un sistema financiero global más inclusivo. Combinado con la futura abstracción integrada de paymaster, los usuarios podrán pagar comisiones en stablecoins locales, mejorando drásticamente la usabilidad para aplicaciones no centradas en USD.

Arc también está diseñada para ser un lugar de primera para activos tokenizados con rendimiento. En el lanzamiento, la red admitirá USYC de Circle, un token regulado con interés respaldado por valores del Tesoro de EE. UU. de corta duración.⁸ Esto proporciona una fuente nativa de rendimiento de bajo riesgo en cadena, permitiendo que instituciones, empresas y protocolos DeFi cualificados pongan su capital a trabajar en un entorno seguro y conforme. La integración de activos como USYC transforma a Arc en una plataforma poderosa para la gestión de tesorería en cadena, colateral

para préstamos y la creación de nueva infraestructura de mercados de capitales.

Sobre la base multicurrency, la hoja de ruta de Arc incluye un motor de divisas (FX) de grado institucional. Este motor habilita la liquidación PvP (pago contra pago) programable 24/7 entre contrapartes verificadas, aprovechando contratos inteligentes en cadena para el registro de operaciones, ventanas de liquidación configurables y gestión de colateral. También integra una capa de ejecución offchain de solicitud de cotización (RFQ), permitiendo a tomadores institucionales obtener precios de FX de una red de creadores de mercado. Inicialmente, el motor de FX operará como un sistema con permisos para garantizar el cumplimiento regulatorio, la integridad del mercado y la liquidez profunda en corredores clave. La hoja de ruta a largo plazo también incluye un protocolo sin permisos que democratiza el acceso a la liquidez de FX institucional.⁹

Finalmente, Arc también está diseñada para admitir la siguiente evolución de activos financieros tokenizados de alta calidad. Más allá de las stablecoins y los instrumentos de efectivo tokenizados, la plataforma permite la emisión, liquidación y composabilidad de activos del mundo real (RWA) regulados —incluidas acciones tokenizadas, renta fija, crédito privado, fondos privados y otros valores de grado institucional—. Esto se logrará en asociación con emisores de activos regulados, custodios y administradores de fondos, garantizando que las representaciones tokenizadas sean legalmente robustas, estén debidamente colateralizadas e integradas con obligaciones financieras del mundo real. Una vez emitidos en Arc, estos activos tokenizados pueden componerse de forma nativa con el conjunto completo de primitivas DeFi —incluidos protocolos de préstamo y crédito, venues de negociación e intercambio, mecanismos de staking y estrategias de rendimiento—. Esto permite a asignadores de capital, fintechs y gestores de activos construir productos financieros de próxima generación que sean transparentes, automatizados y accesibles globalmente, manteniéndose anclados al cumplimiento del mundo real.

Al traer el sistema financiero offchain a la cadena, Arc transforma el acceso a instrumentos financieros que históricamente han estado restringidos por geografía, infraestructura o licencias. Crea un entorno unificado donde los inversores de todo el mundo pueden acceder, negociar y liquidar activos de forma continua, con controles de privacidad opcionales para cumplir con las obligaciones de conformidad integradas en la capa del protocolo. Arc es más que una blockchain para activos digitales; es una plataforma para reconstruir los mercados de capital desde cero.

Estas capacidades —emisión de stablecoins, activos tokenizados de alta calidad y FX programable— transforman la red en una plataforma poderosa para construir una nueva generación de aplicaciones financieras globales, desde soluciones de pagos transfronterizos hasta

⁸Consulte la nota de descargo de responsabilidad sobre la disponibilidad de USYC.

⁹Véase Adams et al. [2023] para la discusión sobre FX en cadena y pagos transfronterizos.

cobertura automatizada, mercados de capitales en cadena y herramientas de gestión de riesgo cambiario para tesorerías empresariales.

3.2. Un centro de liquidez y liquidación entre cadenas

Arc está diseñada para servir como el centro de liquidez y aplicaciones de stablecoins. Con finalidad rápida y USDC como token de gas, Arc permitirá a los usuarios acceder instantáneamente a cualquier aplicación a través de más de docenas de blockchains mediante CCTP y Gateway de Circle. A través de estas conectividades, los usuarios pueden usar USDC con aplicaciones independientemente de su cadena subyacente, simplificando la actividad entre cadenas en una experiencia unificada e intuitiva. Arc, USDC y los productos de interoperabilidad de Circle forman juntos la base de un ecosistema financiero sin fricciones.

Esta capacidad está habilitada por un conjunto de productos de Circle integrados de forma nativa:

- **Mint:** los clientes de Circle pueden acuñar USDC y EURC sin fricciones directamente en Arc a partir de depósitos bancarios fiat, creando la rampa de entrada más rápida posible desde las finanzas tradicionales al capital en cadena sin dependencia de crédito ni repositonamiento de liquidez.
- **CCTP (Cross-Chain Transfer Protocol)**¹⁰: como una cadena de emisión nativa para USDC, Arc aprovecha CCTP para habilitar transferencias de liquidez de stablecoins sin permisos, seguras y rápidas hacia cualquier blockchain conectada. Esto permite que el capital fluya a donde más se necesita sin demoras.
- **Gateway:** Arc admite saldos de USDC abstractos entre cadenas a través de Gateway, permitiendo a las empresas satisfacer la demanda de liquidez de stablecoins instantáneamente (<1 segundo) entre cadenas sin profundos ni reequilibrios. Las aplicaciones y billeteras pueden ofrecer experiencias de usuario fluidas con saldos de USDC unificados y composabilidad entre ecosistemas.

Estos productos también buscarán ampliar su utilidad para otras stablecoins para habilitar esta promesa de liquidez entre cadenas.

La piedra angular de este modelo es la finalidad determinista de Arc. Debido a que una transacción es final dentro de un solo bloque (sub-segundo), la liquidez en Arc puede quemarse y luego acuñarse de forma verificable en una cadena de destino casi instantáneamente. Esto elimina los largos períodos de espera asociados con cadenas que dependen de finalidad probabilística o económica, donde los puentes entre cadenas deben esperar una garantía de liquidación. En consecuencia, Arc funciona tanto como la cadena más rápida para la rampa de acceso de fiat a stablecoin como la capa de distribución más eficiente para desplegar esa liquidez en el panorama blockchain más amplio.

3.3. Pagos y liquidación de grado empresarial

La combinación de una unidad de cuenta estable, comisiones predecibles, liquidación rápida y confidencialidad convierte a Arc en una plataforma ideal para pagos y liquidación de grado empresarial. Las funciones nativas de la red están diseñadas para soportar los requisitos complejos de las finanzas empresariales, yendo más allá de la simple transferencia de valor para habilitar flujos de pago sofisticados y programables.

Arc proporciona a desarrolladores y empresas un conjunto de módulos de pago principales que pueden componerse en aplicaciones potentes, contemplados en la hoja de ruta de Arc e incluyendo:

- **Pagos vinculados a facturas:** soporte nativo para adjuntar datos estructurados a las transacciones, como detalles de factura o mensajes.¹¹ Esto simplifica la conciliación y automatiza los procesos de cuentas por pagar y por cobrar.
- **Protocolos de reembolso y disputa:** mecanismos en cadena para gestionar reembolsos y resolver disputas de pago. Esto proporciona un nivel de protección al consumidor y al comerciante esencial para la adopción generalizada, pero a menudo ausente en los sistemas blockchain existentes.
- **Agentes de tesorería inteligentes:** la capacidad de crear agentes autónomos y nativos de IA que puedan gestionar tesorerías corporativas, ejecutar políticas de gasto programables y optimizar el capital de trabajo en tiempo real. Esto desbloquea operaciones financieras escalables y en tiempo real que reducen la carga manual y mejoran la eficiencia del capital.

Estas capacidades se aprovecharán con Circle Payments Network (CPN) para mejorar la eficiencia operativa de los pagos transfronterizos, y también habilitarán una amplia gama de otros casos de uso importantes, desde la automatización de la financiación de la cadena de suministro global y la distribución de regalías hasta la construcción de sistemas de nómina y de infraestructura de mercados de capitales totalmente conformes y en cadena. Al proporcionar estas herramientas como primitivas nativas, Arc reduce significativamente la barrera para que las empresas construyan y desplieguen soluciones financieras seguras, de alto rendimiento y conformes en una blockchain.

4. Hoja de ruta

Se espera que la red de pruebas pública (testnet) de Arc esté disponible en otoño de 2025. El lanzamiento beta de la red principal (mainnet) de Arc contendrá componentes clave como la arquitectura de comisiones estables, finalidad determinista sub-segundo y la hoja de ruta del motor de FX. Además, los productos de la plataforma de Circle (CPN, USDC, EURC, USYC, Mint, Wallets, Contracts, CCTP, Gateway, Paymaster

¹⁰Véase Mayerchak et al. [2025] para detalles sobre CCTP.

¹¹Véase Belenkiy [2025] para "Recibo: mensajes cifrados para transacciones ERC-20".

y más), junto con el soporte de infraestructura del ecosistema de terceros, estarán disponibles.

Las mejoras de privacidad llegarán en una actualización posterior de la red, comenzando con transferencias confidenciales y evolucionando hacia privacidad plenamente programable. Además de la privacidad, también se explorarán en la hoja de ruta técnicas de mitigación de MEV como mempools cifrados, procesamiento por lotes de transacciones y múltiples proponentes, para fomentar un mercado justo y ordenado optimizado para la liquidación financiera de grado institucional.

Por último, la hoja de ruta para garantías adicionales de seguridad de Arc también incluye una transición a un mecanismo de Prueba de Participación (PoS), que será permissioned dentro del conjunto de instituciones validadoras seleccionadas. Esta actualización permite una descentralización de validadores más amplia y una flexibilidad de gobernanza alineadas con el deseo a largo plazo de Circle de garantizar la robustez de la red. También asegura que Arc pueda funcionar independientemente de Circle más allá del conjunto inicial de validadores, proporcionando una resiliencia operativa adicional. La hoja de ruta de Malachite también incluirá un diseño novedoso de múltiples proponentes para incrementar el rendimiento, junto con optimizaciones en toda la pila de consenso, como la reducción de latencia con una variante de Tendermint de dos fases.

5. Conclusión

Arc representa una reinención fundamental de lo que la infraestructura blockchain para finanzas y comercio debería ser. Se fundamenta en una comprensión pragmática de lo que se requiere para construir un sistema financiero global, regulado y eficiente en internet, que satisfaga las demandas del mundo real de instituciones, plataformas y empresas. Al resolver limitaciones centrales relacionadas con la volatilidad de las comisiones, la incertidumbre de liquidación y la falta simultánea de privacidad y cumplimiento normativo, Arc proporciona una base hecha a medida para la era del dinero programable.

Las innovaciones clave presentadas en este documento —una arquitectura nativa de stablecoins con USDC como gas, una finalidad de liquidación determinista y de alto rendimiento, y un compromiso con la privacidad conforme— no son características aisladas. Son componentes integrados de una visión coherente para crear una capa de confianza fundamental para la economía moderna.

Arc es donde la velocidad y apertura de internet se encuentran con la confianza y fiabilidad de las finanzas reguladas.

Desde pagos globales y remesas hasta mercados de capitales tokenizados y tesorerías corporativas autónomas, las aplicaciones potenciales son vastas. Arc está diseñada para ser la capa de liquidación segura, transparente y de alto rendimiento sobre la cual se construyan los servicios y aplicaciones financieras en internet. Es una

invitación a las principales instituciones financieras, empresas e innovadores del mundo para construir el futuro de las finanzas y el comercio, a escala de internet.

Referencias

- 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*, Ju-

ne 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.

DESCARGO DE RESPONSABILIDAD Este documento es solo para fines informativos generales. No constituye asesoramiento de inversión ni una recomendación o solicitud para comprar o vender ninguna inversión, y no debe utilizarse para evaluar el mérito de tomar decisiones de inversión. No debe confiarse en él para contabilidad, asesoría legal o fiscal, ni recomendaciones de inversión. Arc es ofrecido por Circle Technology Services, LLC ("CTS"). CTS es un proveedor de software y no presta servicios financieros o de asesoría regulados. Todas las características del producto descritas en este documento pueden ser modificadas, retrasadas o canceladas sin previo aviso, en cualquier momento y a la sola discreción de CTS. Usted es el único responsable de los servicios que brinda a los usuarios, incluyendo obtener las licencias o aprobaciones necesarias y cumplir con las leyes aplicables. Este documento refleja las opiniones actuales de los autores y no se realiza en nombre de Circle Internet Group ni de sus afiliadas, y no necesariamente refleja las opiniones de Circle, sus afiliadas o de las personas asociadas a ellas. Las opiniones aquí reflejadas están sujetas a cambio sin ser actualizadas.

USYC es un token de activo digital. Cada token USYC sirve como una representación digital de una acción del Hashnote International Short Duration Fund Ltd. (el "Fondo"), un fondo mutual registrado en las Islas Caimán. El Fondo ha designado a Circle International Bermuda Limited ("CIBL"), un negocio de activos digitales con licencia de la Autoridad Monetaria de Bermudas, como su administrador de tokens, responsable de la gestión de USYC en nombre del Fondo.

Las participaciones del Fondo y USYC están disponibles solo para Personas no estadounidenses (Non-U.S. Persons), según lo definido en la Ley de Valores de 1933 de los Estados Unidos, según enmienda. Pueden aplicarse restricciones de elegibilidad adicionales. La información proporcionada en este documento es únicamente para fines educativos e informativos y no debe interpretarse como una oferta para vender ni una solicitud para comprar ningún valor, instrumento financiero u otro producto.