La Blockchain de Aptos: Infraestructura Segura, Escalable y Actualizable para Web3

Agosto 11, 2022
Versión 1.0

Abstracto

El auge de las blockchains como nueva infraestructura de Internet ha llevado a los desarrolladores de código a implementar decenas de miles de aplicaciones descentralizadas a un ritmo de rápido crecimiento. Desafortunadamente, el uso de blockchain aún no es omnipresente debido a interrupciones frecuentes, costos elevados, límites de rendimiento bajos y numerosos problemas de seguridad. Para permitir la adopción masiva de la era Web3, la infraestructura blockchain debe seguir el camino de la infraestructura en la nube como una plataforma confiable, escalable, rentable y en continua mejora para crear aplicaciones ampliamente utilizadas.

Presentamos en este documento la *blockchain de Aptos*, diseñada con escalabilidad, seguridad, confiabilidad y capacidad de actualización como principios fundamentales para abordar estos desafíos. La blockchain de Aptos ha sido desarrollada durante los últimos tres años por más de 350 desarrolladores en todo el mundo [1]. Ofrece innovaciones novedosas en consenso, diseño de contratos inteligentes, seguridad del sistema, rendimiento y descentralización. La combinación de estas tecnologías proporcionará un componente fundamental para llevar la Web3 a las masas:[1]

- Primero, la blockchain de Aptos integra de forma nativa e utiliza internamente el lenguaje de código *Move* para una ejecución de transacciones rápida y segura [2]. El *Move prover* , un verificador formal para contratos inteligentes escritos en el lenguaje Move, proporciona garantías adicionales para el comportamiento y errores en el contrato. Este enfoque en la seguridad permite a los desarrolladores de código proteger mejor su software de entidades maliciosas.

- Segundo, el modelo de datos de Aptos permite una gestión flexible de claves y opciones de custodia híbrida. Lo anterior, junto con transacciones transparentes antes de firmarlas y protocolos de cliente ligeros, proporciona una experiencia de usuario más segura y confiable.

- Tercero, para lograr un alto rendimiento y una baja latencia, la blockchain de Aptos aprovecha un enfoque modular y canalizado para las etapas principales del procesamiento de transacciones. Específicamente, la difusión de transacciones, el ordenamiento de metadatos en bloque, la ejecución de transacciones de forma paralela, el almacenamiento por lotes y la certificación del *ledger* operan simultáneamente. Este enfoque aprovecha al máximo todos los recursos físicos

disponibles, mejora la eficiencia del hardware y permite una ejecución altamente paralela.

- Cuarto, a diferencia de otros motores de ejecución paralela que rompen la atomicidad de las transacciones al requerir un conocimiento previo de los datos que se van a leer y escribir, la blockchain de Aptos no impone tales limitaciones a los desarrolladores de código. Puede respaldar eficientemente la atomicidad con transacciones arbitrariamente complejas, lo que permite un mayor rendimiento y una menor latencia para aplicaciones del mundo real y simplifica el desarrollo.

- Quinto, el diseño de la arquitectura modular de Aptos respalda la flexibilidad del cliente y lo optimiza para actualizaciones frecuentes e instantáneas. Además, para implementar rápidamente nuevas innovaciones tecnológicas y permitir nuevos casos de uso Web3, la blockchain de Aptos proporciona protocolos integrados de gestión de cambios *on-chain*.

- Finalmente, la blockchain de Aptos está experimentando con iniciativas futuras para escalar más allá del rendimiento de un validador individual: su diseño modular y su motor de ejecución paralela soportan la fragmentación interna de un validador y la fragmentación de estado homogéneo proporciona el potencial para la escalabilidad horizontal del rendimiento sin agregar complejidad adicional para los nodos operadores.

1 Introducción

En la versión web2 de Internet, servicios como mensajería, redes sociales, finanzas, juegos, compras y transmisión de audio/vídeo son proporcionados por empresas centralizadas que controlan el acceso directo a los datos del usuario (por ejemplo, Google, Amazon, Apple y Meta). Estas empresas desarrollan infraestructura utilizando software específico de aplicaciones optimizado para casos de uso específicos y aprovechan las infraestructuras de la nube para implementar estas aplicaciones para los usuarios. La infraestructura en la nube proporciona acceso a servicios de infraestructura virtualizados y/o físicos, como máquinas virtuales (VM) alquiladas y hardware físico que opera dentro de centros de datos en todo el

mundo (por ejemplo, AWS, Azure y Google Cloud). Como resultado, crear servicios de Internet web2 que puedan escalar a miles de millones de usuarios nunca ha sido tan fácil como lo es hoy. Sin embargo, web2 requiere que los usuarios confíen explícitamente en entidades centralizadas, un requisito que se ha vuelto cada vez más preocupante para la sociedad.

Para combatir esta preocupación, ha comenzado una nueva era de Internet: web3. En la versión web3 de Internet, las blockchains han surgido para proporcionar libros de contabilidad descentralizados *(ledgers)* e inmutables que permiten a los usuarios interactuar entre sí de forma segura y confiable, todo sin requerir confiar en intermediarios controladores o entidades centralizadas. De manera similar a cómo los servicios y aplicaciones de Internet web2 dependen de la infraestructura de la nube como parte fundamental, las aplicaciones descentralizadas pueden usar blockchains como una capa de infraestructura descentralizada para llegar a miles de millones de usuarios en todo el mundo.

Sin embargo, a pesar de la existencia de muchas blockchains en la actualidad, aún no se ha generado una adopción masiva de web3 [3]. Si bien la tecnología continúa haciendo avanzar la industria, las blockchains existentes no son confiables, imponen altas tarifas de transacción para los usuarios, tienen limitaciones de rendimiento bajas, sufren pérdidas regulares de activos digitales debido a problemas de seguridad y no pueden soportar la capacidad de respuesta en tiempo real. En comparación con cómo la infraestructura en la nube ha permitido que los servicios web2 alcancen miles de millones de personas, las blockchains aún no han permitido que las aplicaciones web3 hagan lo mismo.

2 La visión de Aptos

La visión de Aptos es ofrecer una blockchain que pueda llevar la adopción generalizada de web3 y potenciar un ecosistema de aplicaciones descentralizadas para resolver problemas de los usuarios del mundo real. Nuestra misión es avanzar en lo más nuevo en confiabilidad, seguridad y rendimiento de blockchain proporcionando una arquitectura de blockchain flexible y modular. Esta arquitectura debería permitir actualizaciones frecuentes, una rápida adopción de los últimos avances tecnológicos y soporte de primera clase para casos de uso nuevos y emergentes.

Visualizamos una red descentralizada, segura, escalable, gobernada y operada por la comunidad que la utiliza. Cuando las demandas de infraestructura crecen en todo el mundo, los recursos computacionales de blockchain aumentan horizontal y verticalmente para satisfacer esas necesidades. A medida que surgen nuevos casos de uso y avances tecnológicos, la red debe actualizarse con frecuencia y sin interrupciones para los usuarios.

Las preocupaciones por la infraestructura deberían pasar a un segundo plano. Los desarrolladores y usuarios tendrán acceso a muchas opciones diferentes para recuperación de claves, modelado de datos, estándares de contratos inteligentes, compensaciones en el uso de recursos, privacidad y componibilidad. Los usuarios saben que sus activos digitales están seguros, siempre disponibles y se puede acceder a ellos con tarifas cercanas al costo. Cualquiera puede realizar transacciones de forma segura, sencilla e inmutable con partes que no son de confianza en todo el mundo. Las blockchains son tan omnipresentes como la infraestructura de la nube.

Para lograr esta visión, se deben realizar avances tecnológicos significativos. Nuestras experiencias en la construcción, desarrollo, avance e implementación de la blockchain Diem (la predecesora de Aptos) durante los últimos tres años han demostrado que una red puede actualizar continuamente sus protocolos sin interrumpir a sus clientes [4]. La red principal de Diem se implementó en más de una docena de operadores de nodos con múltiples proveedores de billeteras a principios de 2020. Durante el año siguiente, nuestro equipo publicó dos actualizaciones importantes que cambiaron el protocolo de consenso y el marco de código principal. Ambas actualizaciones se completaron sin tiempo de inactividad para los usuarios. Con la blockchain de Aptos, hemos realizado una serie de mejoras radicales en la pila de tecnología y al mismo tiempo incorporamos actualizaciones seguras, transparentes y frecuentes como característica principal, inspiradas en la blockchain Diem. En particular, destacamos métodos novedosos de procesamiento de transacciones (como se describe en la Sección 7) y nuevos enfoques para la descentralización y la gobernanza de la red.

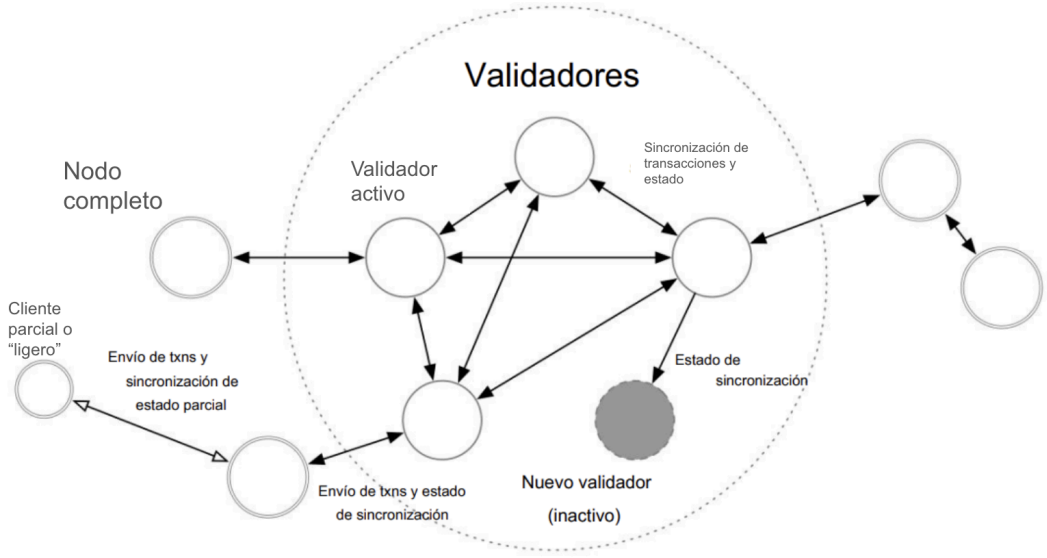

Figura 1: Componentes del ecosistema de Aptos.

A medida que la blockchain de Aptos continúe mejorando y creciendo, publicaremos versiones actualizadas de este documento técnico con la última versión de nuestros protocolos y opciones de diseño. En el resto de este documento, describimos el estado actual de la blockchain de Aptos, así como los planes futuros.

3 Descripción general

La blockchain de Aptos, como se muestra en la Figura 1, se compone de un conjunto de *validadores* que reciben y procesan conjuntamente transacciones de los usuarios utilizando un mecanismo de consenso de prueba de participación bizantino tolerante a fallas (BFT). Los

acreedores de tokens guardan o proveen *(stake)* tokens en sus validadores seleccionados. El peso de la votación por consenso de cada validador es proporcional a la cantidad apostada en él. Un validador puede estar activo y participar en el consenso. Del mismo modo, un validador también puede estar inactivo si no tiene suficiente balance para participar, sale del conjunto de validadores, elige estar fuera de línea mientras sincroniza el estado de la blockchain o el protocolo de consenso lo considera no participante debido a un desempeño histórico deficiente.

Los clientes son cualquier parte del sistema que necesita enviar transacciones o consultar el estado y el historial de la blockchain. Los clientes pueden optar por descargar y verificar pruebas firmadas por el validador de los datos consultados. Los nodos completos son clientes que replican la transacción y el estado de la blockchain desde los validadores o desde otros nodos completos de la red. Pueden optar por eliminar el historial de transacciones y el estado de la blockchain según lo deseen para recuperar el almacenamiento. Los clientes parciales o ligeros solo mantienen el conjunto actual de validadores y pueden consultar el estado parcial de la blockchain de forma segura, generalmente desde nodos completos. Las billeteras son un ejemplo común de cliente parcial o *ligero*.

Para satisfacer las necesidades de una infraestructura web3 segura, rápida, confiable y actualizable para una adopción masiva, la blockchain de Aptos se basa en los siguientes principios de diseño básicos:

- Ejecución rápida y segura junto con auditabilidad simple y analizabilidad mecánica a través de un nuevo lenguaje de programación de contratos inteligentes, *Move* [5]. Move se originó con el predecesor de la blockchain de Aptos y continúa progresando con la evolución de este proyecto.

- Rendimiento extremadamente alto y baja latencia a través de una aplicación canalizada y por lotes que se enfoca en el procesamiento de transacciones de forma paralela.

- Nuevo procesamiento de transacciones paralelas que soporta eficientemente la atomicidad con transacciones arbitrariamente complejas a través de Block-STM, a diferencia de los motores de ejecución paralela existentes que requieren conocimiento previo de las ubicaciones de los datos para ser leídos y escritos.

- Optimizaciones para el rendimiento y la descentralización a través de una rotación rápida del conjunto de validadores con peso de participación y monitoreo de su reputación.

- Capacidad de actualización y configuración como principios de diseño de primera clase para abarcar nuevos casos de uso y la última tecnología.

- Diseños modulares que permiten pruebas rigurosas a nivel de componentes junto con un modelado de amenazas adecuado y una implementación perfecta, todo lo cual garantiza operaciones altamente seguras y confiables.

- Escalabilidad del rendimiento horizontal en donde se preserva la descentralización, donde la fragmentación es una opción de primera clase que se expone a los usuarios y que es nativa a la programación y al modelo de datos.

La sección 4 explica cómo los desarrolladores interactúan con Move en la blockchain de Aptos. La sección 5 describe el modelo lógico de datos. La sección 6 detalla cómo la blockchain de Aptos permite una experiencia de usuario segura a través de métodos seguros de verificación. La Sección 7 describe innovaciones clave en el rendimiento en torno al ordenamiento, el procesamiento por lotes y la paralelización de transacciones. La sección 8 detalla varias opciones para que diferentes clientes sincronicen el estado con otros nodos. La Sección 9 describe nuestros planes para la gobernanza comunitaria. Finalmente, la Sección 10 analiza las direcciones de desempeño futuro mientras se mantiene la descentralización.

4 El lenguaje Move

Move es un nuevo lenguaje de programación de contratos inteligentes con énfasis en la seguridad y la flexibilidad. La blockchain de Aptos utiliza el modelo de objetos de Move para representar el estado de su libro contable *(ledger)* (consulte la Sección 5.5) y utiliza código de Move (módulos) para codificar reglas de transiciones de estado. Los usuarios envían transacciones que pueden publicar nuevos módulos, actualizar módulos existentes, ejecutar funciones de entrada definidas dentro de un módulo o contener scripts que pueden interactuar directamente con las interfaces públicas de los módulos.

El ecosistema Move contiene un compilador, una máquina virtual y muchas otras herramientas de desarrollo. Move está inspirado en el lenguaje de programación Rust, que hace explícita la propiedad de los datos en el lenguaje a través de conceptos como tipos lineales. Move enfatiza la escasez de recursos, la preservación y el control de acceso. Los módulos Move definen la vida útil, el almacenamiento y el patrón de acceso de cada recurso. Esto garantiza que recursos como **Coin** no se produzcan sin las credenciales adecuadas, no se puedan gastar
dos veces y no desaparezcan.

Move aprovecha un verificador de código de bytes para garantizar la seguridad del tipo y la memoria incluso en presencia de código que no es de confianza. Para ayudar a escribir código más confiable, Move incluye un verificador formal, Move Prover [6], capaz de verificar la corrección funcional de un programa Move frente a una especificación determinada, formulada en el lenguaje de especificación integrado en Move.

Más allá de las cuentas de usuario y el contenido de la cuenta correspondiente, el estado del *ledger* también contiene la configuración *on-chain* de la blockchain Aptos. Esta configuración de red incluye el conjunto de validadores activos, propiedades de participación *staking* y la configuración de varios servicios dentro de la blockchain de Aptos. Move tiene la capacidad de actualización de módulos y la programabilidad integral que permite cambios de configuración fluidos y actualizaciones de la blockchain de Aptos (ambos conjuntos de actualizaciones fueron ejecutados varias veces sin tiempo de inactividad en una red principal privada).

El equipo de Aptos ha mejorado aún más Move con soporte para casos de uso web3 más amplios. Como se menciona más adelante en la Sección 5.5, la blockchain de Aptos permite un control detallado de los recursos. Esto no solo admite la paralelización de la ejecución, sino que también logra un costo casi fijo asociado con el acceso y la mutación de los datos. Además, la blockchain de Aptos proporciona soporte para tablas construidas sobre almacenamiento detallado, lo que permite conjuntos de datos a gran escala (por ejemplo, colecciones masivas de NFT) en una sola cuenta. Además, Aptos soporta cuentas compartidas o autónomas que están completamente representadas *on-chain.* Esto permite que organizaciones autónomas descentralizadas (DAOs) complejas compartan cuentas de forma colaborativa, así como también utilicen estas cuentas como contenedores para una colección heterogénea de recursos.

5 Modelo de datos lógicos

El estado del libro contable (*ledger*) de la blockchain de Aptos representa el estado de todas las cuentas. El estado del ledger se versiona utilizando un entero de 64 bits sin firma corresponde al número de transacciones que el sistema ha ejecutado. Cualquiera puede enviar una transacción a la blockchain de Aptos para modificar el estado del ledger. Tras la ejecución de una transacción, se genera una transacción de salida. La transacción de salida contiene cero o más operaciones para modificar el estado del libro contable (llamados *write sets*), un vector de eventos resultantes (consulte la Sección 5.1.1), la cantidad de gas consumido y el estado de la transacción ejecutada.

5.1 Transacciones

Una transacción firmada contiene la siguiente información:

- **Autenticador de transacciones:** el remitente utiliza un autenticador de transacciones que incluye una o más firmas digitales para verificar que una transacción está autenticada.

- **Dirección del remitente:** la dirección de la cuenta del remitente.

- **Pago:** el pago se refiere a una función de entrada existente en la blockchain o contiene la función que se ejecutará como código de bytes en línea (llamado script). Además, un conjunto de argumentos de entrada está codificado en matrices de bytes. Para una transacción de tipo *peer-to-peer*, las entradas contienen la información del destinatario y el monto que se le transfiere.

- **Precio del gas** (en moneda/unidades de gas específicas): Este es el monto que el remitente está dispuesto a pagar por unidad de gas para ejecutar la transacción. El gas es una forma de pagar por el procesamiento, las redes y el almacenamiento. Una unidad de gas es una medida abstracta de cálculo sin valor inherente en el mundo real.

- **Cantidad máxima de gas:** La cantidad máxima de gas son las unidades máximas de gas que la transacción puede consumir antes de cancelar. La cuenta debe tener al menos el precio del gas multiplicado por la cantidad máxima de gas o la transacción será descartada durante la validación.

- **Número de secuencia:** El número de secuencia de la transacción. Este debe coincidir con el número de secuencia almacenado en la cuenta del remitente cuando se ejecuta la transacción. Tras la ejecución exitosa de la transacción, el número de secuencia de la cuenta se incrementa para evitar ataques de repetición.

- **Tiempo de vencimiento:** Marca de tiempo después de la cual la transacción deja de ser válida.

- **ID de cadena:** identifica la blockchain para la que es válida esta transacción, lo que ofrece mayor protección y prevenir errores de firmas.

En cada versión i, el cambio de estado está representado por la tupla (Ti, Oi, Si), que contiene la transacción, la transacción de salida y el estado del ledger resultante, respectivamente. Dada una función determinista **Apply**, la ejecución de la transacción Ti con el estado del ledger S$i-1$ produce la transacción de salida Oi y un nuevo estado del ledger Si . Es decir, **Apply** (S$i-1$, Ti) $\rightarrow \langle$Oi, S$i\rangle$.

5.1.1 Eventos

Los eventos se emiten durante la ejecución de una transacción. Cada módulo Move puede definir sus propios eventos y seleccionar cuándo emitir estos eventos durante la ejecución. Por ejemplo, durante una transferencia de *coin*, las cuentas del remitente y del destinatario emitirán SentEvent y ReceivedEvent, respectivamente. Estos datos se almacenan en el ledger y se pueden consultar a través de un nodo Aptos. Cada evento registrado tiene una clave única y la clave se puede utilizar para consultar los detalles del evento.

Varios eventos emitidos a la misma clave de evento producen canales de eventos, una lista de eventos en la que cada entrada contiene un número que aumenta secuencialmente comenzando en 0, un tipo y datos. Cada evento debe estar definido por algún tipo. Puede haber varios eventos definidos por tipos iguales o similares, especialmente cuando se utilizan genéricos. Los eventos tienen datos asociados. Para los desarrolladores del módulo Move, el principio general es incluir todos los datos necesarios para comprender los cambios en los recursos subyacentes antes y después de la ejecución de la transacción que cambió los datos y emitió el evento.

Las transacciones sólo pueden generar eventos y no pueden leer eventos. Este diseño permite que la ejecución de la transacción sea una función sólo del estado actual y de las transacciones de entrada, no de información histórica (por ejemplo, eventos generados previamente).

5.2 Cuentas

Cada cuenta se identifica mediante un valor único de 256 bits conocido como dirección de cuenta. Se crea una nueva cuenta en el estado del libro contable (consulte la Sección 5.5) cuando una transacción enviada desde una cuenta existente invoca la función Move **create_account(addr)**. Esto suele suceder cuando una transacción intenta enviar tokens Aptos a una dirección de cuenta que aún no se ha creado. Para mayor comodidad, Aptos también soporta una función de **transferencia (from, to, amount)** que crea implícitamente una cuenta si aún no existe antes de la transferencia.

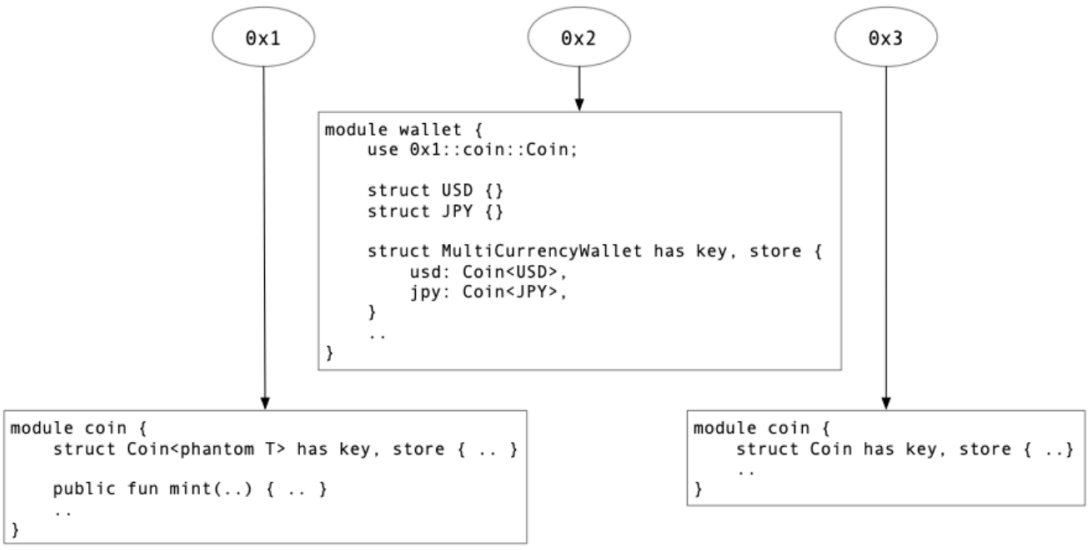

Figura 2: Ejemplo de módulos Move *on-chain*

Para crear una nueva cuenta, el usuario primero genera un par de claves de firma: (vk, sk). A continuación, la nueva dirección de cuenta para un esquema de firma determinado se deriva utilizando el hash criptográfico *H* de la clave de verificación pública vk que se concatena con el identificador del esquema de firma (*ssid*): donde addr = *H(vk, ssid)*.

Después de crear la nueva cuenta en la dirección **addr**, el usuario puede firmar las transacciones que se enviarán desde la cuenta en la dirección **addr**, utilizando la clave de firma privada *sk*. El usuario también puede rotar sk, ya sea para cambiar sk de forma proactiva o para responder a un posible ataque. Esto no cambiará la dirección de la cuenta, ya que la dirección de la cuenta se deriva solo una vez, durante su creación, de la clave de verificación pública.

La blockchain de Aptos no vincula las cuentas a una identidad del mundo real. Un usuario puede crear varias cuentas generando múltiples pares de claves. Las cuentas controladas por el mismo usuario no tienen ningún vínculo inherente entre sí. Sin embargo, un solo usuario aún puede administrar varias cuentas en una sola billetera para una administración

de activos sencilla. Esta flexibilidad proporciona pseudo anonimato a los usuarios mientras experimentamos con primitivas que preservan la privacidad para futuras versiones. Varias cuentas de un solo usuario o un conjunto de usuarios también proporcionan canales para aumentar la concurrencia de ejecución, como se describe en la Sección 7.4.

5.3 Módulos Move

Un módulo Move contiene código de bytes Move que declara tipos de datos (structs) y procedimientos. Se identifica por la dirección de la cuenta donde se declara el módulo junto con un nombre del módulo. Por ejemplo, el identificador del primer módulo de moneda en la Figura 2 es 0x1::**coin**. Un módulo puede depender de otros módulos on-chain, como se muestra en el módulo de billetera en la Figura 2, lo que permite la reutilización de código. Un módulo debe tener un nombre exclusivo dentro de una cuenta, es decir, cada cuenta puede declarar como máximo un módulo con cualquier nombre. Por ejemplo, la cuenta en la dirección 0x1 en la Figura 2 no pudo declarar otro módulo llamado **coin**. Por otro lado, la cuenta en la dirección 0x3 podría declarar un módulo llamado coin y el identificador de este módulo sería 0x3::**coin**. Tenga en cuenta que 0x1::**coin**::**Coin** y 0x3::**coin**::**Coin** son tipos distintos y no se pueden usar indistintamente ni compartir código de módulo común. Por el contrario, 0x1::**coin**::**Coin**<0x2::**wallet**::**USD**> y 0x1::**coin**::**Coin**<0x2::**wallet**::**JPY**> son instancias diferentes del mismo tipo genérico que no se pueden usar indistintamente pero pueden compartir código de módulo común.

Los módulos se agrupan en paquetes ubicados en la misma dirección. El propietario de esta dirección hace publico el paquete como un todo on-chain, incluido el código de bytes y los metadatos del paquete. El paquete de metadatos determina si un paquete se puede actualizar o es inmutable. Para un paquete actualizable, se realizan comprobaciones de compatibilidad antes de permitir la actualización: no se deben cambiar funciones de punto de entrada existentes y no se pueden almacenar recursos en la memoria. Sin embargo, se pueden agregar nuevas funciones y recursos.

El marco Aptos, que consta de las bibliotecas principales y la configuración para la blockchain de Aptos, se define como un paquete de módulos actualizable periódicamente (consulte la Sección 9.2).

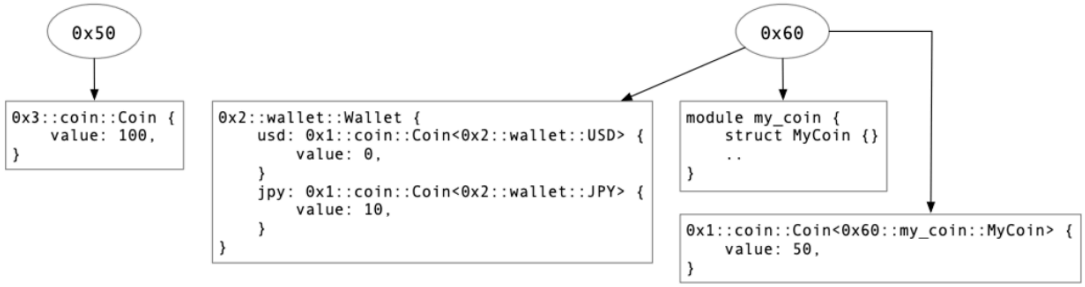

Figura 3: Ejemplo de datos on-chain.

5.4 Recursos

Al igual que los módulos, las direcciones de cuentas también pueden tener valores de datos asociados. Dentro de cada dirección de cuenta, los valores se codifican por sus tipos, y como máximo un valor de cada tipo pertenece a la cuenta. La figura 3 proporciona un ejemplo de esto. La dirección 0x50 tiene un valor único, siendo 0x3::**coin**::**Coin** el tipo totalmente calificado. 0x3 es la dirección donde se almacena el módulo de **coin**, **coin** es el nombre del módulo y **Coin** es el nombre del tipo de datos. También se permiten valores de tipos genéricos, y las diferentes instancias se tratan como tipos distintos. Esto es esencial para la extensibilidad, permitiendo que diferentes instancias compartan el mismo código funcional.

Las reglas para mutar, eliminar y publicar un valor están codificadas en el módulo que define el tipo de datos. Las reglas de seguridad y verificación de Move evitan que otros códigos o entidades creen, modifiquen o eliminen directamente instancias de tipos de datos definidos en otros módulos.

Tener como máximo un valor de nivel superior de cada tipo bajo una dirección puede parecer al principio limitante. Sin embargo, esto no es un problema en la práctica ya que los programadores pueden definir tipos de contenedor con otros datos como campos internos, evitando así cualquier limitación. La **Wallet** *struct* en la Figura 3 es un ejemplo de cómo usar tipos de contenedor *(wrapper types)*.

También cabe señalar que no todos los tipos de datos se pueden almacenar *on-chain*. Para que las instancias de datos califiquen como valores de nivel superior, el tipo de datos debe tener la capacidad de clave. De manera similar, se requiere la capacidad de almacenar valores anidados. Los tipos de datos con ambas capacidades también se denominan *recursos*.

5.5 Estado del Ledger

Desde la perspectiva de la máquina virtual Move (*Move VM*), cada cuenta consta de un conjunto de valores y estructuras de datos *key-value*. Estas estructuras de datos se denominan tablas de entrada *(table entries)* y se almacenan en el formato de serialización canónica binaria (*BCS*).

Este diseño de datos permite a los desarrolladores escribir contratos inteligentes que pueden operar de manera eficiente en pequeñas cantidades de datos replicados en una gran cantidad de cuentas, así como en grandes cantidades de datos almacenados en una pequeña cantidad de cuentas. Los módulos Move se almacenan de manera similar a los datos de la cuenta, pero en un espacio de nombres independiente. El estado del ledger (libro contable) génesis define el conjunto inicial de cuentas y su estado asociado en la inicialización de la blockchain.

En el lanzamiento, la blockchain de Aptos estará representada por un estado de ledger único. Sin embargo, a medida que aumente la adopción y se desarrolle la tecnología, Aptos aumentará la cantidad de fragmentos (shards) para aumentar el rendimiento (es decir, habilitar múltiples estados del ledger) y respaldará transacciones que muevan o accedan a activos entre fragmentos. Cada estado del ledger mantendrá todos los activos en cadena para el fragmento específico y proporcionará el mismo modelo de cuenta con un almacén de datos *key-value* detallado que ofrece costos casi fijos para el acceso al almacenamiento.

6 Una experiencia de usuario segura

Para llegar a miles de millones de usuarios de Internet, la experiencia del usuario de Web3 debe ser segura y accesible. En las secciones siguientes, describimos varias innovaciones proporcionadas por la blockchain de Aptos que trabajan para lograr este objetivo.

6.1 Protección de la viabilidad de la transacción

Firmar una transacción significa que el firmante autoriza que la blockchain confirme y ejecute la transacción. En ocasiones, los usuarios pueden firmar transacciones sin querer o sin considerar plenamente todas las formas en que sus transacciones podrían ser manipuladas. Para reducir este riesgo, la blockchain de Aptos limita la viabilidad de cada transacción y protege al firmante de una validez ilimitada. Actualmente, la blockchain de Aptos proporciona tres protecciones diferentes: el número de secuencia del remitente, el tiempo de vencimiento de la transacción y un identificador de cadena designado.

- El número de secuencia de una transacción sólo se puede confirmar exactamente una vez para la cuenta de cada remitente. Como resultado, los remitentes pueden observar que si el número de secuencia de la cuenta actual es ≥ al número de secuencia de una transacción *t*, entonces *t* ya se ha comprometido o nunca se confirmará (ya que el número de secuencia utilizado por *t* ya ha sido consumido por otra transacción).

- El tiempo de la blockchain avanza con alta precisión y frecuencia (normalmente menos de un segundo), como se detalla en la Sección 7.3.1. Si el tiempo de la blockchain excede el tiempo de vencimiento de la transacción *t*, entonces, de manera similar, *t* ya se ha comprometido o nunca será comprometido.

- Cada transacción tiene un identificador de cadena designado para evitar que entidades maliciosas reproduzcan transacciones entre diferentes entornos de blockchain (por ejemplo, a través de una red de prueba (testnet) y una red principal (mainnet).

6.2 Gestión de claves basada en Move

Como se analizó en la Sección 5.2, las cuentas Aptos admiten la rotación de claves, una característica importante que puede ayudar a reducir los riesgos asociados con el compromiso de la clave privada, los ataques de largo alcance y los avances futuros que podrían romper los algoritmos criptográficos existentes. Además, las cuentas Aptos también son lo suficientemente flexibles como para permitir nuevos modelos híbridos de custodia. En uno de esos modelos, un usuario puede delegar la capacidad de rotar la clave privada de la cuenta a uno o más custodios y otras entidades confiables. Luego, un módulo Move puede definir una política que permita a estas entidades confiables rotar la clave en circunstancias específicas. Por ejemplo, las entidades podrían estar representadas por una clave multifirma *k-out-of-n* en poder de muchas partes confiables y ofrecer servicios de recuperación de claves para evitar la pérdida de claves del usuario (por ejemplo, el 20% de Bitcoin está actualmente bloqueado en cuentas irrecuperables [7]).

Además, si bien muchas billeteras admiten varios esquemas de recuperación de claves, como la copia de seguridad de claves privadas en la infraestructura de la nube, la computación multipartita y la recuperación social, generalmente se implementan sin soporte de blockchain (es decir, *off-chain*). Como resultado, cada billetera necesita implementar su propia infraestructura de administración de claves y las operaciones relacionadas se vuelven opacas para los usuarios. Por el contrario, admitir la funcionalidad de administración de claves en la capa blockchain de Aptos proporciona total transparencia de todas las operaciones relacionadas con claves y simplifica la implementación de una billetera con mejor administración de claves.

6.3 Transparencia de la transacción previa a la firma

Hoy en día, las billeteras brindan muy poca transparencia sobre las transacciones que se firman. Como resultado, a menudo se engaña fácilmente a los usuarios para que firmen transacciones maliciosas que pueden robar fondos y tener consecuencias devastadoras. Esto es cierto incluso para las blockchains que requieren enumerar todos los datos en cadena a los que accede cada transacción. Como resultado, actualmente existen pocos protectores para los usuarios, lo que los hace vulnerables a una amplia variedad de ataques.

Para abordar esto, el ecosistema Aptos proporciona servicios para la *pre ejecución de transacciones*: una medida de precaución que describe a los usuarios (en forma legible por humanos) los resultados de sus transacciones antes de firmar. Combinar esto con un historial conocido de ataques anteriores y contratos inteligentes maliciosos ayudará a reducir el fraude.
Además, Aptos también permite que las billeteras dicten restricciones a las transacciones durante la ejecución. La violación de estas restricciones dará como resultado la cancelación de

las transacciones, para proteger aún más a los usuarios de aplicaciones maliciosas o ataques de ingeniería social.

6.4 Protocolos prácticos para clientes ligeros

Depender únicamente de los certificados TLS/SSL de los proveedores de API para establecer la confianza entre los clientes y servidores de blockchain no protege suficientemente a los clientes. Incluso en presencia de certificados válidos, las billeteras y los clientes no tienen garantías en cuanto a la autenticidad e integridad de los datos que se presentan a ellos.

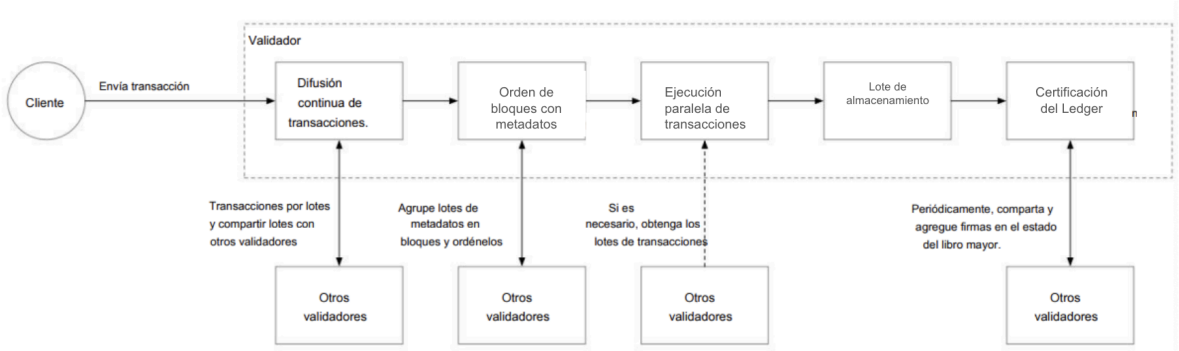

Figura 4: El ciclo de vida del procesamiento de transacciones. Todas las etapas son completamente independientes y paralelizables individualmente.

Como resultado, los proveedores de API pueden devolver datos de blockchain incorrectos o maliciosos, engañando a terceros y realizando ataques de doble gasto.

Para evitar esto, Aptos proporciona pruebas de estado (state proofs) y protocolos ligeros de verificación de clientes que pueden ser utilizados por billeteras y clientes para verificar la validez de los datos presentados por un servidor de terceros que no es de confianza.

Además, al aprovechar las pruebas de estado basadas en marcas de tiempo de la Sección 7.6.2, los clientes ligeros siempre pueden garantizar límites estrictos en la actualidad del estado de la cuenta (por ejemplo, en cuestión de segundos) y solo necesitan realizar un seguimiento de los cambios en la configuración de la red (*epoch changes*) o utilizar puntos de control confiables (*waypoints*) actuales para mantenerse actualizado [8]. Al combinar marcas de tiempo de alta frecuencia y pruebas de estado económicas, la blockchain de Aptos ofrece mayores garantías de seguridad a los clientes.

Además, los nodos de Aptos también exponen excelentes interfaces de almacenamiento y de alto rendimiento que se pueden ajustar aún más para permitir suscripciones a pruebas dirigidas a datos y cuentas específicas en la blockchain. Los clientes ligeros pueden aprovechar esto para retener datos mínimos verificables sin la necesidad de ejecutar un nodo completo o procesar una cantidad sustancial de transacciones.

7 Canalización, procesamiento por lotes y transacciones paralelas

Para maximizar el rendimiento, aumentar la concurrencia y reducir la complejidad de la ingeniería, el procesamiento de transacciones en la blockchain de Aptos se divide en etapas separadas. Cada etapa es completamente independiente y paralelizable individualmente, asemejándose a las arquitecturas de procesadores modernos super escalables. Esto no solo proporciona importantes beneficios de rendimiento, sino que también permite que la blockchain de Aptos ofrezca nuevos modos de interacción validador-cliente. Por ejemplo:

- Se puede notificar a los clientes cuando se hayan incluido transacciones específicas en un lote de transacciones persistentes. Es muy probable que las transacciones persistentes y válidas se confirmen de forma inminente.

- Se puede informar a los clientes cuando se ha ordenado un lote de transacciones persistentes. Por lo tanto, para reducir la latencia de determinar los resultados de las transacciones ejecutadas, los clientes pueden seleccionar ejecutar transacciones localmente en lugar de esperar a que los validadores completen la ejecución de forma remota.

- Los clientes pueden optar por esperar la ejecución de la transacción certificada por parte de los validadores y realizar el estado de sincronización de los resultados comprobados (por ejemplo, consulte la sección 8).

El diseño modular de Aptos ayuda a acelerar el desarrollo y admite ciclos de lanzamiento más rápidos, ya que los cambios pueden dirigirse a módulos individuales, en lugar de a una única arquitectura monolítica. De manera similar, el diseño modular también proporciona una ruta estructurada para escalar los validadores más allá de una sola máquina, brindando acceso a recursos informáticos, de red y de almacenamiento adicionales. La Figura 4 muestra el ciclo de vida de la transacción en las distintas etapas de procesamiento.

7.1 Procesamiento por lotes

El procesamiento por lotes es una importante optimización de la eficiencia que forma parte de cada fase de operación en la blockchain de Aptos. Cada validador agrupa las transacciones en lotes durante la difusión de las transacciones, y los lotes se combinan en bloques durante el consenso. La ejecución, almacenamiento y las fases de certificación del ledger también funcionan en lotes para brindar oportunidades de reordenamiento, reducción de operaciones (por ejemplo, cálculo duplicado o verificación de firmas) y ejecución paralela.

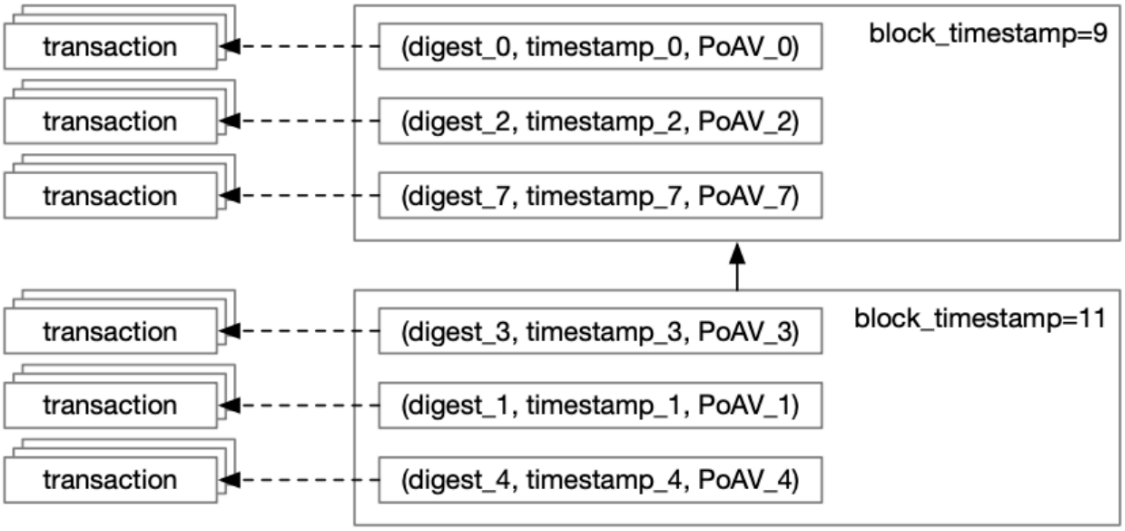

Figura 5: El orden de los metadatos de los bloques que se producen independientemente de la difusión de las transacciones.

Agrupar transacciones en lotes puede inducir pequeñas cantidades de latencia, por ejemplo, esperar 200 milisegundos para acumular un lote de transacciones antes de realizar la difusión. Sin embargo, el procesamiento por lotes es fácilmente configurable con respecto a un periodo de espera máximo y tamaño máximo de lote, lo que permite una red descentralizada para optimizar automáticamente la latencia y la eficiencia. El procesamiento por lotes también permite para mercados de tarifas eficientes para priorizar las transacciones y evitar ataques involuntarios de denegación de servicio (DoS) de clientes maliciosos.

7.2 Difusión continua de transacciones

Siguiendo la idea principal de Narwhal & Tusk [9], la difusión de transacciones en la blockchain de Aptos está desvinculada del consenso. Los validadores transmiten continuamente lotes de transacciones entre sí, utilizando todos los recursos de red disponibles al mismo tiempo. Cada lote distribuido por un validador *v* es persistente y se envía una firma en el resumen del lote a *v*. Siguiendo los requisitos de consenso definidos en la Sección 7.3, cualquier firma *stake* por participación 2f + 1 en el resumen del lote constituye una prueba de disponibilidad (*PoAv*). Tal prueba garantiza que al menos *f + 1* validadores honestos ponderados por participación tienen almacenado el lote y, por lo tanto, todos los validadores honestos podrán recuperarlo antes de la ejecución.

Los lotes de transacciones que persisten infinitamente pueden abrir un vector de ataque DoS al hacer que los validadores se queden sin almacenamiento y fallen. Para evitar esto, cada lote de transacciones tiene una marca de tiempo asociada (*timestamp*). La marca de tiempo en el lote permite una recolección de basura eficiente en cada validador. Además el mecanismo de

cuota separado por validador está diseñado para proteger a los validadores de quedarse sin espacio incluso en las circunstancias más extremas, como pueden ser posibles ataques bizantinos. Los lotes también tienen restricciones de tamaño que se validan antes del acuerdo para persistir en el almacenamiento estable. Finalmente, varias optimizaciones para eliminar duplicados y almacenar en caché las transacciones reducen los costos de almacenamiento y garantizan el rendimiento con el motor de ejecución paralela.

7.3 Orden de metadatos del bloque

Un error común es pensar que el consenso es lento y, por lo tanto, es el principal cuello de botella para el rendimiento de la blockchain y la latencia. Una de las innovaciones clave de la blockchain de Aptos es desacoplar de la fase de consenso las tareas no relacionadas con acuerdos, como la difusión de transacciones, las transacciones ejecución/almacenamiento y certificación del ledger. Al desacoplar la difusión de transacciones de la fase de consenso, los pedidos pueden ocurrir con un ancho de banda muy bajo (bloquear metadatos y pruebas únicamente), lo que resulta en alto rendimiento de transacciones y latencia minimizada.

Hoy en día, la blockchain Aptos aprovecha la última versión de DiemBFTv4 [10], una versión optimista del protocolo de consenso responsivo para BFT. El consenso en el caso común solo requiere dos rondas de viajes (con tiempos de ida y vuelta generalmente inferiores a 300 milisegundos en todo el mundo) y se ajusta dinámicamente a validadores defectuosos a través de un mecanismo de reputación líder [11]. El mecanismo de reputación líder on-chain promueve a los validadores que han confirmado bloques con éxito en una ventana y degrada a los validadores que no participan. Este novedoso mecanismo mejora significativamente el rendimiento en entornos descentralizados, proporciona infraestructura para incentivos adecuados y minimiza rápidamente el impacto de los validadores fallidos en el rendimiento y la latencia.

DiemBFTv4 garantiza vida bajo sincronía parcial y garantiza la seguridad bajo asincronía donde la participación total del validador es ≥ 3f + 1 con hasta f validadores defectuosos ponderados por participación. DiemBFTv4 ha sido probada exhaustivamente en varias iteraciones desde 2019 con docenas de operadores de nodos y un ecosistema de múltiples billeteras. También estamos experimentando con nuestra investigación reciente (por ejemplo, Bullshark [12]) y otros protocolos que se basan en el historial de bloques y la comunicación asociada para determinar el orden y la finalidad de los metadatos en los bloques.

Un líder propone un bloque de consenso y una propuesta de marca de tiempo mientras los otros validadores los aceptan, como se muestra en la Figura 5. Tenga en cuenta que cada bloque de consenso contiene solo las pruebas y los metadatos del lote. No se requieren transacciones reales en el bloque, ya que el *PoAV* garantiza que los lotes de transacciones estarán disponibles en la fase de ejecución después de realizar el ordenamiento (consulte la Sección 7.2). Los validadores pueden votar sobre la propuesta de un líder después de verificar que la prueba y los criterios de metadatos del bloque se cumplan (por ejemplo, marca de tiempo de la propuesta ≤ tiempo de vencimiento del bloque).

7.3.1 Tiempo de la blockchain

La blockchain de Aptos adopta una marca de tiempo física aproximada y acordada para cada bloque propuesto y, en consecuencia, para todas las transacciones dentro de ese bloque. Esta marca de tiempo permite muchos casos de uso importantes. Por ejemplo:

- Lógica dependiente del tiempo en contratos inteligentes. Por ejemplo, a un desarrollador le gustaría codificar que todas las ofertas en una subasta deben recibirse antes del mediodía del jueves.

- A medida que los oráculos publican datos on-chain, se requiere una marca de tiempo precisa y confiable para correlacionar eventos y manejar retrasos a partir de datos del mundo real.

- Los clientes pueden discernir qué tan actualizados están con respecto a la blockchain. Por razones de seguridad, para evitar datos obsoletos y ataques de largo alcance, un cliente debe tener acceso a una marca de tiempo de alta precisión sobre cuándo se actualizó el estado de la cuenta.

- Auditar la blockchain con una marca de tiempo confiable proporciona una fuerte correlación con eventos fuera de la cadena, como garantizar que los pagos exigidos legalmente cumplan con los requisitos esperados.
- La caducidad de la transacción se basa en la marca de tiempo confirmada más reciente. Como protección adicional para las transacciones de los clientes, los clientes pueden seleccionar un tiempo de vencimiento para una transacción, como se describe en la Sección 6.1.

La blockchain de Aptos ofrece las siguientes garantías con respecto a las marcas de tiempo *(timestamps)* para todas las transacciones dentro de un bloque:

- El tiempo aumenta monótonamente en la blockchain. Es decir, si el bloque B1 <bloque B2, entonces B1.Time < B2.Time.

- Si se autoriza un bloque de transacciones con la marca de tiempo T, entonces al menos f + 1 validadores honestos han decidido que T está en el pasado. Un validador honesto solo votará en un bloque cuando su propio reloj ≥ marca de tiempo T. Consulte la Sección 7.2.

- Si un bloque de transacciones tiene un quórum de firmas en consenso con la marca de tiempo T, un validador honesto no entregará dicho bloque a otros validadores hasta que su propio reloj ≥ marca de tiempo T.

La marca de tiempo más reciente se actualiza en cada bloque comprometido y se utiliza como marca de tiempo para todas las transacciones en ese bloque. Cuando la red es síncrona, se confirma un bloque de transacciones en cada viaje de ida y vuelta de la red y proporciona una

actualización rápida y un reloj altamente confiable. Si se desea, se puede determinar una granularidad más fina de pedidos dentro de bloques de transacciones.

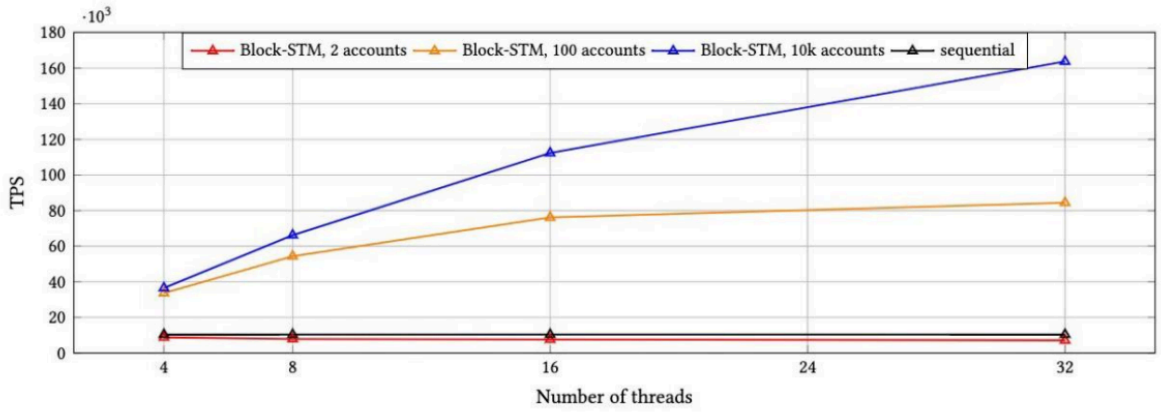

Figura 6: Puntos de referencia de Block-STM (solo componentes) que comparan la cantidad de núcleos físicos con diferentes niveles de contención.

7.4 Ejecución de transacciones paralelas

Una vez que se ordenan los metadatos del bloque de consenso, cualquier validador, nodo completo o cliente puede ejecutar las transacciones. Al menos 2f + 1 validadores con stake participante han permanecido en transacciones para los lotes propuestos. Dado que la difusión de transacciones es continua, con el tiempo, más validadores honestos recibirán los lotes de transacciones. Si un validador honesto no ha recibido las transacciones para los lotes ordenados cuando llega a la etapa de ejecución, puede descargarlas de los validadores con stake 2f + 1, sabiendo que al menos f + 1 validadores con stake (≥ la mitad de los que firman son validadores con stake PoAV) son honestos.

Un objetivo importante para cualquier blockchain es permitir la mayor ejecución paralela posible. La blockchain de Aptos avanza en esta dirección desde el modelo de datos como desde el motor de ejecución.

7.4.1 Modelo de datos paralelo

El modelo de datos Move permite de forma nativa el direccionamiento global de datos y módulos. Las transacciones que no tengan conflictos superpuestos en datos y cuentas se pueden ejecutar en paralelo. Dado el diseño canalizado utilizado por la blockchain de Aptos, reordenar un grupo de transacciones puede reducir la cantidad de conflictos, mejorando así la concurrencia.

Incluso cuando las transacciones modifican el mismo conjunto de valores *on-chain* , gran parte del proceso de ejecución de la transacción aún se puede paralelizar. La blockchain de Aptos introduce un nuevo concepto, *delta writes*, que describe una modificación del estado de la cuenta en lugar del estado modificado de la cuenta (por ejemplo, incrementar un número entero en lugar de simplemente determinar el valor final). Todo el procesamiento de

transacciones se puede completar en paralelo y luego se aplican *delta writes* en la secuencia correcta para valores en conflicto para garantizar resultados deterministas.

Con el tiempo, la blockchain de Aptos continuará mejorando el modelo de datos de manera que mejore la concurrencia (por ejemplo, aprovechando las sugerencias de lectura/escritura) y también mejore la ergonomía, haciendo que sea más natural para los desarrolladores crear, modificar y componer valores on-chain. Move proporciona flexibilidad para realizar estas mejoras tanto a nivel de idioma como a través de funciones específicas de la plataforma.

7.4.2 Motor de ejecución paralela

El motor de ejecución paralela Block-STM detecta y gestiona los conflictos para un conjunto ordenado de transacciones junto con un control de concurrencia optimista para permitir el máximo paralelismo dado un orden particular [13]

Los lotes de transacciones se ejecutan de manera optimista en paralelo y se validan después de la ejecución. Las validaciones fallidas conducen a ejecuciones. Block-STM utiliza una estructura de datos de múltiples versiones para evitar conflictos de escritura. Todas las escrituras en la misma ubicación se almacenan junto con sus versiones, que contienen sus ID de transacción y la cantidad de veces que la transacción de escritura se volvió a ejecutar de manera optimista.

Cuando la transacción *tx* lee una ubicación de memoria, obtiene de la estructura de datos múltiples versiones el valor escrito en esta ubicación por la transacción más alta que aparece antes de tx en el orden preestablecido, junto con la versión asociada.

Block-STM ya está integrado en la blockchain de Aptos. Para comprender todo el potencial del rendimiento de Block-STM, realizamos experimentos con transacciones Move *peer-to-peer* no triviales (es decir, 8 lecturas y 5 escrituras por transacción) como una operación aislada, de sola ejecución (no de un extremo a otro) comparando con la base de datos de la memoria. En la Figura 6 presentamos los resultados de la ejecución de Block-STM. Cada bloque contiene 10,000 transacciones y la cantidad de cuentas determina el nivel de conflictos y contiendas.

En condiciones de baja contención, Block-STM logra una aceleración de 16 veces respecto a la ejecución secuencial con 32 subprocesos, mientras que en condiciones de alta contención, Block-STM logra una aceleración de más de 8 veces. Exclusivo de otros motores de ejecución paralela en el espacio blockchain, Block-STM es capaz de extraer de forma dinámica y transparente (sin ninguna sugerencia por parte del usuario) el paralelismo inherente de cualquier carga de trabajo. En comparación con los entornos de ejecución paralela que requieren un conocimiento previo de las ubicaciones de los datos que se leerán o escribirán, Block-STM puede admitir transacciones más complejas al mismo tiempo. Esta propiedad genera menos transacciones pero más eficientes, reduce los costos y proporciona una latencia más baja para los usuarios. Quizás lo más importante es que dividir una transacción atómica en múltiples transacciones más pequeñas rompe la semántica de todo o nada de una sola transacción con resultados de estado complejos. Combinar la semántica de transacciones expresiva con la ejecución paralela en Block-STM permite a los desarrolladores tener lo mejor de ambos mundos.

Tenga en cuenta que el paso de ordenación de metadatos en bloque no impide reordenar transacciones en la fase de ejecución paralela. Las transacciones se pueden reordenar en uno o más bloques para optimizar la concurrencia para la ejecución paralela. El único requisito es que el reordenamiento debe ser determinista en todos los validadores honestos. La optimización para la ejecución paralela y la adición de aleatorización al reordenamiento pueden aumentar el rendimiento y potencialmente desalentar las técnicas de valor máximo extraíble *(MEV)* para el reordenamiento rentable de transacciones de validación. También se pueden incorporar estrategias resistentes a MEV de “ordenar y luego revelar” en este diseño canalizado.

Block-STM y el reordenamiento de transacciones son técnicas complementarias para aumentar la ejecución paralela. Se pueden combinar con accesos de lectura/escritura para lograr mayor simultaneidad.

7.5 Almacenamiento por lotes

La fase de ejecución paralela da como resultado conjuntos de escritura para todas las transacciones de un grupo. Estos conjuntos de escritura se pueden almacenar en la memoria para obtener la máxima velocidad de ejecución y luego usarse como caché para el siguiente bloque o conjunto de bloques a ejecutar. Cualquier escritura superpuesta solo debe escribirse en el almacenamiento estable una vez. Si un validador falla antes de almacenar los conjuntos de escritura en memoria, simplemente puede reanudar la ejecución paralela desde la fase de ordenación de metadatos en bloque. Desacoplar el almacenamiento por lotes de conjuntos de escritura del paso de ejecución paralela garantiza que la ejecución paralela pueda funcionar de manera eficiente. En resumen, los conjuntos de escritura por lotes reducen la cantidad de operaciones de almacenamiento y aprovechan operaciones de tipo I/O más grandes y eficientes.

La cantidad de memoria reservada para el almacenamiento en caché del conjunto de escritura se puede configurar manualmente por máquina y proporciona un mecanismo de contrapresión natural. La granularidad de los lotes puede ser diferente de la granularidad de los bloques de ejecución paralela si se desea ajustarlo para entornos de memoria I/O.

7.6 Certificación de ledger

En este punto del proceso, cada validador individual ha calculado el nuevo estado para un bloque de transacciones autorizado. Sin embargo, para admitir de manera eficiente a los clientes ligeros verificados y la sincronización del estado, la blockchain de Aptos implementa la certificación del *ledger* para el historial y también para el estado del ledger. Una diferencia importante para la blockchain de Aptos es que la certificación del ledger no se encuentra en la ruta crítica del procesamiento e incluso puede ejecutarse completamente fuera de banda si se desea.

7.6.1 Certificación del historial del ledger

Un validador agrega las transacciones junto con su resultado de ejecución a una estructura de datos del *ledger* autenticado global. Parte del resultado de la transacción es el conjunto de escritura de estado, que consta de las modificaciones realizadas en el estado global al que Move puede acceder. El autenticador breve de esta estructura de datos es un compromiso vinculante con un historial del ledger, que incluye el lote de transacciones recién ejecutadas. De manera similar a la ejecución de transacciones, la generación de esta estructura de datos es determinista.

Cada validador firma el autenticador corto en la nueva versión de la base de datos resultante. Los validadores comparten entre sí su conjunto reciente de autenticadores cortos firmados, agregan colectivamente autenticadores cortos firmados por quórum y también comparten entre sí los autenticadores cortos firmados recientemente por quórum.

Al utilizar esta firma colectiva, los clientes pueden confiar en que una versión de la base de datos representa el historial del ledger, válido e irreversible de acuerdo con las propiedades BFT del protocolo. Los clientes pueden consultar cualquier validador (o cualquier réplica de la base de datos de terceros, como un nodo completo) para leer un valor de la base de datos y verificar el resultado utilizando el autenticador y una prueba de los datos deseados.

7.6.2 Certificación periódica del estado

La totalidad del estado global al que puede acceder Move se puede resumir en un breve autenticador en cualquier punto del historial, similar a un resumen del historial del ledger. Debido a la naturaleza de acceso aleatorio del estado global (a diferencia del historial del ledger que solo se adiciona), el costo de mantener esta autenticación es significativo. Sin embargo, al actualizar la estructura de datos en un lote grande, podemos calcular la actualización en paralelo y también aprovechar cualquier superposición entre las partes que deben actualizarse cuando cambia cada valor de estado individual. La blockchain de Aptos deliberadamente sólo certifica periódicamente el estado global para reducir las actualizaciones compartidas duplicadas.

Durante intervalos determinísticos y configurados, la red emite transacciones de punto de control de estado que incluyen el autenticador de estado global como parte de su salida. Estas versiones se denominan puntos de control estatales. Cuanto mayor sea la brecha entre dos puntos de control, menor será el costo amortizado de actualizar la estructura de datos autenticados por el estado por transacción.

Con los puntos de control de estado, se puede leer cualquier valor de estado de ellos sin confianza sin almacenar todo el estado global. Esta capacidad es útil para aplicaciones como sincronización de estado incremental, almacenamiento fragmentado entre validadores, nodos de validación sin estado y clientes ligeros con almacenamiento limitado. Sin embargo, debido a que los puntos de control de estado son periódicos, obtener una prueba de una versión específica del estado del ledger requiere la ejecución de transacciones adicionales para las alternancias de estado que faltan o una prueba de inclusión de ellas del historial del ledger autenticado.

Los puntos de control de estado están vinculados a las versiones de transacciones específicas en el historial del ledger, por lo tanto, vinculados a la marca de tiempo asociada con

los lotes de transacciones mencionados en la Sección 7. Con la marca de tiempo (timestamp), un cliente ligero puede comprender la actualidad de un valor de estado probado. Sin una marca de tiempo, una prueba de cliente ligera solo puede garantizar la validez de un estado anterior que podría estar muy lejos en el pasado, lo que proporciona poca seguridad de relevancia. Además, las marcas de tiempo para las pruebas estatales son necesarias para rastrear el acceso histórico y con fines de auditoría, como calcular el saldo promedio por hora de tokens en una reserva de tokens.

Los puntos de control de estado se pueden derivar en función de un punto de control de estado anterior y de las alternancias de estado en los resultados de la transacción posteriores. Por lo tanto, no es necesario que los puntos de control de estado persistentes para el almacenamiento estable estén en la ruta crítica para el procesamiento de transacciones. Además, también existen efectos de procesamiento por lotes beneficiosos cuando se mantienen los puntos de control estatales. Almacenar en caché los puntos de control de estado recientes (o más bien el delta entre ellos) en la memoria y volcar solo los puntos de control de estado periódicos en un almacenamiento estable puede reducir en gran medida el consumo de ancho de banda de almacenamiento. La forma en que se eligen los puntos de control para que persistan no afecta el cálculo de la estructura de datos autenticados. Por lo tanto, esta es una elección por nodo: los operadores de nodos pueden configurar el equilibrio adecuado entre capacidad de memoria y ancho de banda de almacenamiento.

8 Sincronización del estado

La blockchain de Aptos tiene como objetivo proporcionar un sistema de alto rendimiento y baja latencia para todos los participantes del ecosistema. Como resultado, la blockchain debe ofrecer un protocolo de sincronización de estado eficiente para difundir, verificar y conservar los datos de la blockchain para clientes ligeros, nodos completos y validadores [14]. Además, el protocolo de sincronización también debe ser tolerante con las limitaciones de recursos y la heterogeneidad dentro de la red, teniendo en cuenta diferentes usuarios y casos de uso. Por ejemplo, debe permitir que los nodos completos se archiven, verifiquen y mantengan todo el historial y el estado de la blockchain, al mismo tiempo que permita a los clientes ligeros rastrear de manera eficiente solo un pequeño subconjunto del estado de la blockchain de Aptos.

Para lograr esta propiedad, la blockchain de Aptos aprovecha el historial del ledger autenticado y las pruebas de estado certificadas (consulte la Sección 7.6.1) que ofrecen los validadores, nodos completos y otros replicadores para proporcionar un protocolo de sincronización flexible y configurable. Específicamente, los participantes en la red pueden seleccionar diferentes estrategias de sincronización para optimizar sus casos de uso y requisitos.

Por ejemplo, en el caso de nodos completos, Aptos permite múltiples estrategias de sincronización, incluida la capacidad de procesar todas las transacciones desde el principio de los tiempos o omitir por completo el historial de la blockchain y sincronizar solo el último estado de la blockchain utilizando puntos de referencia. En el caso de clientes ligeros, las estrategias incluyen sincronizar estados parciales de blockchain, por ejemplo, cuentas específicas o valores de datos, y habilitar lecturas de estado verificadas, por ejemplo, recuperación de saldo

de cuenta verificada. En todos los casos, Aptos permite a los participantes configurar la cantidad y antigüedad de los datos a recuperar, procesar y retener.

Al adoptar un enfoque flexible y configurable para la sincronización de estados, Aptos puede adaptarse a una variedad de requisitos de los clientes y continuar ofreciendo estrategias de sincronización nuevas y más eficientes en el futuro.

9 Propiedad de la comunidad

La blockchain de Aptos será propiedad, operada y gobernada por una comunidad amplia y diversa. Se utilizará un token Aptos nativo para las tarifas de transacción y de red, la votación de gobernanza sobre las actualizaciones del protocolo y los procesos dentro y fuera de la cadena, y para asegurar la blockchain a través de un modelo de prueba de participación proof-of-stake. En una publicación futura se incluirá una descripción completa de la economía del token Aptos.

9.1 Tarifas de la red y transacción

Todas las transacciones de Aptos tienen un precio unitario de gas (especificado en tokens de Aptos) que permite a los validadores priorizar las transacciones de mayor valor en la red. Además, en cada etapa del modelo canalizado, existen múltiples oportunidades para descartar transacciones de bajo valor (lo que permite que la blockchain funcione de manera eficiente cuando el sistema está a su capacidad). Con el tiempo, se implementarán tarifas de red para garantizar que los costos de uso de la blockchain de Aptos sean proporcionales a los costos reales de implementación, mantenimiento y operación de nodos del hardware. Además, los desarrolladores tendrán la oportunidad de diseñar aplicaciones con diferentes compensaciones de costos entre computación, almacenamiento y redes.

9.2 Gobernanza de la red

Cada cambio y mejora importante de las características de la blockchain de Aptos pasará por varias fases, incluida la propuesta, la implementación, las pruebas y el lanzamiento. Esta estructura crea oportunidades para que los participantes y *stakeholders* relevantes proporcionen comentarios, compartan inquietudes y ofrezcan sugerencias.

La fase final, la implementación, normalmente se logra en dos pasos. En primer lugar, se implementará una versión de software con la nueva funcionalidad en cada nodo y, en segundo lugar, la funcionalidad se habilitará, por ejemplo, mediante un indicador de función o una variable de configuración on-chain.

Cada implementación de software por parte de los operadores de nodos debe ser compatible con versiones anteriores para garantizar que el nuevo software sea interoperable con las versiones compatibles. El proceso de implementación de una nueva versión de software puede durar varios días, para tener en cuenta a los operadores en diferentes zonas horarias y cualquier problema externo. Una vez que se haya actualizado una cantidad suficiente de nodos, la habilitación de la nueva funcionalidad puede activarse mediante un

punto de sincronización, como una altura de bloque acordada o un cambio de *epoch.* En condiciones de emergencia (por ejemplo, cuando el tiempo de inactividad es inevitable), la habilitación puede realizarse mediante un cambio manual y forzado por parte de los operadores de nodos y, en el peor de los casos, una bifurcación dura en la red (hard fork).

En comparación con otras cadenas de bloques, la blockchain Aptos codifica su configuración en cadena. Cada validador tiene la capacidad de sincronizarse con el estado actual de la blockchain y seleccionar automáticamente la configuración correcta (por ejemplo, protocolo de consenso y versión del marco Aptos) en función de los valores actuales en la cadena. Las actualizaciones en la blockchain de Aptos son fluidas e instantáneas gracias a esta funcionalidad.

Para brindar flexibilidad y capacidad de configuración al proceso de habilitación, la blockchain de Aptos permitirá la gobernanza en cadena donde los acreedores de tokens pueden votar con respecto a los pesos de sus tokens en *stake*.

Los protocolos de votación en cadena son públicos, verificables y pueden ser instantáneos. La gobernanza on-chain también puede respaldar la habilitación de resultados no binarios sin implementación de software. Por ejemplo, los parámetros del protocolo de elección del líder en cadena se pueden modificar con la gobernanza en cadena, mientras que un punto de sincronización preconocido no podría manejar modificaciones dinámicas ya que todos los cambios tendrían que conocerse de antemano.

Con el tiempo, la gobernanza en cadena se puede implementar en todo el proceso de gestión de actualizaciones. Por ejemplo:

1. Los acreedores de tokens votan on-chain sobre la transición a un nuevo esquema de firma cuántica resistente.

2. Los desarrolladores implementan y verifican el nuevo esquema de firma y crean una nueva versión de software.

3. Los validadores actualizan su software a la nueva versión.

4. Los acreedores de tokens votan on-chain para habilitar el nuevo esquema de firma, la configuración en cadena es actualizada y entra en vigor.

Como proyecto de código abierto, la blockchain de Aptos dependerá de una sólida retroalimentación de la comunidad y utilizará la gobernanza on-chain para gestionar los procesos adecuados. Es posible que aún sea necesaria la habilitación de actualizaciones off-chain en determinadas condiciones, pero se minimizará con el tiempo.

9.3 Consenso *Proof-of-stake*

Para participar en la validación de transacciones en la blockchain de Aptos, los validadores deben tener una cantidad mínima requerida de tokens Aptos guardados o en *stake*. Las cantidades en *stake* afectan proporcionalmente el *PoAv* ponderado de participación *2f + 1* durante la difusión de la transacción, así como las ponderaciones de los votos y la selección del líder durante el orden de los metadatos del bloque. Los validadores deciden la división de las recompensas entre ellos y sus respectivos participantes. Los *stakers* pueden seleccionar cualquier número de validadores en los que apostar sus tokens para una división de recompensa previamente acordada. Al final de cada época (epoch), los validadores y sus respectivos participantes recibirán sus recompensas a través de los módulos Move on-chain correspondientes.

Cualquier operador validador con suficiente participación puede unirse libremente a la blockchain de Aptos. Todos los parámetros, incluida la participación mínima requerida, se pueden establecer mediante los procesos de habilitación en cadena descritos en la Sección 9.2.

10 Rendimiento

Como se mencionó en la Sección 7, la blockchain de Aptos puede lograr un rendimiento y una eficiencia de hardware óptimos a través de su canal de procesamiento de transacciones modular, optimizado por lotes y paralelo. Iniciativas de rendimiento adicionales, como actualizaciones de consenso, delta writes, sugerencias de transacciones y almacenamiento en caché de rutas críticas, seguirán aumentando el rendimiento y mejorando la eficiencia con el tiempo.

Hoy en día, el rendimiento de la blockchain normalmente se mide en transacciones por segundo. Sin embargo, dada la amplia gama de costos y complejidad de las transacciones e infraestructuras, este es un método impreciso para comparar sistemas. La latencia de las transacciones también es igualmente defectuosa, ya que los puntos inicial y final del envío hasta la finalidad varían según los experimentos.

Además, algunos sistemas requieren un conocimiento a priori de las entradas y salidas de las transacciones y obligan a las transacciones lógicas a dividirse en transacciones más pequeñas y menos complejas. Dividir una transacción genera malas experiencias de usuario e impacta artificialmente la latencia y el rendimiento, sin considerar lo que el desarrollador está tratando de lograr. Por el contrario, el enfoque de Aptos es permitir a los desarrolladores la libertad de construir sin límites y medir el rendimiento y la latencia con respecto a casos de uso del mundo real en lugar de transacciones sintéticas.

La blockchain de Aptos continuará optimizando el rendimiento de los validadores individuales, así como también experimentará con técnicas de escalamiento que agreguen más validadores a la red. Ambas direcciones tienen distintas vertientes. Cualquier blockchain con capacidades de ejecución paralela puede admitir concurrencia adicional al requerir hardware

más potente o incluso estructurar cada validador como un grupo de máquinas individuales. Sin embargo, existen límites prácticos para el número de validadores globales que son proporcionales al costo y la complejidad para los operadores de validadores. El aumento y la popularidad de las bases de datos sin servidor en los servicios en la nube ejemplifican cómo pocas entidades pueden implementar y mantener de manera eficiente este tipo de sistemas distribuidos complejos.

10.1 Fragmentación del estado homogéneo

Inicialmente, la blockchain de Aptos se lanzará con un ledger único. Con el tiempo, la red Aptos adoptará un enfoque único hacia la escalabilidad horizontal manteniendo al mismo tiempo la descentralización. Esto ocurrirá a través de múltiples estados ledger fragmentados, cada uno de los cuales ofrecerá una API homogénea y fragmentación como un concepto de primera clase. El token Aptos se utilizará para tarifas de transacción, *staking* y gobernanza en todos los fragmentos (*shards*).

Los datos pueden transferirse entre fragmentos a través de un puente homogéneo. Los usuarios y desarrolladores pueden elegir sus propios esquemas de fragmentación según sus necesidades. Por ejemplo, los desarrolladores pueden proponer un nuevo fragmento o un clúster de usuarios dentro de fragmentos existentes para lograr altas conexiones dentro del fragmento. Además, los fragmentos pueden tener diferentes características del sistema. Un fragmento podría optimizarse para computación con *SSDs* y otro podría optimizarse para discos duros grandes con bajas características de computación. Al proporcionar flexibilidad de hardware entre diferentes fragmentos, los desarrolladores pueden aprovechar las características apropiadas del sistema para sus aplicaciones.

En resumen, la fragmentación de estado homogéneo proporciona potencial para la escalabilidad del rendimiento horizontal, permite a los desarrolladores programar con un único estado universal en todas las particiones y permite que las billeteras incorporen fácilmente datos fragmentados para sus usuarios. Esto proporciona importantes beneficios de rendimiento, así como la simplicidad de una única plataforma unificada de contratos inteligentes Move.

Referencias

[1] “Aptos-core,” 2022. [En línea]. Disponible: https://github.com/aptos-labs/aptos-core
[2] “Move,” 2022. [En línea]. Disponible: https://github.com/move-language/move
[3] D. Matsuoka, C. Dixon, E. Lazzarin, and R. Hackett. (2022) Introducing the 2022 state of crypto report. [En línea]. Disponible: https://a16z.com/tag/state-of-crypto-2022/
[4] Z. Amsden, R. Arora, S. Bano, M. Baudet, S. Blackshear, A. Bothra, G. Cabrera, C. Catalini, K. Chalkias, E. Cheng, A. Ching, A. Chursin, G. Danezis, G. D. Giacomo, D. L. Dill, H. Ding, N. Doudchenko, V. Gao, Z. Gao, F. Garillot, M. Gorven, P. Hayes, J. M. Hou, Y. Hu, K. Hurley, K. Lewi, C. Li, Z. Li, D. Malkhi, S. Margulis, B. Maurer, P. Mohassel, L. de Naurois, V. Nikolaenko, T. Nowacki, O. Orlov, D. Perelman, A. Pott, B. Proctor, S. Qadeer, Rain, D. Russi, B. Schwab, S. Sezer, A. Sonnino, H. Venter, L. Wei, N. Wernerfelt, B. Williams, Q. Wu, X. Yan, T. Zakian, and

R. Zhou, “The libra blockchain,” 2019. [En línea]. Disponible: https://developers.diem.com/papers/the-diem-blockchain/2020-05-26.pdf
[5] S. Blackshear, E. Cheng, D. L. Dill, V. Gao, B. Maurer, T. Nowacki, A. Pott, S. Qadeer, D. R. Rain, S. Sezer, T. Zakian, and R. Zhou, “Move: A language with programmable resources,” 2019. [En línea]. Disponible: https://developers.diem.com/papers/diem-move-a-language-with-programmableresources/2019-06-18.pdf
[6] D. Dill, W. Grieskamp, J. Park, S. Qadeer, M. Xu, and E. Zhong, “Fast and reliable formal verification of smart contracts with the move prover,” in Tools and Algorithms for the Construction and Analysis of Systems, D. Fisman and G. Rosu, Eds. Cham: Springer International Publishing, 2022, pp. 183–200.
[7] N. Popper. (2021) Lost passwords lock millionaires out of their bitcoin fortunes. [Online]. Disponible: https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html
[8] The Diem Team, “State synchronization and verification of committed information in a system with reconfigurations,” 2020. [Online]. Disponible: https://github.com/aptos-labs/aptoscore/blob/main/documentation/tech-papers/lbft-verification/lbft-verification.pdf
[9] G. Danezis, L. Kokoris-Kogias, A. Sonnino, and A. Spiegelman, “Narwhal and tusk: A dag-based mempool and efficient bft consensus,” in Proceedings of the Seventeenth European Conference on Computer Systems, ser. EuroSys ’22. New York, NY, USA: Association for Computing Machinery, 2022, p. 34–50. [Online]. Disponible: https://doi.org/10.1145/3492321.3519594
[10] The Diem Team, “Diembft v4: State machine replication in the diem blockchain,” 2021. [Online]. Disponible: https://developers.diem.com/papers/diem-consensus-state-machine-replication-in-the-diemblockchain/2021-08-17.pdf
[11] S. Cohen, R. Gelashvili, L. Kokoris-Kogias, Z. Li, D. Malkhi, A. Sonnino, and A. Spiegelman, “Be aware of your leaders,” CoRR, vol. abs/2110.00960, 2021. [Online]. Available: https://arxiv.org/abs/2110.00960
[12] A. Spiegelman, N. Giridharan, A. Sonnino, and L. Kokoris-Kogias, “Bullshark: Dag bft protocols made practical,” in Proceedings of the 20th Conference on Computer and Communications Security (CCS), ser. CCS ’22. Los Angeles, CA, USA: Association for Computing Machinery, 2022.
[13] R. Gelashvili, A. Spiegelman, Z. Xiang, G. Danezis, Z. Li, Y. Xia, R. Zhou, and D. Malkhi, “Block-stm: Scaling blockchain execution by turning ordering curse to a performance blessing,” 2022. [Online]. Disponible: https://arxiv.org/abs/2203.06871
[14] J. Lind, “The evolution of state sync: The path to 100k+ transactions per second with sub-second latency at aptos,” 2022. [Online]. Disponible: https://medium.com/aptoslabs/52e25a2c6f10