Radiant: un sistema de activos digitales electrónico peer-to-peer

11 Agosto, 2022

radiantblockchain.org

Traducido al español por Satolight

Resumen. La red Radiant es un sistema de activos digitales entre pares que permite el intercambio directo de valor sin pasar por un ente central. El protocolo original de Bitcoin[1] proporciona lo necesario para crear un sistema de dinero electrónico entre pares, pero carece de la capacidad para verificar los historiales de las transacciones y, por tanto, no puede utilizarse para validar activos digitales. Las firmas digitales y las restricciones de salida proporcionan parte de la solución, pero las principales ventajas se pierden si se sigue necesitando un tercero de confianza para validar los activos digitales. Al igual que Bitcoin, la red Radiant requiere una estructura mínima, y marca el tiempo de las transacciones en una cadena de prueba de trabajo basada en hash. Introducimos dos técnicas para validar los activos digitales: referencias únicas y un sistema de prueba de inducción de propósito general, que funcionan en tiempo y espacio constantes de O(1). Es posible componer las salidas de cualquier manera, sin comprometer el paralelismo inherente y las características de rendimiento de una arquitectura basada en la salida de transacciones no gastadas (UTXO). Por lo tanto, los usuarios pueden salir y volver a entrar en la red Radiant a voluntad y estar seguros de la integridad y autenticidad de sus activos digitales.

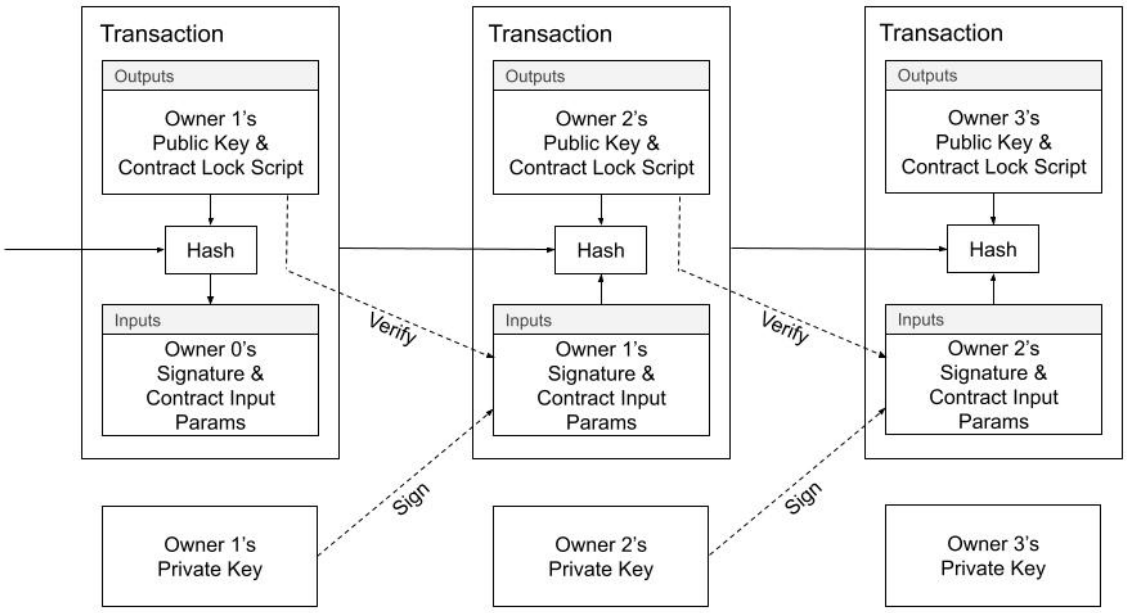
1. Introducción

Los blockchains comerciales, o tecnología de libro mayor digital (DLT), se suelen basar en emisores y custodios que actúan como partes de confianza para autenticar los activos digitales. Si bien estos sistemas funcionan lo suficientemente bien para las transacciones similares a los pagos electrónicos, siguen adoleciendo de las debilidades inherentes al modelo basado en la confianza para usos avanzados. Las cadenas de bloques basadas en la máquina virtual de Ethereum (EVM) [2] son muy flexibles para todo tipo de programas, pero las elevadas tarifas hacen que su uso para aplicaciones con micropagos sea poco práctico.

Lo que se necesita es un sistema de pago electrónico que se pueda utilizar para el sistema de gestión de activos digitales con tarifas bajas, alto rendimiento y capacidades de programación avanzadas. En este documento, proponemos una solución al problema del escalado en blockchain y al uso de contratos inteligentes, utilizando dos técnicas novedosas que proporcionan referencias únicas y un sistema de prueba de inducción general, que hacen posibles los programas turing completo [3] a través de los límites de las transacciones. El sistema propuesto es descentralizado, utiliza un mecanismo de consenso de prueba de trabajo como Bitcoin, pero con un rendimiento significativamente mayor, al tiempo que proporciona la misma flexibilidad que los blockchains basados en EVM, pero con tarifas muy bajas.

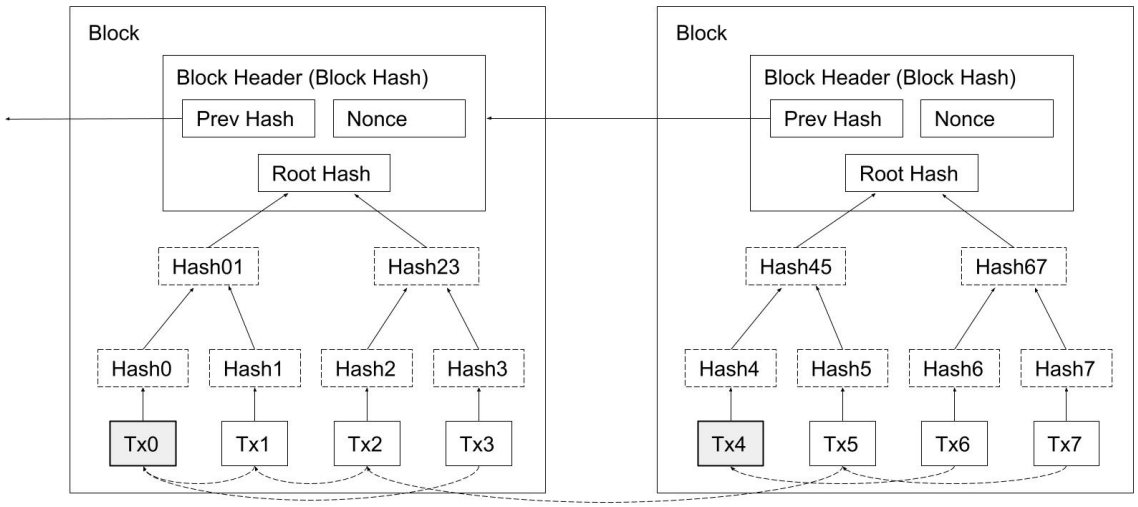
2. Transacciones

Al igual que Bitcoin, definimos una moneda electrónica como una cadena de firmas digitales. La diferencia de las transacciones en Radiant es que cada propietario transfiere la moneda al siguiente firmando digitalmente un hash de la transacción anterior, además de los parámetros de entrada necesarios para desbloquear la moneda. Una transacción también crea nuevas restricciones de bloqueo de salida, que pueden incluir la clave pública del siguiente propietario, entre otras reglas definidas por el usuario.



> **Diagrama 1.** Transacciones en Radiant.

Para verificar que no se ha producido un doble gasto, utilizamos un servidor de marcas de tiempo distribuido, que utiliza un sistema de prueba de trabajo basado en hash para organizar el historial canónico y determinar qué transacción llegó primero. Las transacciones se organizan en bloques. Por convención, la primera transacción, llamada "transacción coinbase", en un bloque es una transacción especial que inicia una nueva moneda propiedad del creador del bloque. Los bloques se encadenan y organizan las transacciones en un árbol de Merkle [4]. Todas las transacciones, a excepción de la primera, deben hacer referencia a una transacción anterior formando un gráfico acíclico dirigido (DAG) en el que todas las monedas acaban conectándose de nuevo a al menos una de las transacciones especiales del principio de un bloque.



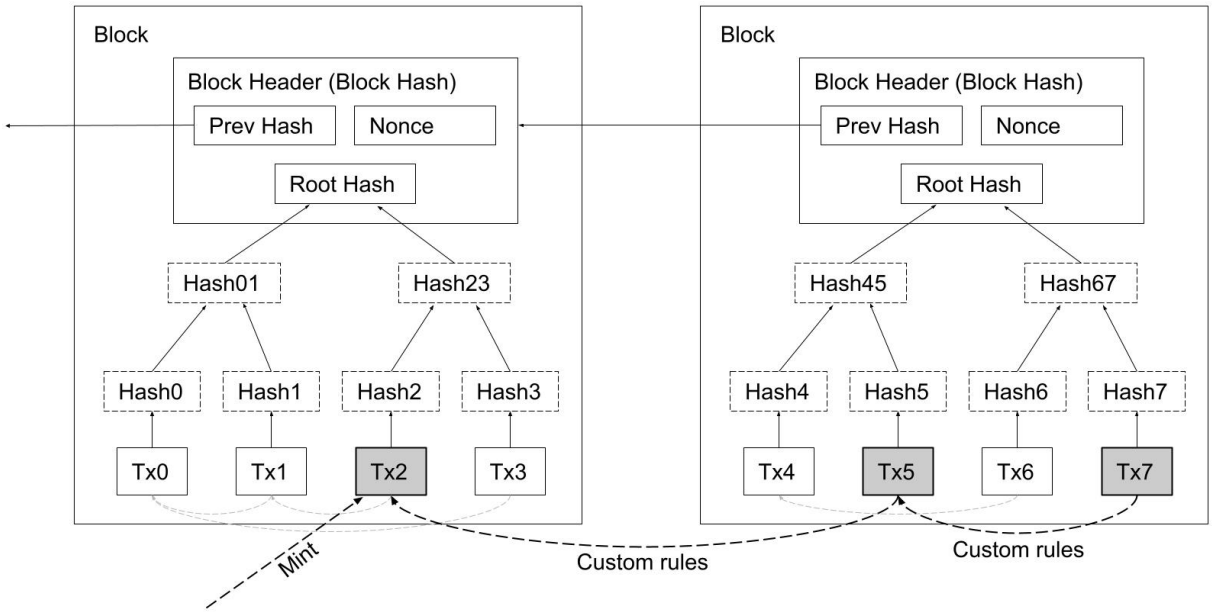
> **Diagrama 2.** Estructura de Bloques; las transacciones se organizan en un árbol de Merkle.

El problema de este diseño, en el contexto de los activos digitales, es que sólo hay un tipo de moneda, o activo digital, y ningún concepto de monedas definidas por el usuario (o tipos de activos digitales). El diseño funciona lo suficientemente bien para las transacciones similares a los pagos electrónicos en la unidad de cuenta nativa, sin embargo, no se presta inmediatamente a ser utilizado para otros tipos de monedas o activos digitales. Una solución común es introducir un servicio, como un indexador de transacciones, que supervise las transacciones en busca de secuencias de datos especiales que signifiquen la creación de un activo digital. El problema de esta solución es que depende de la empresa que gestiona el servicio, y la autenticidad de los activos digitales debe ser de confianza, al igual que cualquier otro servicio en la web.

Necesitamos una forma para que los usuarios indiquen la creación de tipos de moneda personalizados, pero que no dependan de un servicio de confianza para la presentación de datos.

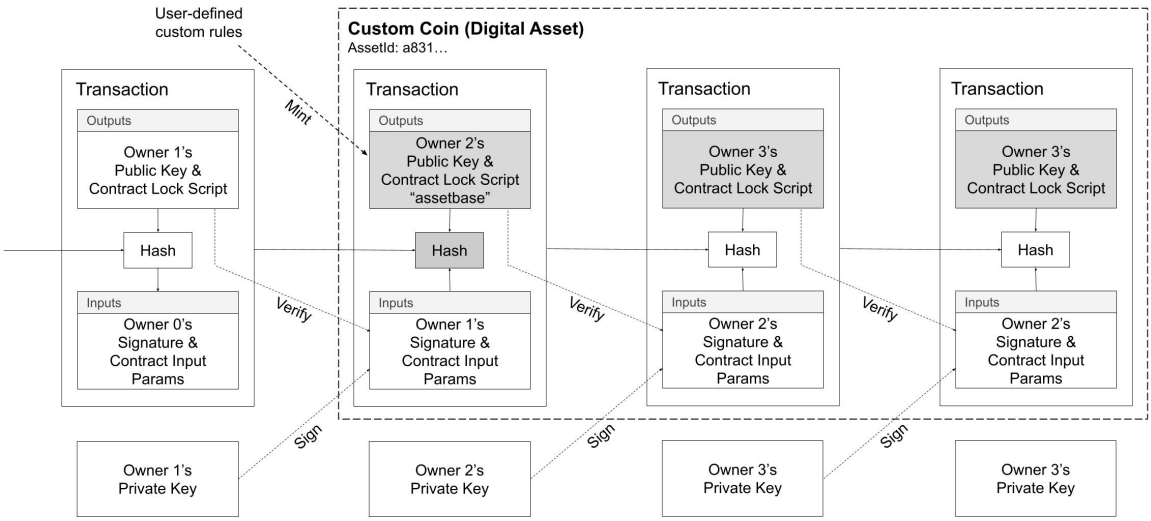
3. Activos Digitales

Definimos una moneda electrónica personalizada, o activo digital, como una cadena de firmas digitales. Un activo digital es un tipo de moneda definido por el usuario que utiliza un marcador de transacción especial, llamado transacción "assetbase", para crear o acuñar un activo digital. De forma similar a las transacciones de coinbase, que inyectan nuevas monedas en el sistema, la transacción de "assetbase" colorea o etiqueta la moneda electrónica con un identificador único de 36 bytes para toda su vida. La moneda electrónica personalizada se superpone al tipo de moneda base y funciona de manera similar. La transacción de assetbase puede aparecer en cualquier parte del bloque y puede aplicar cualquier regla y restricción personalizada que se decida por adelantado.



> **Diagrama 3.** Transacciones que representan tipos de moneda definidos por el usuario — o activos digitales.

Para lograrlo, necesitamos crear un identificador único estable y un mecanismo de transacción para rastrear la autenticidad del tipo de moneda (activo digital). Los usuarios del sistema necesitan tener pruebas de que los tipos de moneda personalizados no son falsificaciones y representan con exactitud los activos digitales.

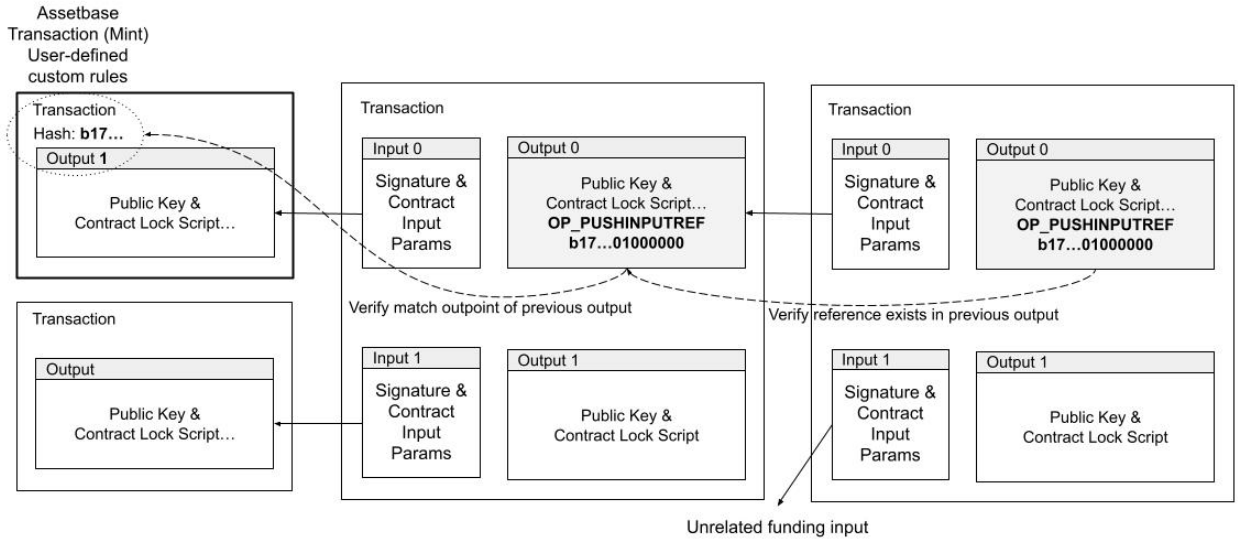


> **Diagrama 4.** Los tipos de moneda definidos por el usuario se definen a partir de una transacción especial de la Fábrica de Moneda. Se utiliza un identificador único para clasificar el tipo de moneda.

4. Identificadores Únicos

Para implementar un identificador único para un tipo de moneda, utilizamos una transacción marcadora especial, llamada "transacción de base de activos", que actúa como el inicio (ceca) de la cadena de firmas digitales. En lugar de requerir una nueva estructura de datos para el identificador único, reutilizamos el identificador de la transacción y el índice de salida, llamado "outpoint", como identificador único para el tipo de moneda. Se garantiza que los puntos de salida (36 bytes) son aleatorios y globalmente únicos.

Una instrucción de programación, llamada `OP_PUSHINPUTREF`, se utiliza para adjuntar una referencia a una salida. La instrucción acepta exactamente un parámetro de 36 bytes que debe coincidir con 1) el punto de salida de una de las salidas que se están gastando, o 2) el mismo valor de 36 bytes que ya aparece en un `OP_PUSHINPUTREF` previamente especificado en una de las salidas que se están gastando. La única manera de que un valor determinado aparezca en la salida de una transacción es que, a través de alguna transacción antecesora, coincida con el punto de salida de la transacción inicial de assetbase. Las transacciones que especifican un valor que no cumple ninguna de las dos condiciones no son válidas.

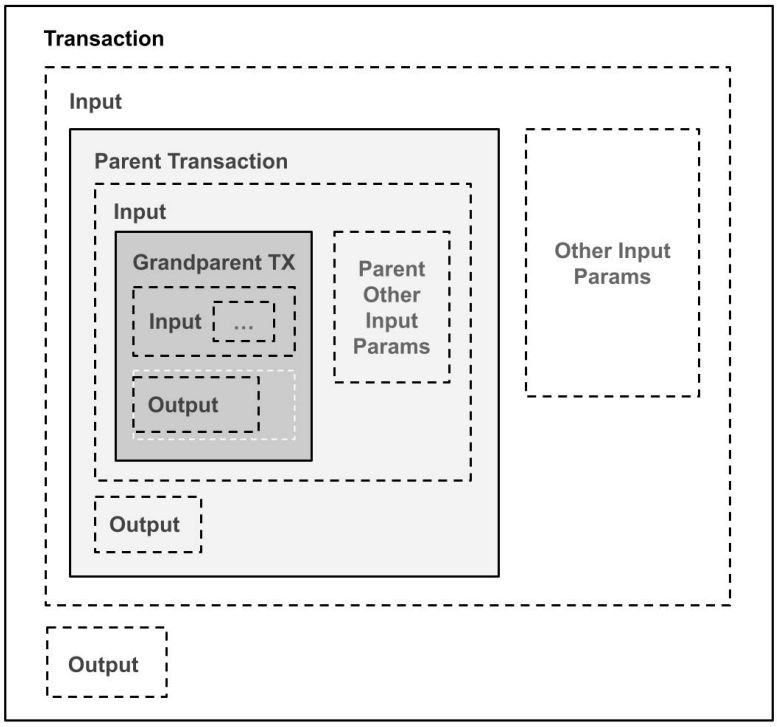


> **Diagrama 5.** Los identificadores únicos se inician al coincidir con un punto de salida de una de las salidas que se gastan, y luego se mantienen mientras al menos una de las salidas que se gastan contenga el mismo identificador único en el cuerpo del script.

Esta sencilla instrucción de programación proporciona un identificador único que puede utilizarse como referencia estable para crear reglas avanzadas. Por ejemplo, diferentes tipos de monedas, activos digitales, pueden ahora depender de otros tipos de monedas. Dado que todos los datos son locales a la transacción, a través de sus transacciones de entrada inmediatas, es fácil para los clientes y servicios validar la autenticidad de un activo digital en O(1) tiempo y espacio constantes, evitando la necesidad de un tercero de confianza.

5. Pruebas por inducción

Es posible crear identificadores únicos de forma alternativa y también proporcionar un mecanismo para pruebas de inducción matemática [5] utilizando un algoritmo de hash de transacciones modificado. Permitiendo que los scripts de entrada acepten que se gaste la transacción padre, las reglas pueden verificar que el padre, y su abuelo, se ajustan a las reglas requeridas. El problema obvio es que a medida que se incrusta cada copia completa de las transacciones padre, se produce una explosión de tamaño exponencial que impide el uso práctico de la técnica. Lo que se necesita es una forma de comprimir la transacción, de modo que se pueda utilizar una estructura de datos de tamaño fijo para derivar el hash de la transacción, en lugar de requerir el contenido completo de la transacción.



> **Diagrama 6.** Validación de la transacción completa de los padres, prueba de inducción matemática mediante la incorporación de las transacciones completas de los padres en las entradas, lo que resulta en un aumento exponencial del tamaño de la transacción.

Podemos lograrlo modificando el algoritmo de hash de transacciones utilizado en Bitcoin, en el que se calcula un doble hash de sha-256 a partir de la transacción serializada, en una nueva versión que primero resume el contenido de la transacción para derivar el hash. Introducimos la versión 3 del algoritmo de hash de transacciones, para distinguirlo del uso de la versión 1 y la versión 2 en Bitcoin. El proceso consiste en hacer un hash de cada campo, o componente de una transacción, a un hash intermedio, que puede ser utilizado como una entrada de tamaño fijo y así evitar el crecimiento exponencial del tamaño de la transacción.

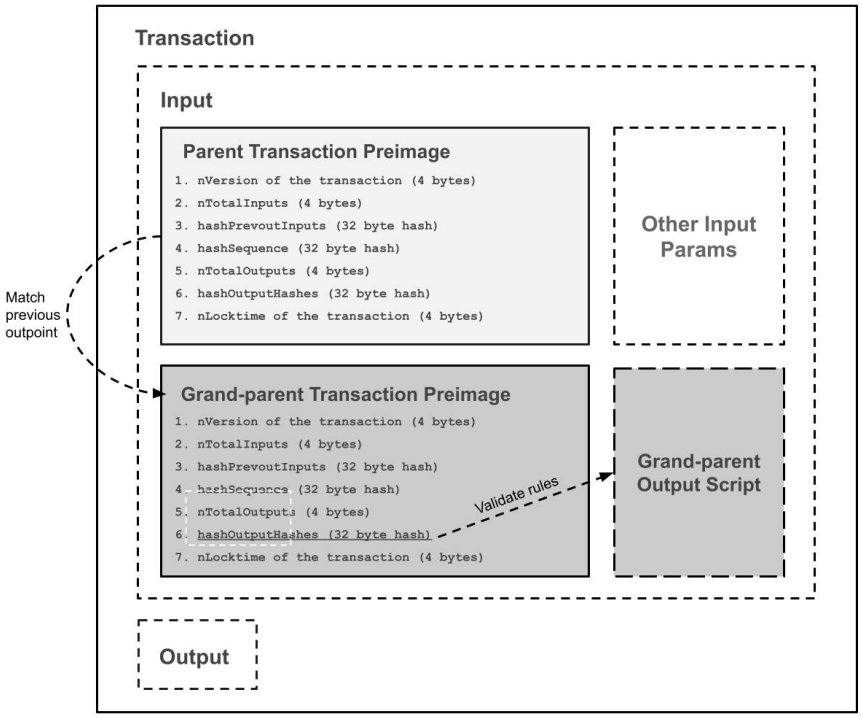
Utilizamos la siguiente estructura de datos de 112 bytes, en lugar de los bytes completos de la transacción serializada, que a su vez se somete a un doble hash sha-256 para obtener finalmente el hash de la transacción.

Campos de preimagen Hash de la transacción versión 3:

> 1. nVersion(=3) de la transacción (4 byte little endian)
> 2. nTotalInputs (4 byte little endian)
> 3. hashPrevoutInputs (32 byte hash)
> 4. hashSequence (32 byte hash)
> 5. nTotalOutputs (4 byte little endian)

> 6. hashOutputHashes (32 byte hash)
> 7. nLocktime de la transacción (4 byte little endian)

Al utilizar el algoritmo de hash de transacciones de la versión 3, podemos incrustar la transacción del padre y del abuelo en cada paso de una prueba de inducción matemática para evitar el aumento del tamaño de la transacción, y podemos aplicar cualquier regla necesaria.



> **Diagrama 7.** Validación comprimida de la transacción de los padres, prueba de inducción matemática mediante la incrustación de la estructura de datos de preimagen de la versión 3 del hash de la transacción de los padres y los abuelos para hacer cumplir reglas y restricciones arbitrarias.

6. Red

La topología de la red es un grafo casi completo, en el que cada Nodo Minero está conectado a cualquier otro Nodo Minero. Los pasos para hacer funcionar la red son los mismos que en Bitcoin, con algunas distinciones para los diferentes tipos de nodos: Nodos Mineros, Nodos Agentes y Nodos de Archivo. Los Nodos Mineros son los que publican activamente los bloques y mantienen el consenso con todos los demás nodos, los Nodos de Archivo sirven los datos históricos de los bloques, y los Nodos de Agente están diseñados para filtrar los bloques y seguir las transacciones de interés para las aplicaciones a las que sirven. Los Nodos de Archivo y los Nodos Agentes pueden operar en la misma red peer-to-peer y, sin embargo, no producen bloques. Los nodos no mineros, como los de archivo y los de agente, se denominan a veces "nodos oyentes" para distinguir su función en la red.

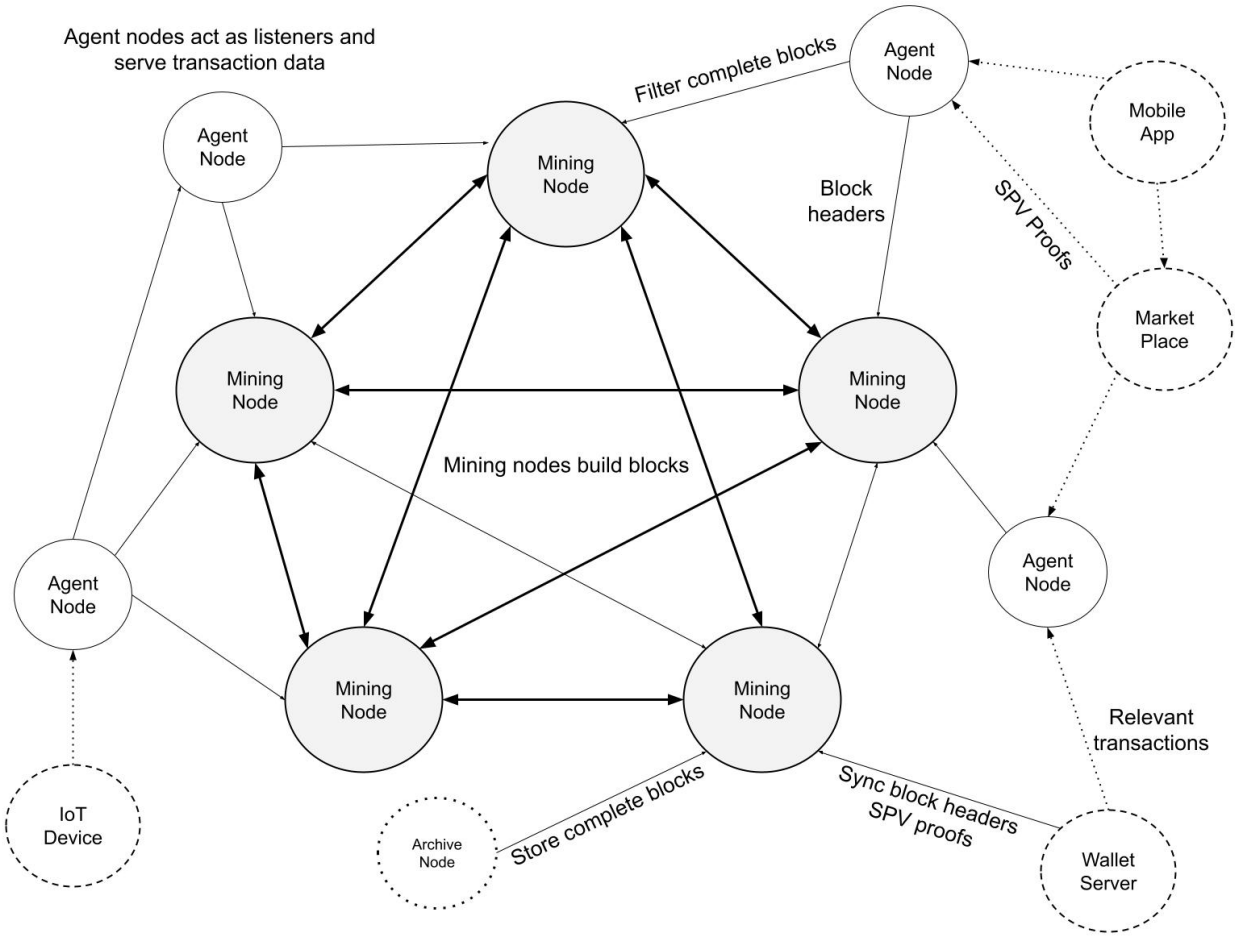


Diagrama 8. Los nodos de minería están bien conectados y construyen sobre los bloques de los demás. Los nodos de archivo almacenan bloques completos para fines de análisis histórico y de arranque. Los nodos de agente son nodos de escucha que filtran y almacenan transacciones para servir a los clientes.

Los nodos mineros están bien conectados en un gráfo casi completo entre otros nodos mineros. Su trabajo es construir sobre los bloques de los demás y mantener el consenso para los últimos cientos de bloques, y mantener el conjunto UTXO para la prevención del doble gasto.

Los Nodos Agente sólo necesitan almacenar un subconjunto de transacciones, por ejemplo, un tipo de moneda o activo digital específico. Incluso con bloques grandes, un nodo agente puede filtrar rápidamente las transacciones por referencias o secuencias de bytes específicas, y luego almacenar esas transacciones para servirlas a través de una interfaz de programador de aplicaciones. Entre los agentes que cooperan, se puede anunciar públicamente el hash de la raíz del árbol de Merkle para las transacciones de cada bloque que coincidan con un patrón predeterminado para señalar a otros Agentes y consumidores con transacciones que ha procesado ese Agente

Los nodos de archivo se utilizan para crear copias de seguridad de bloques enteros para diversas aplicaciones, como el almacenamiento de datos, el análisis y el aprendizaje automático. Como los nodos de archivo no participan directamente en la minería, no tienen los mismos requisitos de rendimiento y ancho de banda en tiempo real que los nodos de minería o de agente.

7. Cálculos

Consideramos el escenario en el que la red Radiant sigue creciendo y lo que supone para los requisitos de procesamiento de los nodos de minería, archivo y agente. A modo de comparación, en el momento de escribir este artículo, hay unos 83 millones de salidas de transacciones sin gastar para el blockchain de Bitcoin, lo que supone un total de unos 6 GB de datos necesarios para evitar el doble gasto. Sólo es necesario que los Nodos Mineros conserven los cientos de bloques más recientes, estando los bloques más antiguos disponibles en los Nodos de Archivo. Para los Nodos Agentes, es necesario mantener la partición relevante de los resultados de las transacciones no gastadas que pertenecen a las aplicaciones que sirven, el escalado es una función del ancho de banda y no de los requisitos de almacenamiento.

Para nuestros propósitos, suponemos que habrá bloques de 3 GB de tamaño cada 5 minutos que se marcarán con el tiempo y se distribuirán por la red, o unas 20.000 transacciones por segundo con un tamaño medio de transacción de 500 bytes, o unos 6.000.000 de transacciones por bloque. Demostramos que para cada tipo de nodo, la red es capaz de escalar adecuadamente para satisfacer la demanda global. Esto equivale a una transacción cada 5 días para cada uno de los 8.000 millones de habitantes del planeta.

Nodos mineros

Los nodos mineros son el único tipo de nodo que construye sobre los bloques de los demás. Para mantener el consenso, basta con sincronizar el conjunto de transacciones no gastadas (UTXO) y mantener sólo unos cien bloques. En el momento de escribir este artículo, las unidades de estado sólido de alto rendimiento son capaces de alcanzar más de 120.000 IOPS, con un coste de unos 500 dólares por 280 GB, y por lo tanto pueden manejar unas 20.000 transacciones por segundo (suponiendo que cada transacción tiene 2 entradas y 2 salidas). Hay 2 lecturas para las entradas, 2 actualizaciones para las entradas y 2 escrituras para la nueva salida: 120.000 / 6 = 20.000 transacciones/segundo.

Nodos de archivo

Los Nodos de Archivo proporcionan datos históricos en bloque y son adecuados para aplicaciones de aprendizaje automático, análisis y almacenamiento de datos. Los nodos de archivo pueden complementar el arranque de los nodos de minería y ejecutar comprobaciones periódicas de consistencia en el conjunto UTXO. En el momento de escribir estas líneas, se pueden adquirir discos duros básicos de 18 TB por unos 350 dólares. Suponiendo 3 GB de datos cada 5 minutos, se necesitan 732 GB de almacenamiento de datos al día, o unos 22 TB al mes. El coste de hardware para un año es de 15 discos duros, con 18 TB de capacidad, por un coste incremental anual de 5.000 USD.

Nodos Agente

Los Nodos Agentes son los que escalan más fácilmente entre los tipos de nodos porque sólo procesan los tipos de transacciones relevantes para las aplicaciones a las que sirven. Como resultado, los Nodos Agentes pueden ser desde un servidor web hasta un dispositivo IoT ligero con capacidades limitadas de procesamiento y almacenamiento, y aún así mantener la estabilidad con bloques de 3 GB, o 20.000 transacciones por segundo. Por ejemplo, una empresa puede querer hacer un seguimiento del uso de sus puntos de fidelidad, creados como un activo digital, y por lo tanto sólo necesita seleccionar un pequeño subconjunto de actualizaciones de transacciones de cada bloque que coincidan con el identificador único para ese tipo de moneda.

En el momento de escribir este artículo, un dispositivo informático comercial, Raspberry Pi 4, se vende por unos 275 dólares y tiene un procesador de cuatro núcleos a 1,5 GHZ y 4 GB de RAM, que puede utilizarse para filtrar rápidamente y descartar las transacciones irrelevantes, a un ritmo de 5.000 transacciones por núcleo. Por supuesto, esto es sólo un ejemplo de lo razonable que es procesar grandes bloques, en una aplicación web típica puede haber muchos más núcleos disponibles.

La velocidad media del ancho de banda de los 25 principales países supera los 100 MBPS, es decir, unos 10 MB/segundo de descarga, y muchos proveedores de servicios de Internet ofrecen descargas ilimitadas. Los requisitos de ancho de banda para bloques de 3 GB cada 5 minutos son de unos 10 MB/segundo para un total de 22 TB al mes. También se pueden crear jerarquías de Nodos Agentes para filtrar los requisitos totales de ancho de banda para los Nodos Agentes con menor capacidad de ancho de banda.

8. Conclusión

Hemos propuesto un sistema de gestión de activos digitales sin depender de la confianza. Empezamos con los bloques de construcción básicos de monedas hechas de firmas digitales, lo que proporciona un fuerte control de la propiedad. A partir de las reglas e incentivos necesarios, introducimos dos métodos novedosos para autenticar y rastrear los activos digitales en tiempo y espacio constantes de O(1). Ambos métodos proporcionan de forma independiente un sistema general de pruebas de inducción matemática que puede codificar cualquier configuración posible de activos digitales. El sistema es Turing completo dentro y a través de los límites de las transacciones, sin necesidad de capas secundarias. Radiant tiene un diseño innovador que proporciona las ventajas de rendimiento y paralelismo de una blockchain de salida de transacciones no gastadas (UTXO), pero con la capacidad de crear contratos inteligentes de las blockchains basadas en cuentas y basadas en la máquina virtual de Ethereum (EVM).

Referencias

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" URL https://bitcoin.org/bitcoin.pdf, 2009.

[2] Vitalik Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." URL https://ethereum.org/en/whitepaper/, 2014.

[3] Wikipedia contributors. "Turing completeness." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, URL https://en.wikipedia.org/wiki/Turing_completeness, 21 Jul. 2022

[4] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[5] Britannica, T. Editors of Encyclopaedia. "mathematical induction." Encyclopedia Britannica, URL https://www.britannica.com/science/mathematical-induction, 2018