1. Red

La red Bitcoin funciona mediante un conjunto de reglas codificadas y acciones de los nodos participantes, sin requerir una autoridad central. Cada nodo en la red realiza 5 funciones críticas:

1. **Difusión de Transacciones:** los nodos reciben transacciones de los usuarios y las propagan a través de la red. Esto asegura que las transacciones lleguen a los mineros, quienes las incluirán en los bloques.
2. **Formación de Bloques:** los mineros recolectan transacciones no confirmadas, validándolas según las reglas de consenso de la red. Luego, intentan crear un nuevo bloque resolviendo un desafío criptográfico (PoW).
3. **Validación de Bloques y Transacciones:** cuando un minero resuelve el desafío, el nuevo bloque es enviado a la red. Cada nodo independientemente verifica la validez del bloque y las transacciones contenidas. Los bloques válidos se añaden a la cadena existente.
4. **Consolidación del Consenso:** la cadena más larga y con mayor trabajo acumulado se acepta como la versión correcta del libro de contabilidad. Los nodos continúan construyendo sobre la cadena más larga, asegurando la coherencia y resistencia del sistema ante intentos de alteración.
5. **Mecanismo de Resolución de Conflictos**: si dos mineros producen bloques casi simultáneamente, la red puede bifurcarse temporalmente. La resolución ocurre naturalmente cuando los siguientes bloques se añaden a una de las bifurcaciones, haciéndola más larga. Los nodos entonces reorganizan sus cadenas para alinearse con la rama más larga.

Además de estas funciones básicas descritas por Nakamoto, la red Bitcoin ha evolucionado para incorporar características adicionales y optimizaciones:

Protocolos de Seguridad Mejorados: implementación de mejoras en la seguridad de la comunicación entre nodos para prevenir ataques de intermediarios y asegurar la privacidad de los usuarios.

Optimización de la Propagación de Bloques: técnicas como el "compact block relay" han sido introducidas para acelerar la difusión de bloques nuevos a través de la red, minimizando la latencia y el riesgo de bifurcaciones accidentales.

Servicios de Nodo Ligero: permiten a usuarios con recursos limitados participar en la red sin necesidad de descargar la blockchain completa, utilizando el método de verificación de pago simplificado (SPV) para confirmar transacciones.

Ajustes en el Mecanismo de Dificultad: la red ajusta dinámicamente la dificultad del PoW para mantener el tiempo promedio de generación de bloques, adaptándose a cambios significativos en el poder computacional total de la red.

2. Privacidad

Otra característica esencial del Blockchain es su transparencia, y se va a analizar cómo se maneja la privacidad de los usuarios.

La imagen contrasta dos modelos de privacidad. En el modelo tradicional, las identidades y las transacciones pasan por un tercero de confianza antes de llegar a la contraparte y, finalmente, al conocimiento público. En el nuevo modelo de privacidad, representado por la tecnología blockchain, las identidades y transacciones van directamente al dominio público sin intermediarios de confianza.

La privacidad en la blockchain, especialmente en Bitcoin, es un tema de doble filo. Aunque todas las transacciones son públicas y cualquiera puede ver los flujos de fondos entre direcciones, la identidad real detrás de cada dirección se mantiene en el anonimato, a menos que se revele a través de otros medios. Esto significa que mientras tus transacciones son transparentes, tu identidad no lo es necesariamente. Sin embargo, es importante ser consciente de que esta privacidad es relativa. Técnicas avanzadas de análisis de blockchain pueden, en algunos casos, vincular direcciones a identidades reales, especialmente cuando se interactúa con servicios que requieren verificación de identidad. Así, aunque la blockchain ofrece un nivel de privacidad más alto en comparación con los sistemas financieros tradicionales, la verdadera anonimidad requiere precaución y, a veces, el uso de herramientas adicionales de privacidad.

3. Seguridad

En este punto analizar los cálculos de Satoshi Nakamoto en el punto 11 de su Whitepaper. Véase como la Blockchain es prácticamente inmutable gracias a su sistema de PoW.

Modelo de la Caminata Aleatoria Binomial

El modelo utilizado para calcular la probabilidad de éxito de un atacante es la caminata aleatoria binomial. Este modelo considera dos posibles resultados en cada paso: o bien el atacante añade un nuevo bloque a su cadena alternativa, o bien la cadena honesta crece añadiendo un nuevo bloque. La probabilidad de que el atacante logre añadir un bloque se

denota como 'q', y la probabilidad de que la cadena honesta añada un bloque se denota como 'p'.

Cálculo de la Probabilidad de Éxito de un Ataque

La probabilidad de que un atacante pueda alcanzar o superar a la cadena honesta después de estar 'z' bloques detrás se puede calcular utilizando la fórmula de la "ruina del jugador", adaptada a este contexto. Si se designa 'qz' como la probabilidad de que el atacante, comenzando 'z' bloques detrás, eventualmente alcance a la cadena honesta, esta probabilidad se calcula como:

Si 'q' (la probabilidad de que el atacante mine un bloque) es menor o igual a 'p' (la probabilidad de que la cadena honesta mine un bloque), entonces:

$$q_z = (q/p)^z$$

Esto significa que si el atacante tiene menos poder computacional que la cadena honesta ('q' es menor que 'p'), la probabilidad de que alcance a la cadena honesta disminuye exponencialmente con cada bloque adicional añadido a la cadena honesta ('z').

Ejemplo de Cálculo

Suponga que un atacante controla el 10% del poder computacional de la red, lo que significa que 'q = 0.1' y la cadena honesta controla el 90%, por lo tanto, 'p = 0.9'. Si el atacante intenta modificar una transacción que está confirmada por 6 bloques (z = 6), la probabilidad de que tenga éxito sería:

Esto significa que la probabilidad de que el atacante tenga éxito es de aproximadamente 0.000188%, una probabilidad extremadamente baja. Este ejemplo ilustra cómo el diseño de Bitcoin asegura que, a medida que se añaden más confirmaciones (bloques adicionales después de una transacción), el riesgo de un ataque exitoso disminuye exponencialmente, reforzando la seguridad de las transacciones conforme se integran más bloques a la cadena.

Ataques y Doble Gasto

Un ataque en el contexto de Bitcoin implica que un actor malintencionado intente crear un fork en la cadena de bloques desde un bloque más antiguo. Esto puede conducir al problema de doble gasto, donde un usuario intenta gastar la misma cantidad de bitcoin dos veces. Por ejemplo, si un atacante logra crear una cadena alternativa más larga que la cadena honesta y realiza una transacción en la cadena alternativa en la que envía bitcoins a una dirección, y luego revierte esa transacción al hacer que la cadena alternativa se convierta en la cadena principal, puede intentar gastar los mismos bitcoins nuevamente en la cadena principal, lo que resultaría en un doble gasto.

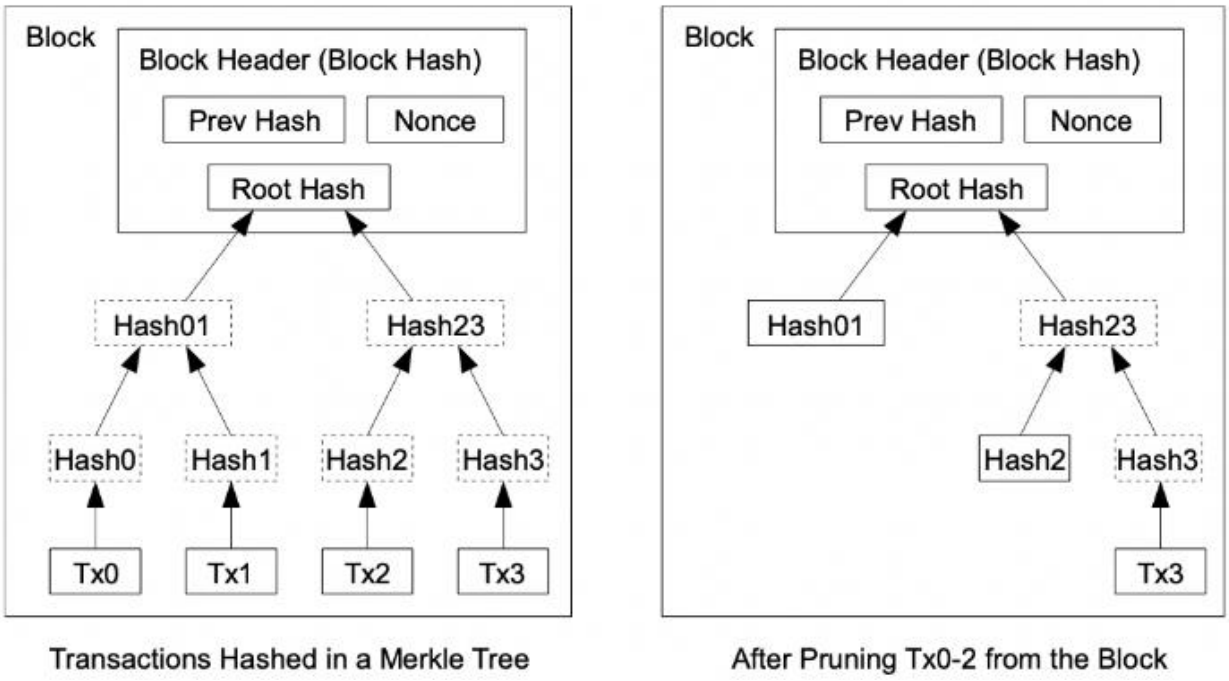
Importancia de las Cadenas Alternativas

Las cadenas alternativas son cruciales en el contexto de los ataques en la red Bitcoin. Cuando un atacante intenta modificar la cadena de bloques, crea una cadena alternativa que diverge de la cadena principal en un punto específico. La red Bitcoin está diseñada para que los nodos sigan la cadena más larga y trabajen en la construcción de ella. Por lo tanto, si un atacante quiere que su cadena alternativa se convierta en la cadena principal, tendría que superar la dificultad de encontrar bloques más rápido que el resto de la red combinada. Como hemos visto en el cálculo de la probabilidad de éxito de un ataque, este escenario es extremadamente improbable si el atacante controla menos poder computacional que la red honesta.

4. Eficiencia del Almacenamiento

Además, se pensó en el tamaño de los datos, por eso Nakamoto tenía una respuesta en su propuesta.

La idea central es que, una vez confirmada una transacción por bloques posteriores, no es necesario conservar todos los detalles de las transacciones antiguas, especialmente las que gastaron todas sus salidas.



La imagen compara dos estados de un bloque en la blockchain. A la izquierda, muestra el bloque con un conjunto completo de transacciones (Tx0 a Tx3) estructuradas en un árbol de Merkle, donde cada transacción se resume en un hash individual que contribuye al hash raíz. A la derecha, ilustra el bloque después de la poda de las transacciones Tx0 a Tx2, manteniendo solo Tx3, pero aún verificable por el hash raíz en el encabezado del bloque.

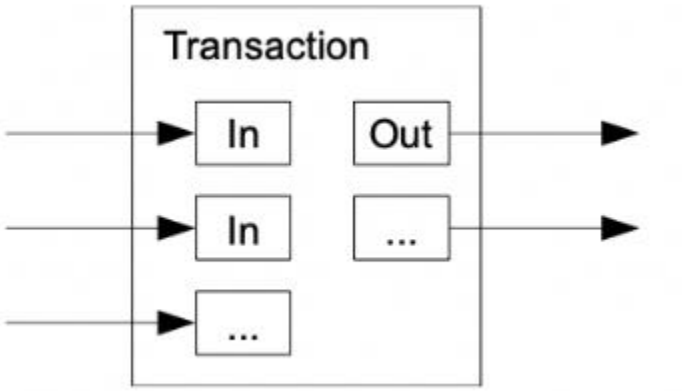
Para lograr esto, Nakamoto introduce el concepto de poda de transacciones, utilizando estructuras de datos de árboles de Merkle. Cada bloque no almacena la lista completa de transacciones directamente; en su lugar, almacena un árbol de Merkle que resume las transacciones incluidas en el bloque. La raíz de este árbol (Merkle Root) es lo que se incluye en el encabezado del bloque. Este método permite que nodos y usuarios verifiquen la existencia de una transacción específica dentro de un bloque sin necesidad de descargar todas las transacciones.

A medida que las transacciones se agrupan y se resumen en este árbol, se puede eliminar información redundante o innecesaria de las transacciones completamente gastadas, liberando espacio en el disco. Sin embargo, es crucial mantener la raíz del árbol de Merkle en el encabezado del bloque para seguir permitiendo la verificación de la existencia y validez de las transacciones.

5. Transacciones Compartidas

Una sola transacción en Bitcoin puede combinar fondos de varias entradas, saldos previamente recibidos en direcciones de Bitcoin controladas por el remitente. Esto permite al usuario agrupar diferentes montos de Bitcoin que ha recibido a lo largo del tiempo en una sola transacción. Del mismo modo, una transacción puede dividir su valor entre varias salidas, permitiendo al remitente enviar fondos a varios destinatarios en una sola operación. Este diseño ofrece flexibilidad para realizar pagos de manera eficiente, ajustándose a las necesidades específicas de cada usuario.

Además, este sistema de entradas y salidas facilita la devolución de cambio a la persona que realiza el pago. Si el valor total de las entradas excede el monto que se desea enviar, se puede generar una salida adicional que redirija los fondos excedentes de vuelta a una dirección controlada por el remitente, similar al cambio que se recibe al pagar con efectivo.



La imagen ilustra la estructura de una transacción de Bitcoin, mostrando entradas (In) que combinan fondos previos y salidas (Out) que distribuyen esos fondos. Esto refleja la capacidad de una transacción para consolidar varios montos y distribuirlos a múltiples destinatarios, optimizando así el proceso de pago y permitiendo la devolución de cambio al remitente.

6. Incentivos

Ahora bien, surgen las siguientes preguntas:

¿Por qué habría más nodos honestos? ¿Que los lleva a gastar su tiempo y dinero?

El sistema de incentivos de Bitcoin es fundamental en el funcionamiento y seguridad de la red. Este sistema se basa en dos componentes principales: las recompensas por bloque y las tarifas de transacción.

Recompensas por Bloque

Los mineros, al resolver complejos problemas criptográficos a través del proceso conocido como prueba de trabajo (PoW), contribuyen a la creación de nuevos bloques y, por ende, al crecimiento de la cadena de bloques. Por este esfuerzo, son recompensados con bitcoins recién acuñados y con las tarifas de las transacciones incluidas en dicho bloque. Originalmente, esta recompensa era de 50 bitcoins por cada bloque minado, pero se ha diseñado para que se reduzca a la mitad aproximadamente cada cuatro años en un proceso llamado "halving".

El halving de Bitcoin es un evento programado que tiene lugar cada cuatro años cuando la recompensa por extraer un bloque de Bitcoin se reduce a la mitad. Esto significa que la oferta de Bitcoin está disminuyendo, lo que podría provocar un aumento de la demanda y, por tanto, un aumento del precio.

Este diseño garantiza una emisión controlada de bitcoins, manteniendo la oferta limitada hasta alcanzar el máximo estipulado de 21 millones de bitcoins.

Tarifas de Transacción

Adicionalmente a la recompensa por bloque, los mineros reciben las tarifas asociadas a las transacciones que deciden incluir en su bloque. Estas tarifas las ofrecen los usuarios como incentivo para procesar sus transacciones con rapidez, especialmente en momentos de alta demanda en la red. Con el tiempo, y a medida que la recompensa por bloque se reduce, se anticipa que estas tarifas representarán una porción creciente de los ingresos para los mineros.

Este mecanismo de incentivos asegura la participación de los mineros, quienes invierten recursos computacionales significativos, garantizando así la seguridad y la fiabilidad de la red. La competencia entre mineros por resolver el problema de PoW y obtener las recompensas sirve como una barrera eficaz contra ataques maliciosos, ya que dominar la red requeriría un poder computacional prohibitivamente costoso.