1. Fundamentos

Autor del texto: Jorge Bravo Mayo

En la última década, la tecnología blockchain ha emergido como una de las innovaciones más disruptivas, redefiniendo la forma en que se concibe las transacciones digitales y la seguridad de los datos.

La historia de la blockchain se remonta a esfuerzos previos por crear sistemas de pago electrónicos peer-to-peer, como lo demuestra el trabajo pionero de Satoshi Nakamoto con Bitcoin. Nakamoto introdujo una solución al problema del doble gasto sin la necesidad de una autoridad central, mediante una red distribuida que valida transacciones mediante un consenso computacional.

Este sistema de prueba de trabajo no solo garantiza la integridad y la secuencia de las transacciones, sino que también sienta las bases para una nueva forma de confianza digital. Como bien reflejo en su whitepaper de bitcoin: "Lo que se necesita es un sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza, que permita a dos partes interesadas realizar transacciones directamente entre sí sin la necesidad de un tercero de confianza"

A su vez, la introducción del concepto de contratos inteligentes y la creación de plataformas como Ethereum han ampliado las posibilidades de la blockchain más allá de las monedas digitales, facilitando el desarrollo de aplicaciones descentralizadas que pueden automatizar, verificar y ejecutar acuerdos complejos sin intermediarios.

El contexto es crucial para entender el estado actual y el potencial de la tecnología blockchain. Desde su conceptualización como un sistema de efectivo electrónico entre pares hasta su evolución como una infraestructura para aplicaciones descentralizadas, la blockchain ha demostrado ser una herramienta poderosa para la innovación en campos tan variados como las finanzas, la salud, el gobierno y más allá.

2. Fundamentos y Criptomonedas

Antes de sumergirnos en el análisis de la tecnología blockchain y su funcionamiento, es importante destacar que las tecnologías disruptivas a menudo emergen de forma sutil y pueden pasar inadvertidas en sus inicios. Es solo con el tiempo que su verdadero potencial se hace evidente y empiezan a redefinir el panorama existente. Se comparte un pequeño texto de Marc Andreessen, un pionero de la Web2, en una entrevista que tuvo con el Washington Post en 2014.

Andreesen fue preguntado lo siguiente:

“Para [los periodistas], el gran desafío ha sido explicar qué es Bitcoin a la gente. Y creo que siempre lo hemos explicado como una moneda, pero ahora que la gente sabe sobre él en términos de una moneda, ¿eso hace eso que no comprendan el pleno potencial de Bitcoin?”

A lo que respondió:

“Tengo muchos amigos que son programadores. Los programadores siempre han pensado, "Esos tipos [de Bitcoin] están locos". Y casi siempre, se sientan, leen el artículo, leen el código — les lleva un par de semanas — y salen con la opinión contraria. "Dios mío, eso es! Es el gran avance. Esto es lo que estábamos esperando. Ha resuelto todos los problemas. Quien sea que lo ha escrito debería recibir el Premio Nobel — es un genio. ¡Eso es! Esta es la red de confianza distribuida que Internet siempre necesitó y nunca tuvo".

Entonces, uno de los desafíos es tomar a personas que no son programadores profesionales o matemáticos y esperar que lo entiendan desde cero. Y es desalentador. Y entonces se le adjunta una palabra, como "moneda" o como quieras llamarlo, y luego la gente piensa que es algo que no es. Y tienes una idea de esto, pero es un concepto mucho más profundo que la moneda. Es la idea de la confianza distribuida.”

3. Criptomonedas y Blockchain: Fundamentos para un Futuro Digital

En esta sección, titulada "Criptomonedas y Blockchain: Fundamentos para un Futuro Digital", se abordan los conceptos esenciales y la arquitectura que componen el marco de la tecnología blockchain. También explorar desde la estructura básica de los bloques hasta el intrincado proceso de creación y validación de transacciones. También se discutirán los diversos tipos de blockchain, las transacciones y cómo funcionan, así como los diferentes protocolos de consenso como Proof of Work (PoW). Se profundizará en la importancia de la red para la blockchain, los aspectos de privacidad y seguridad, la eficiencia en el almacenamiento de datos, y el papel que juegan las transacciones compartidas. Por último, se considera cómo los sistemas de incentivos impulsan la participación y la integridad de la red.

3. Criptomonedas y Blockchain: Fundamentos para un Futuro Digital

3.1. Bitcoin Script

Bitcoin Script es un lenguaje diseñado específicamente para el procesamiento de transacciones en la red de Bitcoin. Este lenguaje es simple y se ejecuta siguiendo un modelo de pila, que opera bajo el principio de LIFO, donde el último elemento en entrar es el primero en salir. Las operaciones se realizan secuencialmente.

El lenguaje fue ideado con el objetivo de establecer condiciones flexibles y sencillas para la ejecución de transacciones. Algunas operaciones, como la multiplicación, fueron omitidas

intencionadamente por Nakamoto para preservar la simplicidad del lenguaje y la red. Por ello, Bitcoin Script juega un papel esencial al determinar la validez de una transacción, en función de si cumple con los criterios programados.

La programabilidad proporcionada por Bitcoin Script es fundamental para la flexibilidad y las capacidades únicas de Bitcoin en comparación con el dinero tradicional. Sin embargo, es un lenguaje no Turing completo, es decir, su capacidad para resolver problemas es intencionadamente limitada para evitar bucles infinitos y posibles abusos por parte de actores malintencionados. Los códigos de operación en Bitcoin (OP CODES) son los que permiten realizar las diversas operaciones necesarias para comunicar instrucciones a la red.

Bitcoin Script, en esencia, es una secuencia de instrucciones codificadas que acompaña cada transacción en la red de Bitcoin. Estas instrucciones detallan cómo los participantes pueden acceder y utilizar los fondos de Bitcoin.

Dentro de este marco, existen dos componentes cruciales: scriptSig y scriptPubKey. El scriptSig funciona como un mecanismo de desbloqueo, requiriendo tanto una clave pública como una firma digital. La necesidad de verificar firmas surgió para solucionar problemas detectados en las versiones tempranas del software de Bitcoin, con el fin de que sólo las transacciones verificadas según reglas específicas sean aceptadas.

Por otro lado, el scriptPubKey es el script de bloqueo, que alberga un hash de la clave pública, también conocida como la dirección de Bitcoin. Cuando se requieren multifirmas para autorizar una transacción, el script se torna más complejo, implicando la aprobación de múltiples participantes. Este script almacena la lógica programática para ejecutar las transacciones en la red de Bitcoin.

Véase un ejemplo del posible contenido de un bitcoin script

SECCIONES	CONTENIDO DEL BITCOIN SCRIPT
scriptPubKey	OP_DUP OP_HASH160 340cfcffe029e6935f4e4e5839a2ff5f29c7a571 OP_EQUALVERIFY OP_CHECKSIG
scriptSig (Signature)	30440220694ff325724a4f4b0f3f0c36bf8e94cac58ad7c9b4d5bd8c7286c0da623f0b 2c02206ae94680a8f31f30cd846da258e919c94afe2dd629b4f4ce11bbe8165ff99a5f01
scriptSig (Pub Key)	04fc60372d27b067ca306ba812ced9c8cd69296b83a40b9b57c593258c1b9e0 ee1c0c621ca558b878395f9645a4b67a96e51843e9c060d43a3833fdd29a91f4f31

La sección `scriptPubKey` contiene operaciones para duplicar y hashear una dirección, seguida de comandos de script que verifican la firma y el hash. La sección `scriptSig (Signature)` muestra una firma digital larga, que es una serie de números y letras en hexadecimal. Finalmente, `scriptSig (Pub Key)` presenta una clave pública, también en formato hexadecimal. Estos elementos se combinan para autorizar una transacción en Bitcoin.

En la ilustración que enseñamos arriba, los comandos OP_DUP, OP_HASH160, OP_EQUALVERIFY y OP_CHECKSIG son códigos de operación en el script de Bitcoin que realizan funciones específicas durante la validación de transacciones. OP_DUP copia el último ítem en la pila de memoria. OP_HASH160 aplica dos rondas de algoritmos criptográficos a los datos: SHA-256 seguido de RIPEMD-160. OP_EQUALVERIFY compara dos elementos para confirmar que son iguales y OP_CHECKSIG comprueba que la firma adjunta corresponde correctamente al hash de la transacción junto con la clave pública dada. Estos pasos colectivamente aseguran que los bitcoins solo puedan ser gastados por su legítimo propietario.

3. Criptomonedas y Blockchain: Fundamentos para un Futuro Digital

3.2. Bitcoin Improvement Proposal (BIP)

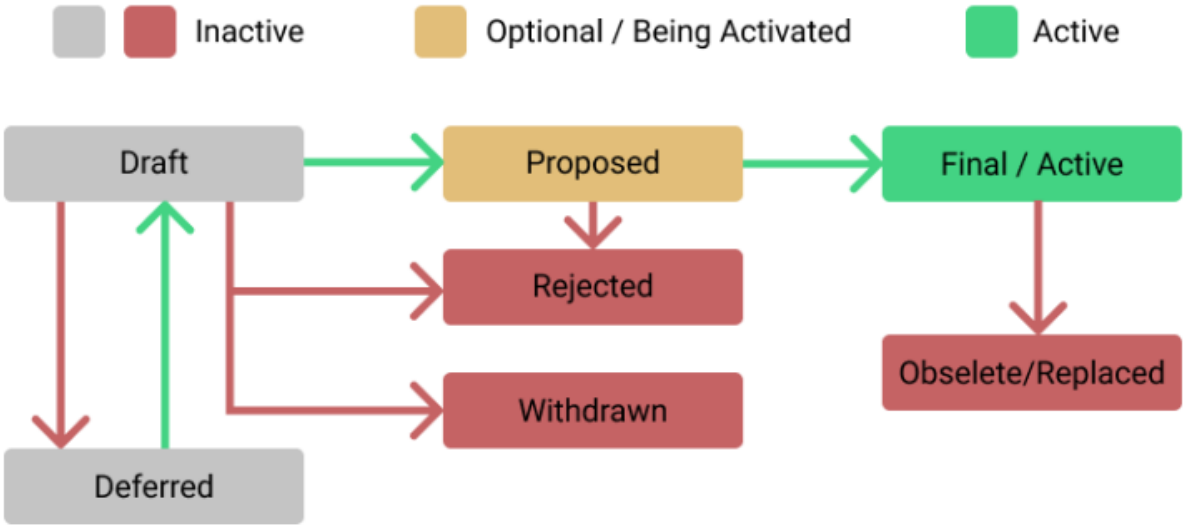
Las Propuestas de Mejora de Bitcoin, o BIPs por sus siglas en inglés, son documentos diseñados para sugerir mejoras y optimizaciones dentro del ecosistema de Bitcoin. Tanto en términos técnicos como comunitarios, estas propuestas se presentan con argumentos claros para su posible adopción. La comunidad de Bitcoin, a través de un proceso de discusión y consenso, decide si una BIP será adoptada o no.

Los BIPs se clasifican en normativos, informativos y de procesos, dependiendo de su propósito y alcance dentro de la red de Bitcoin. Los normativos buscan cambios que afecten a la mayoría de implementaciones, los informativos abordan problemas de diseño con recomendaciones y los de procesos sugieren mejoras en el entorno o las herramientas de desarrollo.

Amir Taaki introdujo el concepto de BIP en 2011, inspirándose en las PEPs de Python. Desde entonces, desarrolladores como Luke Dashjr han contribuido a su evolución.

Los BIPs pueden encontrarse en diversos estados, desde borradores iniciales hasta propuestas activas y aceptadas por la comunidad. Algunas pueden ser pospuestas, rechazadas, retiradas, o incluso reemplazadas y declaradas obsoletas si las circunstancias del ecosistema cambian.

En la siguiente figura se muestra de manera más compresiva el BIP:



La imagen muestra un diagrama de flujo que representa las etapas por las que puede pasar una Propuesta de Mejora de Bitcoin (BIP). Comienza con el estado "Borrador" (Draft), que puede progresar a "Propuesto" (Proposed) o pasar a "Diferido" (Deferred) si no se avanza en el desarrollo. Una BIP propuesta puede ser "Aceptada" (Accepted) y convertirse en "Final/Activa" (Final/Active), "Rechazada" (Rejected), o "Retirada" (Withdrawn) por el autor. Finalmente, una BIP aceptada puede eventualmente ser "Reemplazada" o declarada "Obsoleta" (Obsolete/Replaced) si es superada por una nueva propuesta o se vuelve irrelevante.

3. Criptomonedas y Blockchain: Fundamentos para un Futuro Digital

3.3. Bitcoin Core

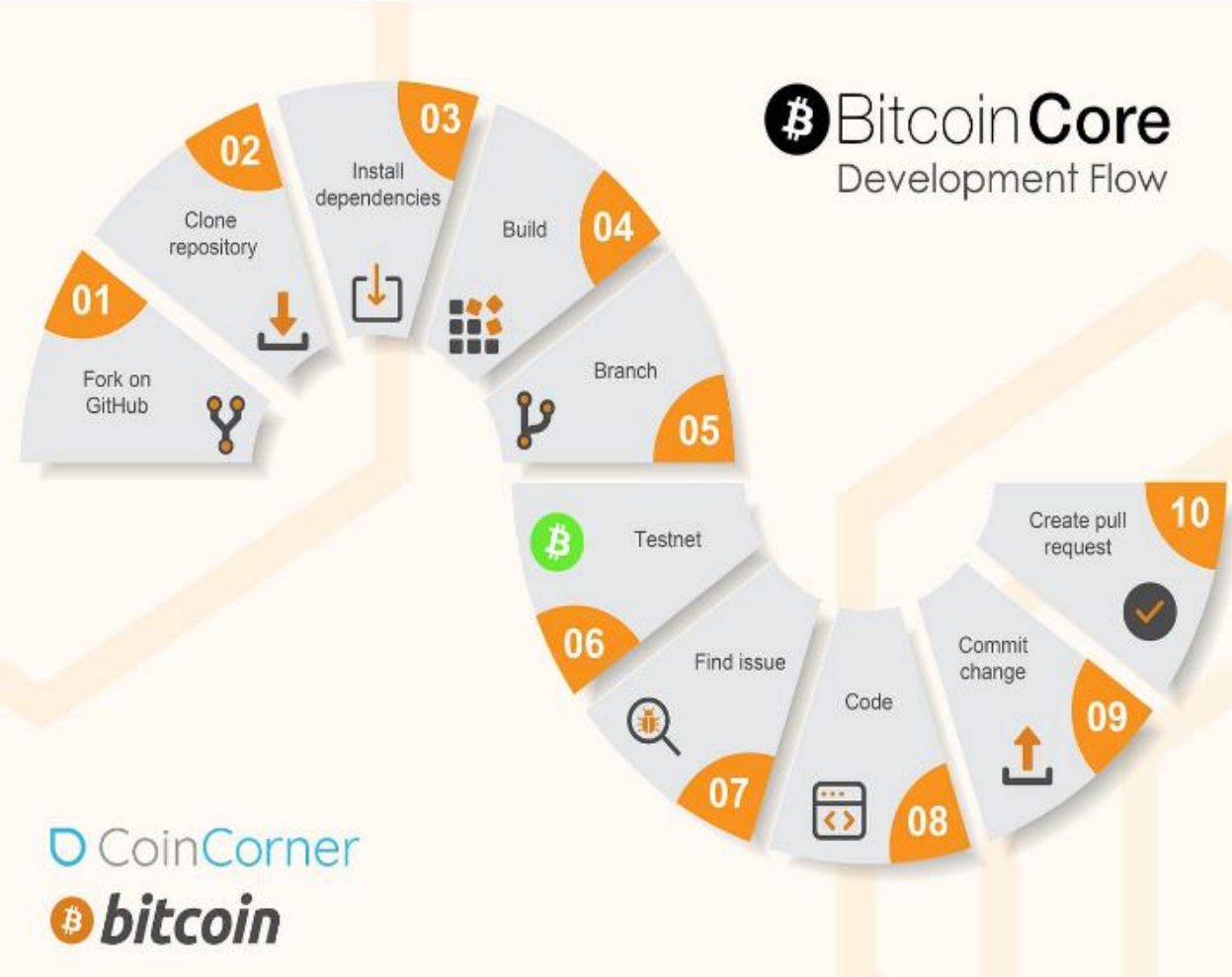
Bitcoin Core es el desarrollo principal de código abierto que se ocupa de la evolución del protocolo de Bitcoin. Esta implementación esencial ofrece todo lo necesario para verificar independientemente las transacciones y mantener la red. Bitcoin Core es notable por ser la continuación directa del trabajo inicial realizado por el propio Satoshi Nakamoto.

Para usar Bitcoin Core, los usuarios pueden descargar el software, que incluye una copia completa del historial de transacciones de Bitcoin desde su inicio, permitiendo a cada nodo validar completamente la cadena de bloques. Aunque proporciona seguridad y privacidad, Bitcoin Core exige una capacidad de almacenamiento considerable y conocimientos avanzados de los usuarios debido a su complejidad y al tiempo requerido para la sincronización inicial.

Bitcoin Core se compone de varios componentes clave, incluyendo el daemon 'bitcoind', que opera en segundo plano y se gestiona mediante comandos, y 'bitcoin-cli', una interfaz de línea de comandos para interactuar con el daemon. También ofrece un entorno de pruebas (testnet) para que los desarrolladores puedan probar nuevas funciones y mejoras.

El desarrollo de Bitcoin Core ha pasado por varias etapas y cambios de nombres, con contribuciones significativas de desarrolladores que asumieron la batuta después de Nakamoto. Se han introducido numerosas mejoras técnicas y optimizaciones en el software a lo largo del tiempo, cada una con el objetivo de mejorar la funcionalidad y la usabilidad del cliente de Bitcoin.

Mostramos a continuación el método de trabajo:



La imagen representa el flujo de desarrollo de Bitcoin Core, detallando cada paso en el ciclo de contribución. Comienza con el proceso de bifurcación (fork) del repositorio en GitHub, seguido de la clonación del repositorio y la instalación de dependencias necesarias. Después, los desarrolladores construyen el software, crean ramas para nuevas características y usan la testnet para probar cambios. Identifican y solucionan problemas, escriben el código correspondiente, y luego hacen un 'commit' de los cambios. Finalmente, crean una solicitud de extracción (pull request) para integrar sus contribuciones al proyecto principal.

Mientras que Bitcoin Core es el cliente principal, también hay otros programas que implementan el protocolo de Bitcoin. Estos programas tienen cierta flexibilidad para decidir qué partes del protocolo implementar, incluyendo las Propuestas de Mejora de Bitcoin (BIPs). A pesar de ser de código abierto y sujeto a propuestas de cambio por parte de la comunidad, solo un grupo pequeño de desarrolladores tiene la autoridad para integrar esos cambios en Bitcoin Core, lo que ha llevado a algunas ramificaciones del proyecto mediante hard forks.

4. Estructura de Bloques y Proceso de Creación

Cada bloque dentro de la cadena de bloques de Bitcoin representa una página en este libro de contabilidad global. La estructura de un bloque se compone de dos partes principales: el encabezado del bloque y la lista de transacciones.

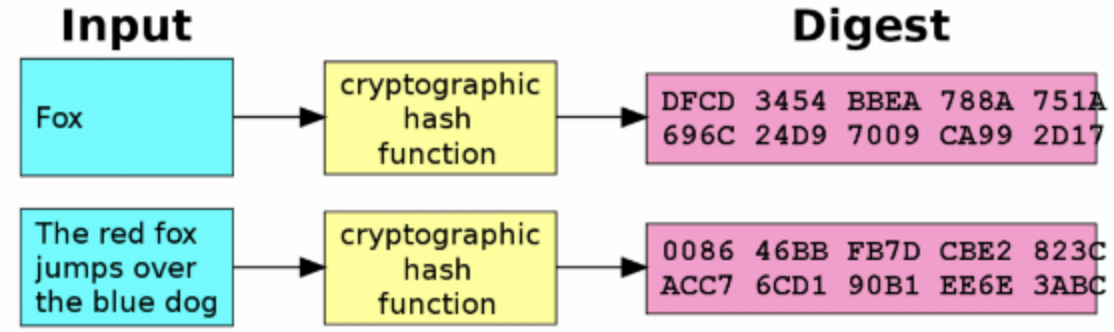
El encabezado del bloque incluye seis campos:

Versión
Indica la versión del protocolo de software utilizado para crear el bloque

Hash del bloque anterior.
Este es un enlace crítico que asegura la integridad de la cadena, conectando cada bloque con su predecesor y, por extensión, con el bloque génesis. Ahora, se estudia la función hash más a fondo para así entender cómo se obtiene este hash:

Función Hash
Una función hash es un procedimiento criptográfico que utiliza un algoritmo específico para transformar información cualquiera en una cadena alfanumérica única de longitud fija, llamada hash.

Un hash no se produce como resultado de un cifrado, sino que es un resumen unidireccional porque el proceso es irreversible. Es decir, no se puede descifrar/recuperar la información original a partir del hash final, sino que se obtiene mediante la prueba de «hashear» sin parar hasta dar con el texto original, puesto que el hash encontrado coincidirá con el que estabas buscando y ya sabías.



La imagen muestra ejemplos de cómo las funciones de hash criptográfico transforman textos de entrada (inputs) de diferentes longitudes en resúmenes de salida (digests) de longitud fija y aparentemente aleatorios. Con solo pequeñas variaciones en la entrada, como "Fox" y "The red fox jumps over the blue dog", los resultados de hash son completamente diferentes, demostrando una propiedad conocida como efecto avalancha en la criptografía.

En Bitcoin, el SHA-256 se utiliza para el proceso de minería (creación de bitcoin), pero también en el proceso de generar direcciones bitcoin (hasta 3 veces se utiliza). La seguridad que ofrece se debe en parte a la utilización de este algoritmo.

Otra de las particularidades del algoritmo de hash SHA-256 es que la longitud del hash resultante es siempre igual, no importa lo extenso que sea el contenido que uses para generar el hash: ya sea de una letra o todas las palabras que hay en el diccionario, el resultado siempre va a ser una cadena de 64 caracteres (con una codificación de 256 bits, 32 bytes). Gracias a esta función se consigue que la dirección sea más corta que la clave pública de la que viene. Además se consigue que sea consistente en su conjunto al generar caracteres de control (checksum)

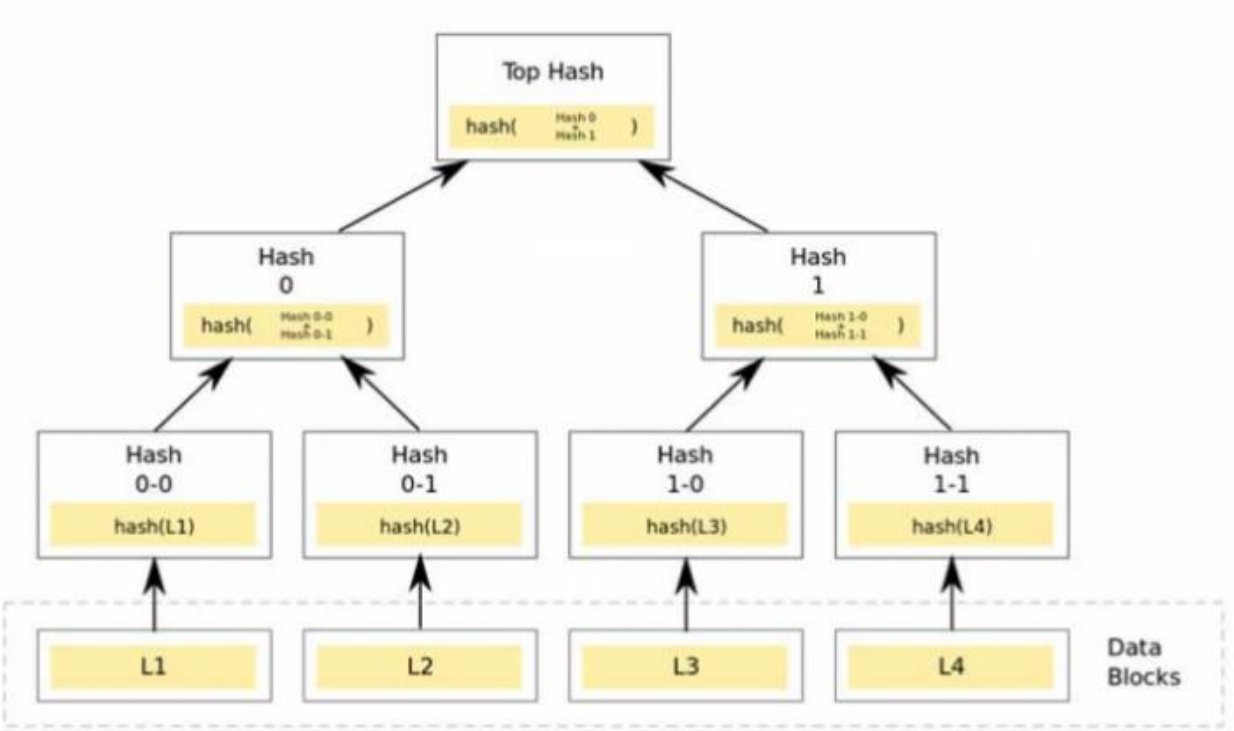
Merkle Tree
Un Merkle Tree, o árbol de Merkle, es una estructura de datos utilizada para verificar de manera eficiente y segura la integridad de grandes conjuntos de datos. Fue introducida por Ralph Merkle en 1979 y se utiliza ampliamente en sistemas de criptomonedas y blockchain.

En un árbol de Merkle, todas las transacciones o piezas de información se representan como hojas, cada una de las cuales tiene un hash único. Estos hashes se agrupan en pares y se combinan para formar nuevos nodos en el siguiente nivel del árbol, cada uno de estos nodos también tiene un hash que se deriva de los hashes de sus nodos hijos. Este proceso de combinación continúa hasta que se llega al nivel superior del árbol, donde un único hash, conocido como la raíz de Merkle (Merkle Root), representa todo el conjunto de datos.

La construcción de un árbol de Merkle sigue estos pasos:

- Hash de las hojas: Cada transacción o pieza de información se convierte en un hash único.
- Combinación en pares: Los hashes individuales se agrupan en pares y se combinan para formar nuevos nodos. El hash de cada nodo se calcula a partir de los hashes de sus nodos hijos.
- Repetición del proceso: Esta combinación se repite en varios niveles hasta que se alcanza un solo hash en la cima del árbol, la raíz de Merkle.

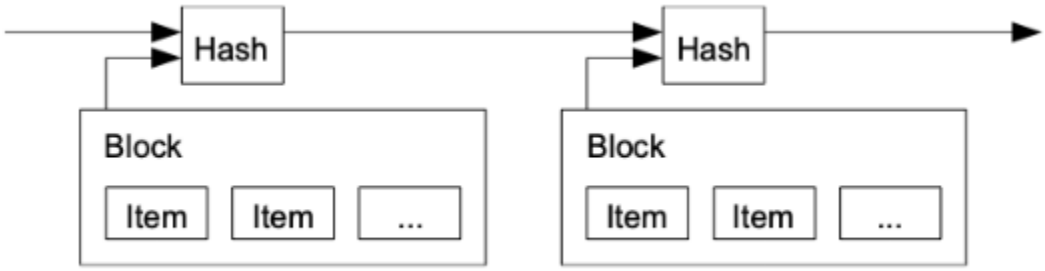
La razón por la cual esta estructura es tan eficaz se debe a su capacidad para verificar la integridad de los datos de manera eficiente. Si un solo hash en cualquier nivel del árbol se modifica, todos los hashes en los niveles superiores cambiarán hasta llegar a la raíz de Merkle. Esto significa que cualquier alteración en los datos originales se reflejará inmediatamente en la raíz, invalidando la integridad del árbol completo. Esta propiedad asegura que la verificación de los datos pueda realizarse de manera rápida y con alta seguridad, ya que solo es necesario comparar el hash raíz para comprobar la integridad de todo el conjunto de datos. A continuación se muestra de manera gráfica:



La imagen es un gráfico de un árbol de Merkle, que ilustra cómo los bloques de datos (L1 a L4) se organizan en una cadena de blockchain. Cada bloque de datos tiene su propio hash, que se agrupa con otros para formar los hashes de nivel superior (Hash 0-0 a Hash 1-1). Estos, a su vez, se combinan para formar los hashes de nivel aún más alto (Hash 0 y Hash 1), que

finalmente se unen para crear el Top Hash, representando la suma de todos los datos de la cadena.

Timestamp
Marca de tiempo que registra cuándo se creó el bloque. Nakamoto especifica que los nodos no deben aceptar bloques con timestamps más de dos horas en el futuro, según sus relojes de sistema, para prevenir manipulaciones.



Esta imagen ilustra la estructura básica de una blockchain, mostrando dos bloques conectados por su hash. Cada bloque contiene múltiples ítems o transacciones, y el hash único en la parte superior asegura la integridad y la secuencia cronológica de la blockchain.

Objetivo de dificultad
Un valor que representa la dificultad actual para encontrar un hash válido bajo el protocolo de Prueba de Trabajo (PoW). Este valor se ajusta dinámicamente cada 2016 bloques para asegurar que el tiempo promedio entre bloques minados sea de aproximadamente 10 minutos.

Nonce
Un valor aleatorio que los mineros ajustan para producir un hash de bloque que cumpla con el objetivo de dificultad actual.

Una vez claro lo que está en el encabezado se verá cómo funciona la lista de transacciones

5. Transacciones

Antes de explicar cómo se definieron las transacciones en el White Paper de Bitcoin, se van a definir tres conceptos importantes: clave pública, clave privada y firma

La **clave privada** es un número secreto que solo conoce su creador y es generado de forma aleatoria, siendo el elemento esencial que permite a un usuario de Bitcoin gastar sus fondos.

La **clave pública**, obtenida a partir de la clave privada mediante un proceso matemático, se comparte para que otros puedan comprobar la autenticidad de una firma digital.

La **firma** es un número que se produce a partir de la clave privada y el hash de la transacción, generando dos números distintos, "r" y "s", que confirman que la operación de firma digital se ha efectuado correctamente.

Para comprender cómo Bitcoin gestiona las transacciones de forma segura, es fundamental conocer el algoritmo ECDSA, un pilar de la criptografía asimétrica en Bitcoin. Este algoritmo crea un par de claves: una privada y una pública, cuya relación se basa en cálculos matemáticos complejos derivados de las curvas elípticas. Antes de adentrarnos en la mecánica detallada de las transacciones en Bitcoin, véase cómo ECDSA proporciona firmas digitales únicas y prácticamente infalsificables, un componente crítico que subraya la integridad y seguridad del sistema.

En el contexto de Bitcoin, la decisión de Satoshi Nakamoto de utilizar la criptografía ECDSA fue crucial para superar retos específicos en la distribución de claves públicas. Al elegir la criptografía de curva elíptica, se benefició de su capacidad para generar claves seguras, de reducido coste computacional y fácil uso. Esto se alinea con el enfoque en la seguridad, eficiencia y la facilidad para crear un número ilimitado de claves públicas. Además, para hacer frente a la extensión de las claves ECDSA de 256 bits, Nakamoto implementó un sistema de refactorización para acortar las claves públicas, utilizando codificación Base58 y funciones hash como SHA-256 y RIPEMD-160, lo que culminó en la creación de las compactas direcciones Bitcoin.

Véase cómo funcionan estas **transacciones**:

Se define una moneda electrónica como una secuencia de firmas digitales. Cada propietario transfiere la moneda al siguiente firmando digitalmente un hash de la transacción anterior y la clave pública del nuevo propietario, añadiendo estos elementos al final de la cadena de la moneda. El receptor puede verificar las firmas para confirmar la cadena de propiedad.

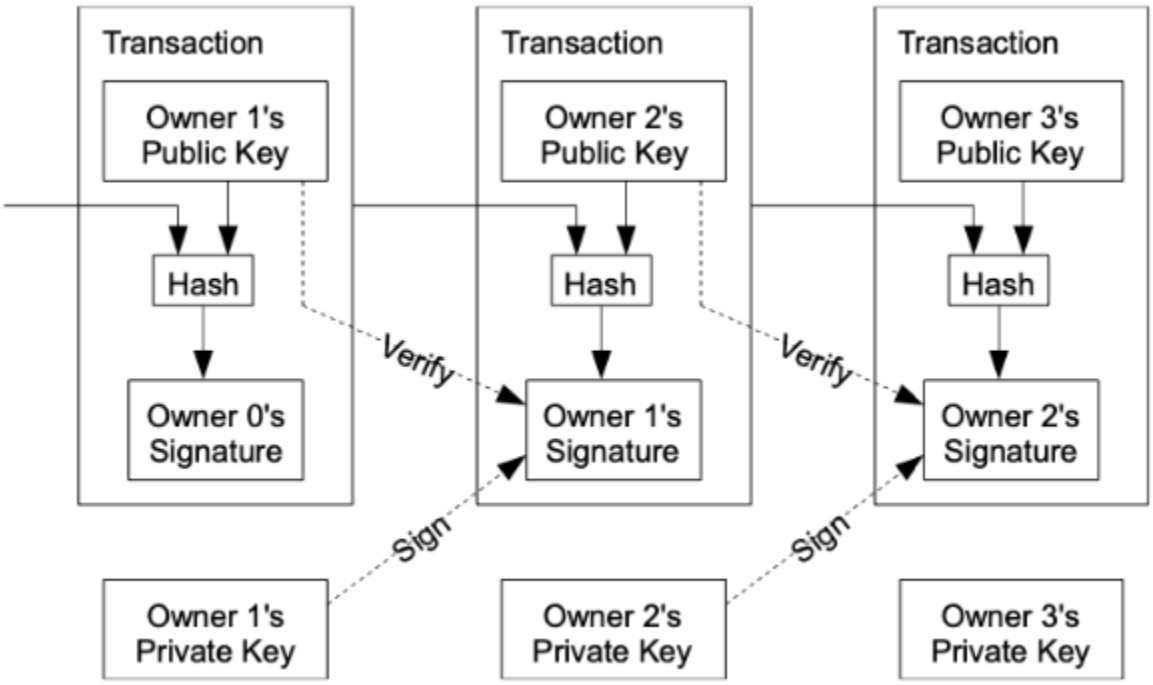
El problema surge cuando el receptor no puede asegurarse de que uno de los propietarios anteriores no haya gastado la moneda más de una vez.

Una solución común es recurrir a una autoridad central de confianza, o casa de moneda, que verifica cada transacción en busca de dobles gastos. Después de cada transacción, la moneda debe ser devuelta a la casa de moneda para emitir una nueva, y solo las monedas emitidas directamente por esta autoridad se consideran confiables y libres de doble gasto. El inconveniente de este enfoque es que el destino del sistema monetario entero queda en

manos de la entidad que opera la casa de moneda, ya que todas las transacciones deben pasar por ella, similar a un banco.

Es necesario un método que permita al receptor saber que los propietarios anteriores no han realizado transacciones previas con esa misma moneda. Para nuestros fines, la transacción inicial es la que tiene validez, por lo que no nos preocupan intentos posteriores de doble gasto. La única forma de confirmar la ausencia de una transacción es estar al tanto de todas las transacciones realizadas. En el modelo basado en la casa de moneda, esta tenía conocimiento de todas las transacciones y decidía cuál se había realizado primero.
Para lograr esto sin depender de una parte de confianza, y que las transacciones se anuncien públicamente, se requiere un sistema que permita a los participantes acordar una historia única del orden en el que fueron recibidas. El receptor necesita una prueba de que, en el momento de cada transacción, la mayoría de los nodos estuvieron de acuerdo en que fue la primera en ser recibida.

Se enseña un esquema de cómo se podría ver una serie de transacciones de manera más esquemática.



La imagen muestra el flujo de una transacción en una cadena de bloques a través de firmas digitales y claves públicas. Ilustra cómo cada transacción está vinculada a la siguiente mediante una firma que verifica la propiedad, usando la clave pública del próximo propietario y la clave privada del actual para firmar el hash de la transacción.

6. Tipos de Blockchain

Hay tres tipos principales de Blockchain hoy en día que se van a explicar a continuación.

Blockchain Pública
Una red de blockchain pública funciona como un ecosistema descentralizado y abierto, accesible para cualquier persona interesada en participar. Caracterizadas por su naturaleza de código abierto y transparencia, estas redes no requieren permisos específicos para acceder o contribuir, posibilitando que cualquiera pueda verificar transacciones y participar en la minería. Ejemplos emblemáticos de blockchain pública incluyen Bitcoin y Ethereum, ambos pioneros en proporcionar un entorno seguro y sin permisos para transacciones digitales y contratos inteligentes.

Blockchain Privada
En contraste, una blockchain privada es una red más exclusiva, diseñada para operar bajo el control de una entidad única o una organización. Estas redes se centran en aplicaciones empresariales, donde la privacidad y la eficiencia operativa son cruciales. A diferencia de las blockchains públicas, el acceso a una blockchain privada es restringido y requiere autorización, lo que permite un mayor control sobre quién puede participar en la red. Aunque este enfoque limita la descentralización, ofrece ventajas en términos de escalabilidad y gestión de la privacidad, manteniendo las transacciones y la información lejos del ojo público.

Un ejemplo de blockchain privada puede ser **Hyperledger**.

Hyperledger es un proyecto de código abierto liderado por la Linux Foundation que ofrece herramientas para el desarrollo de blockchains privadas. A diferencia de las públicas, las blockchains de Hyperledger se utilizan en aplicaciones empresariales, donde la privacidad y la escalabilidad son esenciales. Con acceso restringido y controlado, Hyperledger permite una gestión eficiente de la privacidad y una mayor escalabilidad, siendo utilizado en diversas aplicaciones empresariales como la gestión de la cadena de suministro y la trazabilidad de productos.

Se muestra un esquema de los tipos de blockchain, no se explica la hibrida a pesar de aparecer en este ya que no es una blockchain muy común.

La imagen muestra una comparación entre diferentes tipos de blockchain:

Permissionless (sin permisos) y Permissioned (con permisos). A la izquierda, la blockchain pública es abierta y sin una autoridad central. A la derecha, están las blockchains privadas y de consorcio, controladas por una entidad o un grupo, respectivamente. En el centro, la blockchain híbrida combina elementos de ambas, gestionada por una autoridad con procesos sin permisos.

Blockchain de Consorcio
Uniendo lo mejor de ambos mundos, la blockchain de consorcio representa una solución intermedia entre las redes públicas y privadas. Esta modalidad reúne a varias organizaciones para administrar colectivamente una red blockchain, estableciendo un equilibrio entre la transparencia y la privacidad. A diferencia de las blockchains públicas, donde el anonimato y la participación abierta es esencial, y a las privadas, que se centran en el aislamiento y control centralizado, las blockchains de consorcio ofrecen un modelo gobernado conjuntamente que puede ser parcialmente abierto o restringido según los acuerdos entre los miembros.

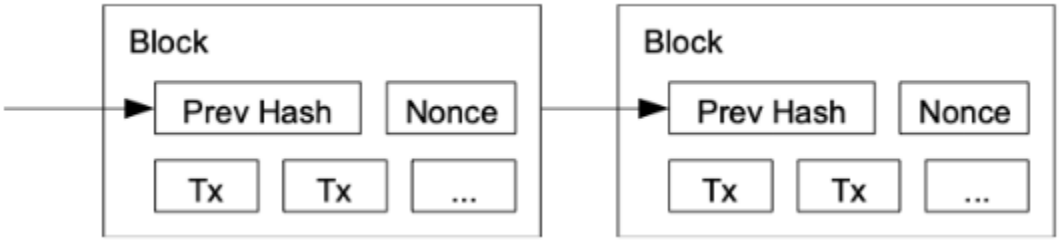
Estas redes permiten una distribución equitativa de los derechos de validación entre las entidades participantes, garantizando que ningún participante individual tenga control total sobre la red. La flexibilidad en la configuración de visibilidad de la cadena permite adaptar la red a necesidades específicas, ya sea limitando el acceso a la información a ciertos miembros autorizados o permitiendo una mayor transparencia dentro de un marco regulador. El consenso en una blockchain de consorcio facilita la implementación ágil de cambios, siempre y cuando haya acuerdo entre las partes validadoras. Este enfoque colaborativo asegura la integridad del sistema mientras se adapta a las necesidades de múltiples stakeholders, manteniendo la eficiencia y la seguridad como prioridades.

7. Prueba de Trabajo (PoW)

Para implementar un servidor de marca temporal en una red de pares, es necesario utilizar un sistema de prueba de esfuerzo (PoW, por sus siglas en inglés), siguiendo un enfoque similar al propuesto por Adam Back con **Hashcash,** pero evitando métodos tradicionales como anuncios en periódicos o publicaciones en Usenet (Red global de grupos de discusión distribuida en internet.) La esencia de la prueba de esfuerzo se encuentra en buscar un valor que, una vez procesado por una función hash como SHA-256, produzca un hash que inicie con una secuencia determinada de bits en cero. La dificultad de este trabajo crece exponencialmente con el número de bits en cero que se requieran y este esfuerzo se puede comprobar con la ejecución de un único hash. Además cabe destacar que el PoW solo es necesario en las blockchains públicas ya que no es necesario en las privadas.

En el contexto de nuestra red para marcar tiempo, la PoW se realiza mediante el incremento de un valor nonce en el bloque, hasta que se descubre un valor que logra que el hash del bloque cumpla con la condición específica de tener los bits iniciales en cero. Este proceso asegura que, una vez invertido el esfuerzo computacional necesario para cumplir con la prueba de esfuerzo, cambiar el contenido de dicho bloque requeriría repetir todo el trabajo desde el inicio. Si se quisieran alterar bloques anteriores, sería necesario rehacer el trabajo de esos bloques y de todos los que le siguen en la cadena.

La prueba de esfuerzo soluciona también el problema de cómo representar la mayoría en las decisiones colectivas. Si se basara en un sistema de un voto por dirección IP, cualquier persona con la capacidad de asignar múltiples direcciones IP podría manipular el resultado. Por lo tanto, la PoW establece un modelo de un-voto-por-CPU, donde la cadena más larga y con mayor trabajo invertido es considerada la representación de la decisión mayoritaria. Si la mayor parte del poder computacional está en manos de nodos honestos, estos generarán la cadena más larga más rápidamente que cualquier cadena competidora. Para alterar un bloque pasado, un atacante necesitaría no solo rehacer el trabajo de ese bloque, sino también superar el trabajo acumulado por los nodos honestos, lo cual es prácticamente inviable.



La imagen representa dos bloques en una cadena de blockchain, destacando componentes clave como el hash del bloque anterior (Prev Hash) y el nonce. Cada bloque contiene múltiples transacciones (Tx), y el hash conecta secuencialmente cada bloque con el anterior, asegurando la integridad de la cadena. El nonce es un número que se ajusta para que el hash del bloque cumpla con los requisitos de la red, un proceso central en el mecanismo de consenso Proof of Work.

Muéstrese una descripción del propio algoritmo, en la que figuran 4 puntos importantes:

Problema Computacional

- PoW requiere que los mineros resuelvan un problema matemático basado en encontrar un valor nonce tal que, cuando se concatena con los datos del bloque y se aplica una función hash criptográfica (p. ej., SHA-256), el resultado cumpla con una

condición específica de dificultad (generalmente, producir un hash con un número determinado de ceros iniciales).

Proceso de Minería

- Los mineros recogen transacciones pendientes y las agrupan en un bloque.
- Se añade un nonce al bloque y se calcula el hash del bloque.
- Los mineros iteran a través de diferentes valores de nonce hasta encontrar uno que produzca un hash que cumpla con el requisito de dificultad

Verificación y Consenso

- Cuando un minero encuentra un nonce válido, el bloque y su hash se transmiten a la red.
- Otros nodos verifican la validez del hash y el cumplimiento de la dificultad.
- Si la mayoría de los nodos aceptan el bloque, este se añade a la cadena de bloques.

Recompensa y Ajuste de Dificultad

- El minero que encuentra el nonce válido recibe una recompensa en criptomonedas y las tarifas de transacción del bloque.
- La dificultad del problema se ajusta periódicamente (cada 2016 bloques en Bitcoin) para mantener un intervalo de tiempo constante para la generación de bloques (aproximadamente cada 10 minutos).

Para mayor claridad, un sencillo **ejemplo**:

Imagina que estás participando en un concurso donde debes adivinar un número secreto que, al ser introducido en una calculadora especial (función hash), el resultado debe empezar con ceros. Todos los participantes tienen calculadoras idénticas y el número secreto cambia para cada ronda del concurso. El primero en adivinar el número correcto gana la ronda, pero cualquier intento de hacer trampa requiere empezar a adivinar desde el inicio y por ello más rápido que los demás, una tarea que se vuelve más difícil conforme el juego avanza y se añaden más rondas. Este concurso simboliza cómo la PoW asegura la integridad y el consenso en la blockchain.

¿Cómo se suele hacer el minado?

Hoy en día la mayoría de minado se hace con mineros **ASIC**, application-specific integrated circuit, que son básicamente una serie de equipos informáticos diseñados de principio a fin para ofrecer el máximo rendimiento en tareas de minería de criptomonedas. Estos sistemas ofrecen un minado muy rápido de bitcoin, pero también tienen sus desventajas:

- Concentración en la minería: las grandes operaciones mineras dificultan la participación de usuarios individuales.

- Disponibilidad limitada: la adquisición de ASICs puede ser complicada debido a su rápida venta y escasez en el mercado.
- Alto costo: estos dispositivos son caros y requieren una inversión considerable.
- Monopolio del mercado: bitmain, como líder del mercado, tiene un control significativo, lo que influye en la disponibilidad y precios de los equipos.
- Consumo energético elevado: los ASICs consumen mucha energía y necesitan sistemas de enfriamiento eficientes debido al calor que generan.
- Obsolescencia rápida: la rápida evolución del hardware hace que los ASICs se vuelvan obsoletos en poco tiempo.
- Resistencia a los ASIC: algunas criptomonedas buscan evitar la centralización minera mediante algoritmos que no sean propensos a la minería con ASICs, lo que garantiza una mayor equidad en la participación de la red.

8. Otros Mecanismos de Consenso

Durante las últimas tres décadas, los mecanismos de consenso se han convertido en una parte importante de la integración del procesamiento informático en nuestra vida cotidiana. Hoy en día, los mecanismos de consenso sustentan toda la industria de las criptomonedas, ya que forman el concepto central de todas las cadenas de bloques.

El mecanismo de consenso representa los fundamentos de la validación de bloques en una cadena de bloques. Este define las condiciones que deben cumplir los nodos y validadores antes de que se puedan agregar nuevos bloques a la cadena de bloques. Existen muchos mecanismos de consenso diferentes, todos los cuales sirven como teoremas que sustentan las características centrales de la tecnología blockchain: descentralización, distribución y libro público.

La prueba de trabajo (PoW) fue el primer mecanismo de consenso de blockchain creado. Se introdujo con el concepto de blockchain de Bitcoin.

Bitcoin inspiró a los desarrolladores a comenzar a experimentar con la tecnología blockchain y comenzaron a surgir nuevos mecanismos de consenso. Actualmente, algunos de los mecanismos de consenso más establecidos incluyen Ethereum y Prueba de participación (PoA) y VeChain con Prueba de autoridad (PoA). Todos estos diferentes mecanismos de consenso dan significado al requisito elegido (trabajo, tarifa, permisos) asegurando el contrato y permitiendo la verificación de la transacción y la generación de claves.

Un mecanismo de consenso es un requisito esencial para que cualquier protocolo blockchain funcione correctamente. Garantizan que todos los nodos funcionen sincrónicamente y que toda la red de operadores de nodos distribuidos cumpla con las mismas condiciones. El mecanismo de consenso también garantiza la seguridad de los usuarios de blockchain. El validador de nodos es responsable de eliminar las transacciones no válidas y esta acción se realiza con éxito mediante reglas predefinidas establecidas en el mecanismo de consenso. No solo la transacción debe registrarse exitosamente en el libro mayor y agregarse al bloque, sino que también se debe alcanzar un consenso entre todos los nodos. La división equitativa de responsabilidades entre los operadores de nodos garantiza que el mecanismo de consenso seguirá funcionando eficazmente incluso si uno o más nodos no cumplen con sus funciones.

Básicamente, los mecanismos de consenso preservan los fundamentos de la tecnología blockchain y permiten la gobernanza distribuida y la verificación de múltiples transacciones en tan solo unos segundos. Crear un mecanismo de consenso viable y aplicable no es una tarea fácil; Sin embargo, a medida que evoluciona la tecnología blockchain, los desarrolladores adoptan enfoques más innovadores.

La tecnología detrás de los mecanismos de consenso se basa en un problema teórico formulado por informáticos en 1982. El problema de los generales bizantinos pregunta si es posible crear consenso en una red informática formada por nodos independientes y distribuidos geográficamente, y la respuesta la proporcionan los mecanismos de consenso.

8. Otros Mecanismos de Consenso

8.1. Proof of Stake (PoS)

Proof of Stake es uno de los dos protocolos de consenso más utilizados en la tecnología blockchain. De aquí proviene el acrónimo PoS por el que se le conoce. El objetivo de este algoritmo, al igual que PoW, es lograr el consenso entre todas las partes que componen la red.

Los nodos que admiten PoS se denominan validadores. La decisión sobre qué nodo comprobará un bloque se toma de forma aleatoria, pero lo más probable es que la tomen aquellos que cumplan una serie de criterios. Estos criterios incluyen la cantidad de reservas y el tiempo de permanencia en la red, pero se pueden definir otros. Una vez instalado, el proceso de selección de nodos comienza de forma aleatoria y, una vez completado, los nodos seleccionados podrán realizar transacciones o crear nuevos bloques.

Esto muestra que la Prueba de participación es un proceso completamente diferente al famoso protocolo Prueba de trabajo (PoW). Donde cada uno de sus nodos realiza un pesado trabajo computacional para resolver problemas criptográficos. A diferencia de PoW, que requiere mucha energía y equipos especializados, PoS es un proceso mucho más simple

y energéticamente eficiente. Por este motivo, muchos proyectos blockchain están interesados en este nuevo protocolo.

La primera moneda en utilizar este protocolo fue PeerCoin en 2012. Posteriormente surgieron otros como NXT y Bitshares que también utilizaban este protocolo.

¿Cómo funciona?

El funcionamiento del protocolo Prueba de participación es muy específico. Este sistema pretende incentivar a los participantes a tener siempre cierta cantidad de monedas. Esto les permite elegir el proceso de selección de accidentes, realizado para indicar las tareas. Según este programa, las personas que tienen más reservas son más importantes en la web y mayores oportunidades de ser elegidos. Después de ser elegidos, la Web3 puede verificar las transacciones y crear nuevos bloques. Les permite lograr ganancias e incentivos para su trabajo.

Imagina una red de criptomonedas con tres grupos de inversores. El Grupo A tiene 10 inversores con 1,000 monedas cada uno, el Grupo B tiene 5 inversores con 4,000 monedas cada uno, y el Grupo C tiene 2 inversores con 10,000 monedas cada uno. La tabla de abajo muestra cómo esta distribución afecta sus posibilidades de ser seleccionados como validadores en un sistema Proof of Stake, donde una mayor cantidad de monedas aumenta la probabilidad de selección:

Grupo	Número de Inversores	Monedas por Inversor	Total de Monedas	Participación (%)
A	10	1,000	10,000	20%
B	5	4,000	20,000	40%
C	2	10,000	20,000	40%

En este ejemplo, aunque el Grupo C tiene menos inversores, su participación en la red es igual al Grupo B debido a la mayor cantidad de monedas. Esto ilustra cómo Proof of Stake democratiza la red pero también favorece a quienes invierten más.

La mayor tenencia, no garantiza la selección como nodo, pero va a dar más oportunidades. Con esto se busca que todos los que están dentro de la red se beneficien sin sufrir discriminación. Además, cualquiera de los inversores en el Grupo A, siempre pueden invertir más para incrementar su nivel de participación.

Una vez seleccionados, los inversores pueden realizar las tareas permitidas. Los inversores realizan dichas tareas con el fin de recibir incentivos y ganancias proporcionales a su

participación dentro del sistema. Terminada la ronda, se reinicia el proceso de selección para que otros inversores puedan participar. Además de esto, los fondos usados como tenencia no se pueden usar, y serán bloqueados dentro de la blockchain. Así, se garantiza que los fondos siempre estarán disponibles como garantía del nodo validador. El nodo puede agregar fondos en cualquier momento, para aumentar más su nivel de participación.

8. Otros Mecanismos de Consenso

8.2. Proof of Authority (PoA)

La prueba de autoridad pretende ser una solución práctica y eficaz, específicamente dirigida a blockchains privadas. El término PoA fue acuñado por Gavin Wood, cofundador y ex CTO de Ethereum. Este protocolo de consenso es claramente diferente de otros protocolos como PoW y PoS. Esto se debe a que PoA utiliza identidades del mundo real para proporcionar verificación en la cadena de bloques. Esto significa que los validadores confían en su verdadera identidad y reputación como garantía de transparencia. Un proceso que selecciona aleatoriamente validadores confiables específicos. Una situación completamente diferente con la minería PoW, pero existe un programa de participación en PoS.

Además, PoA se basa en un número limitado de validadores. Esta característica le otorga una clara ventaja, que es la alta escalabilidad de blockchain. Esto tiene un impacto positivo en aplicaciones donde la velocidad es primordial. Además, mantiene un alto nivel de control de acceso sobre dicha cadena de bloques, ya que sólo los nodos autorizados pueden participar en ella.

¿Cómo funciona el protocolo PoA?

El mecanismo del protocolo Proof of Authority (PoA) es relativamente simple y directo. Inicialmente, para el correcto funcionamiento de la red, es necesario seleccionar a los validadores de manera aleatoria. La incorporación y elección de estos nodos se lleva a cabo a través de un sistema de votación implementado por nodos que ya han sido autorizados anteriormente. Este método previene la inclusión de nodos malintencionados que podrían comprometer la estabilidad de la red. Además, se establece que cada validador tiene el derecho de firmar un solo bloque dentro de una secuencia de bloques asignados durante su periodo de validación. A diferencia del esquema de minería utilizado por sistemas como Bitcoin, PoA es considerado amigable con el medio ambiente ya que no requiere de un proceso de minería intensivo en recursos.

Al igual que el protocolo Proof of Stake (PoS) utiliza la participación como criterio para la selección y la confianza dentro de la red, PoA se basa en la identidad y la reputación del validador. La identidad es un recurso limitado y la reputación es extremadamente valiosa. Al utilizar la identidad como parte del protocolo, se requiere que los validadores revelen

voluntariamente quiénes son. Esta divulgación hace fácil asignar responsabilidades por el desempeño de la red. Cualquier acción que comprometa la integridad y la transparencia de la red afecta directamente a la persona o entidad detrás del nodo validador, lo que puede tener un impacto negativo significativo en su reputación.

Por lo tanto, los validadores en una red basada en PoA tienen un fuerte incentivo para proteger su reputación e identidad. Esto asegura su compromiso con el mantenimiento de la red, garantizando su transparencia y fiabilidad. La identidad comprometida actúa como un poderoso factor de igualdad, reconocido y valorado por todos los participantes de la red. Las entidades cuya identidad está en riesgo están más motivadas a actuar en favor de la preservación de la red.

Las condiciones operativas del protocolo Proof of Authority (PoA) son los requisitos necesarios para asegurar su correcto funcionamiento. Estas condiciones incluyen los siguientes pasos:

- Validación de identidades de los posibles validadores: Cada individuo o entidad que desee participar en la red debe verificar y hacer públicas sus identidades reales. Esto garantiza la transparencia y la responsabilidad dentro de la red.
- Compromiso financiero y reputacional del candidato a validador: El candidato a ser validador debe estar dispuesto a invertir recursos financieros y poner su reputación en juego como garantía. Este proceso asegura que los candidatos estén motivados a participar a largo plazo en la red y se comprometan con su buen funcionamiento
- Establecimiento de un sistema estándar para la aprobación de validadores: Se necesita un método estandarizado para aprobar a los validadores, asegurando que la selección sea equitativa y justa para todos los candidatos.
- Capacidad para eliminar a actores maliciosos: El sistema debe contar con mecanismos para identificar y eliminar a validadores que actúen de manera maliciosa o deshonesta dentro de la red. Esto es crucial para mantener la confianza y la transparencia en el ecosistema de la red blockchain.

Cumplir con estas condiciones es fundamental para garantizar la integridad y la eficacia del protocolo PoA, y para mantener la confianza de todos los participantes en la red.

8. Otros Mecanismos de Consenso

8.3. Proof of Burn (PoB)

La creación y adopción inicial de la criptomoneda pionera, Bitcoin, y su tecnología subyacente, la cadena de bloques o blockchain, han generado un vasto campo de posibilidades y nuevas innovaciones en los ámbitos criptográficos y financieros. Una de estas innovaciones emergentes es el protocolo de consenso conocido como Proof of Burn o Prueba de Quemado.

Este protocolo fue concebido por Iain Stewart, quien presentó su concepto de Proof of Burn en el popular foro Bitcointalk en diciembre de 2012. Stewart utilizó una analogía para explicar el algoritmo: las monedas quemadas son similares a las plataformas mineras. En esta analogía, un minero quema sus monedas para adquirir una plataforma minera virtual que le otorga la capacidad de extraer bloques. Cuantas más monedas queme el minero, más grande será su "plataforma" minera virtual.

Aunque otro usuario del foro había propuesto una idea similar en enero de 2012, su propuesta no logró materializarse.

A pesar de que los protocolos de consenso más comúnmente utilizados en las blockchains de criptomonedas son el Proof of Work (PoW) y el Proof of Stake

(PoS), el Proof of Burn (PoB) promete abordar las limitaciones presentadas por estos algoritmos. Para lograrlo, busca ofrecer una solución más eficiente mientras garantiza la seguridad y la estabilidad de la red.

¿Cómo funciona?

El Proof of Burn no implica el proceso de minería para crear nuevas criptomonedas. En su lugar, implica la quema de ciertos tokens de la criptomoneda nativa o alternativa para obtener el derecho a minar. A primera vista, esta metodología puede parecer poco convencional, pero su funcionamiento es claro una vez entendido.

En el protocolo Proof of Burn, los mineros deben enviar criptomonedas a una dirección pública y verificable conocida como "eater address" o dirección comedora, donde las monedas se vuelven inaccesibles e inutilizables para siempre, ya que estas direcciones son creadas de forma aleatoria y no tienen claves privadas asociadas conocidas. Esta acción representa una inversión en la blockchain, y cuanto mayor sea la cantidad de criptomonedas quemadas, mayor será el poder de minería adquirido por el minero.

La principal motivación detrás del diseño y creación del protocolo Proof of Burn, era crear un protocolo de consenso que exigiera un trabajo realmente costoso de realizar y más eficiente que Proof of Work. De esa manera, nació la idea de consumir recursos reales y tangibles como lo es una criptomoneda o token con un valor real, con el fin de conseguir capacidad para minar dentro de la blockchain.

8. Otros Mecanismos de Consenso

8.4. Proof of Elapsed Time (PoET)

Entre los algoritmos de consenso y minería blockchain, uno de los más destacados es el Proof of Elapsed Time (PoET), conocido en español como Prueba de Tiempo Transcurrido.

Este algoritmo de consenso está diseñado desde su base para ser altamente escalable y está dirigido principalmente a blockchains privadas. Por lo tanto, es poco probable que lo véase siendo utilizado para sustentar la actividad de una blockchain de una criptomoneda pública, como es el caso de Bitcoin.

Sin embargo, el potencial del algoritmo PoET radica en su capacidad para ser aplicado en el desarrollo de blockchains que forman parte de sistemas con alto volumen de información. Por ejemplo, en empresas que requieran sistemas integrados de auditoría que garanticen la inmutabilidad de los datos. Esto podría incluir líneas de producción altamente tecnificadas y automatizadas, laboratorios químicos y farmacéuticos, entre otros ejemplos.

El enfoque de PoET es ideal para entornos donde la escalabilidad y la seguridad de la información son primordiales. Al garantizar una alta escalabilidad, el algoritmo permite que las blockchains privadas puedan manejar grandes cantidades de datos de manera eficiente, lo que resulta fundamental en entornos empresariales y de producción donde se genera y procesa una gran cantidad de información en tiempo real.

¿Cómo funciona?

La esencia del funcionamiento de PoET radica en el proceso de selección gestionado por el algoritmo de verificación del proceso. Este algoritmo asigna a cada participante un objeto de tiempo, que funciona como un contador regresivo con una cantidad de tiempo predeterminada. Este objeto de tiempo representa un periodo durante el cual el participante espera para ser activado como generador de bloques. La asignación de este objeto de tiempo se realiza de manera aleatoria, utilizando instrucciones de generación de números aleatorios como RDRAND de Intel.

Cuando el objeto de tiempo del participante llega a cero, se activa como generador de bloques. En esta fase, el participante recopila las transacciones de la red, las organiza en un bloque y genera un hash para ese bloque. Este proceso no requiere una prueba de trabajo intensiva como en Bitcoin. Una vez generado el bloque, se emite a la red junto con el certificado del participante, validando así su participación en la generación de bloques.

En PoET, los participantes son seleccionados aleatoriamente para generar bloques utilizando un objeto de tiempo, y luego generan bloques de manera eficiente y rápida, sin necesidad de realizar una prueba de trabajo intensiva.