
Más Allá de Bitcoin
La Revolución Completa de Blockchain
Cristopher Pereyra Andrade
Primera Edición 2024

Más Allá de Bitcoin: La Revolución Completa de Blockchain

Primera edición

Cristopher Pereyra Andrade

Información de contacto:

Linkedin: https://www.linkedin.com/in/cointor/

Índice

1. **Introducción** - 3.
2. **¿Qué es la Blockchain?** - 4.
3. **La historia de Blockchain** - 6.
4. **Tipos de Blockchain** - 7.
5. **Satoshi Nakamoto** - 9.
6. **¿Qué es el Hash?** - 11.
7. **Ecuaciones matemáticas** - 15.
8. **Descentralización** - 19.
9. **Dominio público** - 21.
10. **Nodos** - 24.
11. **Llaves privadas y públicas** - 25.
12. **Criptomonedas** - 27.
13. **Minería** - 29.
14. **CPU** - 31.
15. **51%** - 32.
16. **¿Que es fungible?** - 34.
17. **Nfts** - 35.
18. **Web 3.0** - 36.
19. **Metaverso** - 37.
20. **Documentos de riesgo** - 39.
21. **Política** - 41.
22. **Medicina** - 43.
23. **Financieras** - 45.
24. **Logística** - 47.
25. **Tokenización en personas** - 48.
26. **Monetización** - 50.

27. **Especulación** - 52.
28. **Bitcoin vs Ethereum** - 54.
29. **¿Somos el producto?** - 57.
30. **Glosario** - 58.
31. **Bibliografía** - 62.
32. **Agradecimientos** - 63.

Introducción

¡Hola! Estoy emocionado de compartir contigo esta increíble aventura por el mundo de la criptografía y blockchain. Imagina que estamos sentados juntos en un café, disfrutando de un buen café mientras charlamos sobre este tema fascinante.

Primero, te llevaré de la mano a través de los conceptos básicos de la blockchain. Te explicaré de manera sencilla qué es exactamente y cómo funciona. ¿Te imaginas una cadena de bloques interconectados que contienen información segura y transparente? Eso es básicamente la blockchain.

Después, te sumergiré en su historia. Hablaremos sobre Satoshi Nakamoto, el misterioso creador de Bitcoin, y cómo su visión revolucionaria dio inicio a todo este fenómeno. Te contaré sobre los primeros días de la blockchain y cómo ha evolucionado desde entonces.

Luego, exploraremos juntos las diversas funcionalidades de la blockchain. Desde la seguridad criptográfica hasta la descentralización, te mostraré cómo esta tecnología está transformando industrias enteras y cambiando la forma en que interactuamos en línea.

No puedo esperar para compartir contigo las infinitas posibilidades de aplicación de la blockchain. Desde las criptomonedas hasta los contratos inteligentes y los NFTs (Tokens No Fungibles), te sorprenderá descubrir cómo esta tecnología está redefiniendo la forma en que hacemos negocios y nos relacionamos digitalmente.

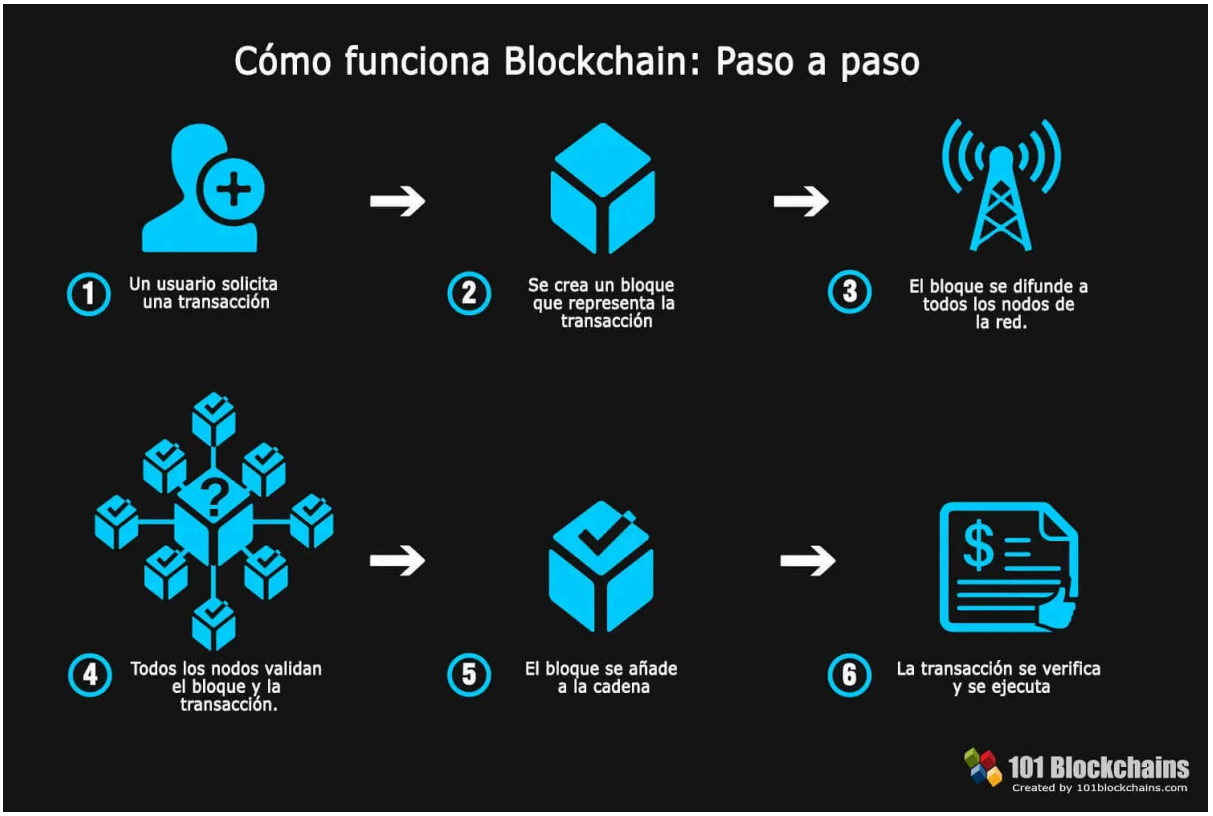
Y lo mejor de todo, este viaje de descubrimiento es completamente gratuito. Quiero que tengas acceso a este conocimiento sin barreras, para que puedas empoderarte y ser parte de esta revolución tecnológica.

Así que ¿estás listo para sumergirte en el emocionante mundo de la criptografía y blockchain? ¡Vamos a empezar este viaje juntos!

¿Qué es la Blockchain?

Imagina el blockchain como un libro mayor compartido entre múltiples participantes, una especie de "libro mágico" que registra todas las transacciones y activos de una red de negocios. Este libro mayor es inmutable, lo que significa que una vez que se registra una transacción, no se puede alterar ni eliminar. ¿Te imaginas la seguridad que esto proporciona?

Cuando hablamos de blockchain, nos referimos a un registro confiable y casi imposible de hackear de todas las transacciones y la propiedad de los activos. Piénsalo como una base de datos donde la información se almacena en bloques, y estos bloques se replican en múltiples computadoras, manteniendo una sincronización perfecta entre todas ellas. Cada bloque es tan seguro como la banca online más avanzada, lo que lo convierte en una herramienta ideal para el intercambio seguro de información en tiempo real.



Funcionamiento de blockchain [https://101blockchains.com]

Pero, ¿qué tipo de información puede almacenar el blockchain? La respuesta es casi cualquier cosa de valor: desde préstamos y títulos inmobiliarios hasta manifiestos de logística. Además, la capacidad del blockchain para compartir grandes cantidades de datos en un entorno seguro y verificable lo hace ideal para una variedad de aplicaciones empresariales.

A medida que la tecnología avanza, los casos de uso del blockchain continúan evolucionando. Cada vez más empresas de diferentes sectores están adoptando esta tecnología para mejorar la eficiencia y la seguridad de sus operaciones. Y con esta

adopción viene la necesidad de cumplir con las leyes de confidencialidad de datos, lo que hace que la seguridad del blockchain sea aún más crucial.

Es aquí donde entra en juego el concepto de "Blockchain como servicio" (BaaS). Esta es una plataforma que integra la tecnología blockchain en un modelo de entrega de software basado en la nube. ¿El objetivo? Proporcionar todas las ventajas del blockchain, como la transparencia y la seguridad, sin que las empresas tengan que invertir en recursos internos. Los proveedores de servicios mantienen la red de BaaS en la nube, lo que significa que las empresas pueden centrarse en sus operaciones principales mientras aprovechan los beneficios del blockchain.

¿Por qué es importante la Blockchain?

Primero, hablemos de seguridad. ¿Te imaginas una caja fuerte digital impenetrable? Bueno, eso es más o menos lo que ofrece el blockchain. Gracias a su avanzada tecnología de criptografía y su estructura descentralizada, los datos almacenados en la red son como tesoros protegidos por una fortaleza digital. Esto significa que tus transacciones y activos están a salvo de las manos curiosas de los hackers y los estafadores.

Otro punto clave es la transparencia. En un mundo donde la confianza es crucial, el blockchain ofrece un nivel de transparencia sin precedentes. Todas las transacciones registradas en la red son visibles para todos los participantes autorizados, lo que significa que puedes ver quién hizo qué en cualquier momento. Esta transparencia no solo promueve la confianza entre los usuarios, sino que también hace que sea fácil detectar cualquier actividad sospechosa.

La descentralización es otro factor importante. En lugar de depender de una sola autoridad central, el blockchain opera en una red descentralizada de computadoras conectadas entre sí. Esto significa que no hay un solo punto de fracaso, lo que hace que la red sea resistente a la manipulación y la censura. Además, al eliminar intermediarios, el blockchain puede acelerar los procesos y reducir los costos, lo que lo convierte en una herramienta invaluable para la eficiencia empresarial.

Y finalmente, el blockchain es un motor de innovación. Su capacidad para tokenizar activos y ejecutar contratos inteligentes programables ha abierto un mundo de posibilidades para nuevas aplicaciones y modelos de negocio. Desde la tokenización de bienes raíces hasta la creación de mercados descentralizados, el blockchain está cambiando la forma en que pensamos sobre la propiedad y el intercambio de valor en el mundo digital.

La historia de Blockchain

La tecnología blockchain, que conocemos hoy en día como una herramienta revolucionaria para la seguridad y la transparencia en las transacciones digitales, tiene sus raíces en el trabajo pionero de los científicos de investigación Stuart Haber y W. Scott Stornetta en 1991. En ese momento, estos visionarios introdujeron una solución computacionalmente práctica para proteger los documentos digitales con sellos de tiempo, garantizando que no pudieran ser modificados ni manipulados.

Este sistema utilizaba una cadena de bloques con seguridad criptográfica para almacenar los documentos con sellos de tiempo, proporcionando así un registro inmutable de la información. Posteriormente, en 1992, se incorporaron los árboles Merkle al diseño, lo que mejoró la eficiencia al permitir que múltiples documentos se agruparan en un solo bloque. Aunque esta tecnología prometedora no se utilizó ampliamente en ese momento y la patente caducó en 2004, sentó las bases para lo que más tarde se convertiría en el blockchain tal como lo conocemos hoy.

Un paso importante en la historia de las criptomonedas llegó en 2004, cuando Hal Finney, un informático y activista criptográfico, introdujo el concepto de Prueba de Trabajo Reutilizable (RPoW). Este sistema resolvió el problema del doble gasto al mantener la propiedad de los tokens registrados en un servidor confiable, permitiendo a los usuarios verificar su exactitud e integridad en tiempo real.

Sin embargo, fue en 2008 cuando el mundo presenció un hito crucial con la aparición de Bitcoin. Bajo el seudónimo de Satoshi Nakamoto, una persona o grupo publicó un libro blanco que presentaba un sistema de efectivo electrónico descentralizado entre pares. Basado en el algoritmo de Prueba de Trabajo de Hashcash, Bitcoin proporcionaba una solución innovadora para la doble protección contra gastos mediante un protocolo descentralizado de igual a igual.

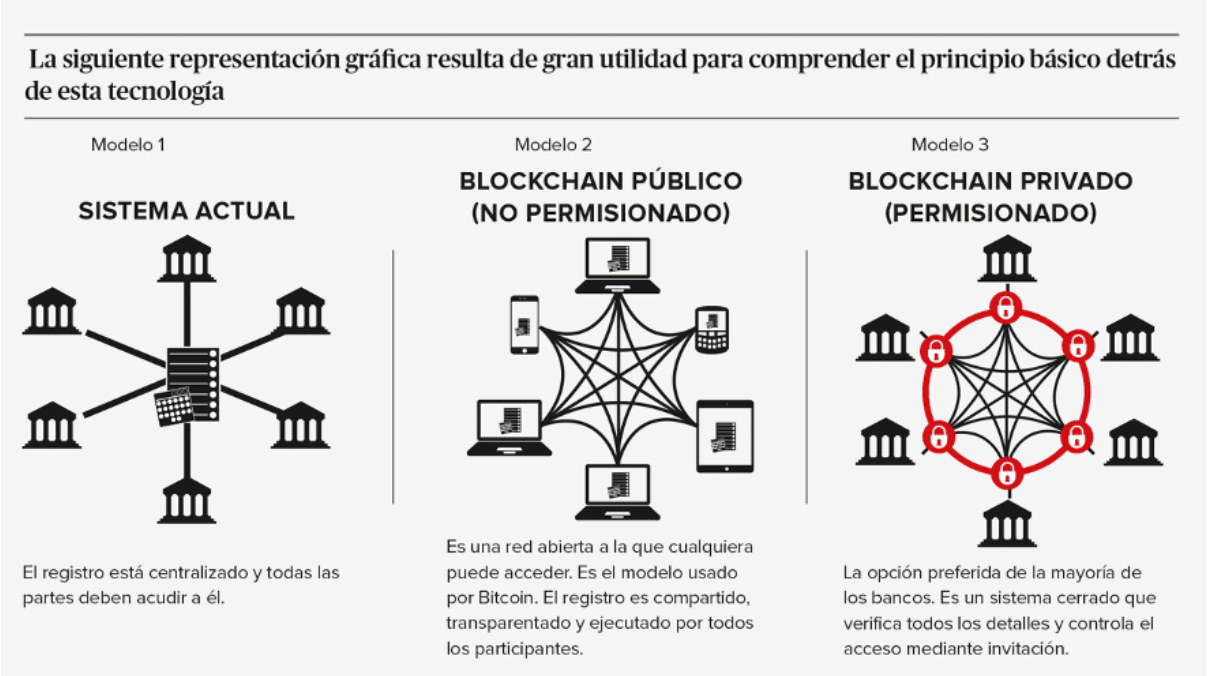
El 3 de enero de 2009, nació oficialmente Bitcoin cuando se minó el primer bloque de bitcoin, con una recompensa de 50 bitcoins. Este evento marcó el comienzo de una nueva era en las finanzas y la tecnología, y el primer receptor de Bitcoin fue Hal Finney, quien recibió 10 bitcoins en la primera transacción de bitcoin del mundo el 12 de enero de 2009.

Más tarde, en 2013, Vitalik Buterin, programador y cofundador de la revista Bitcoin, inició el desarrollo de Ethereum. Reconociendo la necesidad de un lenguaje de scripting para crear aplicaciones descentralizadas en Bitcoin, Vitalik fundó Ethereum, una plataforma de computación distribuida basada en blockchain que presentaba una funcionalidad de scripting conocida como contratos inteligentes.

Estos contratos inteligentes permiten la ejecución de programas o scripts en la cadena de bloques Ethereum, lo que abre un mundo de posibilidades para una amplia gama de aplicaciones descentralizadas. Desde plataformas de redes sociales hasta juegos de azar e intercambios financieros, cientos de aplicaciones descentralizadas se ejecutan en la cadena de bloques Ethereum, utilizando la criptomoneda Ether para pagar las comisiones de la potencia de cálculo utilizada al ejecutar contratos inteligentes.

Tipos de Blockchain

En principio, podemos distinguir tres tipos principales de blockchain: públicas, privadas e híbridas o federadas. Cada una tiene sus características únicas que las hacen adecuadas para diferentes propósitos y necesidades en el mundo digital.



Esta foto de Autor desconocido está bajo licencia CC BY-NC-ND

Blockchain Públicas:

- Son redes abiertas y descentralizadas, donde cualquier persona puede participar en la validación de transacciones y la creación de nuevos bloques.
- Ejemplo: Bitcoin. Cualquier persona puede unirse a la red y convertirse en un minero, contribuyendo así a la seguridad y verificación de transacciones.

Blockchain Privadas:

- Son redes cerradas y controladas por una organización o entidad central.
- Solo las personas autorizadas pueden acceder a la red y validar transacciones.
- Ejemplo: Hyper Ledger Fabric. Utilizado por empresas y organizaciones para gestionar sus transacciones internas de manera más rápida y escalable.

Blockchain Híbridas o Federadas:

- Se generan a partir de la combinación de una blockchain privada y una pública.
- Mantienen una red cerrada con acceso restringido, pero guardan el hash de los bloques en una blockchain pública.
- Proporcionan una capa adicional de seguridad y privacidad.

- Ejemplo: R3 Corda. Utilizado por bancos y empresas financieras para compartir información y validar transacciones de forma segura y confiable.

Es esencial comprender estas diferencias al elegir el tipo de blockchain adecuado para un proyecto específico. Las blockchains públicas son ideales para redes abiertas y descentralizadas, las privadas son más adecuadas para entidades centralizadas que necesitan controlar el acceso, y las híbridas ofrecen una combinación de seguridad y privacidad para diversas aplicaciones empresariales y organizacionales.

Satoshi Nakamoto

Bajo el pseudónimo de Satoshi Nakamoto (サトシ・ナカモト), esta figura misteriosa es el cerebro detrás del desarrollo del protocolo Bitcoin y su software de referencia. En 2008, Nakamoto presentó un artículo en la lista de correo de criptografía, detallando un sistema P2P para el dinero digital, y en 2009 lanzó el software Bitcoin, dando origen a la red y a las primeras unidades de la criptomoneda, los bitcoins.

Aunque Nakamoto colaboró con otros programadores en el proyecto hasta mediados de 2010, su identidad real sigue siendo un enigma. Se estima que las direcciones de Nakamoto contienen alrededor de un millón de bitcoins, pero su verdadera identidad y si el nombre es un seudónimo o representa a una sola persona o a un grupo sigue siendo un misterio.

La especulación sobre quién es realmente Satoshi Nakamoto ha sido un tema de discusión constante desde el lanzamiento del Bitcoin. Se han propuesto varios candidatos, como Wei Dai y Hal Finney, pero ninguno ha sido confirmado como el verdadero Nakamoto. Incluso se ha especulado sobre la nacionalidad de Nakamoto, dado su perfecto uso del inglés y su supuesta residencia en Japón.

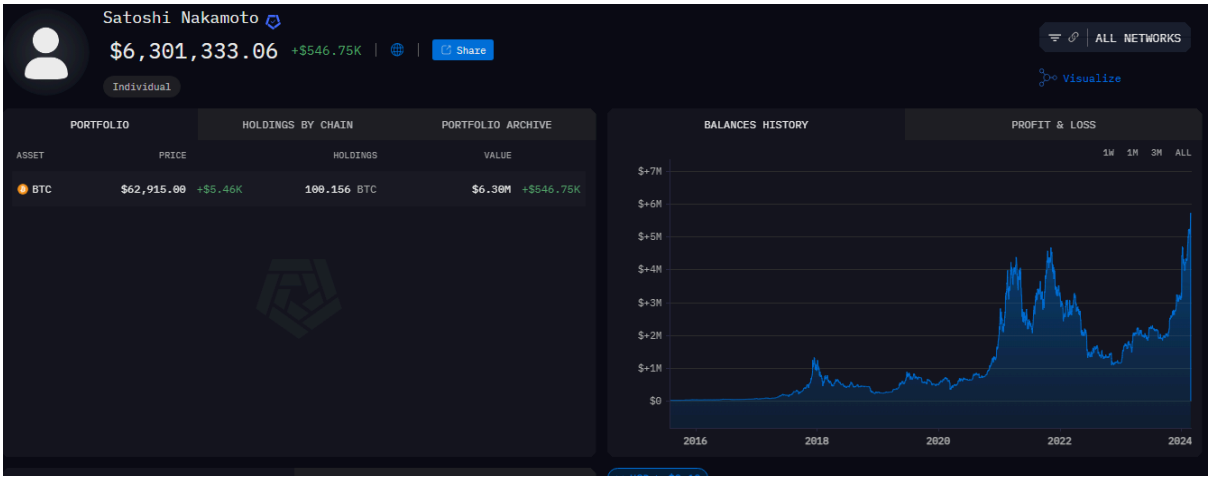
La naturaleza enigmática de Nakamoto ha llevado a una serie de teorías y especulaciones sobre su identidad y motivaciones. Algunos investigadores sugieren que Nakamoto podría ser un genio individual, mientras que otros creen que podría ser un grupo de personas trabajando juntas.

El uso ocasional de ortografía y terminología británica en los mensajes de Nakamoto ha llevado a especulaciones sobre su posible origen en un país de la Commonwealth. Además, el análisis de los patrones de actividad en los foros Bitcoin sugiere que Nakamoto podría estar ubicado en un huso horario que coincide con el meridiano de Greenwich.

En resumen, hablar de Satoshi Nakamoto continúa siendo un enigma pero algo interesante de lo que se puede tomar en cuenta es que el primero en formar parte de Bitcoin después de satoshi fue Hal Finney.

https://twitter.com/halfin/status/1110302988

La cartera digital de Satoshi Nakamoto:



[Satoshi Nakamoto (arkhamintelligence.com)]

¿Qué es el Hash?

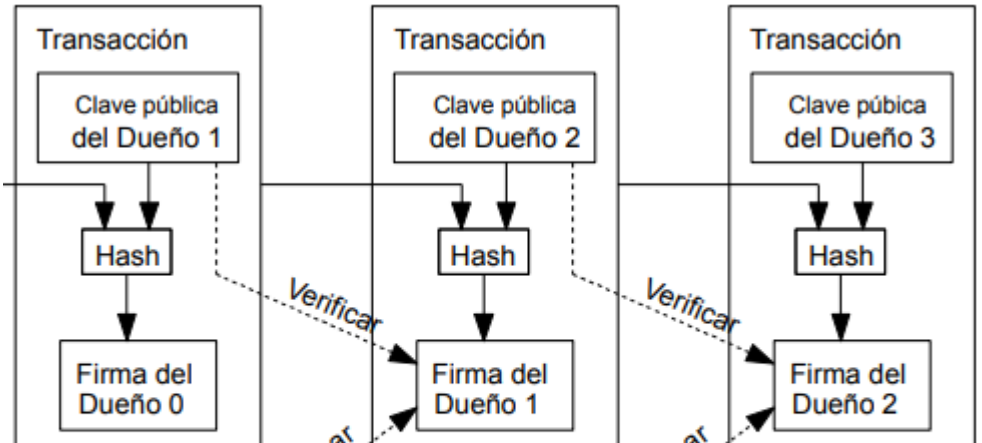
En términos simples, un hash es una función matemática que toma una entrada (también conocida como mensaje o datos) y produce una cadena de caracteres alfanuméricos de longitud fija, que es única para cada entrada. Este proceso de "resumir" los datos en una cadena de caracteres de longitud fija se conoce como "hashing". Es importante destacar que incluso una pequeña modificación en la entrada generará un hash completamente diferente e igualmente es importante destacar que tales funciones no cifran ni descifran mensajes.

Hash 256 y su uso en Blockchain

El algoritmo de hash más comúnmente utilizado en la tecnología blockchain de Bitcoin es el SHA-256 (Secure Hash Algorithm 256 bits). Este algoritmo, como su nombre indica, produce un hash de 256 bits (o 64 caracteres hexadecimales) a partir de los datos de entrada. La robustez y seguridad del SHA-256 lo hacen ideal para su uso en la creación de bloques en la cadena de bloques.

En el contexto de blockchain en Bitcoin, el hash SHA-256 se utiliza para varios propósitos críticos:

1. **Seguridad de la información:** El hash SHA-256 se utiliza para garantizar la integridad de los datos en la blockchain de Bitcoin. Cada bloque en la cadena contiene un hash que representa la totalidad de los datos incluidos en este bloque. Cualquier cambio en los datos del bloque resultará en un hash completamente diferente, lo que alertará a la red sobre cualquier intento de manipulación o alteración de los datos.
2. **Creación de bloques:** En el proceso de minería entraremos más a detalle en los siguientes capítulos pero en formas simples puedes entender que los mineros compiten para resolver complejos problemas matemáticos y encontrar un hash que cumpla con ciertos criterios predefinidos. Este hash, conocido como "hash de bloque", debe comenzar con un número específico de ceros para ser considerado válido. Al encontrar este hash, el minero puede agregar un nuevo bloque a la cadena de bloques y ser recompensado con nuevas unidades de criptomoneda.
3. **Vinculación de bloques:** Cada bloque en la cadena de bloques contiene el hash del bloque anterior en la secuencia. Esto crea una estructura de datos inmutable y secuencial donde cada bloque está vinculado al anterior, lo que dificulta la modificación de los datos almacenados en la cadena. Cualquier cambio en un bloque anterior afectará los hashes de todos los bloques subsiguientes, lo que garantiza la seguridad y la integridad de toda la cadena de bloques.



Sus aplicaciones se han extendido de forma considerable a otros ámbitos relacionados, en general, con la protección de la información y, en particular, para garantizar su integridad. Una función se dice que es una “función unidireccional con trampilla” (TOWF, Trapdoor One-Way Function) si la función definida entre los conjuntos X e Y

$$f : X \to Y, con f(x) = y$$

cumple las siguientes condiciones:

1. f es una función unidireccional, esto es, es fácil, computacionalmente hablando, calcular f(x) = y, para todos los elementos x de X. Además, para la mayor parte de los elementos del conjunto Y que proceden de algún elemento de X es difícil, desde el punto de vista computacional, encontrar algún elemento x de X, para el que f(x) = y.
2. Si se conoce alguna información adicional, denominada “trampilla”, entonces es factible calcular, en un breve periodo de tiempo, un elemento x de X de modo que vaya a parar por f a un elemento y de Y dado.

Estas funciones son fácilmente construibles haciendo uso de herramientas matemáticas relacionadas con la aritmética modular (para una introducción elemental a este tipo de aritmética, puede consultarse Hernández Encinas, 2016), es decir, con una aritmética en la que el resultado final de una operación determinada es el resto que se obtiene una vez hecha la división, entre un número dado, del resultado inicial. El número dado se conoce como “módulo”. En esta aritmética se incluye la expresión (mod n) para indicar el número por el que se hace módulo. Por ejemplo, si se considera como módulo el número entero 13, se tienen los siguientes resultados:

$$8 + 7 = 15 = 13 \cdot 1 + 22(mod 13), 8 \cdot 7 = 56 = 13 \cdot 4 + 44(mod 13)$$

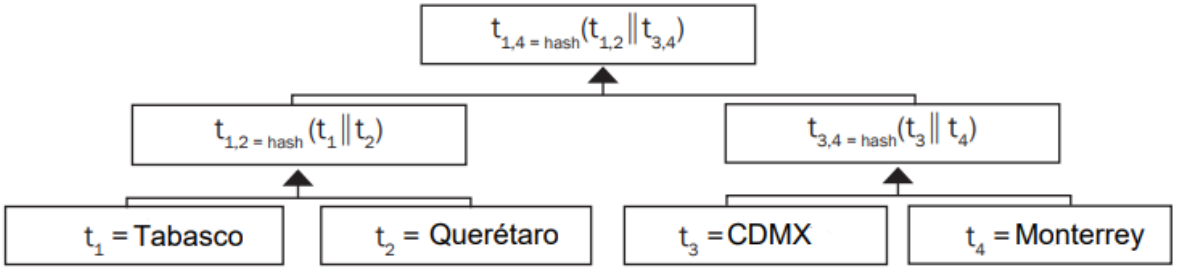
A partir de las funciones unidireccionales se pueden definir directamente las funciones resumen de la siguiente manera: una función resumen o una función hash es una función unidireccional que se aplica a un mensaje dado de tamaño variable, m, perteneciente a un conjunto de mensajes, M, de modo que proporciona un resumen del mismo que tiene un tamaño fijo y predeterminado de bits, sea este tamaño n. Así pues, el resumen o hash de un mensaje de longitud variable es una colección de bits (ceros y unos) de longitud prefijada. Por tanto, se puede considerar que una función resumen, h, está definida de la siguiente manera:

$$h : M \to 0, 1n, conh(m) = m,$$

donde m es una secuencia de ceros y unos.

Árbol de Merkle

Los árboles de Merkle son una forma de organizar estos códigos hash de manera eficiente. En lugar de simplemente agregar los códigos hash uno tras otro, los árboles de Merkle agrupan los códigos hash en una estructura jerárquica. Esto hace que sea más rápido y eficiente verificar la integridad de toda la cadena de bloques.

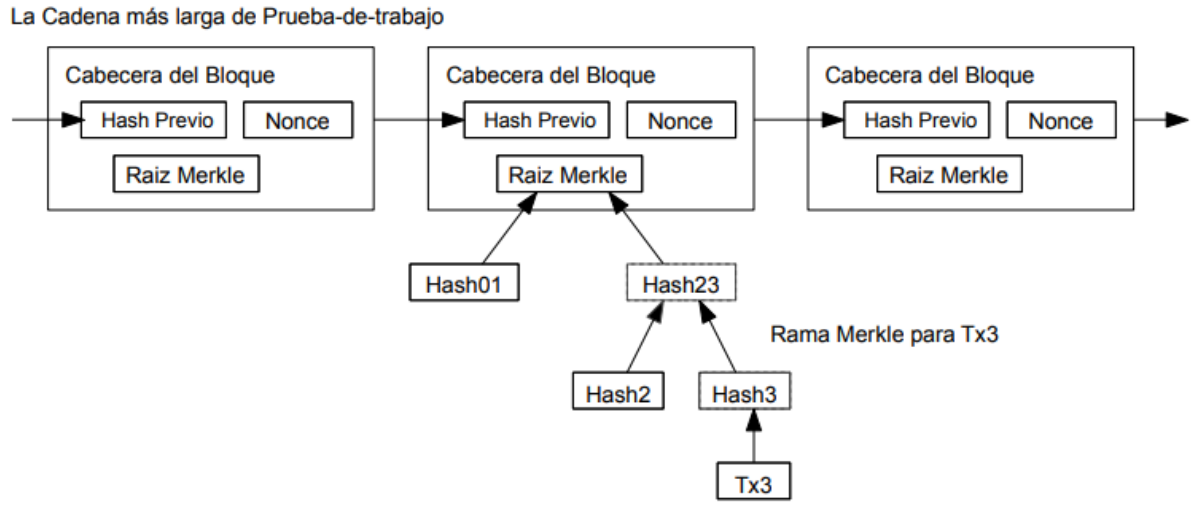


Imagina que tienes una lista de datos, como los nombres de algunos estados, y quieres asegurarte de que nadie los ha alterado. Podrías asignar a cada dato un código único basado en su contenido, como una especie de huella digital. Luego, podrías combinar estos códigos de una manera especial para crear una "huella digital" de toda la lista.

Ahora, en lugar de simplemente juntar todos los códigos en una lista larga, puedes organizarlos en un árbol. En este árbol, los datos originales (llamados "nodos hoja") están en la parte inferior. Luego, cada nivel del árbol combina los códigos hash de los nodos hoja de manera especial para crear códigos hash para los nodos superiores. Este proceso continúa hasta que tienes un solo código hash en la parte superior del árbol, llamado "nodo raíz".

Entonces, si alguien intenta cambiar uno de los datos en la lista, cambiará el código hash del nodo hoja correspondiente. Y como los códigos hash de cada nivel del árbol están basados en los códigos hash de los niveles inferiores, cualquier cambio se propagará hacia arriba en el árbol. Esto significa que el código hash del nodo raíz cambiará, lo que indica claramente que se ha alterado la lista de datos.

Por lo tanto, los árboles de Merkle proporcionan una forma eficiente de verificar la integridad de grandes conjuntos de datos. En una blockchain, se utilizan para crear una estructura de datos que permite verificar rápidamente la integridad de toda la cadena de bloques, lo que garantiza que los datos no hayan sido alterados. Es como tener una especie de "sello de garantía" para cada bloque de datos en la blockchain.


La Cadena más larga de Prueba-de-trabajo
Cabecera del Bloque
Hash Previo
Nonce
Raiz Merkle
Cabecera del Bloque
Hash Previo
Nonce
Raiz Merkle
Cabecera del Bloque
Hash Previo
Nonce
Raiz Merkle
Hash01
Hash23
Rama Merkle para Tx3
Hash2
Hash3
Tx3

Ecuaciones matemáticas

En este fragmento del white paper de Bitcoin escrito por Satoshi Nakamoto, se aborda el escenario en el que un atacante intenta generar una cadena de bloques alternativa más rápido que la cadena principal (o honesta). Aunque un atacante pueda lograr esto, el sistema no se verá comprometido para permitir cambios arbitrarios, como la creación de valor de la nada o la apropiación de dinero que no le pertenece al atacante. Esto se debe a que los nodos de la red no aceptarán transacciones inválidas como pagos, y los nodos honestos rechazará cualquier bloque que las contenga. En otras palabras, un atacante solo puede intentar modificar sus propias transacciones para recuperar dinero que ha gastado recientemente.

Un atacante puede únicamente intentar cambiar solo una de sus propias transacciones para retomar dinero que ha gastado recientemente. La carrera entre una cadena honesta y la cadena de un atacante puede ser caracterizada como una Caminata Aleatoria Binomial. El evento de éxito es la cadena honesta siendo extendida por un bloque, incrementando esta ventaja por +1, y el evento de fracaso es la cadena del atacante siendo extendida por un bloque reduciendo la distancia por -1. La probabilidad de que un atacante pueda alcanzar desde un déficit dado es análogo al problema de la Ruina del Apostador. Supóngase que un apostador con crédito ilimitado empieza en un déficit y juega potencialmente un número infinito de intentos para intentar llegar a un punto de equilibrio. Podemos calcular la probabilidad de que llegase al punto de equilibrio, o que un atacante llegue a alcanzar a la cadena honesta:

p = probabilidad de que un nodo honesto encuentre el próximo bloque

q = probabilidad de que el atacante encuentre el próximo bloque

qz = probabilidad de que el atacante llegue a alcanzar desde z bloques atrás.

$$q_z = \begin{cases} 1 & if\ p \leq q \\ (q/p)^z & if\ p > q \end{cases}$$

Dada nuestra suposición de que la probabilidad de que un nodo honesto encuentre el próximo bloque es mayor que la probabilidad de que el atacante lo haga (p > q), la probabilidad de que el atacante tenga éxito disminuye exponencialmente a medida que el número de bloques que necesita alcanzar aumenta. Con estas probabilidades en su contra, si el atacante no logra una jugada afortunada desde el principio, sus posibilidades se vuelven extremadamente pequeñas a medida que se queda rezagado.

Ahora, veamos cuánto tiempo debe esperar el destinatario de una nueva transacción antes de estar lo suficientemente seguro de que el remitente no puede cambiar la transacción. Supongamos que el remitente es un atacante que quiere hacer creer al destinatario que le

ha pagado durante un tiempo, para luego cambiar la transacción y pagarse a sí mismo después de un tiempo. El destinatario será alertado cuando esto suceda, pero el remitente espera que sea demasiado tarde.

El destinatario genera un nuevo par de claves y entrega la clave pública al remitente poco después de firmar la transacción. Esto evita que el remitente prepare una cadena de bloques de antemano, trabajando continuamente hasta que tenga la suerte de adelantarse lo suficiente, y luego ejecute la transacción en ese momento. Una vez que se envía la transacción, el remitente deshonesto comienza a trabajar en secreto en una cadena paralela que contiene una versión alterna de su transacción.

El destinatario espera a que la transacción se agregue al bloque y z bloques hayan sido enlazados después de la transacción. No necesita saber la cantidad exacta de progreso que ha logrado el atacante, pero asumiendo que los bloques honestos tardan el tiempo esperado promedio por bloque, el progreso potencial del atacante seguirá una distribución de Poisson con un valor esperado.

$$\lambda = z\frac{q}{p}$$

Para calcular la probabilidad de que el atacante aún pueda alcanzar en este momento, multiplicamos la densidad de Poisson por cada cantidad de progreso que podría haber logrado, y luego multiplicamos este resultado por la probabilidad de que pudiera haber alcanzado desde ese punto.

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Re-organizamos para evitar la suma de la cola infinita de la distribución...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Convertimos a código en C:

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

}

Ejecutando algunos resultados, podemos ver que la probabilidad cae exponencialmente con z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Resolvemos para P menor que 0.1%...

```
P < 0.001
q=0.10    z=5
q=0.15    z=8
q=0.20    z=11
q=0.25    z=15
q=0.30    z=24
q=0.35    z=41
q=0.40    z=89
q=0.45    z=340
```

Descentralización

La descentralización es un concepto fundamental en el ámbito de las tecnologías de la información y las finanzas. Se refiere a la distribución del control y la toma de decisiones en un sistema, en lugar de que esté concentrado en una autoridad centralizada. En términos más simples, significa que no hay una sola entidad o individuo que tenga el control absoluto sobre un sistema, sino que dicho control es compartido entre múltiples participantes de manera equitativa.

En el contexto de las criptomonedas y las block chains, la descentralización es una característica clave. En lugar de depender de un banco central o una institución financiera para verificar y registrar las transacciones, las criptomonedas como Bitcoin operan en una red descentralizada de nodos distribuidos en todo el mundo. Cada nodo en la red tiene una copia del libro mayor (ledger) de todas las transacciones, y todas las transacciones deben ser verificadas y consensuadas por la mayoría de los nodos para ser confirmadas y agregadas al libro mayor.

Esta descentralización tiene varias ventajas. En primer lugar, elimina la necesidad de confiar en una sola entidad centralizada, lo que reduce el riesgo de manipulación o censura. Además, al distribuir el control entre múltiples participantes, se mejora la resistencia a la censura y la resiliencia del sistema ante ataques o fallos.

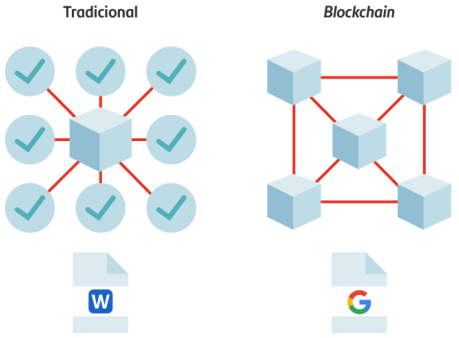
La importancia de la descentralización en Blockchain

La descentralización es un principio fundamental en la tecnología blockchain que desempeña un papel crucial en su funcionamiento y en la provisión de varios beneficios. Te explico algunas razones clave por las que la descentralización es importante en el contexto de las black chains:

1. **Resistencia a la censura:** En un sistema descentralizado, no hay una autoridad central que pueda controlar o censurar la red. Esto significa que no puede haber un único punto de falla que pueda ser atacado o manipulado para detener o controlar la red.
2. **Transparencia:** La naturaleza pública de las black chains descentralizadas permite que cualquier persona acceda y verifique las transacciones registradas en la cadena de bloques. Esto promueve la transparencia y la confianza en el sistema, ya que las transacciones son visibles para todos los participantes.
3. **Inmutabilidad:** En una red descentralizada, una vez que se registra una transacción en la cadena de bloques y se confirma por la mayoría de los nodos de la red, es prácticamente imposible alterar o revertir esa transacción. Esto garantiza la integridad de los registros y protege contra la manipulación de datos.
4. **Autonomía del usuario:** La descentralización empodera a los usuarios al permitirles tener el control directo sobre sus activos y transacciones, sin depender de intermediarios o terceros. Los usuarios pueden realizar transacciones de forma segura y directa sin necesidad de autorización previa.
5. **Eliminación de intermediarios:** Al eliminar intermediarios y terceros de confianza, las blockchains descentralizadas reducen los costos asociados con la intermediación

y eliminan la necesidad de confiar en instituciones centralizadas. Esto puede conducir a una mayor eficiencia y menores tarifas para los usuarios.

6. **Distribución del poder:** En un sistema descentralizado, el poder de tomar decisiones y validar transacciones se distribuye entre todos los participantes de la red, en lugar de estar concentrado en unas pocas entidades. Esto democratiza el proceso de toma de decisiones y evita el control monopolístico.



Mientras que un sistema centralizado ofrece control y eficiencia, también presenta riesgos significativos y limitaciones. Por otro lado, la descentralización en blockchain aborda estos problemas al proporcionar transparencia, seguridad y resistencia a la censura, lo que la convierte en una opción atractiva para una variedad de aplicaciones y sectores.

Dominio público

La cantidad de Bitcoin

Bitcoin, la primera y más famosa criptomoneda, tiene un suministro limitado de 21 millones de monedas. A medida que el tiempo avanza, la cantidad total de bitcoins en circulación aumenta gradualmente a través del proceso de minería, pero eventualmente alcanzará un límite. Actualmente, se estima que se han minado alrededor de 18.8 millones de bitcoins, lo que deja aproximadamente un 11% aún por ser extraído.

El último momento

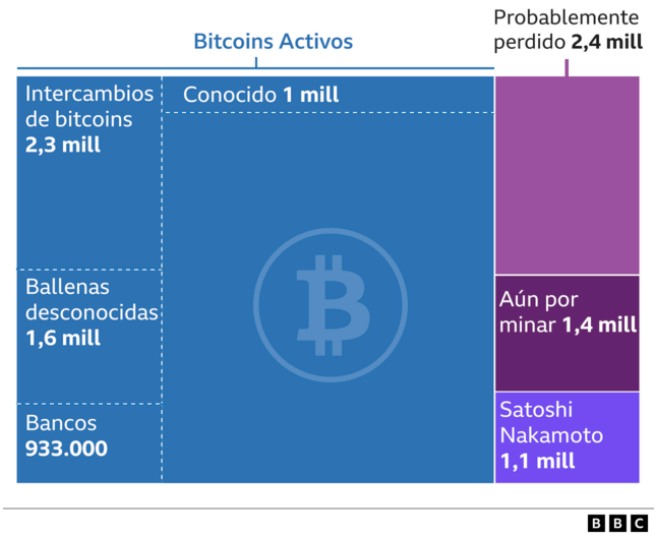
Se prevé que el último bitcoin se mine alrededor del año 2140, un evento que marca un hito en la historia de Bitcoin y que lleva consigo una serie de implicaciones económicas y financieras.

Minería diaria

Cada día, aproximadamente se crean 144 bloques nuevos de Bitcoin, lo que equivale a una recompensa total de 900 bitcoins (actualmente 3,125 bitcoins por bloque 2024). Esta tasa constante de producción disminuye con el tiempo debido a un fenómeno conocido como halving, que reduce a la mitad las recompensas de bloque cada cuatro años.

La búsqueda de bitcoin perdido

Se estima que una cantidad significativa de bitcoins se ha perdido irremediablemente debido a claves privadas perdidas o inaccesibles. Esta pérdida de bitcoins contribuye a la escasez del activo y agrega un elemento de misterio a la economía de Bitcoin.



https://www.bbc.com/mundo/articles/c84jxlxl4k7o

El Papel de las Empresas

Empresas notables como Tesla y MicroStrategy han adquirido grandes cantidades de bitcoins como parte de sus reservas de tesorería. Este movimiento ha legitimado aún más a Bitcoin como un activo financiero y ha llevado a un mayor interés institucional en la criptomoneda.

La Adopción por Parte del Público

La aceptación de Bitcoin como forma de pago ha ido en aumento, con un número creciente de empresas y comerciantes que ahora aceptan la criptomoneda como método de transacción. Este aumento en la adopción ha sido impulsado por la creciente conciencia pública sobre Bitcoin y su utilidad como reserva de valor y medio de intercambio.

El Temor y la Confianza

Sin embargo, a pesar de su creciente popularidad, algunas personas aún sienten temor o desconfianza hacia Bitcoin debido a su volatilidad de precios y su percepción como un activo especulativo. La falta de comprensión sobre cómo funciona Bitcoin y la tecnología blockchain también puede contribuir a estos temores.

El Futuro Brillante:

A pesar de los desafíos y la incertidumbre, el futuro de Bitcoin parece prometedor. Con un suministro limitado, una creciente aceptación global y un interés institucional en aumento, Bitcoin continúa desafiando las normas financieras tradicionales y allanando el camino para una nueva era de la economía digital.

Bitcoin en El Salvador: Una Revolución en Marcha

El Salvador ha captado recientemente la atención mundial al convertirse en el primer país en adoptar oficialmente Bitcoin como moneda de curso legal. Este movimiento audaz, liderado por el presidente Nayib Bukele, ha generado un debate global sobre el futuro del dinero y el papel de las criptomonedas en la economía mundial.

La Adopción Oficial

El 7 de septiembre de 2021, la Asamblea Legislativa de El Salvador aprobó la Ley Bitcoin, que reconoce al Bitcoin como moneda de curso legal en el país. Esto significa que los ciudadanos y las empresas ahora pueden usar Bitcoin para realizar transacciones comerciales y pagar impuestos.

Implicaciones Económicas

La adopción de Bitcoin tiene el potencial de transformar la economía salvadoreña de varias maneras. Se espera que aumente la inclusión financiera al proporcionar acceso a servicios

financieros a personas no bancarizadas. Además, se espera que fomente la innovación tecnológica y atraiga inversión extranjera al país.

Desafíos y Controversias

La decisión de El Salvador de adoptar Bitcoin no ha estado exenta de controversia y desafíos. Algunos críticos argumentan que la volatilidad de Bitcoin podría representar riesgos para la estabilidad económica del país. Además, ha habido preocupaciones sobre la capacidad de infraestructura tecnológica del país para manejar la adopción de Bitcoin a gran escala.

Iniciativas de Implementación

El gobierno de El Salvador ha lanzado una serie de iniciativas para facilitar la adopción de Bitcoin en el país. Esto incluye la instalación de cajeros automáticos de Bitcoin en todo el país, así como el lanzamiento de la aplicación Chivo Wallet, que permite a los ciudadanos almacenar y gastar Bitcoin.

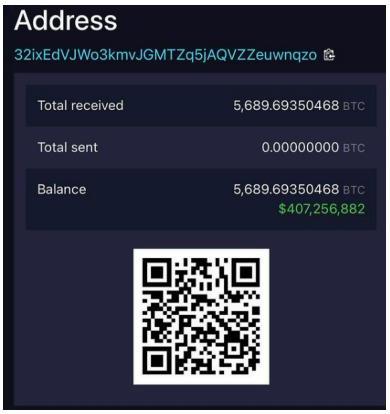
Recepción Pública

La adopción de Bitcoin ha generado una mezcla de entusiasmo y escepticismo entre la población salvadoreña. Si bien algunos ven a Bitcoin como una oportunidad para la inclusión financiera y el empoderamiento económico, otros tienen preocupaciones sobre su estabilidad y seguridad.

El Futuro de Bitcoin en El Salvador

El experimento de Bitcoin en El Salvador está siendo observado de cerca por otros países de todo el mundo. Si tiene éxito, podría allanar el camino para una mayor adopción de Bitcoin y otras criptomonedas a nivel global. Sin embargo, también es un recordatorio de los desafíos y riesgos asociados con la adopción de nuevas tecnologías financieras.

La importancia de que un gobierno sea transparente con los recursos de un país es importante a lo que el Salvador al momento de publicar su cartera digital todas las personas pueden ver cuánto dinero entra a la cuenta del país, cuanto sale y a donde.



Nodos

Los nodos son componentes fundamentales en la red de Bitcoin y otras blockchains. Estos son equipos informáticos que se encargan de mantener una copia completa y actualizada del libro de contabilidad descentralizado de la red, conocido como blockchain. Cada nodo en la red tiene la capacidad de validar y transmitir transacciones, así como de participar en el proceso de consenso para añadir nuevos bloques a la cadena.

Funciones de los Nodos:

1. **Validación de Transacciones:** Los nodos verifican la autenticidad y la validez de cada transacción que se produce en la red. Esto implica verificar que el remitente tenga fondos suficientes para la transacción y que la firma digital asociada sea correcta.
2. **Mantenimiento del Libro Mayor:** Cada nodo almacena una copia completa de la blockchain, que es el registro público de todas las transacciones que han tenido lugar en la red. Esto garantiza que cada nodo tenga acceso a la misma información y que no haya un único punto de fallo en la red.
3. **Participación en el Proceso de Consenso:** Los nodos colaboran en la creación de nuevos bloques para añadirlos a la blockchain. Utilizando un algoritmo de consenso, como Prueba de Trabajo (PoW) en Bitcoin, los nodos compiten por resolver complejos problemas matemáticos para demostrar que han realizado un trabajo computacional válido.
4. **Transmisión de Transacciones y Bloques:** Una vez que se ha verificado una transacción o se ha añadido un nuevo bloque a la cadena, los nodos lo transmiten al resto de la red para su validación y almacenamiento. Esto garantiza que la información se propague de manera eficiente por toda la red.

Tipos de Nodos:

1. **Nodos Completos (Full Nodes):** Son aquellos que almacenan una copia completa de la blockchain y participan en todas las funciones mencionadas anteriormente. Estos nodos son cruciales para la seguridad y la descentralización de la red.
2. **Nodos Ligeros (Lightweight Nodes):** También conocidos como nodos SPV (Simplified Payment Verification), estos nodos no almacenan una copia completa de la blockchain, sino que confían en otros nodos completos para verificar las transacciones. Son más rápidos y requieren menos recursos, pero son menos seguros que los nodos completos.
3. **Nodos Mineros:** Son nodos que participan en el proceso de minería, compitiendo por resolver los complejos problemas matemáticos para añadir nuevos bloques a la blockchain y recibir una recompensa en forma de criptomonedas.

Llaves privadas y públicas

Las claves privadas y públicas son componentes esenciales de la criptografía asimétrica, utilizada en sistemas como Bitcoin y otras criptomonedas. Estas claves forman la base de la seguridad y la autenticación en las transacciones digitales.

Te explico más sobre ellas:

Clave Privada

- **Definición:** La clave privada es una cadena de números y letras generada de manera aleatoria que se utiliza para cifrar y descifrar información en criptografía asimétrica. Es única y debe mantenerse en secreto por su propietario.
- **Función:** La clave privada se utiliza para firmar digitalmente transacciones, lo que garantiza que solo el propietario de esa clave puede autorizar y realizar transacciones en su nombre.
- **Generación:** Se genera a partir de un algoritmo criptográfico seguro y produce una cadena larga de caracteres, generalmente en formato hexadecimal.
- **Seguridad:** Es esencial proteger la clave privada de acceso no autorizado. Se recomienda almacenarla en un lugar seguro, como una cartera digital segura o un dispositivo de hardware dedicado.

Clave Pública

- **Definición:** La clave pública es una derivada matemática de la clave privada y se utiliza para verificar la autenticidad de las firmas digitales generadas con la clave privada correspondiente.
- **Función:** La clave pública se utiliza para cifrar información que solo puede ser descifrada por el propietario de la clave privada correspondiente. También se utiliza para verificar la autenticidad de las firmas digitales generadas con la clave privada.
- **Distribución:** A diferencia de la clave privada, la clave pública se comparte abiertamente y se utiliza para recibir fondos en criptomonedas. Por lo general, se presenta como una dirección pública, que es una cadena de caracteres única a la que se pueden enviar fondos.
- **Relación con la Clave Privada:** La clave pública se deriva de la clave privada a través de operaciones matemáticas criptográficamente seguras, pero no se puede calcular la clave privada a partir de la clave pública.

Seguridad y Criptografía Asimétrica:

La combinación de claves privadas y públicas permite la autenticación y la seguridad en las transacciones digitales. Cuando una transacción se firma digitalmente con una clave privada, la clave pública correspondiente se utiliza para verificar la firma y confirmar que la transacción proviene del propietario legítimo de la clave privada. Esta infraestructura de clave pública también permite la encriptación segura de datos, ya que solo el propietario de la clave privada correspondiente puede descifrar la información cifrada con su clave pública.

Criptomonedas

Las criptomonedas son un fenómeno en constante evolución con una gran diversidad de proyectos y tecnologías subyacentes. Aquí te proporcionaré una visión general de algunas de las principales criptomonedas, sus blockchains asociadas y algunos proyectos destacados:

Bitcoin (BTC):

- **Blockchain:** Bitcoin opera en su propia blockchain, que es la primera y más conocida del mundo. Utiliza un algoritmo de consenso de Prueba de Trabajo (PoW) para validar y asegurar las transacciones.
- **Proyecto Destacado:** Lightning Network, una solución de escalabilidad de capa 2 que permite transacciones de Bitcoin rápidas y de bajo costo fuera de la cadena principal.

Ethereum (ETH):

- **Blockchain:** Ethereum tiene su propia blockchain y es conocido por ser una plataforma que permite la creación de contratos inteligentes y aplicaciones descentralizadas (dApps).
- **Proyecto Destacado:** Ethereum 2.0, una actualización que busca mejorar la escalabilidad, seguridad y sostenibilidad de la red mediante la implementación de la Prueba de Participación (PoS) y la fragmentación.

Binance Coin (BNB):

- **Blockchain:** Binance Coin comenzó como un token en la blockchain de Ethereum, pero luego se trasladó a su propia blockchain llamada Binance Chain.
- **Proyecto Destacado:** Binance Smart Chain, una cadena de bloques paralela a Binance Chain que permite la ejecución de contratos inteligentes y la interoperabilidad con aplicaciones DeFi.

Ripple (XRP):

- **Blockchain:** Ripple utiliza su propia tecnología de consenso conocida como Ripple Protocol Consensus Algorithm (RPCA), pero no es una blockchain pública abierta como Bitcoin o Ethereum.
- **Proyecto Destacado:** RippleNet, una red de pagos globales que facilita transacciones transfronterizas rápidas y de bajo costo entre instituciones financieras.

Cardano (ADA):

- **Blockchain:** Cardano opera en su propia blockchain y se centra en la seguridad y la escalabilidad mediante la implementación de una arquitectura de capas.
- **Proyecto Destacado:** Plutus, un entorno de desarrollo y plataforma para la creación de contratos inteligentes en Cardano.

Polkadot (DOT):

- **Blockchain:** Polkadot es un ecosistema de cadenas de bloques interoperables que se conectan entre sí y con cadenas de bloques externas.
- **Proyecto Destacado:** Parachains, cadenas de bloques personalizadas que se conectan a la red principal de Polkadot y comparten su seguridad.

Solana (SOL):

- **Blockchain:** Solana utiliza su propia blockchain y se destaca por su alta escalabilidad y velocidad de transacción.
- **Proyecto Destacado:** Serum, un exchange descentralizado construido en la red de Solana que ofrece trading rápido y sin custodia.

Minería

La minería de criptomonedas es el proceso mediante el cual se verifica y se asegura la validez de las transacciones en una red blockchain, así como la creación de nuevas unidades de la criptomoneda. Aquí hay una explicación más detallada

Verificación de Transacciones

Cuando se realizan transacciones con criptomonedas, éstas se agrupan en bloques. Los mineros tienen la tarea de verificar la validez de estas transacciones, asegurándose de que el remitente tenga los fondos necesarios y de que la transacción cumpla con las reglas de la red.

Creación de Nuevas Monedas

Además de verificar transacciones, los mineros compiten para resolver un complejo problema matemático que requiere una gran cantidad de poder computacional. El primer minero en encontrar la solución correcta a este problema tiene derecho a agregar un nuevo bloque a la cadena y recibir una recompensa en forma de nuevas unidades de la criptomoneda. Este proceso se conoce como "minería de bloques" y es fundamental para la emisión controlada y descentralizada de nuevas monedas en muchas criptomonedas, como Bitcoin.

Prueba de Trabajo (PoW)

La mayoría de las criptomonedas, incluyendo Bitcoin, utilizan un algoritmo de consenso llamado Prueba de Trabajo (PoW) para la minería. En PoW, los mineros compiten entre sí para resolver el problema matemático mencionado anteriormente, y la dificultad de este problema se ajusta automáticamente para mantener un ritmo constante de creación de bloques.

Consumo de Energía

La minería de criptomonedas requiere una gran cantidad de energía eléctrica debido al intenso poder computacional necesario para resolver los problemas matemáticos. Esto ha llevado a críticas sobre el impacto ambiental de la minería, especialmente cuando se utiliza electricidad generada a partir de fuentes no renovables.

Piscinas de Minería:

Dado que la minería puede ser muy competitiva y requiere una gran inversión en hardware y electricidad, muchos mineros optan por unirse a piscinas de minería. En estas piscinas, varios mineros combinan su poder computacional para aumentar sus posibilidades de resolver el problema matemático y recibir recompensas de forma más regular.

Consolidación de la Minería

Con el tiempo, la minería de criptomonedas ha experimentado una consolidación significativa, con grandes empresas y operaciones de minería a gran escala controlando una parte significativa de la red. Esto ha llevado a preocupaciones sobre la centralización y la descentralización de las redes blockchain.

CPU

En el contexto de la minería de blockchain, el CPU juega un papel importante, aunque su relevancia ha disminuido significativamente en comparación con otros componentes más especializados.

Funcionamiento en Minería

Inicialmente, cuando se lanzaron criptomonedas como Bitcoin, la minería se podía realizar eficazmente utilizando el CPU de una computadora común. Los algoritmos de minería, como el algoritmo de Prueba de Trabajo (PoW) utilizado por Bitcoin, eran lo suficientemente simples como para ser resueltos por el CPU de una manera rentable. Sin embargo, a medida que la popularidad de Bitcoin y otras criptomonedas aumentó, el proceso de minería se volvió más competitivo y los algoritmos de minería se hicieron más complejos.

Evolución de la Minería

Con el tiempo, la minería de criptomonedas ha evolucionado hacia el uso de hardware especializado conocido como ASIC (Circuito Integrado de Aplicación Específica) y GPU (Unidad de Procesamiento Gráfico). Estos dispositivos están diseñados específicamente para realizar operaciones de minería de manera mucho más eficiente que un CPU convencional. Los ASIC, en particular, son extremadamente eficientes en términos de energía y rendimiento para la minería de ciertas criptomonedas.

Impacto en la Vida Útil del Dispositivo

Si bien es posible utilizar un CPU para la minería de criptomonedas, hacerlo puede afectar negativamente la vida útil del dispositivo. La minería de criptomonedas es un proceso intensivo en términos de recursos computacionales y energéticos. Esto puede resultar en un aumento del calor generado por el CPU, lo que puede acortar su vida útil si no se toman medidas adecuadas de enfriamiento y gestión térmica. Además, el uso continuo y exigente del CPU puede provocar un desgaste prematuro de los componentes, lo que también contribuye a una disminución de la vida útil del dispositivo en general.

Rendimiento Relativo

En comparación con ASIC y GPU, los CPU son menos eficientes en términos de rendimiento para la minería de criptomonedas. Esto se debe a que los algoritmos de minería modernos están diseñados para ser resueltos de manera más eficiente por hardware especializado. Como resultado, aunque es posible utilizar un CPU para la minería, es poco probable que genere un retorno significativo de la inversión en comparación con hardware más especializado.

51%

El concepto del "ataque del 51%" es una preocupación fundamental en la seguridad de las blockchains, especialmente en aquellas que utilizan algoritmos de consenso de Prueba de Trabajo (Proof of Work). Se refiere a una situación en la que un solo participante o un grupo de participantes controlan más del 50% del poder de procesamiento de la red. Aquí te explico cómo funciona y por qué es una preocupación.

Control de la mayoría del poder de procesamiento

En una blockchain que utiliza el algoritmo de Prueba de Trabajo, como Bitcoin, los nodos compiten para agregar bloques a la cadena resolviendo problemas criptográficos complejos. El primer nodo en resolver el problema criptográfico es recompensado con la capacidad de agregar el siguiente bloque a la cadena. El poder de procesamiento se mide en términos de la cantidad de cálculos por segundo que un nodo o grupo de nodos puede realizar.

Capacidad para dictar la validez de las transacciones

Si un solo participante o un grupo de participantes controla más del 50% del poder de procesamiento de la red, tienen la capacidad de imponer su voluntad sobre la cadena de bloques. Esto significa que podrían reescribir el historial de transacciones, realizar transacciones fraudulentas o doble gastar criptomonedas.

Doble gasto

Uno de los mayores riesgos asociados con un ataque del 51% es el doble gasto. Esto ocurre cuando un atacante envía una transacción a un destinatario y luego, después de que la transacción ha sido confirmada en la cadena de bloques, revierte la transacción al crear una cadena alternativa que excluye la transacción original. En esencia, el atacante estaría gastando la misma moneda dos veces.

Impacto en la confianza y la integridad de la red

Un ataque del 51% plantea serias preocupaciones sobre la confianza y la integridad de la red. Si los usuarios y los participantes en la red pierden la confianza en la capacidad de la blockchain para validar y proteger las transacciones de manera segura, podría socavar toda la infraestructura y el valor de la criptomoneda asociada.

Medidas de protección

Para prevenir un ataque del 51%, las blockchains implementan una serie de medidas de seguridad, como aumentar el número de confirmaciones requeridas para considerar una transacción como válida, alentar la distribución geográfica de los nodos mineros para evitar

la centralización del poder de procesamiento, y explorar otros algoritmos de consenso que no sean vulnerables a este tipo de ataques.

¿Que es fungible?

"Fungible" es un término que se utiliza para describir un bien o activo que es intercambiable y que puede ser reemplazado por otro del mismo tipo y valor sin afectar su utilidad o calidad. En el contexto financiero y económico, la fungibilidad se refiere a la capacidad de un activo para ser intercambiado por otro activo idéntico sin pérdida de valor o utilidad.

En el mundo de las criptomonedas, como Bitcoin y Ethereum, los tokens nativos suelen ser fungibles. Esto significa que un token de Bitcoin o Ether es completamente intercambiable por otro token del mismo tipo y valor. Por ejemplo, si tienes un Bitcoin, puedes intercambiarlo por otro Bitcoin y no habrá ninguna diferencia en su valor o utilidad.

La fungibilidad es una propiedad importante en las finanzas y el comercio, ya que facilita el intercambio y la transferencia de activos sin complicaciones. Los activos fungibles son altamente líquidos y se pueden utilizar como medio de intercambio en transacciones comerciales diarias. Por otro lado, los activos no fungibles, como obras de arte únicas o bienes raíces, no son intercambiables de la misma manera, ya que cada uno tiene características únicas que los hacen diferentes de otros activos de su tipo.

Nft

Los NFTs (Tokens No Fungibles, por sus siglas en inglés) son activos digitales únicos y no intercambiables que se registran en una blockchain, lo que les confiere autenticidad, propiedad y escasez verificables. A diferencia de las criptomonedas tradicionales como Bitcoin o Ethereum, que son fungibles y pueden intercambiarse entre sí en la misma proporción, los NFTs representan activos digitales únicos, como obras de arte digitales, vídeos, música, memes, artículos de colección, entradas para eventos, bienes virtuales en juegos, entre otros.

La tecnología blockchain permite crear NFTs mediante la emisión de tokens únicos asociados a activos digitales específicos. Cada NFT tiene su propia identidad y características únicas registradas en la blockchain, lo que garantiza su autenticidad, propiedad y trazabilidad. Esta característica de unicidad los hace valiosos para los coleccionistas y aficionados que buscan poseer y comerciar con activos digitales exclusivos.

Los NFTs se han vuelto especialmente populares en el ámbito del arte digital y los juegos en línea, donde los creadores pueden monetizar su trabajo vendiendo ediciones limitadas o únicas a través de mercados NFT. Además, los NFTs pueden contener información adicional sobre el activo, como la historia de su creación, el propietario anterior y su historial de transacciones, lo que aumenta su valor y autenticidad.

Si bien los NFTs han abierto nuevas oportunidades en el mundo digital, también han generado debates sobre cuestiones como la propiedad intelectual, la autenticidad, la especulación y la sostenibilidad energética debido al consumo de energía asociado con algunas blockchains. Sin embargo, su crecimiento continuo demuestra su potencial para transformar la manera en que percibimos, poseemos y comerciamos con activos digitales en el futuro.

Web 3.0

La Web 3.0, también conocida como "Web descentralizada", es la próxima evolución de Internet que busca descentralizar el poder y control de la información, los servicios y las transacciones en línea. A diferencia de la Web 2.0, que se caracteriza por plataformas centralizadas controladas por empresas, la Web 3.0 está impulsada por tecnologías descentralizadas como blockchain, criptomonedas y contratos inteligentes.

La importancia de la Web 3.0 radica en su capacidad para democratizar el acceso a la información y los servicios en línea, así como para brindar mayor seguridad, privacidad y control a los usuarios. Al descentralizar la infraestructura de Internet, la Web 3.0 elimina la necesidad de intermediarios y terceros de confianza, permitiendo a los usuarios interactuar directamente entre sí de forma segura y transparente.

Las criptomonedas y las blockchains juegan un papel fundamental en la Web 3.0 al proporcionar una infraestructura descentralizada para el almacenamiento de datos, la ejecución de contratos inteligentes y la transferencia de valor. Las blockchains permiten la creación de aplicaciones descentralizadas (dApps) que funcionan sin un servidor centralizado, lo que garantiza la resistencia a la censura y la inmutabilidad de los datos.

Además, las criptomonedas se utilizan como medio de intercambio en la Web 3.0, permitiendo transacciones peer-to-peer sin la necesidad de intermediarios financieros. Esto brinda mayor libertad y control sobre los activos digitales, así como la capacidad de realizar transacciones de forma rápida, segura y económica en cualquier parte del mundo.

La Web 3.0 ha experimentado un crecimiento significativo en los últimos años, con el surgimiento de nuevas tecnologías y plataformas descentralizadas que están transformando la forma en que interactuamos en línea. Desde aplicaciones financieras y de intercambio de activos digitales hasta sistemas de votación y redes sociales descentralizadas, la Web 3.0 está impulsando la innovación y la inclusión en Internet.

Metaverso

El término "metaverso" se refiere a un universo virtual en línea tridimensional, interactivo y en constante evolución, donde las personas pueden interactuar entre sí y con el entorno digital de diversas formas. En esencia, el metaverso es una convergencia de mundos virtuales, experiencias de realidad virtual (RV) y aumentada (RA), y entornos digitales compartidos.

En el metaverso, los usuarios pueden crear avatares personalizados que representen su identidad digital y explorar entornos digitales diversos, que van desde ciudades virtuales y mundos fantásticos hasta simulaciones de la vida real. Además de la exploración, el metaverso permite a los usuarios socializar, colaborar, crear y comerciar dentro del entorno digital.

La idea del metaverso ha sido popularizada en la cultura popular, especialmente en la literatura de ciencia ficción y los videojuegos. Ejemplos como "Second Life", "Decentraland" y "Roblox" son plataformas que se asemejan al concepto de metaverso, donde los usuarios pueden construir, interactuar y vivir experiencias digitales compartidas.

El metaverso también está ganando relevancia en sectores como los juegos, el entretenimiento, la educación, el comercio electrónico y la colaboración empresarial. Se vislumbra como un espacio donde las personas pueden trabajar, aprender, jugar y socializar en un entorno digital inmersivo y altamente interactivo.

Tecnologías como la realidad virtual, la realidad aumentada, la inteligencia artificial y las criptomonedas están impulsando el desarrollo del metaverso al permitir experiencias más inmersivas, personalizadas y seguras. Se espera que el metaverso continúe evolucionando y expandiéndose en los próximos años, ofreciendo nuevas oportunidades y desafíos para la sociedad digital.

Transacciones en el metaverso

Las criptomonedas pueden utilizarse como medio de intercambio dentro del metaverso. Los usuarios pueden comprar bienes virtuales, pagar por servicios, realizar transacciones entre pares y participar en economías digitales dentro de los mundos virtuales utilizando criptomonedas. Esto proporciona una forma descentralizada y segura de realizar transacciones en un entorno virtual.

Tokenización de activos virtuales

La tecnología blockchain permite la tokenización de activos virtuales en el metaverso. Esto significa que los bienes digitales, como terrenos virtuales, arte digital, objetos coleccionables y otros activos virtuales, pueden representarse como tokens en una blockchain. Estos tokens pueden ser intercambiados, transferidos y poseídos de manera descentralizada y verificable, lo que brinda a los usuarios mayor propiedad y control sobre sus activos digitales en el metaverso.

NFTs (Tokens No Fungibles)

Los NFTs son activos digitales únicos que se pueden utilizar para representar la propiedad de activos virtuales en el metaverso, como obras de arte digitales, pieles de juegos, parcelas de tierra virtual, entre otros. La tecnología blockchain se utiliza para crear y gestionar estos NFTs, lo que garantiza su autenticidad, escasez y propiedad verificable. Los NFTs permiten a los usuarios poseer y comercializar activos digitales únicos dentro del metaverso.

Gestión de identidad digital

La blockchain puede utilizarse para gestionar la identidad digital de los usuarios en el metaverso de forma segura y descentralizada. Los usuarios pueden tener identidades digitales únicas, verificables y protegidas por blockchain que les permitan acceder a diferentes plataformas, interactuar con otros usuarios y realizar transacciones en el metaverso de manera confiable y segura.

Documentos de riesgo

La tecnología blockchain puede desempeñar un papel importante en la gestión y el almacenamiento de estos documentos de riesgo.

Almacenamiento seguro y distribuido

La blockchain proporciona un método seguro y distribuido para almacenar documentos de riesgo. Los documentos se pueden almacenar en bloques de la cadena de bloques, lo que garantiza que estén protegidos contra alteraciones y accesos no autorizados.

Inmutabilidad

Una vez que un documento de riesgo se ha registrado en la cadena de bloques, no se puede modificar ni eliminar sin dejar un rastro. Esto garantiza la integridad y autenticidad de los documentos almacenados.

Acceso controlado

La blockchain permite establecer permisos de acceso para los documentos de riesgo. Los inversores y otras partes interesadas pueden acceder a los documentos de acuerdo con los permisos establecidos, lo que garantiza la confidencialidad y la privacidad de la información.

Transparencia y trazabilidad

La tecnología blockchain ofrece transparencia y trazabilidad en la gestión de documentos de riesgo. Cada cambio realizado en un documento se registra en la cadena de bloques, lo que permite realizar un seguimiento completo de todas las modificaciones y revisiones.

Automatización de procesos

Mediante el uso de contratos inteligentes, los procesos relacionados con la gestión de documentos de riesgo se pueden automatizar en la blockchain. Por ejemplo, se pueden establecer reglas predefinidas para la distribución de documentos, la notificación de actualizaciones o la verificación de la autenticidad de los documentos.

Interoperabilidad

La blockchain puede facilitar la interoperabilidad entre diferentes sistemas y plataformas utilizados para gestionar documentos de riesgo. Los datos almacenados en la cadena de bloques pueden integrarse fácilmente con otros sistemas, lo que permite un intercambio fluido de información entre las partes interesadas.

Política

Blockchain tiene el potencial de influir significativamente en la política al proporcionar una mayor transparencia, seguridad y eficiencia en varios aspectos del proceso político.

Votación electrónica segura y transparente

La implementación de sistemas de votación electrónica basados en blockchain puede mejorar la seguridad y la integridad de los procesos electorales. Al utilizar una cadena de bloques descentralizada y segura, se pueden prevenir fraudes electorales y garantizar que los votos sean contados de manera precisa y transparente. Cada voto se registra de forma inmutable en la cadena de bloques, lo que permite una verificación transparente por parte de los votantes y las autoridades electorales.

Identificación y verificación de votantes

La tecnología blockchain también puede utilizarse para crear sistemas de identificación digital seguros y verificables para los votantes. Los registros de votantes se pueden almacenar en la cadena de bloques de manera segura, lo que garantiza que solo los votantes autorizados puedan emitir su voto. Esto ayuda a prevenir la suplantación de identidad y otros tipos de fraude electoral.

Auditoría y supervisión de elecciones

La transparencia es fundamental en cualquier proceso electoral. Con blockchain, se pueden realizar auditorías transparentes y verificables de los resultados de las elecciones. Cada voto y cada etapa del proceso electoral se registran en la cadena de bloques, lo que permite a las autoridades electorales y a los observadores independientes verificar la integridad de los resultados.

Participación ciudadana

Blockchain también puede facilitar una mayor participación ciudadana en el proceso político. Mediante la creación de plataformas basadas en blockchain para la participación y el debate público, los ciudadanos pueden tener un mayor acceso a la información y la toma de decisiones política. Esto puede fomentar una mayor transparencia y rendición de cuentas por parte de los funcionarios electos.

Financiamiento electoral transparente

La tecnología blockchain puede utilizarse para rastrear y verificar las donaciones políticas y el financiamiento de campañas de manera transparente. Al registrar todas las transacciones relacionadas con el financiamiento electoral en la cadena de bloques, se puede garantizar

que no haya influencia indebida en el proceso político y que los ciudadanos estén informados sobre quién financia a los candidatos.

Medicina

Blockchain puede tener un impacto significativo en el campo de la medicina al proporcionar una plataforma segura y descentralizada para el almacenamiento y la gestión de datos médicos.

Almacenamiento seguro de datos médicos

Blockchain puede utilizarse para crear registros médicos electrónicos seguros y accesibles. Los pacientes pueden almacenar sus historias clínicas, resultados de pruebas, imágenes médicas y otros datos de salud en la cadena de bloques de manera segura y privada. Esto garantiza que los datos médicos estén protegidos contra la manipulación y el acceso no autorizado, y permite a los pacientes tener un mayor control sobre su información de salud.

Gestión de recetas médicas

Blockchain puede facilitar la gestión segura de recetas médicas electrónicas. Los médicos pueden emitir recetas médicas digitalmente y registrarlas en la cadena de bloques, lo que permite a los pacientes acceder a sus recetas de forma segura desde cualquier lugar. Además, la tecnología blockchain puede rastrear el historial de recetas de los pacientes y prevenir el abuso de sustancias controladas al garantizar que las recetas no se dupliquen ni se utilicen de manera indebida.

Acceso a medicamentos difíciles de conseguir

Blockchain puede facilitar el acceso a medicamentos difíciles de conseguir mediante la creación de plataformas descentralizadas de intercambio y distribución de medicamentos. Los pacientes pueden utilizar blockchain para buscar medicamentos específicos y conectarse con proveedores confiables que puedan proporcionar los medicamentos necesarios de manera segura y legal.

Gestión de ensayos clínicos

La tecnología blockchain puede mejorar la gestión y la transparencia de los ensayos clínicos al garantizar la integridad y la trazabilidad de los datos recopilados durante los ensayos. Los investigadores pueden utilizar blockchain para registrar y auditar de manera segura los datos de los ensayos clínicos, lo que ayuda a prevenir el fraude y la manipulación de los resultados.

Seguimiento de la cadena de suministro de medicamentos

Blockchain puede utilizarse para rastrear la cadena de suministro de medicamentos desde el fabricante hasta el paciente final. Al registrar cada etapa del proceso de fabricación, distribución y venta de medicamentos en la cadena de bloques, es posible garantizar la autenticidad y la calidad de los medicamentos, así como prevenir la falsificación y el comercio ilegal de medicamentos.

Financieras

La tecnología blockchain ofrece numerosas oportunidades para las instituciones financieras y las empresas en el ámbito financiero.

Pagos y transferencias internacionales

La blockchain permite realizar pagos y transferencias de forma más rápida, segura y económica que los métodos tradicionales. Las empresas pueden utilizar la tecnología blockchain para simplificar los procesos de remesas internacionales y reducir los costos asociados con las transferencias de dinero transfronterizas.

Smart contracts y automatización de procesos

Los smart contracts son contratos autoejecutables que se ejecutan automáticamente cuando se cumplen ciertas condiciones predefinidas. Las empresas financieras pueden utilizar smart contracts para automatizar una amplia variedad de procesos, como la liquidación de transacciones, la emisión de préstamos y la gestión de seguros, lo que ayuda a reducir los costos operativos y mejorar la eficiencia.

Crowdfunding y financiación colectiva

La tecnología blockchain facilita el crowdfunding y la financiación colectiva al permitir a las empresas recaudar fondos de manera descentralizada a través de la emisión de tokens digitales. Esto elimina la necesidad de intermediarios financieros y proporciona a las empresas acceso a una base de inversores global.

Gestión de identidad y KYC

La blockchain puede utilizarse para mejorar la gestión de identidad y el cumplimiento de los requisitos de conozca a su cliente (KYC, por sus siglas en inglés). Almacenando de forma segura la información de identidad en la blockchain, las empresas financieras pueden reducir el riesgo de fraude y mejorar la seguridad de los datos de los clientes.

Tokenización de activos

La tokenización de activos implica representar activos físicos o financieros en forma de tokens digitales en la blockchain. Esto permite a las empresas fraccionar la propiedad de activos, como bienes raíces, obras de arte y acciones, y facilita la negociación y transferencia de estos activos de forma más eficiente.

Auditoría y transparencia

La blockchain proporciona un registro inmutable y transparente de todas las transacciones realizadas, lo que facilita la auditoría y garantiza la transparencia en el sistema financiero. Las empresas pueden utilizar la blockchain para mejorar la rendición de cuentas y la integridad de sus operaciones financieras.

Logística

La tecnología blockchain tiene un gran potencial para transformar las operaciones logísticas al ofrecer transparencia, seguridad y eficiencia en la gestión de la cadena de suministro.

Seguimiento de la cadena de suministro

La blockchain proporciona un registro inmutable y transparente de todas las transacciones realizadas a lo largo de la cadena de suministro. Esto permite a las empresas rastrear el movimiento de productos desde su origen hasta su destino final, lo que mejora la visibilidad y la trazabilidad de los productos en toda la cadena de suministro.

Gestión de inventario

La blockchain puede utilizarse para gestionar de manera eficiente el inventario al proporcionar un registro actualizado y preciso de todos los productos y materiales en tránsito. Esto ayuda a reducir los errores y las discrepancias en el inventario, lo que a su vez mejora la planificación y la gestión de la cadena de suministro.

Contratos inteligentes para la logística

Los contratos inteligentes son programas informáticos que se ejecutan automáticamente cuando se cumplen ciertas condiciones predefinidas. En el ámbito logístico, los contratos inteligentes pueden utilizarse para automatizar una variedad de procesos, como la emisión de órdenes de compra, la programación de entregas y el pago de servicios logísticos, lo que ayuda a reducir los costos operativos y mejorar la eficiencia.

Gestión de documentos y aduanas

La blockchain puede utilizarse para gestionar de manera segura y eficiente la documentación asociada con las operaciones logísticas, como facturas, contratos de transporte y documentos de aduanas. Almacenando estos documentos en la blockchain, las empresas pueden reducir los errores y los retrasos en el procesamiento de la documentación, lo que mejora la eficiencia en las operaciones logísticas.

Gestión de la calidad y autenticidad

La blockchain puede utilizarse para verificar la autenticidad y la calidad de los productos a lo largo de la cadena de suministro. Al registrar información detallada sobre el origen, la producción y el transporte de los productos en la blockchain, las empresas pueden garantizar la calidad y la autenticidad de los productos y proporcionar a los consumidores una mayor confianza en los productos que adquieren.

Tokenización en personas

La tokenización de personas es un concepto emergente en el mundo de las finanzas descentralizadas (DeFi) y la blockchain, que permite convertir los derechos de propiedad o participación de una persona en tokens digitales intercambiables en una plataforma blockchain. Aunque este concepto aún está en sus etapas iniciales y plantea desafíos éticos y regulatorios, podría tener aplicaciones interesantes en industrias como el entretenimiento y el deporte.

Tokenización de futbolistas o músicos

En teoría, los futbolistas, músicos u otras personas con una marca personal fuerte podrían ser tokenizados mediante contratos inteligentes en una blockchain. Esto implicaría la emisión de tokens digitales que representan una participación en los ingresos futuros generados por la persona tokenizada. Por ejemplo, un músico podría tokenizar y los inversores que compren sus tokens podrían recibir una parte de los ingresos generados por la venta de su música, conciertos, merchandising, etc.

Al momento de empezar su carrera las personas que vean un potencial en él pueden decidir invertir en él de cierta forma por así llamarlo, invertir en su tokenización y de esta forma el “músico” al iniciar su carrera con los ingresos podría permitirle darle una ventaja para poder mejorar su calidad adquiriendo diferentes herramientas, después cuando el músico haya alcanzado mas fama las personas con tokens iniciales podrían venderlos para recibir un % de ganancia e incluso al momento de la transacción el músico podría ganar igualmente una %.

Igualmente podrían las personas recibir un cierto % de las ventas totales del músico dividió entre los que tienen tokens del músico que ayudaron en un inicio.

Inversión en talento emergente

La tokenización de personas también podría facilitar la inversión en talento emergente. Por ejemplo, un cantante prometedor podría tokenizar y ofrecer una parte de sus futuros ingresos a los inversores que compren sus tokens. Si el cantante se vuelve exitoso en el futuro, los inversores podrían recibir dividendos o regalías en función del rendimiento de su carrera.

Facilitación del financiamiento

La tokenización de personas podría proporcionar una nueva vía para que los talentos emergentes obtengan financiamiento para desarrollar sus carreras. En lugar de depender exclusivamente de discográficas, agencias deportivas u otras entidades tradicionales, los artistas podrían recurrir a la financiación descentralizada a través de la emisión de tokens.

Desafíos regulatorios y éticos

Sin embargo, la tokenización de personas plantea varios desafíos regulatorios y éticos. Por ejemplo, podría haber preocupaciones sobre la protección de los derechos de imagen y privacidad de las personas tokenizadas, así como sobre la posibilidad de que los inversores exploten a los talentos emergentes. Además, la regulación en torno a la tokenización de personas varía según el país y aún no está completamente definida.

Monetización

La monetización en el contexto de blockchain y criptomonedas se refiere al proceso de convertir activos digitales, como tokens o criptomonedas, en valor tangible o dinero real.

Comercio y especulación

El comercio de criptomonedas es una actividad popular donde los inversores compran y venden activos digitales en diferentes plataformas de intercambio. Estos inversores buscan aprovechar las fluctuaciones en los precios del mercado para obtener ganancias. Por ejemplo, un inversor puede comprar Bitcoin a un precio relativamente bajo y venderlo cuando su valor aumenta, obteniendo así una ganancia en la diferencia de precios. Esta actividad puede realizarse en intercambios centralizados o descentralizados, y se puede realizar tanto en el corto como en el largo plazo.

Minería de criptomonedas

La minería de criptomonedas implica utilizar poder computacional para validar y asegurar transacciones en una blockchain. Los mineros compiten para resolver complejos problemas matemáticos, y el primero en encontrar la solución valida y agrega un nuevo bloque a la cadena recibe una recompensa en forma de nuevas criptomonedas. Esta actividad puede ser rentable, pero requiere hardware especializado y consume mucha energía. La rentabilidad de la minería depende del costo de la electricidad, la dificultad de la red y el precio de las criptomonedas.

Staking

El staking es un proceso mediante el cual los usuarios bloquean una cierta cantidad de criptomonedas en una cartera digital para respaldar la seguridad y la operación de una blockchain. A cambio de este compromiso, los usuarios pueden recibir recompensas en forma de nuevas criptomonedas o tarifas de transacción. El staking es una forma de participar en la validación de transacciones y asegurar la red, y puede generar ingresos pasivos para los usuarios que participan en él.

Recompensas por participación en protocolos DeFi

En el ámbito de las finanzas descentralizadas (DeFi), los usuarios pueden obtener ingresos al participar en diversos protocolos. Por ejemplo, pueden proporcionar liquidez a pools de liquidez, participar en préstamos o préstamos de criptomonedas, o realizar actividades de arbitraje. A cambio de su participación, los usuarios pueden recibir recompensas en forma de intereses, tarifas de transacción o tokens de gobernanza.

Crear y vender tokens

Los proyectos y empresas pueden monetizar blockchain emitiendo sus propios tokens y vendiéndolos a inversores interesados. Estos tokens pueden representar diversos activos, derechos o utilidades dentro de la red del proyecto. Por ejemplo, una empresa puede emitir tokens que representen acciones de la empresa, derechos de voto en decisiones de gobernanza o acceso a servicios específicos. Los inversores pueden comprar estos tokens durante una oferta inicial de monedas (ICO) o en intercambios de criptomonedas posteriores.

NFTs (Tokens no fungibles)

Los NFTs permiten la monetización de activos digitales únicos, como arte digital, música, videos, juegos y otros activos digitales coleccionables. Los creadores pueden tokenizar estos activos y venderlos en mercados de NFTs, donde los compradores pueden adquirirlos como inversiones o para coleccionar. Los NFTs son únicos e indivisibles, lo que les otorga un valor especial y exclusivo en el mercado.

Especulación

La especulación en el contexto de las criptomonedas se refiere a la práctica de comprar y vender activos digitales con la intención de obtener ganancias a corto plazo mediante la explotación de las fluctuaciones en los precios del mercado. Los especuladores no están necesariamente interesados en el valor intrínseco o en el uso práctico de una criptomoneda, sino en capitalizar las oportunidades de ganancias que ofrece el mercado.

La especulación en criptomonedas funciona de manera similar a la especulación en otros mercados financieros, como el mercado de valores o el mercado de divisas. Los especuladores intentan predecir las futuras tendencias de precios de las criptomonedas y toman decisiones de compra o venta en función de esas predicciones. Utilizan análisis técnico, análisis fundamental y otros métodos para evaluar el mercado y tomar decisiones de inversión.

Sin embargo, la especulación en criptomonedas conlleva ciertas desventajas y riesgos:

Volatilidad extrema

El mercado de criptomonedas es conocido por su alta volatilidad, lo que significa que los precios pueden experimentar cambios significativos en períodos cortos de tiempo. Esta volatilidad puede resultar en ganancias sustanciales, pero también puede llevar a pérdidas significativas para los especuladores.

Manipulación del mercado

Dado que el mercado de criptomonedas aún es relativamente joven y menos regulado que otros mercados financieros, está más expuesto a la manipulación y actividades fraudulentas. Los especuladores deben tener cuidado con las prácticas de manipulación del mercado, como las bombas y vertidos, que pueden influir artificialmente en los precios de las criptomonedas.

- Las "bombas y vertidos" son prácticas fraudulentas en el mercado de criptomonedas donde un grupo de individuos coordina la compra masiva de una criptomoneda de bajo valor para inflar artificialmente su precio (bomba), y luego venden rápidamente sus activos a precios más altos, dejando a los inversores menos informados con pérdidas significativas (vertido). Estas acciones pueden ser manipulativas y perjudiciales para los inversores desprevenidos.

Riesgos de seguridad

La especulación en criptomonedas a menudo implica el uso de intercambios y plataformas de comercio en línea, que pueden ser vulnerables a hackeos y ciberataques. Los

especuladores deben tomar medidas para proteger sus activos y asegurarse de utilizar plataformas de comercio confiables y seguras.

Falta de regulación

La falta de regulación en el mercado de criptomonedas puede hacer que sea más susceptible a la manipulación y a las actividades fraudulentas. Los especuladores deben ser conscientes de los riesgos asociados con la falta de protecciones regulatorias y tener en cuenta que pueden no tener los mismos derechos y protecciones que en otros mercados financieros más tradicionales.

Bitcoin vs Ethereum

Bitcoin y Ethereum son dos de las criptomonedas más importantes y reconocidas en el mercado, cada una con sus propias características, usos y ecosistemas.

Historia

- **Bitcoin:** Fue creado en 2008 por una persona o grupo de personas bajo el seudónimo de Satoshi Nakamoto. El objetivo principal de Bitcoin era crear un sistema de efectivo digital descentralizado que permitiera transacciones peer-to-peer sin la necesidad de intermediarios.
- **Ethereum:** Fue propuesto por Vitalik Buterin en 2013 y posteriormente desarrollado por un equipo de desarrolladores. Ethereum se creó con el objetivo de ofrecer una plataforma para la ejecución de contratos inteligentes y aplicaciones descentralizadas (dApps) mediante el uso de la tecnología blockchain.

Blockchain

- **Bitcoin:** Utiliza una blockchain que se centra principalmente en la transferencia de valor (criptomoneda) a través de transacciones peer-to-peer. Es una red descentralizada que registra las transacciones en bloques enlazados de manera inmutable.
- **Ethereum:** También utiliza una blockchain descentralizada, pero su enfoque va más allá de las transacciones de valor. Ethereum permite la ejecución de contratos inteligentes, que son programas informáticos autónomos que operan en la blockchain y pueden automatizar procesos financieros y legales.

Monetización

- **Bitcoin:** Es considerado como una reserva de valor digital, similar al oro digital. Muchos inversores lo ven como un activo seguro para proteger su riqueza contra la inflación y la volatilidad del mercado.
- **Ethereum:** Además de servir como una criptomoneda (Ether), Ethereum permite la creación de tokens personalizados a través de contratos inteligentes. Estos tokens pueden representar activos digitales, participaciones en empresas, derechos de voto y más.

Mercado y Adopción

- **Bitcoin:** Es la criptomoneda más antigua y ampliamente adoptada. Muchas instituciones financieras, empresas y particulares lo consideran como una reserva de valor confiable y una forma de inversión.
- **Ethereum:** Es la segunda criptomoneda más grande por capitalización de mercado y ha ganado popularidad principalmente debido a su capacidad para ejecutar

contratos inteligentes y dApps. Ethereum también ha sido utilizado para financiar proyectos a través de las Ofertas Iniciales de Moneda (ICO).

Ventajas y Desventajas

- **Bitcoin:**
    - **Ventajas:** Es la criptomoneda más establecida y ampliamente aceptada. Tiene una comunidad fuerte y lealtad de los inversores. Su simplicidad y seguridad son altamente valoradas.
    - **Desventajas:** La escalabilidad es un problema persistente. Las transacciones pueden ser lentas y costosas en períodos de alta demanda. La funcionalidad limitada más allá de las transferencias de valor.
- **Ethereum:**
    - **Ventajas:** Ofrece más funcionalidades que Bitcoin, incluida la ejecución de contratos inteligentes y dApps. Su blockchain es más flexible y puede adaptarse a una variedad de casos de uso.
    - **Desventajas:** La escalabilidad también es un desafío para Ethereum. La complejidad de los contratos inteligentes puede llevar a errores y vulnerabilidades de seguridad.

Despliegue y Versiones

Bitcoin

Bitcoin ha experimentado varias actualizaciones y mejoras a lo largo de los años, aunque ha sido más conservador en términos de cambios en su protocolo base en comparación con algunas otras criptomonedas. Algunas de las actualizaciones más significativas de Bitcoin incluyen:

SegWit (Segregated Witness)

Activado en agosto de 2017, SegWit fue una actualización que modificó la estructura de datos de las transacciones de Bitcoin para permitir una mayor capacidad de la red y solucionar problemas de escalabilidad. También proporcionó una solución parcial al problema del aumento de las tarifas de transacción y la congestión de la red.

Taproot

Activado en noviembre de 2021, Taproot fue una actualización importante diseñada para mejorar la privacidad, la escalabilidad y la flexibilidad de Bitcoin. Introdujo una nueva forma de firmas digitales llamada Schnorr, que permite a los usuarios combinar varias firmas en una sola, lo que ayuda a reducir el tamaño de las transacciones y mejorar la eficiencia de la red.

Actualizaciones de Consenso

A lo largo de los años, ha habido varias actualizaciones de consenso en el protocolo de Bitcoin para corregir errores, mejorar la seguridad y hacer ajustes en la dificultad minera, el tamaño de bloque y otros parámetros. Estas actualizaciones suelen implementarse mediante un proceso de bifurcación dura (hard fork) o un soft fork.

Ethereum

Ha pasado por varias actualizaciones importantes, incluida la transición de Ethereum 1.0 a Ethereum 2.0, que busca abordar los problemas de escalabilidad y eficiencia de su blockchain.

Lanzamiento de Ethereum

30 de julio de 2015.

Homestead

14 de marzo de 2016. Esta actualización marcó la transición de Ethereum desde una versión beta hacia una red más estable y segura.

Byzantium y Constantinople

Ambas actualizaciones se implementaron en octubre de 2017 y febrero de 2019, respectivamente. Introdujeron mejoras en la seguridad, la eficiencia y la escalabilidad de la red.

Istanbul

Implementada en dos partes en diciembre de 2019 y abril de 2020, esta actualización incluyó mejoras en la interoperabilidad, la resistencia a los ataques DoS y la optimización de los costos de transacción.

Berlín

Lanzada en abril de 2021, la actualización de Berlín introdujo mejoras en el gas y el rendimiento de la red, así como correcciones de errores.

London

Implementada en agosto de 2021, la actualización de Londres incluyó la EIP-1559, que modificó la estructura de las tarifas de transacción y quemó parte de las tarifas para reducir el suministro de ETH.

¿Somos el producto?

La idea de que "somos el producto" se refiere a la noción de que, en algunos casos, los usuarios de ciertos servicios en línea son el verdadero foco de monetización de una plataforma. Esta idea se popularizó especialmente con redes sociales como Facebook, donde los usuarios no pagan directamente por usar la plataforma, pero sus datos y actividades en línea se utilizan para generar ingresos a través de la publicidad dirigida.

En el caso de Facebook y otras plataformas de redes sociales, los usuarios son el producto en el sentido de que sus datos personales, comportamientos en línea, intereses y preferencias se recopilan y se utilizan para dirigir anuncios específicos y personalizados. A través de algoritmos sofisticados, estas plataformas pueden segmentar a los usuarios en audiencias específicas, lo que permite a los anunciantes llegar a las personas más propensas a estar interesadas en sus productos o servicios.

Esta situación plantea varias cuestiones éticas y de privacidad. Por un lado, permite una experiencia más personalizada para los usuarios al mostrarles contenido relevante. Por otro lado, también plantea preocupaciones sobre la privacidad de los datos y el potencial abuso de poder por parte de las plataformas en línea.

En comparación, en otros modelos de negocio donde los usuarios pagan directamente por un servicio, como en el caso de Netflix o Spotify, los usuarios son clientes en lugar de ser el producto. Pagan una tarifa por acceder al contenido o servicio sin que sus datos se utilicen para publicidad dirigida.

En el contexto de blockchain y las criptomonedas, la idea de "ser el producto" es diferente en comparación con plataformas como Facebook. En lugar de que los usuarios sean el producto cuyos datos se monetizan, en blockchain y las criptomonedas, los usuarios son más bien participantes activos en la red.

En blockchain, los usuarios contribuyen al funcionamiento de la red al realizar transacciones, validar bloques o ejecutar contratos inteligentes, dependiendo del protocolo específico. A cambio de su participación, pueden recibir recompensas en forma de tokens o criptomonedas.

En este sentido, los usuarios no son el producto en el mismo sentido que en las redes sociales tradicionales. En lugar de ser explotados para la generación de ingresos, los usuarios de blockchain y criptomonedas son una parte integral del ecosistema y pueden beneficiarse directamente de su participación en la red.

Sin embargo, es importante tener en cuenta que en algunos casos, especialmente en proyectos de criptomonedas que se basan en modelos de financiación mediante tokens, los inversores pueden ser vistos como el "producto" en el sentido de que su participación en la red puede aumentar el valor de los tokens o criptomonedas asociados. En este caso, los proyectos de criptomonedas pueden depender del interés de los inversores para aumentar su valor y financiar el desarrollo del proyecto.

Glosario

1. **Blockchain**: Una cadena de bloques es una estructura de datos que registra información de manera permanente y verificable. Cada bloque en la cadena contiene un conjunto de transacciones confirmadas y está enlazado con el bloque anterior, formando una cadena inmutable.
2. **Bitcoin**: La primera y más conocida criptomoneda, creada por una persona o grupo de personas bajo el pseudónimo de Satoshi Nakamoto. Bitcoin se basa en tecnología blockchain y se utiliza como una forma de dinero digital descentralizado.
3. **Criptomoneda**: Una moneda digital descentralizada que utiliza criptografía para asegurar y verificar transacciones y para controlar la creación de nuevas unidades. Bitcoin, Ethereum y Litecoin son ejemplos de criptomonedas.
4. **Criptografía**: La práctica y el estudio de técnicas para asegurar la comunicación y la información mediante la utilización de códigos. En blockchain, la criptografía se utiliza para garantizar la seguridad y la integridad de las transacciones.
5. **Minería**: El proceso de validar y confirmar transacciones en una red blockchain, generalmente mediante la resolución de complejos problemas matemáticos. Los mineros son recompensados con nuevas criptomonedas por su trabajo.
6. **Moneda digital**: Una forma de moneda que existe únicamente en formato electrónico, sin una forma física. Las criptomonedas son un tipo de moneda digital.
7. **Wallet (Cartera)**: Un software o dispositivo que permite a los usuarios almacenar, enviar y recibir criptomonedas. Las carteras pueden ser en línea, de hardware, de papel o móviles.
8. **Dirección**: Una secuencia única de caracteres alfanuméricos que se utiliza para identificar una cuenta en una red blockchain. Las direcciones se utilizan para enviar y recibir criptomonedas.
9. **Transacción**: El acto de enviar o recibir criptomonedas en una red blockchain. Una transacción incluye información sobre el remitente, el destinatario y la cantidad de criptomonedas transferidas.
10. **Contrato inteligente**: Un código informático autónomo que se ejecuta automáticamente cuando se cumplen ciertas condiciones predefinidas. Los contratos inteligentes se utilizan en blockchain para automatizar y hacer cumplir acuerdos digitales.
11. **Descentralización**: El principio de distribuir el control y la autoridad entre múltiples participantes en lugar de depender de una autoridad centralizada. En blockchain, la descentralización se refiere a la ausencia de una autoridad central que controle la red.
12. **Consenso**: El proceso mediante el cual los participantes en una red blockchain llegan a un acuerdo sobre el estado de la red y la validez de las transacciones. El consenso es fundamental para la seguridad y la integridad de la red.
13. **Hash**: Valor único generado por una función hash, utilizado para identificar de forma única datos en una red blockchain.
14. **Nodo**: Punto de conexión en una red blockchain que mantiene una copia completa del libro mayor y participa en la validación y propagación de transacciones.

15. **Consenso de prueba de trabajo (PoW)**: Algoritmo de consenso utilizado en algunas blockchains donde los nodos compiten para resolver problemas computacionales y validar transacciones.
16. **Consensus de prueba de participación (PoS)**: Algoritmo de consenso en el que los participantes que tienen una participación en la criptomoneda pueden validar bloques de transacciones en proporción a su propiedad.
17. **Hard Fork**: Actualización en el protocolo de una blockchain que no es compatible con versiones anteriores, lo que puede resultar en la creación de una nueva cadena de bloques.
18. **Soft Fork**: Actualización en el protocolo de una blockchain que es compatible con versiones anteriores, lo que no resulta en la creación de una nueva cadena de bloques.
19. **Recompensa de bloque**: Cantidad de criptomonedas otorgadas a los mineros por validar y agregar un nuevo bloque a la cadena.
20. **Altcoin**: Cualquier criptomoneda que no sea Bitcoin.
21. **ICO (Oferta Inicial de Monedas)**: Método de recaudación de fondos en el que una empresa emite tokens digitales a cambio de criptomonedas más establecidas.
22. **DApp (Aplicación descentralizada)**: Aplicación que se ejecuta en una red descentralizada de blockchain y no está controlada por una sola entidad.
23. **Fork**: División en la cadena de bloques, que puede ser temporal o permanente, que resulta en dos versiones diferentes de la cadena de bloques.
24. **Tokenización**: Proceso de convertir activos físicos o virtuales en tokens digitales en una blockchain.
25. **Exchange**: Plataforma en línea donde los usuarios pueden comprar, vender y negociar criptomonedas y otros activos digitales.
26. **DeFi (Finanzas Descentralizadas)**: Sistema financiero que opera en una red blockchain y no depende de intermediarios tradicionales como bancos.
27. **Oráculo**: Servicio o fuente de datos externos que proporciona información a una blockchain para ejecutar contratos inteligentes o tomar decisiones.
28. **Gas**: Una unidad de medida utilizada para calcular el costo de las transacciones en una red blockchain, especialmente en Ethereum.
29. **Bloque Génesis**: El primer bloque en una cadena de bloques, que establece el comienzo de la red.
30. **Algoritmo de consenso**: Un conjunto de reglas que determina cómo se alcanza el acuerdo entre los nodos de una red blockchain sobre el estado de la red y qué transacciones son válidas.
31. **Prueba de Autoridad (PoA)**: Un algoritmo de consenso en el que la validación de los bloques se realiza por un grupo selecto de nodos autorizados.
32. **Prueba de Espacio y Tiempo (PoST)**: Un algoritmo de consenso que requiere que los nodos demuestren que han reservado una cantidad específica de espacio de almacenamiento durante un período de tiempo determinado.
33. **Prueba de Participación Agrupada (PoSP)**: Un algoritmo de consenso que combina la prueba de participación (PoS) con la agrupación de recursos para mejorar la eficiencia y la equidad en la validación de bloques.
34. **Contrato inteligente**: Un programa informático autoejecutable que se ejecuta en una blockchain cuando se cumplen ciertas condiciones predefinidas.
35. **Token no fungible (NFT)**: Un tipo especial de token criptográfico que representa la propiedad única o la autenticidad de un activo digital o físico.

36. **Criptografía asimétrica**: Un sistema de cifrado que utiliza dos claves diferentes (pública y privada) para cifrar y descifrar datos.
37. **Criptografía de curva elíptica**: Un tipo de criptografía que utiliza curvas elípticas sobre campos finitos para proporcionar seguridad en las operaciones criptográficas.
38. **Proof of Burn (PoB)**: Un algoritmo de consenso en el que los participantes queman (destruyen) una cierta cantidad de criptomonedas para demostrar su compromiso con la red.
39. **Proof of Authority (PoA)**: Un algoritmo de consenso en el que la validación de los bloques se realiza por nodos con autoridad reconocida en la red.
40. **Staking**: El proceso de bloquear una cierta cantidad de criptomonedas en una red blockchain para participar en la validación de bloques y recibir recompensas.
41. **Tokenización**: El proceso de convertir activos físicos o virtuales en tokens digitales en una blockchain, lo que facilita su intercambio y transferencia.
42. **DAO (Organización Autónoma Descentralizada)**: Una entidad autónoma y descentralizada que opera de acuerdo con un conjunto de reglas codificadas en un contrato inteligente.
43. **Oráculo**: Un servicio o entidad que proporciona datos externos a un contrato inteligente en una blockchain, permitiendo que el contrato tome decisiones basadas en información del mundo real.
44. **Ataque del 51%**: Un escenario en el que un único actor o grupo de actores controla más del 50% del poder de procesamiento de una red blockchain, lo que les permite tomar el control y manipular la red.
45. **Hard Fork (Bifurcación Dura)**: Una actualización del protocolo de una blockchain que introduce cambios significativos y no compatibles con versiones anteriores, lo que resulta en dos cadenas separadas.
46. **Soft Fork (Bifurcación Suave)**: Una actualización del protocolo de una blockchain que introduce cambios compatibles con versiones anteriores, lo que no genera una división en la cadena de bloques.
47. **Minería en la nube**: El proceso de extraer criptomonedas utilizando recursos informáticos remotos, en lugar de hardware minero físico.
48. **Ataque de doble gasto**: Un escenario en el que un usuario gasta las mismas monedas digitales dos veces, aprovechando una laguna en el sistema de confirmación de transacciones.
49. **Ethereum Virtual Machine (EVM)**: Una máquina virtual Turing completa que ejecuta contratos inteligentes en la red Ethereum.
50. **Gas Limit (Límite de Gas)**: El límite máximo de unidades de gas que un usuario está dispuesto a gastar en una transacción en la red Ethereum.
51. **Gas Price (Precio del Gas)**: La tarifa en Ether que un usuario está dispuesto a pagar por cada unidad de gas utilizada en una transacción en la red Ethereum.
52. **Prueba de Trabajo (PoW)**: Un algoritmo de consenso en el que los participantes deben demostrar que han realizado un trabajo computacionalmente costoso para validar transacciones y crear nuevos bloques en la cadena de bloques.
53. **Prueba de Participación (PoS)**: Un algoritmo de consenso en el que los participantes pueden validar bloques y recibir recompensas en proporción a la cantidad de criptomonedas que poseen y están dispuestos a "apostar" en la red.
54. **DEX (Intercambio Descentralizado)**: Una plataforma de intercambio de criptomonedas que opera sin una autoridad centralizada, permitiendo a los usuarios intercambiar activos directamente entre sí.

55. **Fungible**: Se refiere a un activo o token que es intercambiable y no tiene características únicas que lo distingan de otros tokens del mismo tipo. Por ejemplo, la moneda fiduciaria como el dólar es fungible, ya que un billete de $10 es igual a otro billete de $10.
56. **NFT (Tokens No Fungibles)**: Son tokens digitales únicos que representan la propiedad o la autenticidad de un activo digital o físico. Los NFTs se utilizan principalmente en el arte digital, los videojuegos y la música para certificar la propiedad y la rareza de los activos.
57. **Smart Contracts (Contratos Inteligentes)**: Son programas informáticos autoejecutables que se ejecutan en una blockchain y automatizan la ejecución de acuerdos digitales sin necesidad de intermediarios. Los contratos inteligentes están escritos en lenguajes de programación específicos y se ejecutan automáticamente cuando se cumplen las condiciones predefinidas.
58. **Web 3.0**: Se refiere a una visión de internet descentralizada en la que los usuarios tienen mayor control sobre sus datos y transacciones. La Web 3.0 utiliza tecnologías como blockchain, contratos inteligentes y protocolos descentralizados para crear un internet más seguro, transparente y resistente a la censura.
59. **Metaverso**: Es un espacio virtual tridimensional generado por computadora en el que los usuarios pueden interactuar entre sí y con objetos digitales. El metaverso está siendo explorado como un nuevo paradigma para la interacción social, los juegos en línea y la economía digital.
60. **Documentos de Riesgo**: Son documentos que describen los riesgos asociados con una inversión o actividad específica. En el contexto de blockchain, los documentos de riesgo pueden incluir advertencias sobre la volatilidad del mercado de criptomonedas, los riesgos de seguridad y los posibles problemas regulatorios.
61. **Tokenización de Personas**: Es el proceso de convertir la identidad, habilidades o activos de una persona en tokens digitales en una blockchain. Esto permite a las personas monetizar sus habilidades y activos digitales, como la música, el arte o la influencia en las redes sociales.
62. **Monetización**: Es el proceso de generar ingresos a partir de activos digitales o servicios en línea. En el contexto de blockchain y criptomonedas, la monetización puede incluir la creación y venta de tokens, la participación en programas de recompensas y la generación de ingresos a través de contratos inteligentes.
63. **Especulación**: Se refiere a la compra y venta de activos con el objetivo de obtener ganancias a partir de los cambios en su valor. En el mundo de las criptomonedas, la especulación es común debido a la volatilidad del mercado y la posibilidad de obtener rendimientos significativos en un corto período de tiempo.
64. **Bombas y Vertidos**: Se refiere a estrategias fraudulentas utilizadas para manipular el precio de una criptomoneda. Una "bomba" implica la compra masiva de una criptomoneda para inflar su precio, mientras que un "vertido" implica vender repentinamente grandes cantidades de la criptomoneda para provocar una caída en su precio.

Bibliografía

101 Blockchains. (2024, 14 marzo). *Blockchain, Web3 & AI Courses and Certifications - 101 Blockchains*. https://101blockchains.com/

Academy, B. (2023, 17 agosto). *La historia de blockchain*. Binance Academy. https://academy.binance.com/es/articles/history-of-blockchain

Arroyo Guardeño, D., Díaz Vico, J., & Hernández Encinas, L. (2019). *Que sabemos de blockchain* (Versión 1) [Software]. https://climberstrading.com/wp-content/uploads/2022/09/Que-sabemos-de-Blockchain.pdf

Blockchain, S. (2023, 3 noviembre). *Los 3 principales tipos de redes Blockchain - Hypernifty Academy*. Observatorio Blockchain. https://observatorioblockchain.com/hypernifty/redes-blockchain-tipos/

None. (2023, 11 julio). *¿Qué es "blockchain"?* https://www.santander.com/es/stories/blockchain-que-es

¿Qué es blockchain? - IBM Blockchain | IBM. (s. f.). https://www.ibm.com/mx-es/topics/blockchain

¿Qué es la tecnología de blockchain? | SAP. (s. f.). SAP. https://www.sap.com/latinamerica/products/artificial-intelligence/what-is-blockchain.html

Agradecimientos

Únicos agradecimientos a mi madre Ingrid Anaid que siempre me ha apoyado en todos mis proyectos y locuras que se me ocurren.

- Cristopher Pereyra Andrade 16/03/2024 7:40 P.M.

Dejo mis redes en caso de que necesites contactarme

Instagram: https://www.instagram.com/el_cointor/

Facebook: www.facebook.com/dev.tiburino

Linkedin: www.linkedin.com/in/cointor/

Donaciones

Si gustas dejarme alguna donación te dejo formas de hacerlo.

Para donaciones de Ethereum ETH:

0xEd6610bBB22216348d413573a8E82117BB6CA5f0