**Taller sobre tecnología Blockchain**

**Jorge Miller Gutierrez Ospina**

**ANALISIS Y DESARROLLO DE SOFTWARE – 2721520**

**Instructor**

**Ivan Leonardo Medina Gomez**

**SENA**

**Septiembre 2024**

**Tecnología Blockchain: Fundamentos, Objetivos y Aplicaciones**

**Premisa**

La tecnología Blockchain ha emergido como una innovación revolucionaria que ha transformado la manera en que se conciben las transacciones y la seguridad en entornos digitales. Su capacidad para proporcionar un registro descentralizado, inmutable y transparente ha generado un gran impacto en diversos sectores, desde las criptomonedas hasta aplicaciones industriales y gubernamentales. En este texto argumentativo se examinarán los conceptos y características clave de la Blockchain, su relación con la criptografía y el hashing, sus antecedentes y objetivos, así como sus aplicaciones más relevantes.

**¿En qué consiste la tecnología Blockchain?**

Blockchain es una tecnología de registro distribuido que permite llevar un control de transacciones de manera segura y transparente sin necesidad de una autoridad central. Esta tecnología consiste en una cadena de bloques que contienen información sobre transacciones, asegurada mediante criptografía. Cada bloque en la cadena contiene un conjunto de transacciones y está vinculado al bloque anterior mediante un valor hash, lo que asegura su inmutabilidad y dificulta la alteración de la información registrada. La principal característica de Blockchain es su descentralización, ya que los registros son mantenidos por una red de nodos que verifican y validan cada transacción.

**Objetivos de la tecnología Blockchain**

El principal objetivo de Blockchain es proporcionar una plataforma segura, transparente y confiable para realizar transacciones. Entre sus objetivos específicos se destacan:

1. Descentralización: Eliminar la necesidad de intermediarios centralizados como bancos o instituciones financieras, lo que reduce los costos y tiempos de transacción.

2. Seguridad: Garantizar que los datos registrados en la cadena de bloques sean inmutables y no puedan ser alterados sin consenso.

3. Transparencia: Permitir a todas las partes involucradas acceder a un registro compartido que contiene el historial completo de transacciones.

4. Confianza: Fomentar un entorno confiable donde las partes puedan realizar transacciones directas sin depender de terceros para validar la información.

**Antecedentes de la tecnología Blockchain**

Blockchain fue propuesto por primera vez en 2008 por el seudónimo Satoshi Nakamoto como la tecnología subyacente de la criptomoneda Bitcoin. La idea principal era crear un sistema de efectivo electrónico descentralizado, en respuesta a la crisis financiera de 2008, que eliminara la necesidad de instituciones financieras para validar transacciones. La primera implementación de Blockchain fue en 2009 con el lanzamiento de Bitcoin. Desde entonces, Blockchain ha evolucionado y se ha aplicado a diversos campos, incluyendo finanzas, cadenas de suministro, votación electrónica, y más.

**Criptografía en Blockchain**

La criptografía juega un papel fundamental en Blockchain, ya que asegura que los datos y transacciones sean confidenciales y estén protegidos de manipulaciones. Utiliza claves criptográficas para garantizar que solo los propietarios legítimos puedan acceder y realizar transacciones. Además, el uso de firmas digitales asegura que las transacciones no puedan ser modificadas una vez validadas. En Blockchain, se emplean principalmente algoritmos criptográficos asimétricos, como RSA o ECC, que utilizan una clave pública y una clave privada para firmar y verificar transacciones.

**El hash en Blockchain**

El “hash” es un elemento clave en Blockchain que asegura la integridad de los datos. Un hash es el resultado de una función criptográfica que toma una entrada (datos de una transacción) y genera una cadena única de longitud fija. En Blockchain, cada bloque tiene un hash que lo identifica de forma única y lo vincula al bloque anterior. Si alguna información en el bloque es modificada, el hash también cambia, lo que rompe la cadena y alerta a la red sobre una posible alteración. Los algoritmos de hash más comunes en Blockchain incluyen SHA-256, utilizado en Bitcoin.

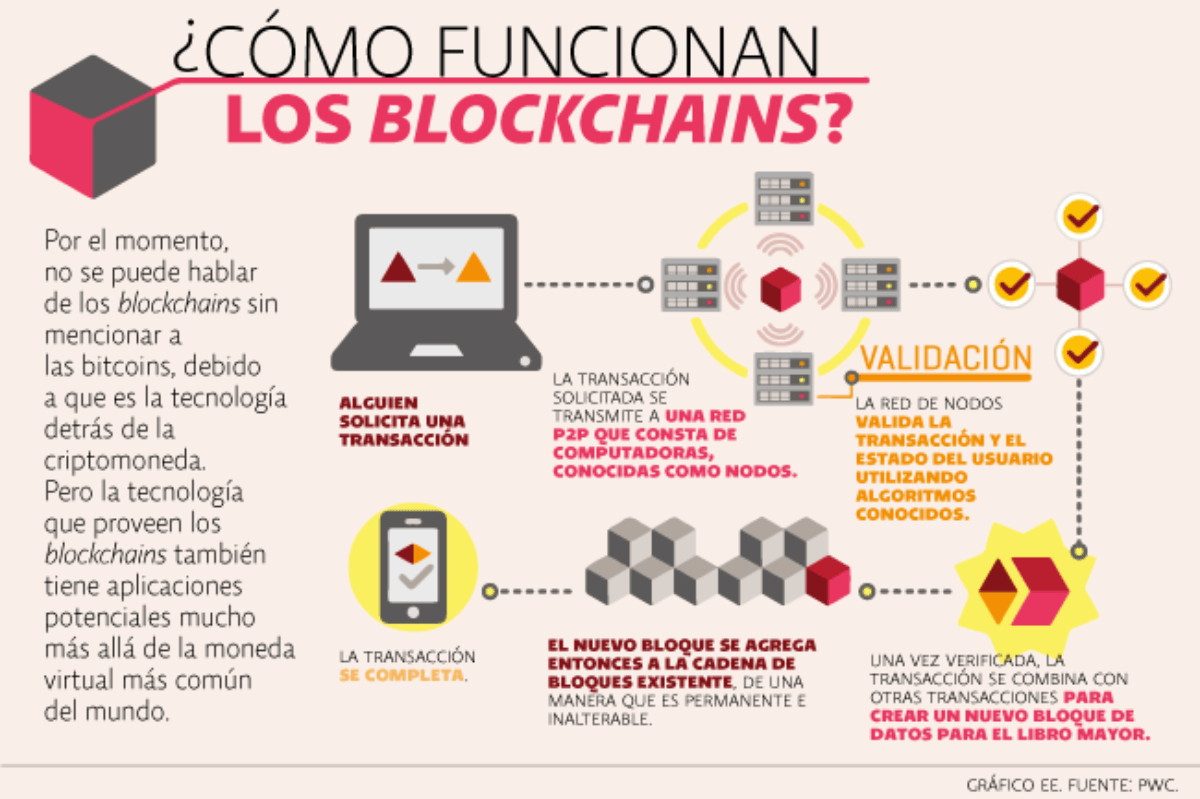
**Bloques en la cadena de bloques**

Un “bloque” en Blockchain es una estructura de datos que almacena un conjunto de transacciones. Cada bloque contiene tres elementos principales: el conjunto de transacciones, el hash del bloque anterior y un valor llamado "nonce", que se utiliza para generar un hash válido en el proceso de minería. El bloque también incluye una marca de tiempo que indica cuándo fue creado. Los bloques están diseñados para ser inmutables, lo que significa que una vez que se ha añadido un bloque a la cadena, no puede ser modificado sin consenso de la red.

**Relación entre los bloques en una cadena de bloques**

Los bloques en Blockchain están relacionados entre sí a través del hash del bloque anterior. Esto crea una cadena lineal donde cada bloque depende del anterior. Si se intenta modificar un bloque anterior, el hash cambia, lo que invalida todos los bloques subsiguientes. Esta estructura de cadena asegura la inmutabilidad de los datos y protege la red de intentos de alteración o fraude. Además, el mecanismo de consenso utilizado por la red (como Proof of Work o Proof of Stake) asegura que las transacciones sean validadas de manera distribuida antes de ser añadidas a la cadena.

**Gráfico de una red Blockchain**



**Aplicaciones y productos de la tecnología Blockchain**

Blockchain ha sido implementada en diversas industrias para crear productos y servicios que aprovechan sus características de seguridad y descentralización. Algunos ejemplos son:

1. Criptomonedas: La más conocida es Bitcoin, pero también existen Ethereum, Litecoin, Ripple, entre otras.

2. Contratos inteligentes: Ethereum permite la creación de contratos autoejecutables que se activan cuando se cumplen ciertas condiciones.

3. Cadenas de suministro: Empresas como IBM y Walmart utilizan Blockchain para rastrear productos desde su origen hasta el consumidor final.

4. Votación electrónica: Se están desarrollando plataformas que permiten votar de manera segura y anónima en elecciones utilizando Blockchain.

**¿Qué es una criptomoneda?**

Una “criptomoneda” es una forma de dinero digital que utiliza criptografía para asegurar las transacciones y controlar la creación de nuevas unidades. Bitcoin fue la primera criptomoneda en ser creada, pero hoy en día existen miles de criptomonedas en el mercado. Las criptomonedas permiten transacciones descentralizadas sin necesidad de intermediarios, lo que las hace atractivas para transferencias internacionales y pagos en línea.

**Minería de criptomonedas**

La “minería de criptomonedas” es el proceso mediante el cual se validan y añaden nuevas transacciones a la cadena de bloques. En el caso de Bitcoin, la minería implica la resolución de complejos problemas matemáticos utilizando poder computacional. Los mineros compiten para resolver estos problemas y, una vez resueltos, pueden añadir un nuevo bloque a la cadena y recibir una recompensa en forma de criptomonedas recién creadas. Este proceso también ayuda a asegurar la red, ya que valida las transacciones y previene el doble gasto.

**Conclusión**

Blockchain es una tecnología disruptiva que tiene el potencial de transformar múltiples industrias al ofrecer un sistema seguro, descentralizado y transparente para realizar transacciones. Su uso de criptografía y hash asegura la integridad de los datos, mientras que la estructura de bloques interconectados evita la manipulación de la información. Las criptomonedas y la minería son aplicaciones directas de esta tecnología, pero su potencial se extiende mucho más allá, con aplicaciones en cadenas de suministro, contratos inteligentes y votación electrónica. A medida que Blockchain continúa evolucionando, es probable que su adopción siga creciendo en diferentes sectores.