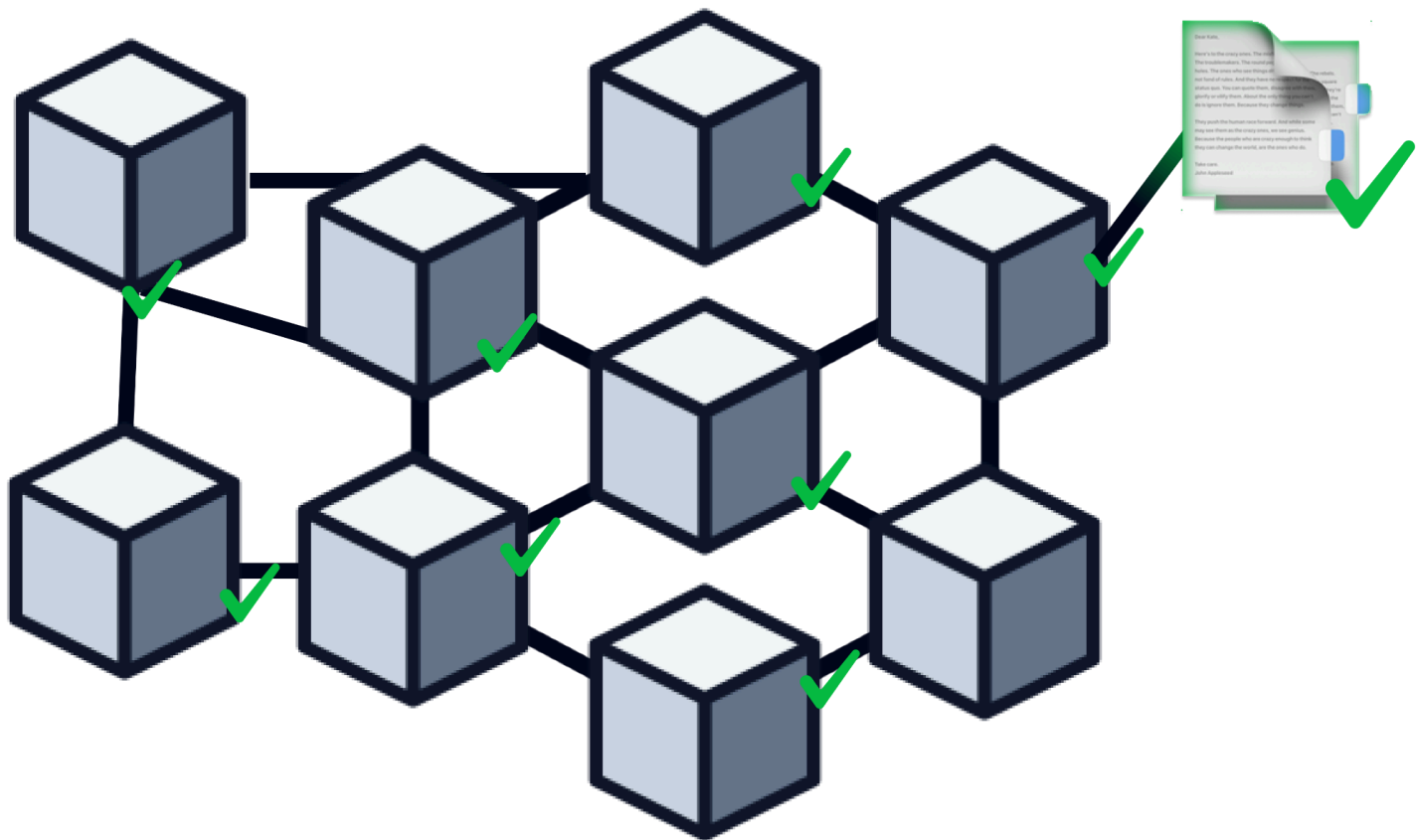


BLOCKCHAIN



Agustín Benítez López
Marcos García Jiménez
Daniel Gómez Ortiz

ÍNDICE

→  Introducción general

→  Aplicaciones actuales

→ Ventajas  y  desventajas

→  Desafíos y riesgos 

→  Tendencias futuras

→  Bibliografía y Webgrafía 



Introducción general

Blockchain es una tecnología de almacenamiento de información en una estructura **descentralizada y segura**.

¿Cómo funciona Blockchain?

Funciona de la siguiente forma: tenemos una base de datos, esa base de datos está dividida por bloques, estos bloques no están centralizados, están distribuidos entre una gran gama de ordenadores, estando duplicados y relacionados entre sí. La principal función es cuando queremos modificar información, para modificar información necesitaremos que todos los bloques distribuidos acepten la modificación, esto añade una capa de seguridad total entre la red, necesitando la aprobación de todos para hacer un cambio.

Si nos adentramos en su funcionamiento, cada bloque almacenará un hash o código único, este código único lo compartirá con el siguiente bloque de la cadena, este bloque lo hará consecutivamente. Esto formará una cadena de bloques "blockchain" .

¿Qué es un Hash?

Es una cadena de texto que representa una ID, hacer cambios en este hash modificara por completo su significado.

¿Cómo funciona su sistema de seguridad?

Su sistema de seguridad se basará en comprobar la información con el bloque de la cadena anterior y confirmar el cambio.

El resultado, un sistema Blockchain, un sistema complejo de usar y de entender pero muy seguro a largo plazo para cualquier tipo de tarea.



Aplicaciones actuales

Hoy en día se utiliza la blockchain en el ámbito de las **Criptomonedas, Contratos inteligentes, Identidad digital**, etc.

Hablaré específicamente del papel que tiene la blockchain en las **Criptomonedas**. Pasos:

1.Creación de la Transacción:

- Un usuario inicia una transacción enviando una cantidad de criptomonedas a otro usuario. Esta transacción incluye las direcciones de las billeteras (wallets) del remitente y del destinatario, así como la cantidad transferida.
- **Ejemplo:** Juan quiere enviar 2 Bitcoins a María.

2.Transmisión a la Red:

- La transacción es transmitida a una red de nodos (computadoras) distribuidos por todo el mundo. Cada nodo contiene una copia de la blockchain y participa en la validación de las transacciones.
- **Ejemplo:** La transacción de Juan se envía a la red de Bitcoin.

3.Validación de la Transacción:

- Los nodos verifican la autenticidad de la transacción. Para ello, se aseguran de que Juan tenga suficientes Bitcoins para realizar la transferencia y que no esté intentando gastar la misma cantidad dos veces (problema de doble gasto).
- **Ejemplo:** Los nodos verifican que la billetera de Juan tiene al menos 2 Bitcoins y que no ha gastado esos Bitcoins en otra transacción.

4.Agrupación en un Bloque:

- Una vez verificada, la transacción se agrupa con otras transacciones recientes en un bloque. Este bloque aún no está confirmado.
- **Ejemplo:** La transacción de Juan se agrupa con otras transacciones en un nuevo bloque en la red de Bitcoin.

5.Prueba de Trabajo (Proof of Work):

- Los nodos compiten para resolver un complejo problema matemático. El primer nodo en resolver el problema añade el nuevo bloque a la blockchain y recibe una recompensa en criptomonedas (minería).
- **Ejemplo:** Un nodo resuelve el problema y añade el bloque con la transacción de Juan a la blockchain de Bitcoin.

6.Confirmación y Añadido a la Blockchain:



- Una vez resuelto el problema, el nuevo bloque se añade a la cadena de bloques existente. Todas las copias de la blockchain en la red se actualizan para incluir el nuevo bloque.
- **Ejemplo:** El bloque que contiene la transacción de Juan se añade a la blockchain de Bitcoin, y todas las copias de la blockchain se actualizan.

7. Transacción Completa:

- La transacción está ahora confirmada y registrada en la blockchain. El destinatario (María) puede ver que ha recibido los Bitcoins, y el saldo de la billetera del remitente (Juan) se actualiza.
- **Ejemplo:** María recibe 2 Bitcoins en su billetera, y el saldo de la billetera de Juan se reduce en 2 Bitcoins.



Ventajas y desventajas

Ventajas

- Alta seguridad:** Posee una gran seguridad ante los datos y accesos.
- Cero redundancia:** Se tienen muchas capas para evitar la redundancia de datos.
- Invulnerable a ataques:** Invulnerable a una gran parte de tipos de ataque (menos a ataques estilo Fishing).
- Estandarización del sistema:** Todos los nodos del sistema siguen el mismo protocolo siempre y cuando sean de la misma blockchain.
- Transparencia y trazabilidad:** Las transacciones en **blockchain** son públicas (dependiendo del tipo de blockchain).
- Integración con IoT (Internet Of Things):** Permite registrar datos en tiempo real de dispositivos conectados, garantizando su autenticidad.
- Acceso global:** Permite la participación de usuarios desde cualquier lugar del mundo, siempre que tengan acceso a internet.
- Confianza en entornos sin intermediarios:** Reduce la necesidad de intermediarios (bancos, notarios, etc.), lo que puede disminuir costes y tiempos de operación.

desventajas

- Consumo enorme de energía:** Estos sistemas consumen grandes cantidades de energía.
- Ingente cantidad de Servidores:** Necesidad de muchos servidores distribuidos.
- Altos costes de transacción:** Las Blockchains congestionadas pueden generar tarifas muy altas para procesar transacciones.
- Falta de interoperabilidad:** Aún no existe un estándar universal que permite que diferentes Blockchains trabajen juntas.
- Complejidad de implementación:** Requiere conocimientos especializados para desarrollar e integrar soluciones basadas en blockchain.



Desafíos y riesgos

Desafíos Técnicos

- **Escalabilidad:** La capacidad de procesar un gran volumen de transacciones de manera rápida y eficiente sigue siendo un desafío.
 - Posibles soluciones:
 - **Sharding:** Dividir la blockchain en fragmentos más pequeños para procesar transacciones en paralelo.
 - **Rollups:** Agrupar múltiples transacciones en una sola para reducir el tamaño de los bloques.
- **Consumo energético:** Algunos algoritmos de consenso, como el Prueba de Trabajo, consumen una gran cantidad de energía.
 - Posibles soluciones:
 - **Prueba de estaca:** Utilizar algoritmos de consenso que no requieran una gran cantidad de energía computacional.
 - **Hardware más eficiente:** Desarrollar hardware especializado para la minería de criptomonedas.

Riesgos de Seguridad

- **Vulnerabilidades:** Los contratos inteligentes, si no están bien diseñados, pueden contener vulnerabilidades que pueden ser explotadas por atacantes.
 - Posibles soluciones:
 - **Auditorías de contratos inteligentes:** Revisar cuidadosamente el código de los contratos inteligentes antes de su despliegue.
- **Pérdida de claves:** La pérdida de las claves privadas puede resultar en la pérdida irrecuperable de los fondos.
 - Posibles soluciones:
 - **Seguros:** Protegerse contra pérdidas financieras mediante seguros especializados.

Desafíos Regulatorios

- **Marco legal:** La falta de un marco regulatorio claro dificulta la adopción de la blockchain en muchos sectores.
 - Posibles soluciones:
 - **Marcos regulatorios claros:** Desarrollar regulaciones específicas para la blockchain que promuevan la innovación y protejan a los consumidores.



Tendencias futuras

Integración con la Inteligencia Artificial (IA)

- **Análisis predictivo:** La IA podrá analizar grandes cantidades de datos almacenados en la blockchain para realizar predicciones y tomar decisiones más informadas.

Nuevas aplicaciones y casos de uso

- **IoT y blockchain:** La combinación de IoT y blockchain permitirá crear redes de dispositivos conectados más seguras y eficientes.

Regulación y estandarización

- **Marco regulatorio claro:** A medida que la blockchain se vuelve más mainstream, los gobiernos y las organizaciones internacionales desarrollarán marcos regulatorios más claros.

Integración con el metaverso

- **Identidad digital descentralizada:** La Blockchain garantizará la propiedad y autenticidad de avatares, bienes virtuales y propiedades en el metaverso.
- **Economías virtuales:** Facilitará transacciones seguras dentro del metaverso mediante criptomonedas y tokens no fungibles (NFT).

Aumento de la eficiencia energética

- **Migración a protocolos menos intensivos:** Muchas Blockchains están adoptando protocolos como Proof of Stake (PoS), que consumen significativamente menos energía que Proof of Work (PoW).

Mejoras Misceláneas

Aparte de todas estas mejoras principales se prevé más integraciones en distintos ámbitos tecnológicos, esto llevará a más oportunidades para optimizar esta tecnología y a una expansión para centralizar esta tecnología en todo el globo.

¿Qué tecnologías reemplazará el Blockchain en el futuro?

Si conseguimos en un futuro que sea sostenible reemplazará:

- **Sistemas de pago tradicionales:** Blockchain permite transferencias rápidas y sin intermediarios.
- **Gestión de identidades digitales:** Ofrece identidades más seguras y autónomas.



Bibliografía y Webgrafía

Información General: [¿Que es La BlockChain? IEBS](#)

Aplicaciones actuales: [¿Qué es la blockchain y cómo funciona? | Binance Academy](#)

- [Proof Of Work \(PoW\) - What Is It, Blockchain, Example, Advantage](#)
-

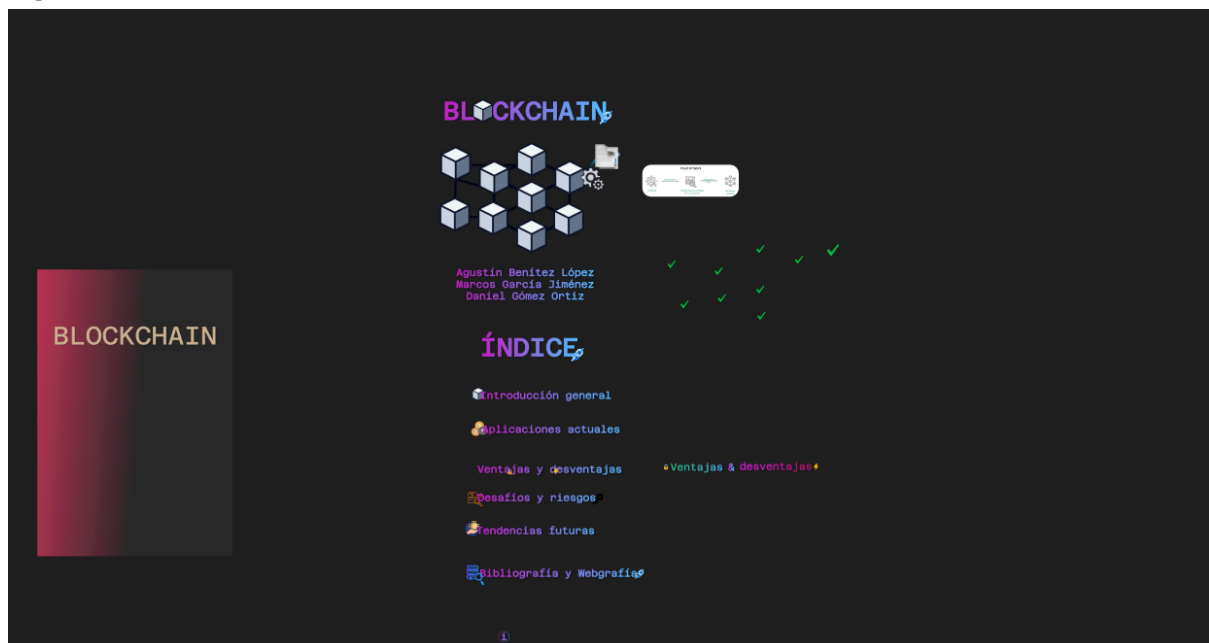
Información Extra: [Entiende Bitcoin y Ethereum - Explicación técnica a fondo en esp...](#)

tecnologías que reemplazará: [Blockchain: desde el frío y listo para revolucionar el mundo de las finanzas | Foro Económico Mundial](#)

Diseño de diagramas en:



Figma



presentación en HTML:

https://agustinbeniteez.github.io/Trabajo_blockchain/