Blockchain

**Integrantes:** Santino Pirraglia Janicki, Valentìn Manuel Gerakios y Nicolas Agustin Gonzalez Sanchez.

Introducción

**Contexto de creación**

Problema: Se busca hacer que las transferencias de dinero electrónico online se puedan hacer sin ninguna institución financiera de por medio. Pero el problema era que hasta el momento las transferencias hechas solamente entre dos entidades y sin un intermediario de por medio podían ser doblemente usadas, esto refiere al término **double-spending** que lo que hace es que se use una copia del dinero enviado en una transferencia para hacer otros pagos.

El resultado de los tipos de transferencias de esa época eran estos:

* Se tenía como inevitable cierta cantidad pequeña de fraudes.
* Los costos de intermediarios hacian que estos se llevaran un gran porcentaje de la transferencia, haciendo que las **transferencias pequeñas y casuales sean inconvenientes**.

Solución: Se crea un sistema en el cual los intermediarios sean los mismos usuarios del sistema, estos trabajan como nodos los cuales mantienen la funcionalidad del mismo. Para esto se establece una red **peer-to-peer** en la que los nodos tienen los mismos derechos, lo que permite que los nodos puedan entrar o salir sin problemas.

La red necesita que ocurran en un orden específico y no se puedan cambiar después de ser registradas, para esto hace un hash por cada transacción que sirve como una prueba de tiempo.

**Hash:** Es un proceso criptográfico que convierte la transacción en una cadena de caracteres única y de longitud fija.

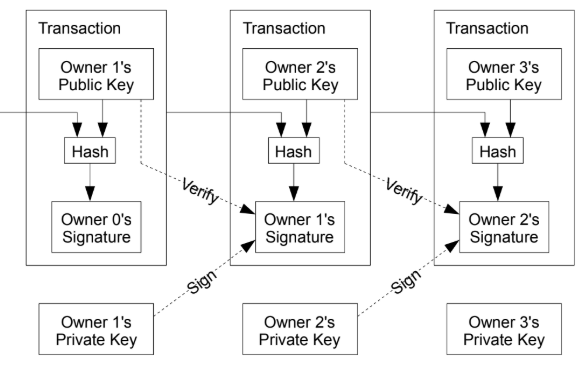
Un **hash** sirve como un código único que representa datos, y sirve para proteger, verificar e identificar información. Se usa para identificar bloques, ya que cualquier cambio en el bloque generaría un hash completamente distinto.

En general se usan para:

* Dejar una prueba de tiempo de cada transacción
* Identificar bloques y enlazarlos
* Encontrar la prueba de trabajo

Manejo de transacciones

Para realizar transacciones cada usuario tiene una clave pública y una clave privada que usa para firmar las mismas.



En este ejemplo se ve como es el funcionamiento, el owner 0 realiza una transferencia en la que firma con su clave privada, la transacción va al owner 1 usando su clave pública y los datos de la transferencia están guardados en un hash. Todo esto garantiza que solo el dueño actual puede transferir esa moneda, ya que es el único que tiene su clave privada.

El hecho de firmar con tu clave privada para hacer una transferencia hace que gastes tu derecho de transferir de vuelta esa moneda, pero hasta que la transacción no sea incluida en la cadena, se puede gastar 2 veces la misma moneda por el mismo dueño. Por lo que **no se puede verificar que un dueño no haya hecho un double-spending**,ya que por ejemplo: El owner 2 puede haber hecho una transferencia con una moneda

Para solucionarlo **se anuncia cada transacción públicamente**, entonces cada nodo que esté intentando agregar un bloque, toma la transacción que haya sido hecha primero, ya que se tiene un hash como sello de tiempo en cada transacción. Así se agrega la transacción al bloque en proceso y luego, si la mayoría de nodos lo aceptan, este bloque se agrega a la cadena.

Agregar bloques a la cadena

Un nodo crea un bloque basado en la agrupación de transferencias elegidas por el mismo, priorizando las que tengan mayores comisiones. Luego de crear el bloque candidato, este intentará resolver la prueba de trabajo para agregar el bloque a la cadena.

¿Qué tiene un bloque?

Un bloque en blockchain entonces poseerá las siguientes características:

* Un hash ligado al bloque anterior para mantener la cadena.
* Un sello de tiempo.
* Un número llamado nonce.

**Prueba de Trabajo**

Para ganar el **derecho de agregar un bloque** a la cadena cada participante debe realizar una **proof-of-work(minar)**, el nodo que resuelve el problema primero puede agregar el bloque a la cadena.

El nodo comienza a probar distintos valores de nonce para encontrar un hash del bloque que cumpla con una condición de dificultad (el hash debe comenzar con cierta cantidad de ceros, por ejemplo). Si alguien agrega un bloque mientras otro nodo está intentando resolver la PoW, el nodo que no llegó a agregar el bloque ahora deberá crear otro porque el anterior queda invalidado.

Cuando se resuelve la PoW, lo último que se hace para finalmente agregar el bloque es validar mediante distintos nodos que el bloque no tenga fines maliciosos, por ejemplo hacer double-spending.

* Nota: Las PoW varían en dificultad dependiendo de la blockchain que se use.

**Incentivos**

La forma de incentivar nodos es dándoles partes de bitcoins que se generan al minar bloques. Similar a la minería de oro, los “mineros” gastan recursos como poder de cómputo y electricidad en agregar bloques a la cadena.

Para los nodos con gran poder de cómputo, se les hace más remunerativo usar ese poder para minar, aún más que usar esa capacidad para hacer double spending.

**Tipos de validaciones:**

Si bien hablamos de las PoW como forma de verificación, ya que esta fue la primera creada y es la más usada (por ejemplo en bitcoin), además existen otros tipos de verificaciones:

* Proof of Stake: Usada por Etherium
* Delegated Proof of Stake
* Proof of Authority

Ejemplos de blockchain

Bitcoin fue la primera criptomoneda del mundo, presentada en octubre de 2008 por una persona o grupo bajo el seudónimo **Satoshi Nakamoto**, a través del famoso documento técnico (whitepaper) titulado *“Bitcoin: A Peer-to-Peer Electronic Cash System”*. Este documento proponía una solución a uno de los grandes problemas del dinero digital: el **double-spending** (gasto doble), es decir, la posibilidad de copiar un archivo digital y utilizarlo varias veces como si fuera dinero real.

La solución propuesta por Nakamoto fue revolucionaria: crear una red **descentralizada** basada en la tecnología **blockchain**, donde cada transacción queda registrada en un “libro contable” público y compartido por miles de computadoras en todo el mundo (llamadas **nodos**). Estas transacciones se agrupan en bloques y se aseguran mediante un proceso llamado **Proof of Work** (prueba de trabajo), que requiere que los nodos gasten poder computacional para validar los datos y agregarlos a la cadena.

El primer bloque de la red, llamado **Génesis Block**, fue minado el **3 de enero de 2009**, y contenía un mensaje oculto con una referencia a una crisis bancaria:

*"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*

Esto no fue casualidad: el mensaje dejaba en claro que Bitcoin surgía como una alternativa al sistema financiero tradicional, controlado por bancos y gobiernos.

En la actualidad, Bitcoin no solo es una criptomoneda utilizada para pagos o inversión, sino que también es considerado por muchos como un **activo digital** de reserva de valor, similar al oro, debido a su cantidad limitada (solo existirán **21 millones de bitcoins**) y su descentralización. Además, su red sigue siendo la más segura y resistente de todas las blockchains, y es ampliamente aceptado como pionero en el mundo de las criptomonedas.

## Finanzas Descentralizadas (DeFi)

### ¿Qué es DeFi?

Las Finanzas Descentralizadas (DeFi) son un ecosistema de aplicaciones financieras construidas sobre blockchain, principalmente en Ethereum, que imitan los servicios de la banca tradicional (como préstamos, ahorros, seguros o intercambios de divisas), pero sin intermediarios como bancos o entidades financieras.

En lugar de confiar en un banco, los usuarios interactúan directamente entre sí mediante contratos inteligentes, que son programas que se ejecutan automáticamente cuando se cumplen ciertas condiciones.

### Características principales de DeFi

* Sin permisos: cualquier persona con conexión a internet puede acceder, sin necesidad de aprobación previa.
* Interoperabilidad: muchas plataformas DeFi se pueden conectar entre sí, creando un ecosistema abierto.
* Código abierto: los contratos inteligentes suelen estar disponibles públicamente para su revisión.
* Autonomía del usuario: los usuarios mantienen el control de sus fondos en todo momento, sin necesidad de cederlos a terceros.

Problemas de blockchain

**Ataque del 51%**

Uno de los principales problemas asociados a la tecnología blockchain es el llamado "ataque del 51%", que ocurre cuando un solo grupo o entidad logra controlar más del 50% del poder de cómputo de una red. Esto le permite al grupo poseedor de esta capacidad poder agregar bloques a la cadena que tengan double-spending o revertir transacciones.

Aunque es difícil de lograr en redes grandes como Bitcoin, sigue siendo una amenaza real para blockchains más pequeñas con menor cantidad de participantes y recursos.

**Escalabilidad**

Otro problema importante de blockchain es su escalabilidad. A medida que más usuarios y transacciones se incorporan a la red, el sistema puede volverse lento y costoso. Las blockchains como Bitcoin y Ethereum, por ejemplo, solo pueden procesar un número limitado de transacciones por segundo, lo que no se compara con los sistemas tradicionales como Visa. Esta limitación genera cuellos de botella, altas comisiones y tiempos de espera prolongados.

**Gran consumo e impacto ambiental**

Un último problema relevante de blockchain es su alto consumo energético, especialmente en redes que utilizan el mecanismo de consenso de prueba de trabajo, como Bitcoin. Este proceso requiere que los mineros realicen cálculos complejos para validar transacciones y añadir nuevos bloques a la cadena, lo que implica el uso constante de hardware especializado y grandes cantidades de electricidad. Este consumo energético tiene un impacto ambiental significativo y ha generado críticas por su sostenibilidad a largo plazo.

Conclusión

Blockchain propuso usar una red entre pares (*peer-to-peer*) que utiliza un sistema de prueba de trabajo (*proof-of-work*) para registrar un historial público de transacciones, el cual se vuelve rápidamente computacionalmente inviable de modificar si los nodos honestos controlan la mayoría del poder de procesamiento. La red es robusta gracias a su simplicidad no estructurada. Los nodos trabajan simultáneamente con poca coordinación. No necesitan ser identificados, ya que los mensajes no se enrutan a lugares específicos y solo requieren ser entregados bajo el criterio de mejor esfuerzo. Los nodos pueden abandonar y reincorporarse a la red libremente, aceptando la cadena de prueba de trabajo como evidencia de lo ocurrido durante su ausencia. Votan con su poder de cómputo, expresando su aceptación de bloques válidos al trabajar en extenderlos, y rechazando bloques inválidos al negarse a trabajar en ellos. Cualquier regla e incentivo necesario puede imponerse mediante este mecanismo de consenso.

Bibliografía

Para realizar el documento y agregar la información nos basamos principalmente en el texto creado por el desarrollador de bitcoin y blockchain Satoshi Nakamoto: “Bitcoin: A Peer-to-Peer Electronic Cash System”.

<http://hackernoon.com/learn-blockchains-by-building-one-117428612f46>

<https://jeiwan.net/posts/building-blockchain-in-go-part-1/>

<https://www.freecodecamp.org/news/how-to-build-a-simple-actor-based-blockchain-aac1e996c177/>

<https://ethereum.org/en/defi/>

<https://bitcoin.org/bitcoin.pdf>