



# **CERTIFICADO DE ESPECIALIDAD**

*CIBERSEGURIDAD APLICADA I*



---



# **CIBERSEGURIDAD APLICADA I**

## *BLOCKCHAIN*





ESCUELA DE CONSTRUCCIÓN E INGENIERÍA  
Director de Escuela / Marcelo Lucero Yáñez

ELABORACIÓN  
Experto disciplinar / Julio Briones  
Diseñador instruccional / Luisa García

VALIDACIÓN  
Experto disciplinar / Andrés del Alcázar Cavallo  
Jefa de diseño instruccional y multimedia / Alejandra San Juan Reyes

DISEÑO DOCUMENTO  
Welearn



## Contenido

APRENDIZAJE ESPERADO DE LA SEMANA.....	6
CONCEPTO MÁS IMPORTANTE .....	6
INTRODUCCIÓN .....	6
BLOCKCHAIN .....	7
¿Qué es Blockchain? .....	7
Diferencia entre Bitcoin y Blockchain .....	7
Analogías de Blockchain al Mundo Real .....	8
Analogía de Blockchain .....	9
Peek Inside Blockchain.....	9
Definición de cadena de bloques.....	9
Características de la cadena de bloques.....	9
¿Por qué Blockchain es Web 3.0? .....	10
Wallets o Monedero .....	11
Los tipos de carteras Blockchain son: .....	11
Firmas digitales .....	11
Protocolos.....	12
TECNOLOGÍA BLOCKCHAIN .....	13
Beneficios sobre las tecnologías tradicionales .....	14
SEGURIDAD DE BLOCKCHAIN .....	16
Claves.....	16
Private Keys.....	16
Public Keys .....	17
Direcciones.....	17
HD Private Key .....	18
Mnemonics Seed .....	18
Smart Contracts .....	18
Ejemplo .....	19
TRANSACCIONES .....	21
¿Qué son los bloques? .....	21
Estructura de bloques.....	21



¿Qué es el Consenso? .....	23
Por qué no puedes hacer trampa en Bitcoin .....	27
Los 5 principales mecanismos de consensos .....	28
IDEAS CLAVE .....	33
CONCLUSIÓN .....	34
LINKS/MATERIAL MULTIMEDIA .....	35
BIBLIOGRAFÍA .....	36

---



## APRENDIZAJE ESPERADO DE LA SEMANA

Relacionan Blockchain con cambio de paradigma de transacciones por internet, considerando tipos de transacciones electrónicas y topologías de red física y lógica, de acuerdo con normativa vigente.

## CONCEPTO MÁS IMPORTANTE

Blockchain.com (anteriormente Blockchain.info) es un servicio de exploración de bloques de Bitcoin, que funciona como una billetera de criptomonedas y para hacer intercambio de criptomonedas que admite Bitcoin, Bitcoin Cash y Ethereum, a su vez, proporciona gráficos de datos de Bitcoin, estadísticas e información de mercado.

## INTRODUCCIÓN

Durante esta semana conoceremos los conceptos básicos relacionados con el Blockchain, su funcionamiento y aplicabilidad como solución de primera clase y reforzando la capacidad tecnológica logrando la escalabilidad, seguridad y sostenibilidad.

---

# BLOCKCHAIN

## ¿Qué es Blockchain?

Blockchain es un libro de contabilidad distribuido y digitalizado para todos los registros. Una transacción de registro de base de datos distribuida en orden cronológico. Desarrollado inicialmente para potenciar Bitcoin.

Las cadenas de bloques se construyen a partir de 3 tecnologías		
1. Private Key Cryptography	2. P2P Network	3. Program (the Blockchain protocol)
ECC	Torrent Networks	Hashing Algorithms
RSA	System of Records	Handshake Algorithms

Figura 1. Briones, J. (2020). Tecnologías *cadena de bloques*.

## Diferencia entre Bitcoin y Blockchain

A continuación, ahondaremos sobre las diferencias entre Bitcoin y Blockchain, a pesar de que están conectados, tienen conceptos distintos. Por lo tanto, se presentará las principales diferencias para entender a fondo estos conceptos.

### Bitcoin

- Bitcoin es una criptomoneda, creado y mantenido digitalmente en su PC o en una cartera virtual.
- Está descentralizado, por lo que ninguna persona, institución o banco controla la moneda.
- Una implementación de Blockchain.
- Se inició en 2009 para deshacerse de los intermediarios de procesamiento de pagos de terceros.
- La cadena de bloques es la tecnología subyacente que mantiene el libro mayor de transacciones Bitcoin.
- En palabras simples "Es oro para los nerds."



Figura 6. Briones, J. (2020). *Bitcoin*.

## *Blockchain*

- Una cadena de bloques en el núcleo es una base de datos distribuida de registros.
- Cada transacción en el libro mayor público se verifica por consenso.
- Las transacciones se cifran y no se pueden replicar ni modificar.
- Actualmente, la aplicación Blockchain más famosa es la cadena de bloques Bitcoin.
- Blockchain puede transferir fácilmente todo, desde derechos de propiedad a acciones y divisas sin tener que pasar por un intermediario.

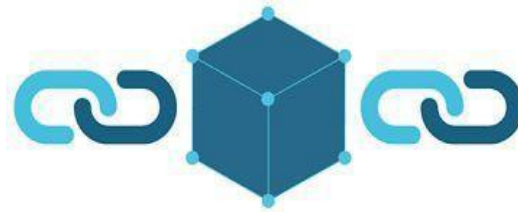


Figura 7. Briones, J. (2020). *Blockchain*

En palabras simples "Blockchain es la tecnología y Bitcoin es simplemente la primera manifestación dominante de su potencial.

## Analogías de Blockchain al Mundo Real

- Transparent Bank Bóvedas.
- Extractos de cuentas bancarias.
- Una hoja de cálculo que se duplica cientos de veces a través de la red de ordenadores.
- Un portátil de gran tamaño distribuido entre todos los lectores.
- Un documento de Google compartido entre varias partes.
- Un partido de fútbol callejero



---

## Analogía de Blockchain

- Imaginen un sistema de bóveda masiva de un banco.
- El almacén está lleno de filas de cajas de depósito.
- Cada caja de depósito está formada por vidrio, lo que permite a todos visualizar el contenido de la caja de depósito, pero solo tienen acceso a su bóveda.
- Cuando una persona abre una nueva caja de depósito, obtiene una llave que es única para esa caja.
- Este es el concepto fundamental de las criptomonedas basadas en Blockchain. Cualquiera puede ver el contenido de todas las demás direcciones.

## Peek Inside Blockchain

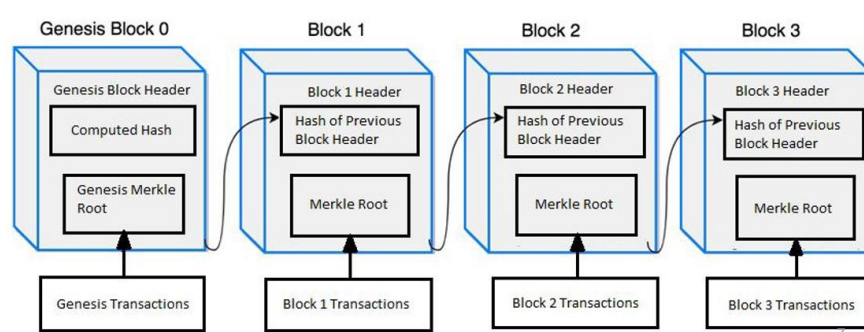


Figura 2. Briones, J. (2020). *Cadena de bloques*

## Definición de cadena de bloques

Una cadena de bloques es un almacenamiento seguro digitalizado, distribuido y basado en el consenso de información protegida contra la revisión y la manipulación a través de la red punto a punto.

## Características de la cadena de bloques

- ✓ Cada bloque se basa en el bloque anterior y utiliza el hash del bloque para formar una cadena.
- ✓ Validar y confirmar bloques sobre la cadena es manejado por mineros.
- ✓ Los bloques creados se sellan criptográficamente sobre la cadena de bloques, lo que significa que es casi imposible eliminar y modificar datos a través de la cadena de bloques.

- ✓ Los algoritmos de consenso se aseguran de que todas las transacciones se validan y solo se agregan una vez a través de la cadena de bloques.
- ✓ Miner recibe una recompensa por ejecutar los algoritmos de consenso; la recompensa actual es 12.5 BTC en el caso de Bitcoin Blockchain y 2 ETH en el caso de Ethereum Blockchain.
- ✓ Todos los bloques añadidos están en orden cronológico y con marca de tiempo.

*¿Por qué Blockchain es Web 3.0?*

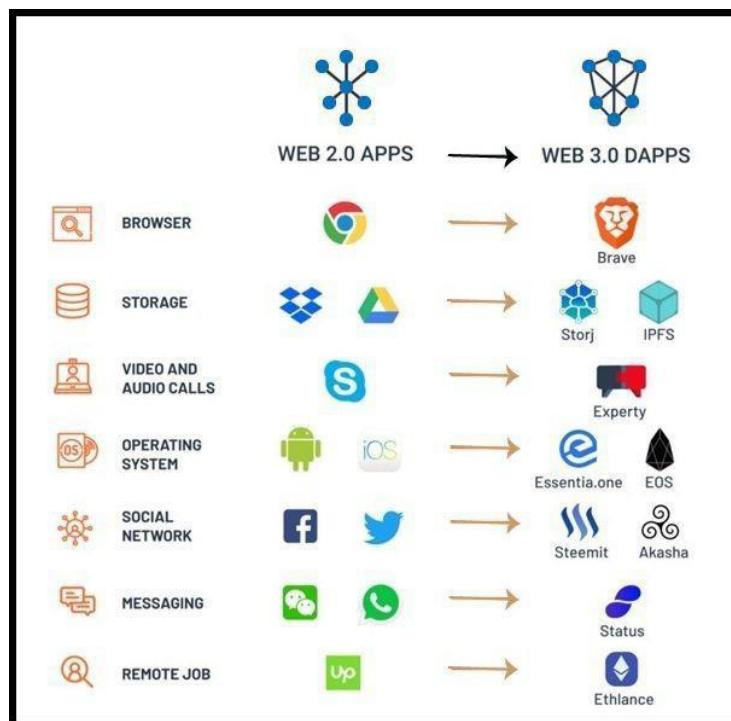


Figura 3. Briones, J. (2020). Web 3.0

- No hay punto central de control.
- Propiedad de los Datos.
- Reducción de Hacks y Violaciones de Datos.
- Servicio ininterrumpido

---

## Wallets o Monedero

- ✓ Una billetera blockchain es similar a una billetera digital que permite a los participantes administrar sus criptomonedas.
- ✓ Un monedero permite a los usuarios generar la clave privada y la dirección pública.
- ✓ La clave privada se utiliza para enviar la transacción y la dirección pública se usa para recibir la transacción.
- ✓ No hay registros visibles de identidad sobre quién hizo qué transacción con quién, sólo la dirección de un monedero es visible en las transacciones.

*Los tipos de carteras Blockchain son:*

- Carteras de papel
- Monederos web
- Carteras móviles
- Carteras de escritorio
- Carteras de hardware
- Carteras físicas



## *Firmas digitales*

- Las firmas digitales similares a las firmas reales son una manera de demostrar que alguien es quien dice ser.
- Las firmas digitales utilizan criptografía que es más segura que las firmas manuscritas.
- La clave privada se utiliza para firmar mensajes digitalmente.
- El destinatario puede comprobar el uso de la clave pública del remitente.
- Cada transacción que se ejecuta en la cadena de bloques está firmada digitalmente por el remitente utilizando su clave privada.
- SSL es un ejemplo de una firma digital.

---



## Protocolos

- ✓ Cada Blockchain consiste en especificaciones de comportamiento que se programan en él.
- ✓ Los protocolos definen la cadena de bloques
- ✓ La clave privada se utiliza para enviar la transacción y la dirección pública se usa para recibir la transacción.

Algunos ejemplos de protocolos:

- ✓ La información de entrada para cada número hash debe incluir el número hash del bloque anterior.
- ✓ La recompensa por extraer con éxito un bloque disminuye a la mitad después de cada 210.000 bloques sellados.
- ✓ Para mantener la cantidad de tiempo necesaria para extraer un bloque a aproximadamente 10 minutos, la dificultad minera se ajusta cada 2.016 bloques.

# TECNOLOGÍA BLOCKCHAIN

## Tradicional

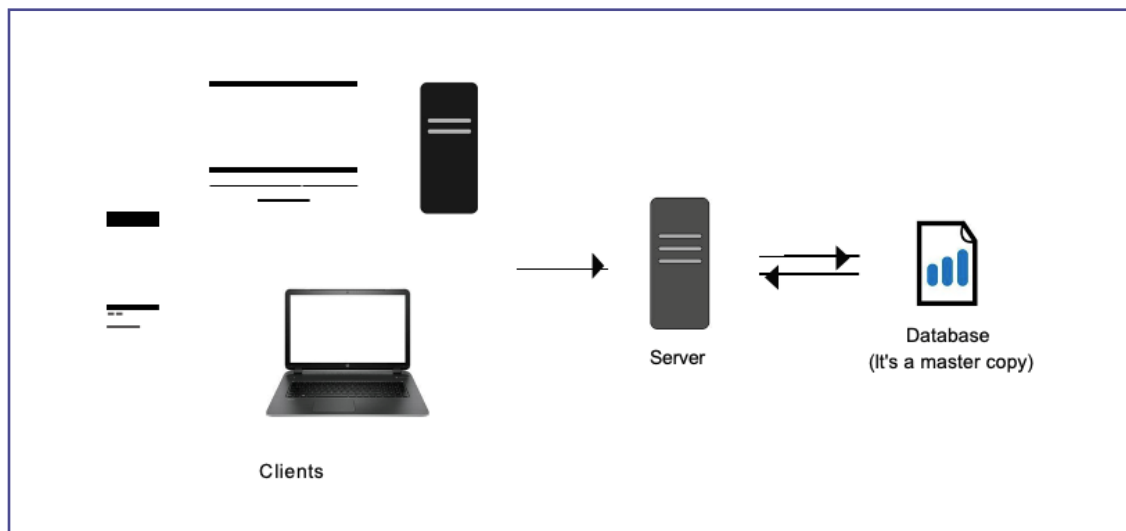


Figura 4. Briones, J. (2020). *Tecnología tradicional*

## Blockchain

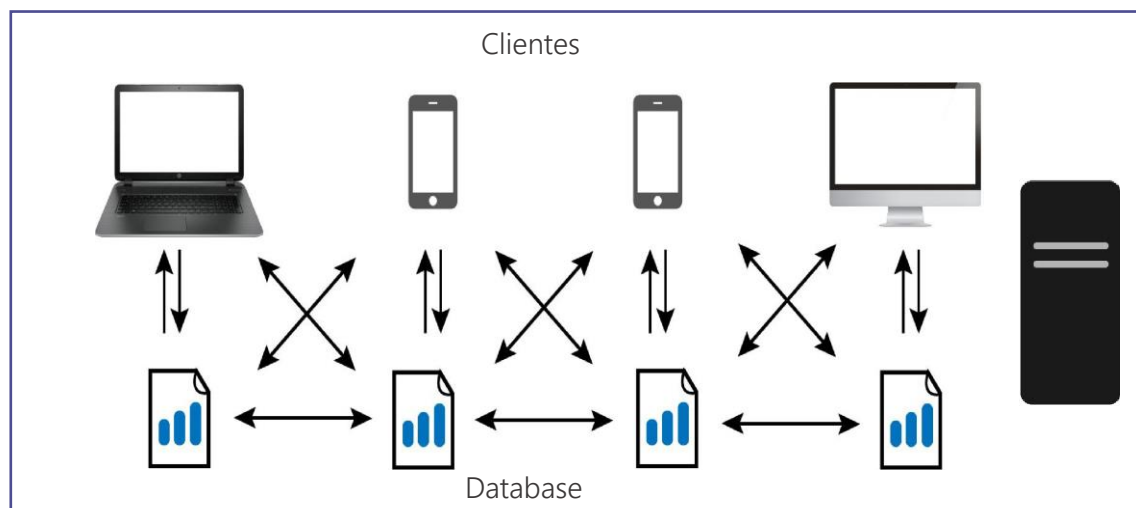


Figura 5. Briones, J. (2020). *Tecnología Blockchain*

### *Control descentralizado*


- Las cadenas de bloques permiten que varias partes que no confían entre sí compartan información sin necesidad de un control central.
- Elimina los riesgos del control centralizado con una base de datos centralizada, cualquier persona con acceso suficiente al sistema puede destruir o corromper los datos dentro.
- También se proporcionan ahorros de costos; por lo general, miles de millones de dólares se gastan en la protección de repositorios centrales de los piratas informáticos.
- Blockchain proporciona un mismo sistema compartido de registro simultáneamente para todos los que están conectados a la red.
- La confianza se establece mediante los protocolos criptográficos que se ejecutan detrás de la
- Todas las partes deben aceptar hacer un cambio en Blockchain que es casi imposible.

### *Integridad y Transparencia*

- La tecnología Blockchain la distingue de la tecnología de base de datos tradicional, ya que es verificable públicamente, lo que está habilitado por la integridad y la transparencia.
- Cada usuario puede estar seguro de que los datos que está recuperando no están dañados e inalterados desde el momento en que se registraron.
- Cada usuario puede verificar los datos anexados a través de la cadena de bloques.
- Blockchain crece como archivos en constante expansión de su historia, al mismo tiempo que proporciona un retrato en tiempo real.
- El árbol de Merkle, garantiza la integridad de los datos mediante el hash de las transacciones a una única raíz.

### *Confidencialidad*

- La cadena de bloques es un libro de contabilidad distribuido abiertamente, sin embargo, se puede establecer un sistema privado para mantener la confidencialidad.
- La confidencialidad de los datos en las cadenas de bloques garantiza que las personas u organizaciones a las que se les impide acceder a los datos no estén autorizadas para acceder a estos.
- Las cadenas de bloques autorizadas han surgido como una alternativa a las públicas para abordar las necesidades de la empresa por tener participantes conocidos e identificables.

- 
- 
- Soluciones como Hyperledger, Fabric, Blockchain y Block Stream ofrecen amplios conjuntos de permisos para mantener la confidencialidad en el sistema.

#### *Seguridad mejorada*

- Las transacciones se cifran y se vinculan a la transacción anterior.
- La información se almacena en una red de equipos en lugar de en un único servidor.
- Blockchain previene el fraude y la actividad no autorizada.
- Los protocolos de criptografía se aseguran de que los datos estén completamente seguros.
- Proteger de los ataques DOS, ya que, los datos están presentes en todos los nodos conectados a la red.
- La huella digital criptográfica (hash del bloque) es única para cada bloque.

#### *Procesamiento más rápido*

- El proceso bancario tradicional tarda días en resolverse, pero el Blockchain ha reducido ese tiempo casi a minutos o incluso segundos.
- Todo el mundo tiene acceso a la misma información, y es más fácil confiar entre sí, sin la necesidad de numerosos intermediarios. Además, el seguimiento de los productos también podría ser eficiente mediante la carga de los datos en Blockchain.
- Los activos digitales y el sistema de confianza se aseguran de que los datos estén protegidos y transaccionados de manera eficiente.

---

## SEGURIDAD DE BLOCKCHAIN

Los sistemas centralizados de almacenamiento y administración de datos son susceptibles a un ataque, intromisión e incumplimientos, por lo anterior, se usa la criptografía asimétrica, es usada generalmente para generar dos claves de seguridad jugando un rol importante para evitar hackeo o pérdida de información ante una vulnerabilidad al usuario.

### Claves

Empezaremos por ver la clasificación de las claves en Blockchain:

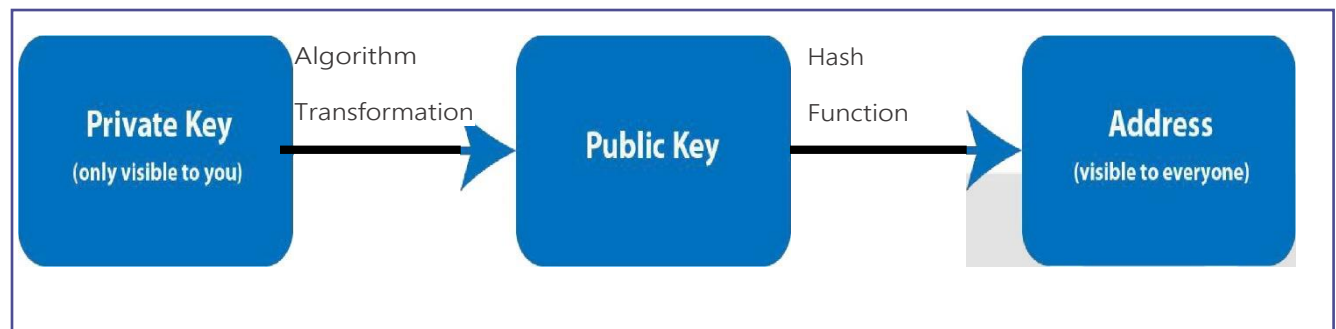


Figura 6. Briones, J. (2020). Claves

### Private Keys

- ❖ La clave privada se utiliza para generar una firma para cada transacción a través de la cadena de bloques.
- ❖ La firma generada se utiliza para confirmar que la transacción procede de un usuario específico y también impide que la transacción sea alterada por cualquier entidad maligna.

En palabras simples "Las claves privadas se utilizan para firmar las criptomonedas que envía a los demás. Si alguien obtiene su clave privada, sería capaz de enviar sus cryptocurrencies a sí mismos, lo que ha sucedido en la mayoría de los hacks de todo el mundo.

Ejemplo: L34EXrFCuxQCorfE66sxQe8Tyh71SyU8cc9z7HnbEWwW8YsgbvTw



## Public Keys

- ❖ La clave privada se utiliza para derivar la clave pública matemáticamente.
- ❖ Las claves públicas son prácticamente irreversibles, es decir, puede derivar fácilmente la clave pública de la clave privada, pero tardaría millones de años en hacer el viceversa, además de poder ser distribuidas a todo el mundo.

Ejemplo: 0237F49F4CCF760BF5FA993616E63B7B2A8611AB71AE7630386738B3BC4D1B84FD

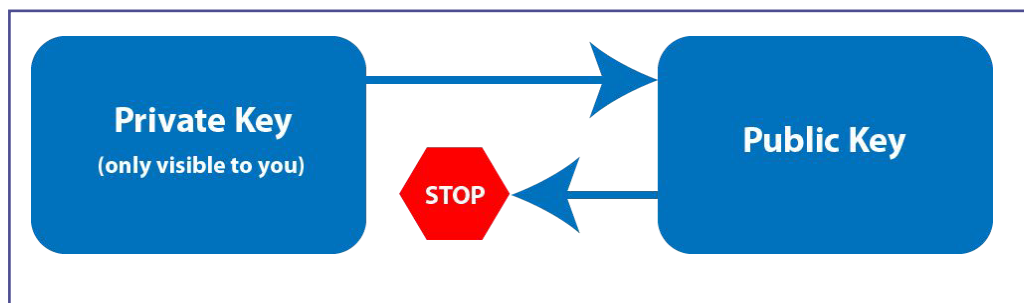


Figura 7. Briones, J. (2020). keys

## Direcciones

- ❖ Una dirección criptomoneda en un núcleo es una representación de la clave pública.
- ❖ Las funciones hash criptográficas unidireccionales se utilizan para derivar la dirección de la clave pública.

Un ejemplo de esto es en Bitcoin, los algoritmos que se utilizan para generar una dirección bitcoin a partir de la clave pública son el algoritmo de hash seguro 256 (SHA-256) y el resumen de mensajes de evaluación de primitivas de integridad RACE 160 (RIPEMD-160). La dirección aparece normalmente en una transacción entre dos partes, con la dirección que significa el destinatario de los fondos: 1JPgMJuAvYJU6mxxbJdmf1XBd7bBPdPV3a



Figura 8. Briones, J. (2020). Resumen de las claves

---



Otros conceptos relacionados con la seguridad en Blockchain:

#### *HD Private Key*

- ❖ La determinista jerárquica es un tipo de cartera de criptomoneda determinista derivada de una semilla conocida, que permite la generación de claves secundarias a partir de la clave principal.
- ❖ La clave secundaria se genera a partir de una semilla conocida. Hay una relación entre las claves secundarias y primarias que es invisible para cualquier persona sin esa semilla.
- ❖ El protocolo BIP 32 puede generar un número casi infinito de claves secundarias a partir de una semilla generada determinadamente desde su elemento primario.
- ❖ Puede volver a crear esas mismas claves secundarias siempre que tenga la semilla.
- ❖ La clave secundaria puede funcionar de forma independiente y la clave principal puede supervisar y controlar cada clave secundaria.

#### *Mnemonics Seed*

- ❖ Una semilla mnemotécnica se utiliza para sustituir una frase de 12, 18 o 24 palabras por las claves privadas que pueden ser memorizadas fácilmente por la mente humana en comparación con el formato codificado hexadecimal.
- ❖ Las frases de palabras mnemotécnicas están atadas con las llaves privadas y la restauración de la cartera de apoyo. Esto proporciona seguridad adicional para el usuario, así como una solución conveniente para recuperar una cartera.
- ❖ BIP 39 introdujo la implementación de la cartera mnemotécnica.
- ❖ La lista de palabras en inglés para BIP 39 contiene 2048 palabras, por lo que, para descifrar una frase de 12 palabras, requeriría averiguar 2048-12 a 2-132 combinaciones posibles bajo un escudo de seguridad de 128 bits.

#### *Smart Contracts*

- ❖ Los contratos inteligentes son los contratos digitales firmados entre dos partes y almacenados a través del libro mayor inmutable.
- ❖ Los contratos inteligentes le ayudan a intercambiar dinero, propiedades, acciones o cualquier cosa de valor de una manera transparente y libre de conflictos, evitando los servicios de un intermediario.

- ❖ Los contratos se pueden codificar en cualquier blockchain, pero Ethereum se utiliza principalmente ya que da capacidad de procesamiento ilimitada.
- ❖ Hyperledger también está proporcionando códigos de cadena que son muy similares a los contratos inteligentes. Ejemplo: Alquilar un apartamento.

### Ejemplo

Solución actual: Alicia en los EE.UU. quiere enviar \$5 a Bob en Australia, ella hará uso de la banca neta o cualquier otro servicio de pago como PayPal. Los servicios de la tercera parte tomarán 3-4 días para la transacción transfronteriza y cobran un corte digamos \$0.5, además, Alice no puede ver todo el proceso de ejecución de su transacción.

Problemas con la solución actual: Los costos de transacción son altos, con 3a parte involucrada, el tiempo necesario para el proceso también es lento. Imagine un escenario en el que Alice necesite transferir una gran suma de dinero para algunas operaciones médicas. Esto tomará tiempo y cobrará un costo masivo sobre la transacción.

¿Podemos hacer las mismas cosas eliminando los problemas actuales?

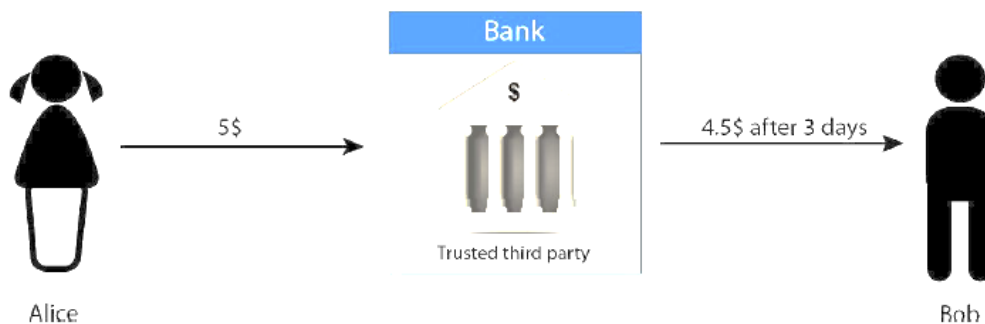


Figura 9. Briones, J. (2020). ejemplo

Blockchain como solución para guardar: Blockchain utiliza un libro mayor, un archivo digital/base de datos que realiza un seguimiento de todas las transacciones. El archivo contable no se almacena en un servidor central, se distribuye globalmente a través de una red de equipos privados que almacenan datos y ejecutan cálculos.

Si Alice quiere enviar dinero a Bob, transmite un mensaje a la red que dice que la cantidad de criptomoneda en su cuenta debe bajar en 5 tokens/5 \$, y la cantidad de la cuenta de Bob debe subir en la misma cantidad. Cada nodo conectado en la red recibirá el mensaje y aplicará la transacción solicitada a su copia del libro mayor, actualizando así los saldos de la cuenta.

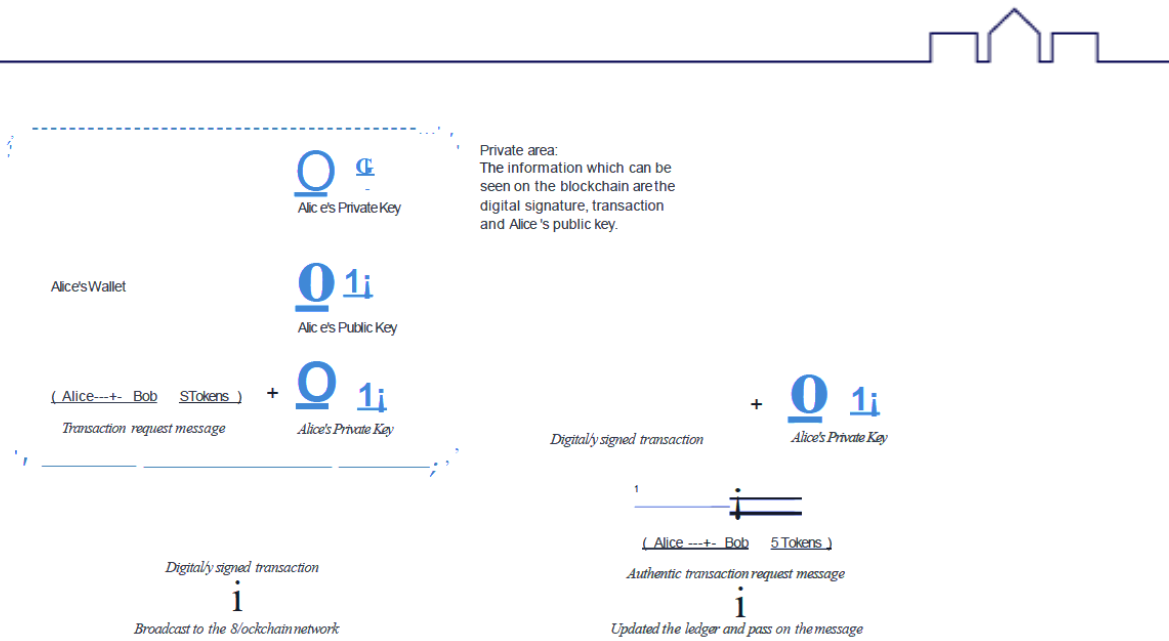


Figura 10. Briones, J. (2020). *transacción*

Distribución de la transacción:

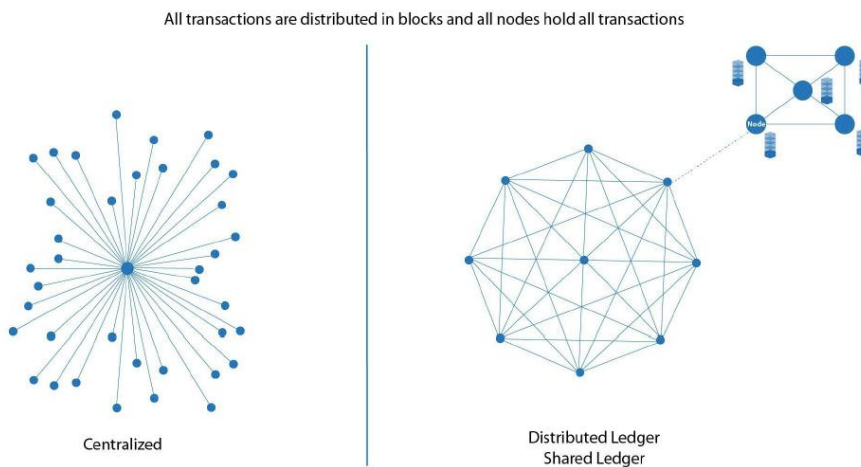


Figura 11. Kuchkovsky, C. (s.f). *Transacciones*

---



## TRANSACCIONES

Las transacciones son registros de datos en orden cronológico que se almacenan en un árbol de Merkle dentro del Bloque. Las transacciones, cuando se envían, son recogidas por la red blockchain y se insertan en un pool de transacciones no confirmadas.

Sin embargo, el grupo de transacciones es una colección de todas las transacciones de esa red que aún no se han confirmado, los mineros de la red seleccionan las transacciones de este grupo y las agregan a su 'bloque', también pueden contener información de metadatos que se puede utilizar para almacenar datos a través de la cadena de bloques.

### ¿Qué son los bloques?

Un bloque es una estructura de datos de contenedor que contiene un conjunto de transacciones confirmadas, también, podría contener información diferente, y una cadena de estos bloques evoluciona en una cadena de bloques siempre y cuando se vincula uno y el otro.

Los bloques se almacenan en los discos duros de muchos mineros repartidos por todo el mundo en una red punto a punto. En el algoritmo Bitcoin, se crea un bloque cada 10 minutos, todas las transacciones que ocurren a través de la red dentro de un intervalo de 10 minutos se crujen en ese bloque y se agregan a la cadena.

#### *Estructura de bloques*

Todos los bloques de la cadena de bloques se componen de un encabezado, identificadores y una larga lista de transacciones. La estructura de un bloque es la siguiente:

1. Encabezado de bloque: el encabezado contiene metadatos sobre un bloque. Hay tres conjuntos diferentes de metadatos:
  - El hash de bloque anterior, en una cadena de bloques, cada bloque se hereda del último bloque, porque usamos el hash del bloque anterior para crear el hash del nuevo bloque.
  - Competencia minera para la red para que cada bloque forme parte de la cadena de bloques, es necesario que se le dé un hash válido. Contiene los valores de la marca de tiempo, el nonce y la dificultad.
  - Raíz de árbol Merkle, se trata de una estructura de datos para resumir las transacciones dentro del bloque.

---

2. Identificador de bloque: para identificar un bloque, necesitamos tener un hash criptográfico, una firma digital. Esto se crea mediante el hash del encabezado del bloque dos veces con el algoritmo SHA256 en el caso de Bitcoin Blockchain, puede utilizar diferentes funciones hash para su Blockchain como:

- Cada bloque utiliza el hash del último bloque para construir su hash.
- Otra forma de identificar un bloque específico es la altura del bloque, esta es la posición del bloque en la cadena de bloques.
- Por ejemplo, si decimos que el bloque está en la posición 7312. Esto significa que hay 7311 bloques antes de éste.

3. Merkle Tree: un árbol Merkle resume todas las transacciones en un bloque mediante la producción de una huella digital de todo el conjunto de transacciones, el usuario puede comprobar si se incluye o no una transacción en un bloque. Los árboles de Merkle se crean mediante el hash de pares de nodos repetidamente hasta que solo queda un hash que se denomina hash raíz.

Cada nodo hoja es un hash de datos transaccionales y cada nodo no hoja es un hash de sus hashes anteriores. Por lo tanto, Los árboles Merkle son binarios y requieren un número par de nodos de hoja. Por consiguiente, si un solo detalle en cualquiera de las transacciones o el orden de los cambios de la transacción cambia, también lo hace La raíz de Merkle.

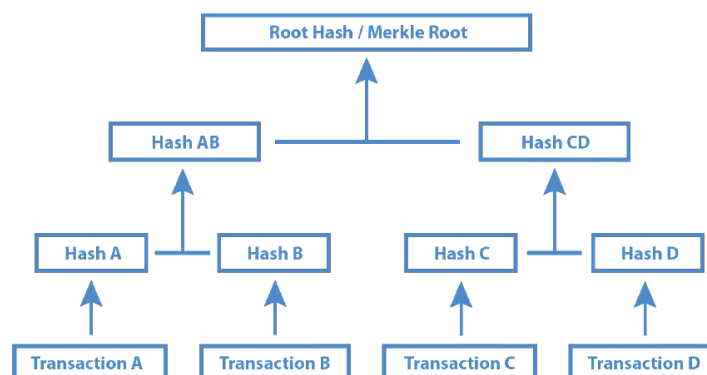


Figura 12. Briones, J. (2020). Merkle

Ejemplo:

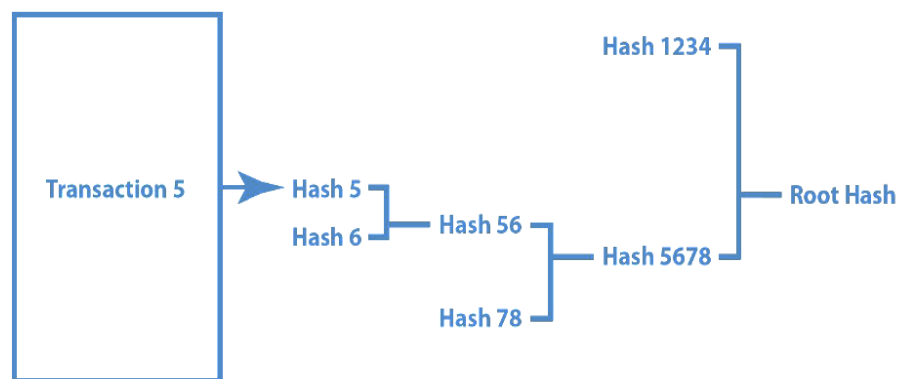


Figura 13. Briones, J. (2020). *Merkle*

### *Ejemplo estructura de bloques de Bitcoin Blockchain*

Field	Description	Size
Magic No	value always 0xD9B4BEF9	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	consists of 6 items	80 bytes
Transaction Counter	positive integer VI = VarInt	1 - 9 bytes
Transactions	The (non empty) list of transactions	Transaction counter-many transactions

Figura 14. Briones, J. (2020). *Estructura de bloques*

## ¿Qué es el Consenso?

Las cadenas de bloques son sistemas descentralizados que consisten en diferentes participantes que actúan dependiendo de los incentivos que reciben y la información que está disponible para ellos. Cuando se difunde una nueva transacción en la red, los nodos conectados a la red tienen la opción de incluir esa transacción en su copia del libro mayor o ignorarla o cuando la mayoría de los nodos que componen la red deciden sobre un solo estado, se logra el consenso. Vamos a profundizar en 2 problemas generales para entender mejor el consenso.

## Problema de dos generales

Este problema describe un esquema donde dos generales están atacando a un enemigo prevalente. el primer general es considerado el líder y el otro general es considerado como el seguidor. El ejército de cada general por sí solo no tiene la fuerza para derrotar al ejército enemigo; por lo tanto, necesitan colaborar y atacar al mismo tiempo.

Para que colaboren y acuerden un tiempo, el General 1 necesita enviar un mensajero a través del territorio enemigo que proporcionará la hora del ataque al otro General. Sin embargo, existe la probabilidad de que el mensajero sea capturado por los enemigos, y por lo tanto el mensaje no será entregado. Esto resultará en que el General 1 ataque mientras el General 2 y su ejército mantienen su posición, incluso si la primera transmisión pasa, el General 2 tiene que reconocer que ha recibido la noticia, por lo que envía un mensajero de vuelta, repitiendo así el escenario anterior donde el mensajero puede ser atrapado. Esto se extiende al intercambio infinito de mensajes y, por lo tanto, los generales no pueden llegar a un acuerdo.

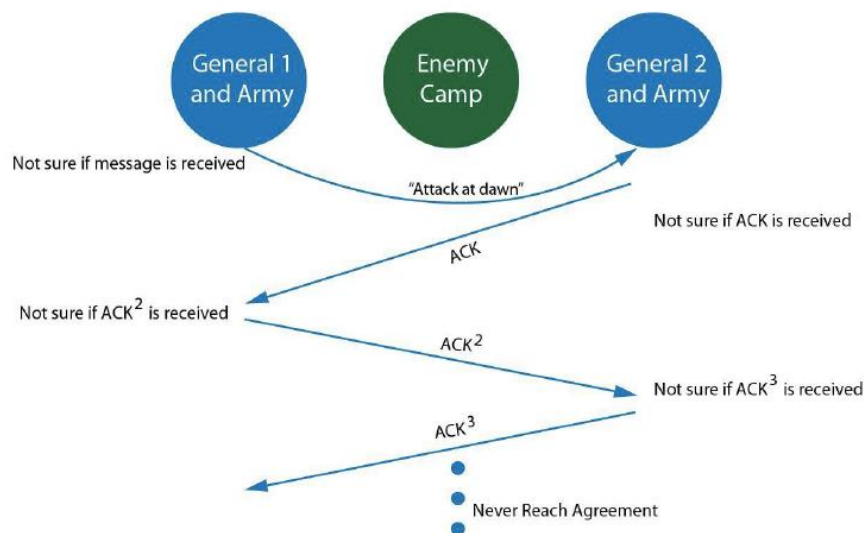


Figura 15. Briones, J. (2020). *Problema dos generales*



---



### *Problema de los generales bizantinos*

Una versión más generalizada del problema de los dos generales describe a más de dos generales que están de acuerdo en la hora del ataque. Además, uno o más generales pueden ser los traidores, lo que significa que pueden mentir sobre su elección de ataque (por ejemplo, dicen que aceptan atacar a las 5 de la mañana, pero en su lugar no atacan). Para llegar a un consenso aquí, el comandante y todos los tenientes deben ponerse de acuerdo en la misma decisión.

Cambiamos el escenario a un enfoque basado en el Comandante General y tenientes. Así que cuando el General emite una orden, cada teniente leal seguirá lo mismo para atacar. Si el comandante es un traidor, el consenso todavía se logra, como resultado, todos los tenientes toman el voto mayoritario sobre el valor predeterminado, esto implica que el algoritmo puede alcanzar un consenso siempre y cuando  $2/3$  de los actores sean honestos. Si los traidores son más de  $1/3$ , no se alcanza el consenso, los ejércitos no coordinan su ataque, y el enemigo gana.

#### *Explicación con ejemplo*

Tomemos un ejemplo; cada teniente necesita transmitir órdenes en 10 minutos., en otras palabras, se requieren 10 minutos para comunicar un mensaje para un ataque. Además, el paso de mensajes está relacionado con anexar el mensaje y luego enviarlos al siguiente teniente.

Ejemplo:

General - Ataque a las 3am

Teniente 1 - Ataque a las 3 am, Ataque a las 3 am

Teniente 2 - Ataque a las 3 am, Ataque a las 3 am, Ataque a las 5 am

Como usted puede ver si el teniente 2 es un traidor, después el 3er teniente puede verificar que el mensaje entrante no está en sincronización. Por otra parte, si el teniente 2 decide cambiar todos los mensajes anteriores también, entonces cada mensaje tomaría 10 minutos por lo que el teniente 2 estará trabajando durante 30 minutos, pero el teniente 3 espera que el mensaje llegue en 10 minutos, por lo que de nuevo ceder que el teniente 2 es un traidor.

Si el comandante es un traidor, entonces podría enviar diferentes órdenes a diferentes tenientes, que llegarán a un consenso, pero como los mensajes no siguen la estructura de proporcionar en el mismo tiempo de ataque, la opción predeterminada de retiro vendrá a la acción.

---

Cuando el teniente es un traidor

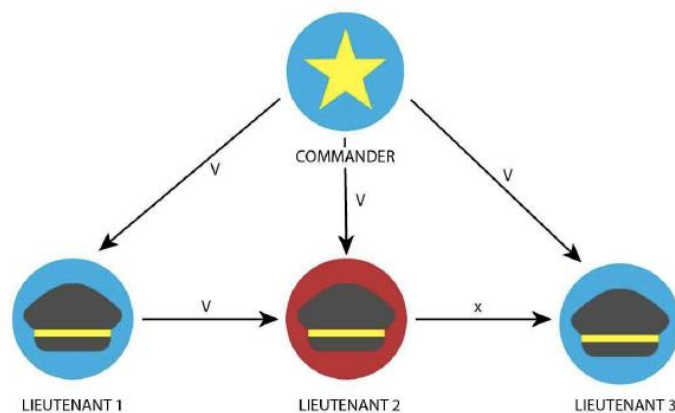


Figura 16. Briones, J. (2020). *Cuando el teniente es un traidor*

Cuando comandante es un Traidor

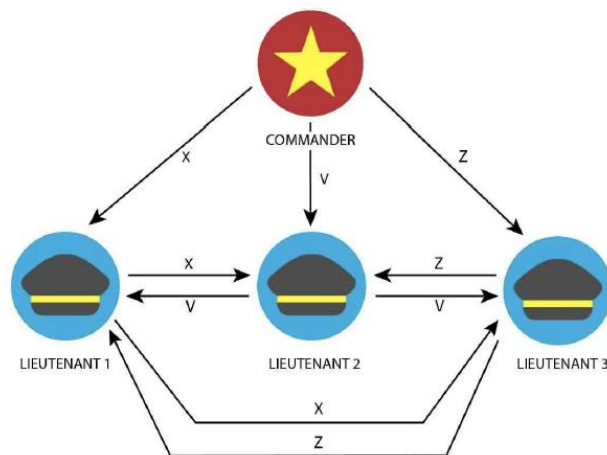


Figura 17. Briones, J. (2020). *Cuando el comandante es un traidor*

¿Cómo se relaciona con Blockchain?

Las cadenas de bloques son libros de contabilidad descentralizados que no están controlados por una autoridad central, debido al valor almacenado en estos libros de contabilidad, los malos actores tienen incentivos económicos sustanciales para tratar de causar fallas.

La prueba de trabajo es una solución probabilística al problema de los generales bizantinos como sató en profundidad por Satoshi Nakamoto. Sigue la regla de cadena más larga donde los mineros se desplazan a la cadena que se está trabajando más, cuando un minero resuelve el rompecabezas y confirma el bloque, todos los nodos de la red verificarán si el bloque es válido



y lo añadirán a su copia de la cadena. Los nodos primero necesitan alcanzar un consenso sobre la validez, sólo entonces la red se sincronizará, y el estado de la cadena de bloques se actualizará.

## Por qué no puedes hacer trampa en Bitcoin

Digamos que todo el mundo está temblando en el bloque 91, pero un minero quiere alterar una transacción en el bloque 743, tendría que hacer sus cambios y rehacer todos los cálculos de los bloques 74-90 y bloque 91. Eso es 18 bloques de computación costosa. Lo que es peor, tendría que hacerlo todo antes de que todos los demás en la red Bitcoin terminaran sólo el bloque (número 91) en el que están trabajando.

### *Ejemplo de conflicto en minería*

Múltiples mineros trabajan en la minería de los bloques, supongamos que dos mineros pueden confirmar un bloque en una fracción de segundos, pero otros mineros comienzan a trabajar en los siguientes bloques. Bitcoin y Ethereum identifican la cadena más larga basada en el trabajo total se hace / dificultad y node prefiere la cadena válida de primera vista con el mayor trabajo medido en términos equivalentes a la suma de la dificultad de todos los bloques.

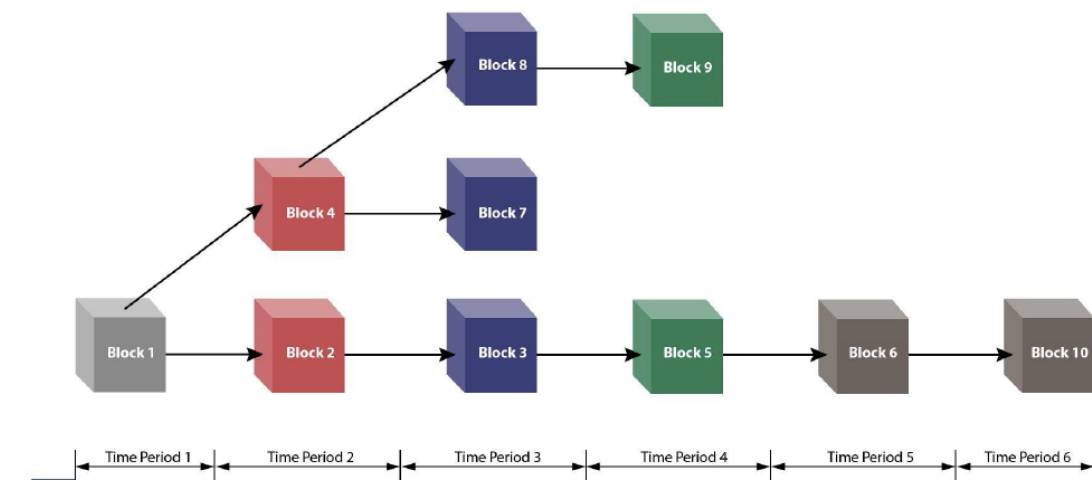


Figura 18. Briones, J. (2020). *Conflicto en minería*

### Regla de cadena más larga

En cadenas de bloques públicas como Bitcoin, los conflictos están siendo resueltos por la regla de cadena más larga. Digamos que un minero recibió el primer Bloque 4 y luego comenzará a construir el siguiente Bloque en la parte superior de ese Bloque 4, ahora, en unos segundos que los mineros ven otro bloque 2, para que el minero mantenga un ojo en ese nuevo bloque.

Si el siguiente bloque 3 se está detectando desde otros nodos en Blockchain, entonces ese minero no tendrá en cuenta el 4 y aceptará la nueva cadena más larga que es 1-> 3-> 5 y así

---

sucesivamente. La sabiduría convencional afirma que, por lo tanto, es prudente esperar a seis bloques para confirmar una transacción.

## Los 5 principales mecanismos de consensos

### 1. Prueba de trabajo

Es el algoritmo de consenso donde los mineros compiten para resolver un problema matemático difícil basado en un algoritmo hash criptográfico, esta prueba demuestra que un minero pasa mucho tiempo y recursos para resolver el problema. Cuando se 'resuelve' un bloque, las transacciones contenidas se consideran confirmadas.

Por problema matemático nos referimos a:

- Función hash: cómo encontrar la entrada conociendo la salida.
- Factorización de enteros: cómo presentar un número como una multiplicación de otros dos números.
- Protocolo de rompecabezas de recorrido guiado: si el servidor sospecha de un ataque DoS, requiere un cálculo de las funciones hash, para algunos nodos en un orden definido. en este caso, es un problema de "cómo encontrar una cadena de valores de función hash".

Los mineros reciben una recompensa cuando resuelven el complejo problema matemático. por ejemplo, en Bitcoin los mineros reciben 12,5 bitcoins para resolver el rompecabezas, otra medida, los mineros también pueden recibir cargos por transacción además de recompensas.

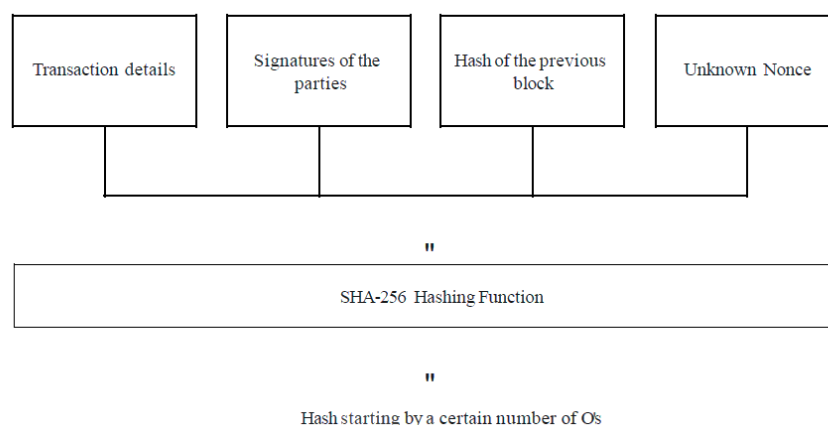


Figura 19. Briones, J. (2020). *Esquema prueba de trabajo*.



Ejemplo de prueba de trabajo de Bitcoin: en Bitcoin, se extrae un bloque cada 10 minutos, la dificultad se ajusta de tal manera que nunca se desvía mucho de este límite. Si la dificultad permanece igual, mientras que la potencia de la computadora aumenta gradualmente, tomará cada vez menos tiempo para extraer un bloque.

Para asegurarse de que esto no sucede a través de Blockchain, el objetivo de prueba de trabajo es un parámetro dinámico en la cadena de bloques Bitcoin, el objetivo se ajusta cada bloque de 2016., con el fin de, computar la cantidad de tiempo que tomó la mina de bloques de 2016.

El tiempo para tomar es de 20160 minutos, el cual, se calcula así:  $(2016 * 10 \text{ minutos a } 14 \text{ días})$ . La dificultad se ajusta dependiendo del tiempo que se tardó en extraer esos bloques.

## *2. Prueba de participación*

Es un algoritmo diferente para validar las transacciones y lograr el consenso distribuido. El algoritmo de prueba de trabajo recompensa a los mineros que resuelven problemas matemáticos complejos con el objetivo final de validar transacciones y crear nuevos bloques. Por otro lado, en el algoritmo de prueba de participación, el creador de un nuevo bloque es elegido de una manera determinista, dependiendo de su riqueza / participación en la cadena de bloques, sin recompensa de bloque y todas las monedas digitales se crean al comienzo de la cadena, y su número nunca cambia.

Los mineros sólo toman las tarifas de transacción. Es por eso por lo que en el sistema PoS los mineros también se llaman forgers.

Ejemplo de Prueba de Participación Neo:

NEO es una plataforma de desarrollo de contratos inteligentes a menudo conocida como "Ethereum de China". La red tiene como objetivo ser el centro de una economía creativa donde los activos digitales se pueden negociar de forma segura con poca sobrecarga.

Staking NEO le permite generar GAS, la moneda interna de la plataforma. Cuanto más NEO hayas apostado, más GAS ganarás con cada pago. NEO recompensa a las partes interesadas con una rentabilidad anual del 4-6%.

### 3. Prueba de participación delegada

Las personas en un ecosistema Blockchain en particular votan por los testigos para salvaguardar su red informática. Imaginemos un sistema de recompensas en el que solo los 100 testigos principales son pagados por su servicio, y solo los 20 primeros ganan un salario regular, a medida que crea una competencia saludable, muchos quieren convertirse en testigos, proporcionando así cientos de testigos de respaldo.

La fuerza de voto de una persona está determinada por la cantidad de fichas que poseen, las personas que tienen más tokens influirán en la red más que las personas que tienen menos tokens. Si un testigo comienza a actuar como un idiota o deja de hacer un trabajo de calidad en la seguridad de la red, las personas en la comunidad Blockchain pueden eliminar sus votos, esencialmente despidiendo al pésimo actor, la votación siempre está en curso.

Los delegados son elegidos testigos. Un delegado se convierte en co-firmante en una cuenta individual que tiene el privilegio de proponer ciertos cambios en los parámetros de red. Esta cuenta se conoce como la cuenta de Genesis. Estos parámetros incluyen todo, desde las tarifas de transacción hasta los tamaños de bloque, el pago de testigos y los intervalos de bloqueo.

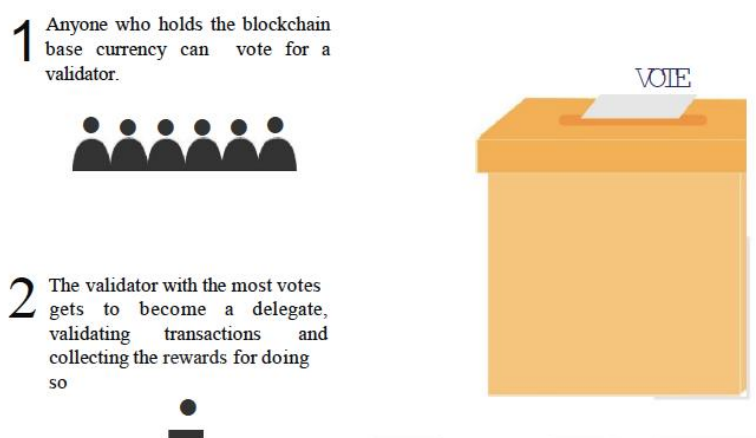


Figura 20. Briones, J. (2020). Esquema prueba de participación.

Ejemplo de Prueba de participación delegada Lisk:

Lisk es una red descentralizada similar a Bitcoin, Ethereum o BitShares, se utiliza una implementación simplificada del algoritmo de consenso Prueba de estaca delegada. Los titulares de tokens Despetor pueden votar por los delegados de mainchain que protegen la red, hay un máximo de 101 delegados activos de la cadena principal que obtuvieron más votos en toda la red, y pueden ganar recompensas de generación de bloques, todos los demás delegados están en espera esperando ser elegidos, o asegurando una cadena lateral de Lisk.

#### 4. Prueba de autoridad

El consenso de la prueba de autoridad es esencialmente un modelo optimizado de prueba de estaca que aprovecha la identidad como la forma de estaca en lugar de apostar tokens. Por lo general, se supone que el grupo de validadores debe permanecer relativamente pequeño (25 o menos) para garantizar la eficiencia y la seguridad manejable de la red, individuos bajo PoA se ganan el derecho de convertirse en un validador, es por eso por lo que no hay ningún incentivo para conservar la posición que mantienen. Los validadores deben verificar formalmente la identidad en la cadena o en algún dominio público, sin embargo, la elegibilidad para convertirse en un validador es difícil de obtener, y las personas necesitan pasar por muchos pasos para convertirse en un validador.

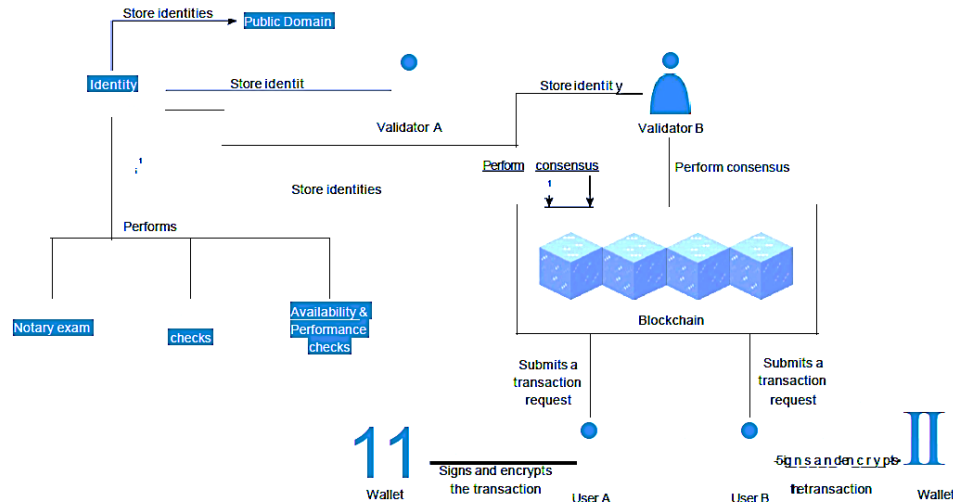


Figura 21. Briones, J. (2020). Esquema prueba de autoridad

Ejemplo de prueba de autoridad red POA:

Proof of Authority Network (POA Network) es una plataforma blockchain fundada en el principio básico de implementar el consenso de PoA en su blockchain. POA Network, es una plataforma pública para contratos inteligentes que existe como una cadena lateral Ethereum con sus nodos que consisten en validadores independientes.

Para que la elegibilidad para la identidad de la apuesta sea muy difícil de obtener, los candidatos a los validadores tienen que superar el obstáculo de aprobar exámenes notariales. No sólo los exámenes atestiguan los antecedentes penales y la buena moral de un candidato, sino que también filtran a aquellos que no están comprometidos.

## 5. Prueba de peso

Es una amplia clasificación de consenso basada en el algoritmo algorand que a su vez especifica un nuevo protocolo conocido como Acuerdo Bizantino. El protocolo BA\* es altamente escalable y seguro, el modelo de consenso de PoW dirige un comité donde los participantes siguen cambiando, y el comité logra el consenso para la red. Cada usuario a través de la red tiene un peso adjunto que está determinado por el dinero que tienen en su cuenta.

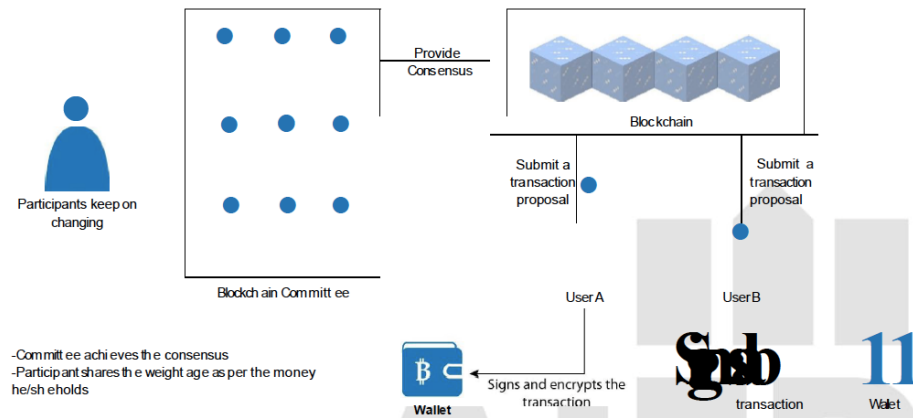


Figura 22. Briones, J. (2020). *Esquema prueba de peso*

Ejemplo de prueba de peso Filecoin:

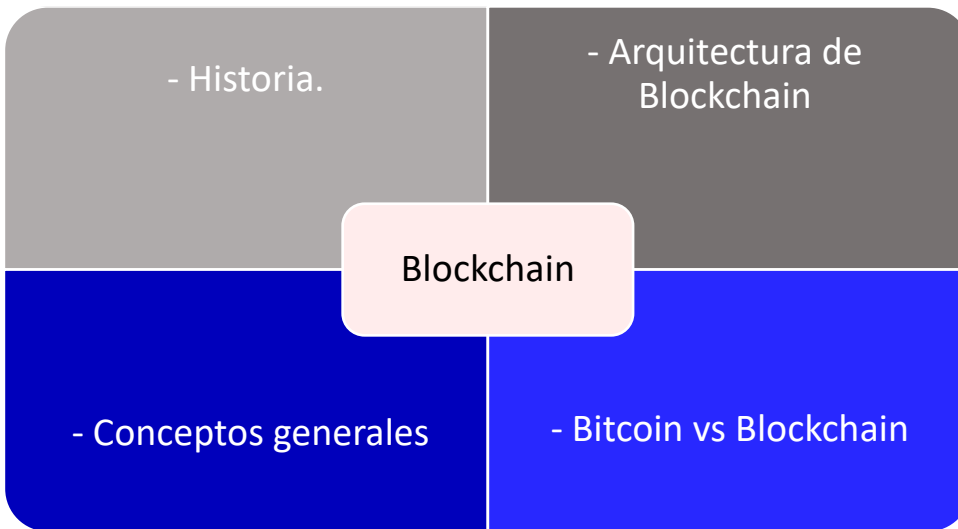
Filecoin está utilizando Proof-of-Spacetime como un consenso ponderado sobre la cantidad de datos IPFS que está almacenando, el peso se basa en diferentes parámetros si la fracción de peso total de los usuarios honestos es superior a dos tercios del peso total que la red permanecerá segura. Este método también ayuda a proteger la red de los ataques de doble gasto, está basada en Algorand. mientras que algunos pueden ver similitudes entre Algorand y la prueba de estaca, no son las mismas.

En un entorno PoS, el número de tokens retenidos en un momento dado determina la cantidad de recompensas adicionales que los usuarios ganan, la prueba de peso utiliza un valor ponderado completamente diferente.



---

## IDEAS CLAVE



Resumiendo, en lo que hemos aprendido esta semana, se puede deducir que Blockchain es:

- Es una tienda digitalizada de información en forma de transacciones.
- Se distribuye. Por lo tanto, nadie lo controla.
- Los algoritmos de consenso se aseguran de la seguridad y la inmutabilidad.
- Cuando se agrega un nuevo bloque a una cadena de bloques, se vincula al bloque anterior mediante un hash criptográfico.
- Los datos se registran en orden cronológico.
- Todos los presentes a través de la red pueden ver las transacciones.

---




## CONCLUSIÓN

Si explica qué es blockchain en palabras simples, entonces imagine, por ejemplo, una “lista de tareas para el día del Sr. G”, que ha sido duplicada miles de veces en la red informática y esta red, a su vez, está diseñada de tal manera que se actualiza regularmente en tiempo real y sincroniza esta “lista” para que nadie externo pueda realizar cambios a su discreción, toda la información se cifra de una manera especial, y el cifrado se considera de muy alta calidad. Además, dado que la lista tiene muchas copias almacenadas en millones de computadoras al mismo tiempo (descentralizadas), no se puede hackear, cambiar ni eliminar. No es como si esta lista sólo la tuviera el propio Sr. G y la perdiera por descuido. En el caso del blockchain, guarda los registros públicamente y son fáciles de comprobar.

---

## LINKS/MATERIAL MULTIMEDIA

MÓDULO:		Unidad: 1
Recurso	Descripción	
 Video	<p>En estos videos encontrarás un breve resumen de Blockchain y su aplicación en el ámbito financiero.</p> <ul style="list-style-type: none"><li>• Playground, (2018), Qué es "Blockchain" en 5 minutos, consultado en diciembre, disponible en: <a href="https://www.youtube.com/watch?v=Yn8WGaO__ak">https://www.youtube.com/watch?v=Yn8WGaO__ak</a></li><li>• CEU, (2019), Blockchain y su aplicación en el ámbito financiero, consultado en diciembre, disponible en: <a href="https://www.youtube.com/watch?v=lkO168P39Z0">https://www.youtube.com/watch?v=lkO168P39Z0</a></li></ul>	

---



## BIBLIOGRAFÍA

- Gómez, B & Blanco, D. (2018). *Blockchain, así es la nueva revolución de internet*, consultado en diciembre, disponible en:  
<https://www.paradigmadigital.com/techbiz/blockchain-asi-es-la-nueva-revolucion-de-internet/?prs=1BLOCKCHAIN> <http://paradig.ma/blockchain>
- Ministerio de Economía, Fomento y Turismo. (s.f). *Blockchain: un camino a la 4ta revolución industrial*, consultado en diciembre, disponible en:  
<https://www.economia.gob.cl/wp-content/uploads/2019/03/libroblockchain-VB-31AGO-v3.pdf>
- Kuchkovsky, C; Fernández, R & Molero, I. (2017). *Blockchain: la revolución industrial de internet. Cap.1-2*, PAIDOS EMPRESA.
- Piscini, E & Kehoe, L (2018). *Blockchain-Ciberseguridad*, consultado en diciembre, disponible en:  
[https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Blockchain%20CiberseguridadESP%20\(1\).pdf](https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Blockchain%20CiberseguridadESP%20(1).pdf)