

Criptomonedas y Blockchain

Gimenez, Christian

May 5, 2025

Outline

- 1 Repaso
 - Repaso
- 2 Criptomonedas
 - Introducción
- 3 Blockchain
 - Introducción
 - Proof of Work
 - Proof of Stake
 - Curiosidades
- 4 Próximamente...
 - Continuará...
- 5 Licencia
 - Licencia de Esta Obra

Outline

1 Repaso

- Repaso

2 Criptomonedas

- Introducción

3 Blockchain

- Introducción
- Proof of Work
- Proof of Stake
- Curiosidades

4 Próximamente...

- Continuará...

5 Licencia

- Licencia de Esta Obra

Outline

- 1 Repaso
 - Repaso

- Funciones Hash
 - Compresión
 - Facilidad de cómputo
 - Unidireccionalidad
 - Difusión de bits
 - Resistencia a la 2da preimagen
 - Resistencia a la colisión
- Cifrado Asimétrico (de Clave Pública)
 - Definición
 - $Enc_{pk}(m)=c$ y $Dec_{sk}(c)=m$
 - Firma digital

Outline

- 1 Repaso
 - Repaso
- 2 Criptomonedas
 - Introducción
- 3 Blockchain
 - Introducción
 - Proof of Work
 - Proof of Stake
 - Curiosidades
- 4 Próximamente...
 - Continuará...
- 5 Licencia
 - Licencia de Esta Obra

- 2 Criptomonedas
 - Introducción

Criptomonedas



Imagen descargada de: imgur.com/hyper-chips-blU8upr todos los derechos reservados.

¿Qué es?

-  Moneda digital
- Propuesta por Satoshi Nakamoto  ¿quién es?

¿Cómo Implementarla?

- ¿Cómo se podría proponer una moneda digital?
- ¿Firmas digitales? ¿Qué hace falta?
- Entidad financiera que regule transacciones

Double-spending problem

No debe ser posible comprar más de una cosa con la **misma moneda**.
Solución actual: entidad financiera reguladora.

¿Qué propone Satoshi Nakamoto?

Bitcoin

-  Moneda electrónica
-  Peer-to-peer
 - Pagos on-line enviados directamente entre personas
-  Resolver el problema Double-Spending
-  **No utilizar instituciones financieras**
 - ¿¡Cómo!? →  **Blockchain**

Outline

- 1 Repaso
 - Repaso
- 2 Criptomonedas
 - Introducción
- 3 **Blockchain**
 - Introducción
 - Proof of Work
 - Proof of Stake
 - Curiosidades
- 4 Próximamente...
 - Continuará...
- 5 Licencia
 - Licencia de Esta Obra

3 Blockchain

- **Introducción**
- Proof of Work
- Proof of Stake
- Curiosidades

¿Qué es?

- Una secuencia de bloques
 - Contienen transacciones
- Cada bloque no debe poder ser alterado
- Distribuido en varias máquinas

¿Para qué sirve?

Satoshi lo concibió como un  *ledger* o registro contable.

3 Blockchain

- Introducción
- **Proof of Work**
- Proof of Stake
- Curiosidades



¿Qué es Proof of Work?

- Mecanismo para confirmar la inocencia
- Debe hacer un trabajo determinado
 -  Con cierta complejidad
 -  Verificable



Consenso

- Los bloques se almacenan distribuidos.
- Los nodos deben estar de acuerdo en que tal bloque se va a agregar.
- Se necesita: **Mecanismo de consenso**
- ¿cuál es el siguiente estado del blockchain? → 51% deben aceptar.

Estructura Transacciones



Transacciones

We define an electronic coin as a chain of digital signatures.

– *Satoshi Nakamoto*

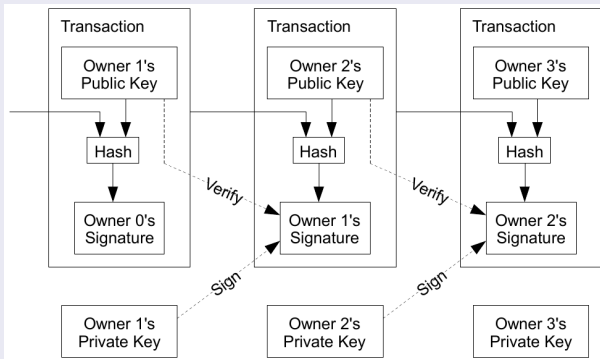


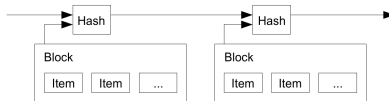
Imagen obtenida desde *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto.

Estructura del Blockchain

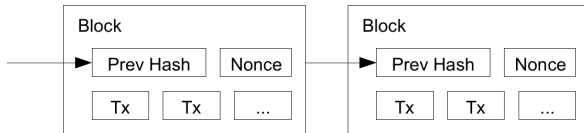
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block.

– Satoshi Nakamoto

Blockchain



Bloque



Ambas imágenes obtenidas desde *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto.

Algunos Links Interesantes

<https://bitcoin.org>

Interactivo

Recomendación de Carlos Mierez:

<https://andersbrownworth.com/blockchain>

Una página para crear bloques con una simplificación del blockchain.

Explorando bloques

- Explorar los bloques: <https://www.blockchain.com/explorer>
- Bloque cero: <https://www.blockchain.com/btc/block/0>
- Bloque cero ethereum: <https://etherscan.io/block/0>
- Bloque 2 EOS.io: <https://eosflare.io/block/2>

Algoritmo de Generación

¿Cómo se generan los hashes?

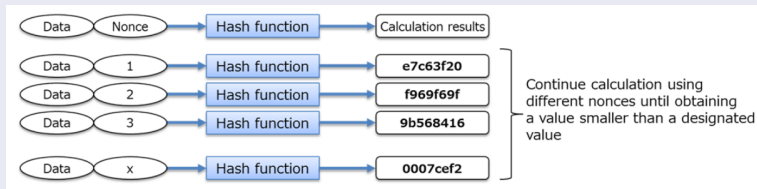


Imagen obtenida desde *Survey on Blockchain Technologies and Related Services*, Nomura Research Institute, 2016.

Bitcoin

- Bitcoin usa SHA-256.
- Busca hashes con varios ceros bits iniciales

¿Me creen?

Primer Bloque: <https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce2>

- Observar que el hash tiene varios ceros iniciales
 - 000000000019...
- Observar que todos los primeros bloques tienen una sola transacción
 - ¡Nadie usaba Bitcoin en sus orígenes!
- Observar que las primeras transacciones son el incentivo (¡50 BTC!)
- También que están asignados a Unknown (se cree que es Satoshi)

Hoy en día

- Las últimas transacciones redujeron el incentivo (12 BTC aprox.)
- La dificultad sigue en aumento (predecido por Satoshi)

¿Y si quisieramos crackearlo?

¿Qué sucede si hay máquinas maliciosas?

El problema de los generales bizantinos

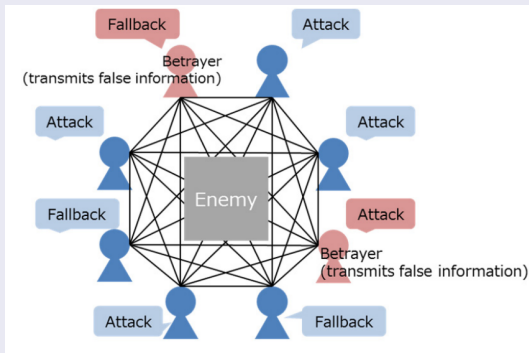


Imagen obtenida desde *Survey on Blockchain Technologies and Related Services*, Nomura Research Institute, 2016.
Se requiere más de un tercio de transmisiones maliciosas para controlar a los generales

¿En el Blockchain?

Para Crear una Transacción Falsa

- Se debe seguir el PoW.
- Se debe aprobar mutuamente el bloque.
- Para agregar bloques falsos:
 - Se debe generar bloques más rápido que el auténtico
 - Recrear bloques pasados
 - **Requiere enormes recursos computacionales**

3 Blockchain

- Introducción
- Proof of Work
- **Proof of Stake**
- Curiosidades

Contras del Bitcoin y PoW

- Validar bloques es muy lento (~10 min en BTC)
 - Bitcoin no está pensado para procesar datos rápidamente
- La capacidad de los bloques es poca (1MB)
- Se requiere mucho procesamiento y mucha energía
- ¿Se puede no crear o ralentizar la creación de monedas nuevas? → estabilizar el precio

Es necesario otra forma de Consenso

- Se requiere otra forma de consenso y validación de bloques
- Una forma más económica (procesamiento y energía) y rápida

Proof-of-Stake (PoS)

- El creador del bloque es designado en parte aleatoriamente
 - Se previene centralización al forger más rico
- No se requieren tantas nuevas monedas a generar
 - PoW pueden crear nuevos bloques sin transacciones solo por el incentivo (¿vieron los primeros?)
 - Se puede estabilizar el precio de la moneda
- Peercoin fue el primero en incorporarlo (2012, ver el White Paper).

Ethereum

- ~~Minero~~ → Se llaman “validadores”.
- Se pone capital 💰 en riesgo: 32ETH
 - Si el validador es deshonesto, pierde los 32ETH.
- Un validador es seleccionado aleatoriamente.
- Crea el bloque y lo envía a la red.
- También, se selecciona un comité de validadores aleatoriamente
 - Validan los bloques propuestos.

Variaciones del PoS

Existen otras variantes:

Randomized block selection RPoS es usado por Nxt y Blackchain.

Coin age-based selection Peercoin selecciona dependiendo del producto entre el tiempo de tenencia $\times$ la cantidad de monedas. Asegura la red y produce monedas gradualmente.

Delegated PoS DPoS es usado por EOS, Bitcoin-SCrypt, Steem, Lisk, etc. Usa un limitado número de nodos para proponer y validar un bloque.

Randomized PoS Orb usa RPoS para seleccionar un comité en vez de un nodo líder.

- https://en.bitcoin.it/wiki/Proof_of_Stake
- Andrew-Poelstra: On Stake and Consensus.
- Andrew-Poelstra: Distributed Consensus.

Lisk es una plataforma Blockchain y tiene un tutorial:

[https://lisk.io/academy/blockchain-basics/
how-does-blockchain-work/proof-of-stake](https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-stake)

[https://web.archive.org/web/20150127033542/https:
//cointelegraph.com/news/113157/
proof-of-work-proof-of-stake-and-the-consensus-debate](https://web.archive.org/web/20150127033542/https://cointelegraph.com/news/113157/proof-of-work-proof-of-stake-and-the-consensus-debate)

3 Blockchain

- Introducción
- Proof of Work
- Proof of Stake
- Curiosidades

Market Cap

Páginas que muestran el precio y la capitalización (market cap) de cada moneda.

- <https://www.blockchain.com/explorer/prices>
- <https://www.livecoinwatch.com>
- <https://coinmarketcap.com>

Blockchain

- <https://txstreet.com>
 - Animación usando analogía de gente en colectivo.
 - Gente: transacciones; colectivos: bloques.
- <https://developers.eos.io/welcome/latest/getting-started-guide/local-development-environment/index>
 - Se puede crear tu propia blockchain local con EOS.

Live Coin Watch

<https://www.livecoinwatch.com>



<https://txstreet.com>



Outline

- 1 Repaso
 - Repaso
- 2 Criptomonedas
 - Introducción
- 3 Blockchain
 - Introducción
 - Proof of Work
 - Proof of Stake
 - Curiosidades
- 4 **Próximamente...**
 - Continuará...
- 5 Licencia
 - Licencia de Esta Obra

- 4 Próximamente...
 - Continuará...



To be continued...



Próximamente: Smart Contracts...

Outline

- 1 Repaso
 - Repaso
- 2 Criptomonedas
 - Introducción
- 3 Blockchain
 - Introducción
 - Proof of Work
 - Proof of Stake
 - Curiosidades
- 4 Próximamente...
 - Continuará...
- 5 **Licencia**
 - **Licencia de Esta Obra**

5 Licencia

- Licencia de Esta Obra

Licencia de Esta obra

Excepto en los lugares que se ha indicado lo contrario:

Criptomonedas, Blockchain y Smart Contract se distribuye bajo una Licencia Creative Commons Atribución-SinDerivadas 4.0 Internacional.



CC-BY-ND

Excepto en los lugares que se ha indicado lo contrario:

Esta obra está licenciada bajo la Licencia Creative Commons Atribución-SinDerivadas 4.0 Internacional. Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nd/4.0/>.

