Criptomonedas, Blockchain y Smart Contract

Gimenez, Christian

27 oct 2018

Outline

Outline

Outline

Criptomonedas

Imagen descargada de: `https://steemitimages.com/0x0/http://i.imgur.com/blU8upr.jpg`

Criptomonedas

¿Qué es?

Criptomonedas

¿Qué es?

- Moneda digital

Criptomonedas

¿Qué es?

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

Criptomonedas

¿Qué es?

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

¿Cómo Implementarla?

Criptomonedas

¿Qué es?

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

¿Cómo Implementarla?

- ¿Cómo se podría proponer una moneda digital?

Criptomonedas

¿Qué es?

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

¿Cómo Implementarla?

- ¿Cómo se podría proponer una moneda digital?
- ¿Firmas digitales? ¿Qué hace falta?

Criptomonedas

¿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

Criptomonedas

¿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 una cosa con la misma moneda.
Solución: Entidad financiera.

¿Qué propone Satoshi Nakamoto?

Bitcoin

¿Qué propone Satoshi Nakamoto?

Bitcoin

- Moneda electrónica

¿Qué propone Satoshi Nakamoto?

Bitcoin

- Moneda electrónica
- Peer-to-peer

¿Qué propone Satoshi Nakamoto?

Bitcoin

- Moneda electrónica
- Peer-to-peer
  - Pagos on-line enviados directamente entre personas

¿Qué propone Satoshi Nakamoto?

Bitcoin

- Moneda electrónica
- Peer-to-peer
  - Pagos on-line enviados directamente entre personas
- Resolver el problema Double-Spending

¿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

¿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!? $\rightarrow$ Blockchain

Outline

Outline

Blockchain

¿Qué es?

Blockchain

¿Qué es?

- Una secuencia de bloques

Blockchain

¿Qué es?

- Una secuencia de bloques
  - Contienen transacciones

Blockchain

¿Qué es?

- Una secuencia de bloques
  - Contienen transacciones
- Cada bloque no debe poder ser alterado

Blockchain

¿Qué es?

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

Blockchain

¿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.

Outline

¿Qué es Proof of Work?

¿Qué es Proof of Work?

- Mecanismo para confirmar la inocencia

¿Qué es Proof of Work?

- Mecanismo para confirmar la inocencia
- Debe hacer un trabajo determinado

Introducción

¿Qué es Proof of Work?

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

¿Qué es Proof of Work?

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

Transacciones

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

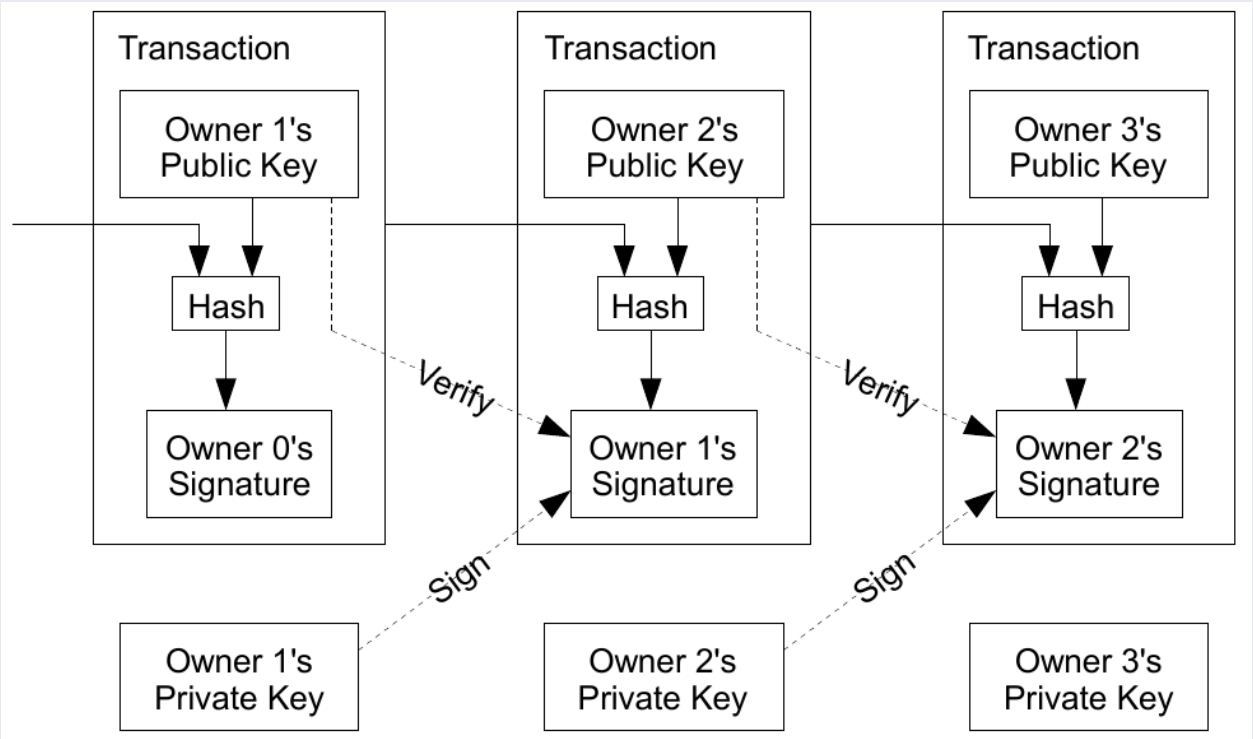


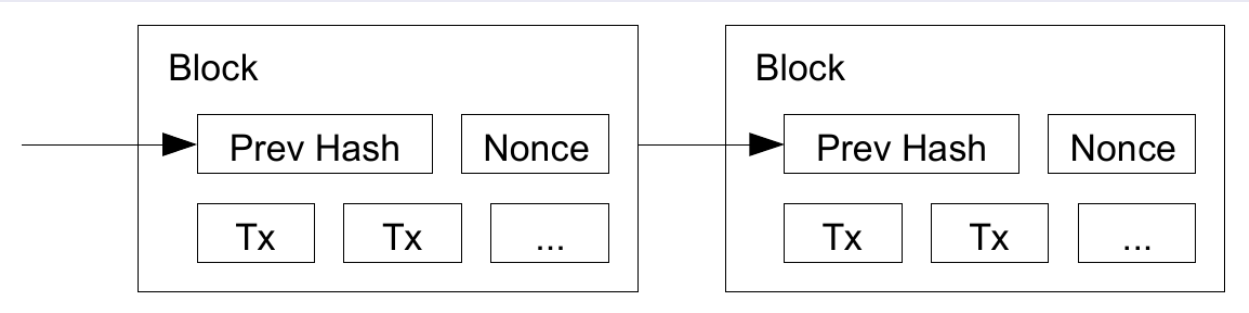
Imagen obtenida desde *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto.

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

Bloque

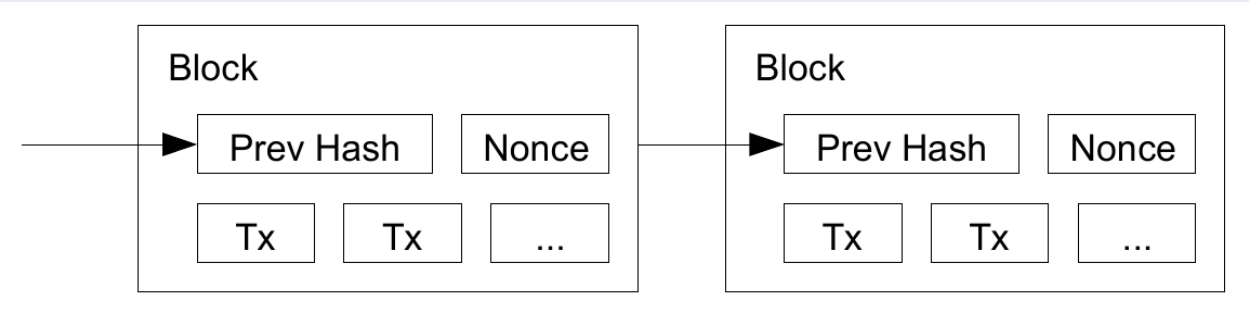


Estructura del Blockchain

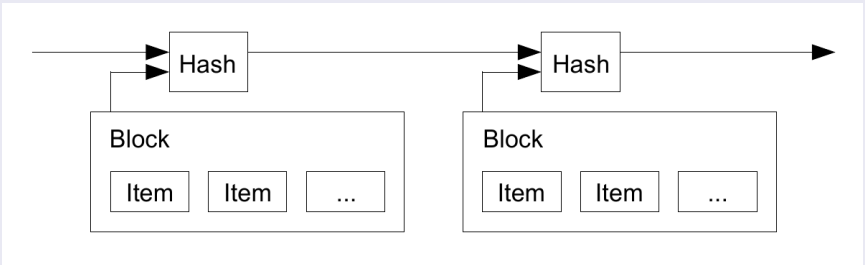
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block.

– Satoshi Nakamoto

Bloque



Blockchain



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

Algunos Links Interesantes

`https://bitcoin.org`

Explorar los bloques:

`https://www.blockchain.com/explorer`

Bloque cero:

`https://www.blockchain.com/btc/block-height/0`

Algoritmo de Generación

¿Cómo se generan los hashes?

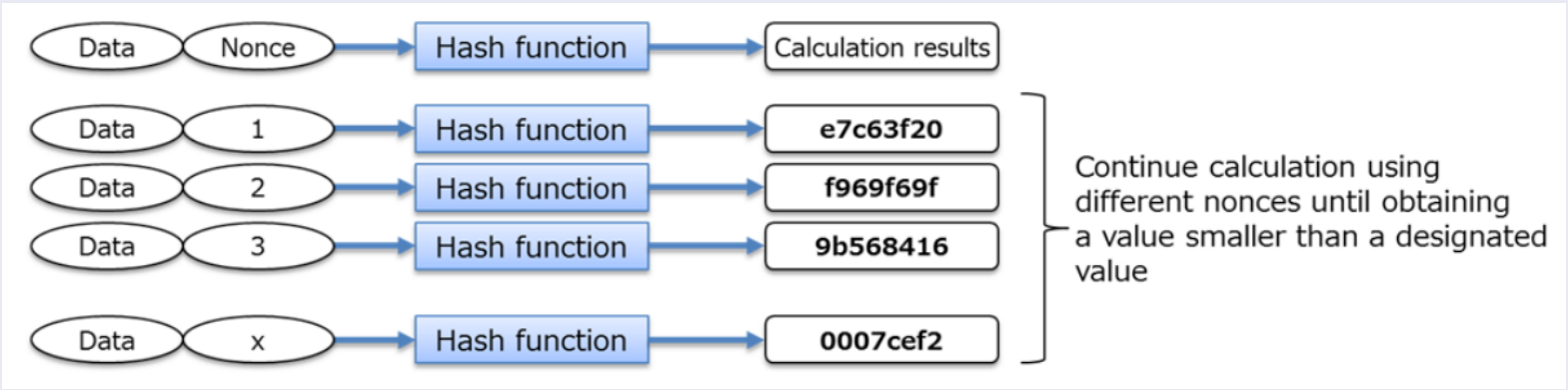


Imagen obtenida desde *Survey on Blockchain Technologies and Related Services*, Nomura Research Institute, 2016.

Algoritmo de Generación

¿Cómo se generan los hashes?

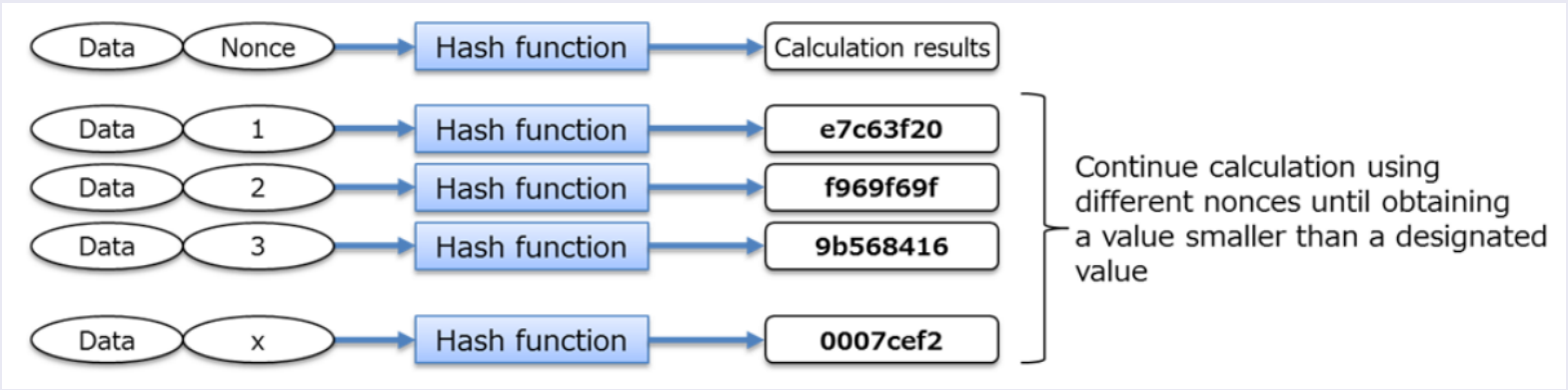


Imagen obtenida desde *Survey on Blockchain Technologies and Related Services*, Nomura Research Institute, 2016.

Bitcoin

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

En la Realidad

¿Me creen?

Primer Bloque: `https://www.blockchain.com/btc/block/`
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26`

En la Realidad

¿Me creen?

Primer Bloque: `https://www.blockchain.com/btc/block/`
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26`

- Observar que el hash tiene varios ceros iniciales

En la Realidad

¿Me creen?

Primer Bloque: `https://www.blockchain.com/btc/block/`
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26`

- Observar que el hash tiene varios ceros iniciales
  - `000000000019...`

En la Realidad

¿Me creen?

Primer Bloque: `https://www.blockchain.com/btc/block/`
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26`

- Observar que el hash tiene varios ceros iniciales
  - `000000000019...`
- Observar que todos los primeros bloques tienen una sola transacción

En la Realidad

¿Me creen?

Primer Bloque: `https://www.blockchain.com/btc/block/`
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26`

- 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!

En la Realidad

¿Me creen?

Primer Bloque: `https://www.blockchain.com/btc/block/`
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26`

- 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!)

En la Realidad

¿Me creen?

Primer Bloque: `https://www.blockchain.com/btc/block/`
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26`

- 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)

En la Realidad

¿Me creen?

Primer Bloque: `https://www.blockchain.com/btc/block/`
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26`

- 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

En la Realidad

¿Me creen?

Primer Bloque: `https://www.blockchain.com/btc/block/`
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26`

- 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.)

En la Realidad

¿Me creen?

Primer Bloque: `https://www.blockchain.com/btc/block/`
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26`

- 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

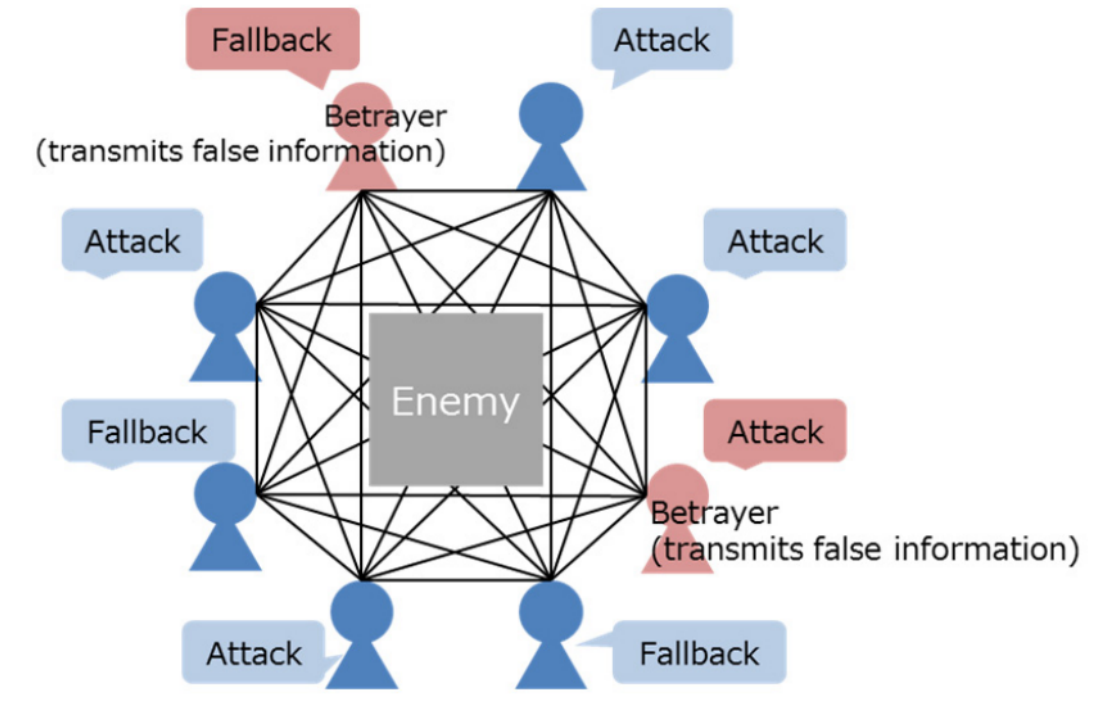


Imagen obtenida desde *Survey on Blockchain Technologies and Related Services*, Nomura Research Institute, 2016.
Se requiere más de un tercio de transmisiones maliciosas para controlar a los generales

¿En el Blockchain?

Para Crear una Transacción Falsa

¿En el Blockchain?

Para Crear una Transacción Falsa

- Se debe seguir el PoW.

¿En el Blockchain?

Para Crear una Transacción Falsa

- Se debe seguir el PoW.
- Se debe aprobar mutuamente el bloque.

¿En el Blockchain?

Para Crear una Transacción Falsa

- Se debe seguir el PoW.
- Se debe aprobar mutuamente el bloque.
- Para agregar bloques falsos:

¿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

¿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

¿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

Outline

Bitcoin y PoW

Bitcoin y PoW

- Validar bloques es muy lento (10 mins en BTC)

Bitcoin y PoW

- Validar bloques es muy lento (10 mins en BTC)
  - Bitcoin no está pensado para procesar datos rápidamente

Bitcoin y PoW

- Validar bloques es muy lento (10 mins en BTC)
  - Bitcoin no está pensado para procesar datos rápidamente
- La capacidad de los bloques es poca (1MB)

Bitcoin y PoW

- Validar bloques es muy lento (10 mins 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

Bitcoin y PoW

- Validar bloques es muy lento (10 mins 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

Otra forma de Consenso

Introducción

Bitcoin y PoW

- Validar bloques es muy lento (10 mins 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

Otra forma de Consenso

- Se requiere otra forma de consenso y validación de bloques

Introducción

Bitcoin y PoW

- Validar bloques es muy lento (10 mins 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

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)

Proof-of-Stake

Proof-of-Stake (PoS)

- El creador del bloque es designado en parte aleatoriamente

Proof-of-Stake

Proof-of-Stake (PoS)

- El creador del bloque es designado en parte aleatoriamente
  - Se previene centralización al forger más rico

Proof-of-Stake

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

Proof-of-Stake

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?)

Proof-of-Stake

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

Proof-of-Stake

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)

Variaciones del PoS

Existen varias variantes:

Randomized block selection RPoS es usaado 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.

Más info

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

Outline

Outline

¿Cómo surge?

Blockchain

¿Cómo surge?

Blockchain

- Es un registro contable

¿Cómo surge?

Blockchain

- Es un registro contable
- Datos:

¿Cómo surge?

Blockchain

- Es un registro contable
- Datos:
  - Quién emite

¿Cómo surge?

Blockchain

- Es un registro contable
- Datos:
  - Quién emite
  - Quién recibe

¿Cómo surge?

Blockchain

- Es un registro contable
- Datos:
  - Quién emite
  - Quién recibe
  - Cuánto

¿Cómo surge?

Blockchain

- Es un registro contable
- Datos:
  - Quién emite
  - Quién recibe
  - Cuánto
  - Fecha

¿Cómo surge?

Blockchain

- Es un registro contable
- Datos:
  - Quién emite
  - Quién recibe
  - Cuánto
  - Fecha

¿Y si...?

¿Qué pasa si se registran otros datos?

¿Cómo surge?

Blockchain

- Es un registro contable
- Datos:
  - Quién emite
  - Quién recibe
  - Cuánto
  - Fecha

¿Y si...?

¿Qué pasa si se registran otros datos?

¿Cómo surge?

Blockchain

- Es un registro contable
- Datos:
  - Quién emite
  - Quién recibe
  - Cuánto
  - Fecha

¿Y si...?

¿Qué pasa si se registran otros datos? $\rightarrow$ ¡Nacen los Smart contracts!

¿Qué es un Smart Contract?

¿Qué Es?

¿Qué es un Smart Contract?

¿Qué Es?

- Es código, un programa

¿Qué es un Smart Contract?

¿Qué Es?

- Es código, un programa
- Representa uno o varios contratos

¿Qué es un Smart Contract?

¿Qué Es?

- Es código, un programa
- Representa uno o varios contratos
- Se embebe en un blockchain

¿Qué es un Smart Contract?

¿Qué Es?

- Es código, un programa
- Representa uno o varios contratos
- Se embebe en un blockchain
- Se ejecuta automáticamente

¿Qué es un Smart Contract?

¿Qué Es?

- Es código, un programa
- Representa uno o varios contratos
- Se embebe en un blockchain
- Se ejecuta automáticamente
- Se programan reglas, condiciones y otra información relevante

¿Qué es un Smart Contract?

¿Qué Es?

- Es código, un programa
- Representa uno o varios contratos
- Se embebe en un blockchain
- Se ejecuta automáticamente
- Se programan reglas, condiciones y otra información relevante

¿Para Qué?

¿Qué es un Smart Contract?

¿Qué Es?

- Es código, un programa
- Representa uno o varios contratos
- Se embebe en un blockchain
- Se ejecuta automáticamente
- Se programan reglas, condiciones y otra información relevante

¿Para Qué?

- Intercambio de cosas de valor

¿Qué es un Smart Contract?

¿Qué Es?

- Es código, un programa
- Representa uno o varios contratos
- Se embebe en un blockchain
- Se ejecuta automáticamente
- Se programan reglas, condiciones y otra información relevante

¿Para Qué?

- Intercambio de cosas de valor
- Se requieren ciertas condiciones

¿Qué es un Smart Contract?

¿Qué Es?

- Es código, un programa
- Representa uno o varios contratos
- Se embebe en un blockchain
- Se ejecuta automáticamente
- Se programan reglas, condiciones y otra información relevante

¿Para Qué?

- Intercambio de cosas de valor
- Se requieren ciertas condiciones
- Ejemplo: Registrar una norma de forma que no se modifique y cobrar por el servicio.

Cita

Para decirlo fácilmente. . .

En Criollo

Cita

Para decirlo fácilmente. . .

En Criollo

Es como programar una clase que tiene una API. Los mensajes son puntos de entradas. Sus métodos implementan chequeos de ciertas condiciones para el intercambio de algo por un poco de cripto. Claro, también hay mensajes para leer información de estado y otras cosas.

– Christian Gimenez, contemporáneo.

Outline

DApps

Son aplicaciones descentralizadas basadas en Smart Contract.

DApps

Son aplicaciones descentralizadas basadas en Smart Contract.

> *DApp = Frontend Web + Smart Contract*
>
> – *Christian Gimenez, contemporáneo.*

Ejemplos

`https://www.stateofthedapps.com/`

DApps

Son aplicaciones descentralizadas basadas en Smart Contract.

> *DApp = Frontend Web + Smart Contract*
>
> – *Christian Gimenez, contemporáneo.*

Ejemplos

`https://www.stateofthedapps.com/`

- CryptoKitties Me pareció ver un lindo gatito...

DApps

Son aplicaciones descentralizadas basadas en Smart Contract.

> *DApp = Frontend Web + Smart Contract*
>
> – *Christian Gimenez, contemporáneo.*

Ejemplos

`https://www.stateofthedapps.com/`

- CryptoKitties Me pareció ver un lindo gatito...
- KittyCoin Club | Descentraland

DApps

Son aplicaciones descentralizadas basadas en Smart Contract.

> *DApp = Frontend Web + Smart Contract*
>
> – *Christian Gimenez, contemporáneo.*

Ejemplos

`https://www.stateofthedapps.com/`

- CryptoKitties Me pareció ver un lindo gatito...
- KittyCoin Club | Descentraland
- Hyperdragons

DApps

Son aplicaciones descentralizadas basadas en Smart Contract.

> *DApp = Frontend Web + Smart Contract*
>
> – *Christian Gimenez, contemporáneo.*

Ejemplos

`https://www.stateofthedapps.com/`

- CryptoKitties Me pareció ver un lindo gatito...
- KittyCoin Club | Descentraland
- Hyperdragons

Bueno, Seamos Serios...

DApps

Son aplicaciones descentralizadas basadas en Smart Contract.

> *DApp = Frontend Web + Smart Contract*
> — *Christian Gimenez, contemporáneo.*

Ejemplos

`https://www.stateofthedapps.com/`

- CryptoKitties Me pareció ver un lindo gatito...
- KittyCoin Club | Descentraland
- Hyperdragons

Bueno, Seamos Serios...

- Everypedia | EtherChat | Electchain (Election test)

DApps

Son aplicaciones descentralizadas basadas en Smart Contract.

> *DApp = Frontend Web + Smart Contract*
> — *Christian Gimenez, contemporáneo.*

Ejemplos

`https://www.stateofthedapps.com/`

- CryptoKitties Me pareció ver un lindo gatito...
- KittyCoin Club | Descentraland
- Hyperdragons

Bueno, Seamos Serios...

- Everypedia | EtherChat | Electchain (Election test)
- CanWork (Work distribution)

DApps

Son aplicaciones descentralizadas basadas en Smart Contract.

> *DApp = Frontend Web + Smart Contract*
> — *Christian Gimenez, contemporáneo.*

Ejemplos

`https://www.stateofthedapps.com/`

- CryptoKitties Me pareció ver un lindo gatito...
- KittyCoin Club | Descentraland
- Hyperdragons

Bueno, Seamos Serios...

- Everypedia | EtherChat | Electchain (Election test)
- CanWork (Work distribution)
- Kleros (Loomio)

DApps

Son aplicaciones descentralizadas basadas en Smart Contract.

> *DApp = Frontend Web + Smart Contract*
> — *Christian Gimenez, contemporáneo.*

Ejemplos

`https://www.stateofthedapps.com/`

- CryptoKitties Me pareció ver un lindo gatito...
- KittyCoin Club | Descentraland
- Hyperdragons

Bueno, Seamos Serios...

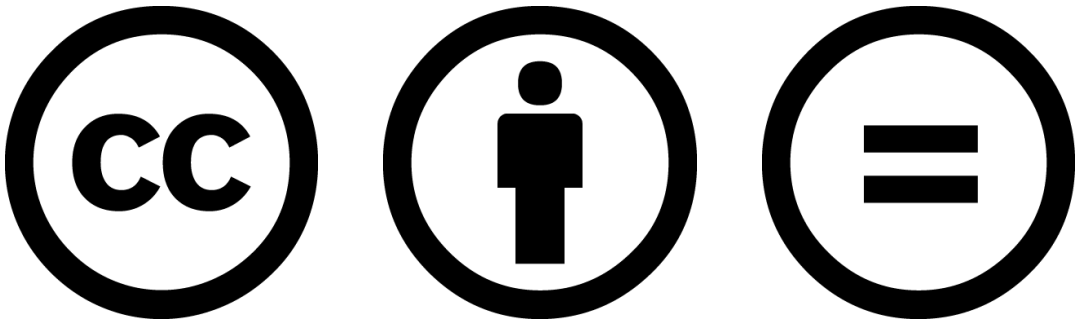
- Everypedia | EtherChat | Electchain (Election test)
- CanWork (Work distribution)
- Kleros (Loomio)
- Landmark | EOS Forum

Outline

Outline

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