Lic. Martín Josué Andrade Salazar

MIS

Descripción breve

El presente documento muestra notas importantes del curso Blockchain de la A a la Z: Crea tu criptomoneda en Python

BLOCKCHAIN

Blockchain de la A - Z: Crea tu propia criptomoneda en Python

**Módulo 1**

**¿Qué es el Blockchain?** (Cadena de bloques)

* Una cadena de bloques es una lista de registros en continuo crecimiento, llamados bloques, que están vinculado y asegurados mediante criptografía.
* Un bloque contiene diferentes tipos de datos, por ejemplo:
  + Data: “Hello World!”
  + Prev.Hash: 034DFA357
  + Hash: 4D56E1F05
* El bloque 1 también se le conoce como **Genesis Block,** al ser el primer bloque no tiene un Hash previo, pero si tiene su hash propio.
* El bloque 2 si tiene un Hash previo y si propio hash, su hash previo es el hash del bloque anterior, en este caso el hash del bloque 1.
* Así sucesivamente hasta llegar al último bloque.

**El Hash SHA256**

* La probabilidad de que 2 personas tengan la misma huella es 1 entre 60,000,000, esto porqué es un identificador único de cada persona, nos ayuda a identificar a las personas. Este principio se puede asociar con el Hash SHA256. Este algoritmo fue desarrollado por NSA
* **S =** Security
* **H =** Hash
* **A =** Algorithm
* Siempre tiene 64 caracteres, al estar escrito en hexadecimal contiene desde el numero 0 hasta el 9 y de la A - F, cada carácter ocupa 4 bits, es decir la multiplicación de 64 \* 4 nos da un total de 256, el numero total de bits que ocupa el algoritmo
* Los 5 requisitos que tienen los algoritmos de Hash (en general):
  + Unidireccionales
  + Deterministas
  + Cómputo Rápido
  + El efecto avalancha
  + Debe soportar colisiones

**Libro mayor inmutable**

Libro mayor tradicional – Este se guarda muy bien porqué de eso depende la información que esta guardada ahí

Al guardar todo en cadena de bloques como va un bloque tras otro bloque nos ayuda que no sea tan fácil de hackear (robar), si se cambia un bloque ya no coincide con el hash previo de los siguientes bloques y ahí es donde no se podría llevar a cabo el robo.

**Red distribuida P2P**

Las cadenas de bloques se copian en miles de millones de ordenadores, así si un bloque cambia en alguno de estos ordenadores, se notifica a los demás ordenadores y si en todos hay un cambio se hace y si no coinciden los cambios se sabe que se trata de un ataque.

**Como funciona el minado de bloques**

El bloque contiene diferentes componentes

* Numero de bloque
* Datos – puede tener varias transacciones, no solo una, si no,multiples
  + Información que contiene el bloque
* Hash previo
* Hash del propio bloque

|  |
| --- |
| Bloque: #3 |
| Nonce: 20 |
| Datos:  Kirill -> Hadelin 500 jbcoins  Kirill -> Ebay 100 jbcoins  Hadelin -> Juan Gabriel 70 jbcoins |
| Prev.Hash: 0000DF2E57FB432A |
| Hash: 82B5V4156AE315F7 |

Si se cambia el Nonce, se cambia el Hash por completo, a esto se le conoce como efecto **AVALANCHA.**

**Tolerancia a faltas bizantinas**

No puede haber más de un 33% de traidores para que funcione el algoritmo, si es menos si funciona.

**Protocolos de consenso**

Retos a los que se enfrenta es

1. Atacantes
2. Cadenas en competición

Tipos de protocolos de consenso

* Proof-of-Work (PoW)
* Proof-of-Stake (PoS)
* Otros

La mitad de la cadena debe de ser que este de acuerdo para que cambie

**Módulo 2**

**¿Qué es bitcoin?**

En [] se dice que el bitcoin consisten en un libro de contabilidad pública digital (Blockchain), que registra todos los movimientos y legitima la autenticidad de cada transacción haciendolas públicas para que sean los propios usuarios, sin intermediarios, los que lleven el control del movimiento y valor de los activos, evitando que haya manipulaciones

Existen 3 capaz muy importantes

* Tecnología
  + Blockchain
* Protocolo / Coin
  + Bitcoin
  + Waves
  + Ethereum
  + Neo
  + Ripple
* Token:
  + TRX, AE, REP, SNT, RHOC, MKR, PPT, BNB
  + WCT, B1, WGR, INTL
  + ACAT, TNC, DBC, RPX, QLC, TKY, ONT, IAM

El creados es Satoshi Nakamoto, el ecosistema de bitcoin es el siguiente

* Nodos
* Mineros
* Granjas mineras
* Mining Pools

**Políticas monetarias del bitcoin**

**Comprender la dificultad del minado**

**Mining Pools**

**El rango del Nonce**

**Transacciones**

**CPUs vs GPUs vs ASICs**

**Mempools**

**Los bosques huérfanos**

**El ataque del 51%**