Desarrollo Blockchain Ethereum con Solidity

Módulo 1 - Introducción a Blockchain

Introducción a Blockchain

Blockchain

- Almacenamiento distribuido y descentralizado.
- El cómputo y almacenamiento se distribuye entre los participantes o nodos.
- Compuesto por conjuntos de transacciones separados en bloques.
- Inmutabilidad: Los registros no pueden ser alterados.
- Seguridad: utiliza criptografía para asegurar los procesos y las transacciones.
- Resuelve problemas del cómputo distribuido como el doble gasto y la falla bizantina.
- No existen entidades que regulen la red si no que los participantes son los que aseguran su funcionamiento.
- Consenso: existen distintos protocolos, el más conocido hoy es el PoW o prueba de trabajo.
- El caso de uso más exitoso de esta tecnología: Bitcoin.

Bitcoin & Ethereum White Paper

- 31 de Octubre de 2008 - Bitcoin WhitePaper
- Es descrito como un sistema de pagos peer to peer sin intermediarios, es decir sin bancos (Peer to Peer Electronic Cash System)
- Diciembre de 2013 - ”Ethereum Whitepaper”
- Se discute sobre la necesidad de tener más control programático sobre las transacciones
- Se introduce la idea de Contratos Inteligentes como una entidad que puede enviar y recibir monedas.

- BTC WhitePaper: https://bitcoin.org/bitcoin.pdf
- ETH Paper: http://web.archive.org/web/20131228111141/http://vbuterin.com/ethereum.html

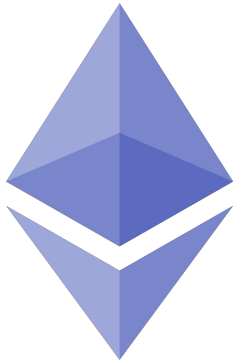
Introducción a Ethereum

Ethereum es una plataforma descentralizada que permite la creación de **acuerdos inteligentes** *(Smart Contracts).*

¿Qué es un Smart Contract? Es un conjunto de promesas, especificadas en formato digital, que incluyen protocolos que los participantes podrán ejecutar sobre dichas promesas. Es decir, en palabras simples, un **Smart Contract es un programa distribuido.**

Hasta la aparición de blockchain no fue posible implementar esta idea, dado que se requiere de un sistema financiero que lo soporte junto con la infraestructura de transacciones programables.

Con los Smart Contracts, en base a una serie de entradas, se pueden ejecutar transacciones, hacer pagos, intercambiar VALOR.



¿Qué es el Ether?

- El **Ether** es la moneda utilizada en la Ethereum Blockchain. Sirve como medio de pago para los Smart Contracts y también como almacén de valor.
- Un Ether que se puede dividir hasta en 18 decimales.
- No hay límite en la cantidad de unidades de ether que pueden ser emitidos.*
- Es muy importante tener en cuenta que los Smart Contracts trabajarán en WEI, ya que al momento los decimales no son soportados por la EVM.

¿Qué es el Ether?

Al igual que cualquier otro criptoactivo, el Ether posee fluctuaciones constantes que pueden verse como en el siguiente gráfico.

WEI

- Es la 1/18 parte de un Ether.
- **1 ETH = 10^18 WEI (1 ETH = 1000000000000000000 WEI)**
- Su finalidad es la de subdividir una unidad de Ether.
- Existen múltiples conversiones a distintas unidades.
- Los Smart Contracts operan en WEI y NO en Ether.

Wei	1000000000000000000
Kwei, Ada, Femtoether	1000000000000000
Mwei, Babbage, Picoether	1000000000000
Gwei, Shannon, Nanoether, Nano	1000000000
Szabo, Microether,Micro	1000000
Finney, Milliether,Milli	1000
Ether	1
Kether, Grand,Einstein	0.001
Mether	0.000001
Gether	0.000000001
Tether	0.000000000001
USD(at 224.172$ p/ ether)	224.172
EUR(at 194.526€ p/ ether)	194.526

Block Time

Es la cantidad de tiempo que toma ejecutar esos cientos de miles de diferentes posibles hashes hasta encontrar el valor que actualmente sea igual al que buscamos.

DATA	+	NONCE	=	OUTPUT HASH	OH BASE 10	En el target? (<1000)
Lorem ipsum	+	0	=	a23042b2e	178917215	NO
Lorem ipsum	+	1	=	cbc1491	29589283	NO
Lorem ipsum	+	2	=	0ca24258	94869869	NO
Lorem ipsum	+	3	=	d9eed91	13938166	NO
Lorem ipsum	+	4	=	1488baec	419386918	NO
Lorem ipsum	+	5	=	0077bbb	100	SÍ

Tiempo en encontrar la solución

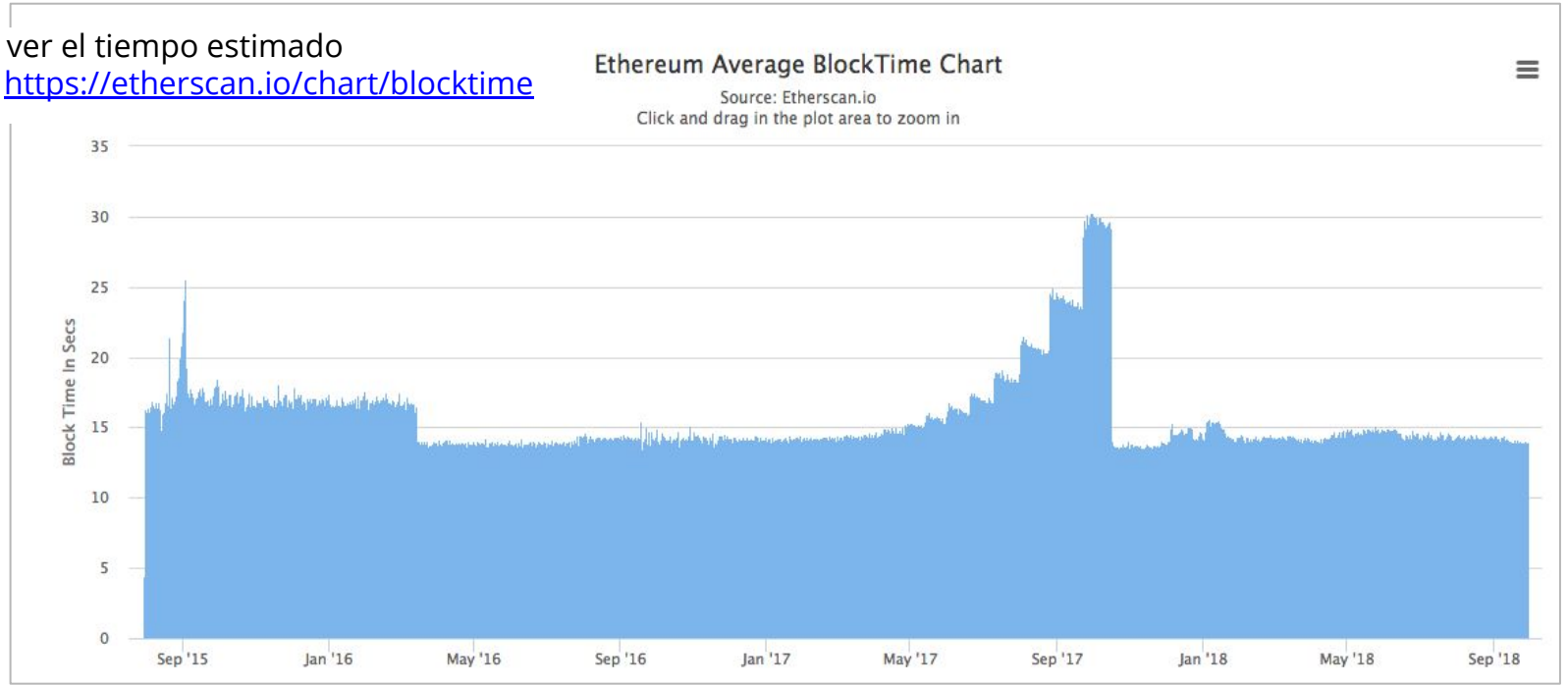
=

BLOCK TIME

OH = Output Hash

Block Time

Se puede ver el tiempo estimado actual en https://etherscan.io/chart/blocktime



Confirmation time

Es el tiempo que se estima esperar hasta tener la certeza de que la transacción está confirmada.

Pero... Si ya escribió en un bloque, ¿no está confirmada? No, puede que exista otra ramificación en la blockchain que termine dejando afuera mi transacción, por lo tanto, el tiempo de confirmación va a considerar la formación de bloques subsiguientes al de nuestra transacción para tener la certeza suficiente de que ya no existe posibilidad alguna de cambio.

En el caso de Ethereum no hay un tiempo definido. En el Whitepaper se habla de 7 bloques (2 minutos aproximadamente), pero algunos autores afirman que se debe esperar hasta unos 250 lo que termina siendo un tiempo cercano a una hora.

¿Cómo podemos hacer para acelerar la confirmación de nuestra transacción? Pagando altos montos de comisión se logra confirmar rápidamente la transacción.

¡Muchas gracias!

¡Sigamos trabajando!