CURSO
BLOCKCHAIN

Módulo 3

Parte 1: Teoría Blockchain

CURSO BLOCKCHAIN

Teoría Blockchain (40m)

1. **Blockchain:** Nodos, Sistema distribuido, transacción, mempool, bloque, minado, doble gasto, comunicación p2p, consenso, Ataque 51%, generales bizantinos, Merkle tree, inmutabilidad, Marco financiero para blockchain, Valor del btc. (1hs 45')
2. **Tipos de blockchain** (5')
3. **Wallets:** Aplicación, cuentas (clave privada, pública y address), Firma criptográfica asimetrica, Verificación, Metamask. Custodial vs Non Custodial (Responsabilidades), Frias vs Calientes. (30')
4. **Explorador de bloques** (10' practico)
5. **Valor de otras criptos:** Filecoin, btt, LanguageNearYou (10')
6. **Inversión:** CEX (Binance) vs DEX (Pancakeswap), Valor tecnológico vs especulativo, HODL, TRADE, BID, ASK, spread, resistencia, soporte. Stake (pool+ PoS), Farm + protocolo de liquidez, apalancamiento, flash loan, p2p. (40')

CURSO
BLOCKCHAIN

Blockchain

Conceptos de su funcionamiento

CURSO BLOCKCHAIN

Escribanos

Situación problemática

¿Qué sucede si:

1. El archivo se pierde o se daña?
2. El escribano modifica algún dato luego de firmado el documento?
3. Si el escribano actúa de mala Fé al validar el contrato?

CURSO BLOCKCHAIN

Sistema Distribuido de Escribanos

1. Tiene que perderse de 4 lugares a la vez.

2. Tendremos 3 copias con datos originales

3. Los otros 3 escribanos no lo validarán. Y si 3 escribanos se ponen de acuerdo? => Ataque 51%

Escribano 1

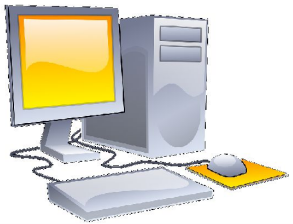
Escribano 2

Escribano 3

Escribano 4

Sistema distribuidos de nodos

Nodo 1



Nodo 2

Nodo 3

Nodo 4

Recompensa vs Castigo

Escribano:

- Recompensa: Honorarios
- Castigo: Destitución de la matrícula.

Nodos Mineros:

- Recompensa: Coinbase + fees
- Castigo: Electricidad + Equipos (PoW) / Dinero (PoS)

Valor de las criptomonedas

Bitcoin: Este por sí solo no tiene dueño. Para adueñarse de él hay que **minarlo**. Para minarlo debo utilizar recursos (Electricidad + ASICs). Además la gente para usar la blockchain tendrá que pagar un fee (No es gratis) lo que obligará a incurrir en el uso de recurso para minarlo o comprarlos con dinero en un Exchange. Esto genera un valor tecnológico.

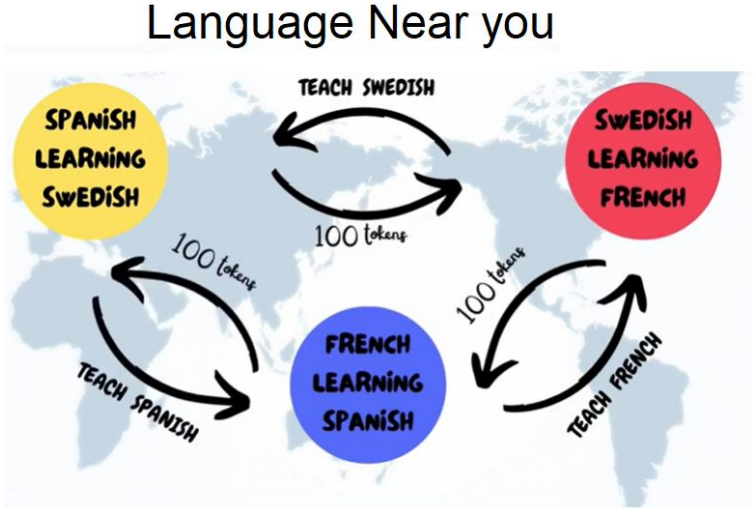
Ethereum: Nos brinda una computadora en la nube con características propias de la blockchain por lo que podemos considerarlo como un servicio. Para usarlo tendremos que pagar en Ethers, la criptomoneda de esta blockchain. Para obtener los ethers podremos conseguirlos brindando el servicio de esta computadora en la nube (minando) o comprando los ethers en un Exchange.

Filecoin: Utiliza un consenso llamado Proof of Space. Básicamente para recibir de esta criptomoneda necesitarás brindar espacio de almacenamiento. Con la criptomoneda podrás luego comprar espacio de almacenamiento por lo que si la necesitas o la minas o la compras.

Al valor tecnológico siempre le sumaremos el especulativo y la oferta/demanda!!!

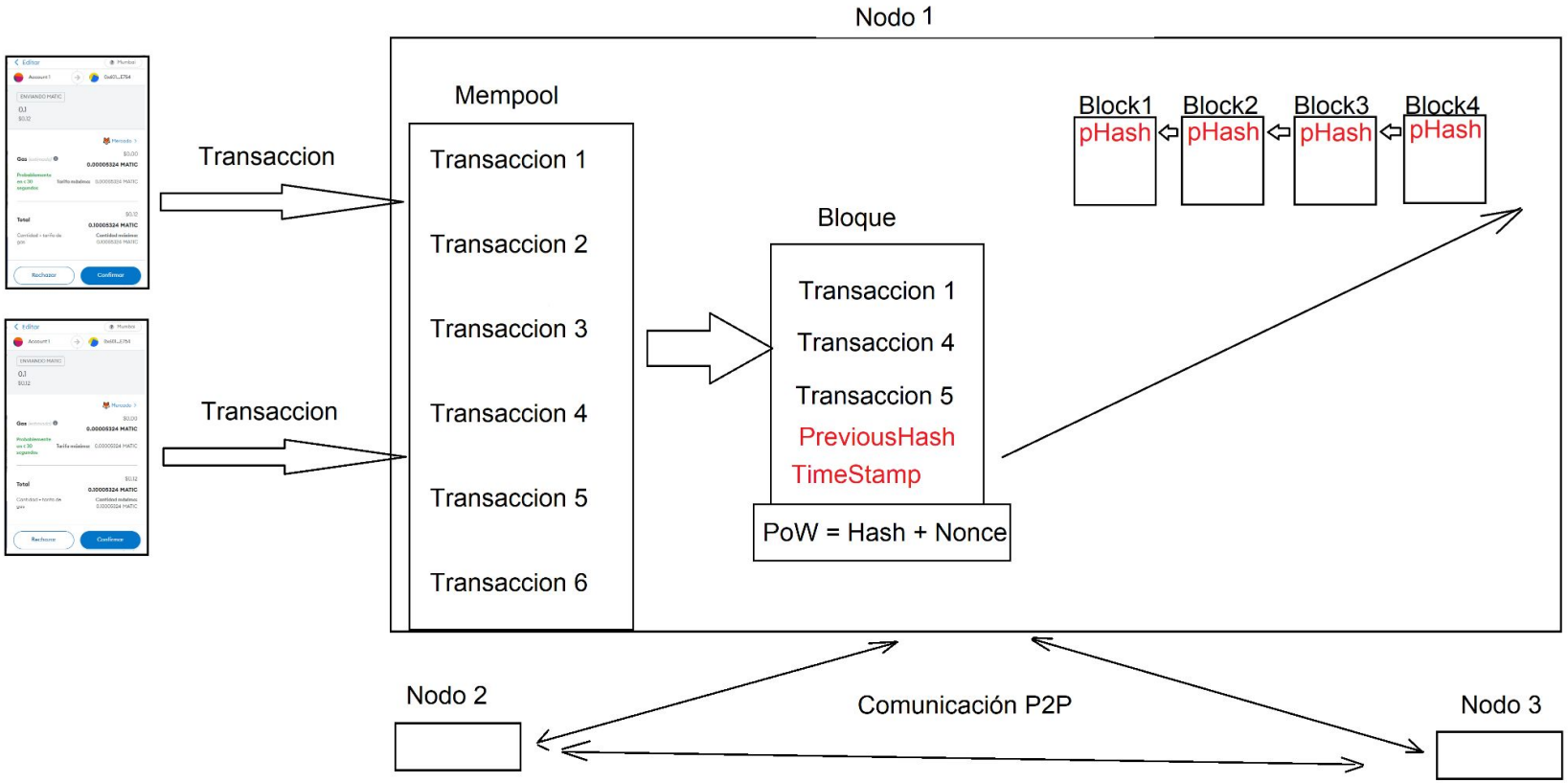
CURSO BLOCKCHAIN

Valor de tokens



CURSO BLOCKCHAIN

Panorama general de la blockchain



Panorama práctico de la blockchain

Para ver la práctica utilizaremos los links que hemos expuesto en el módulo 1.

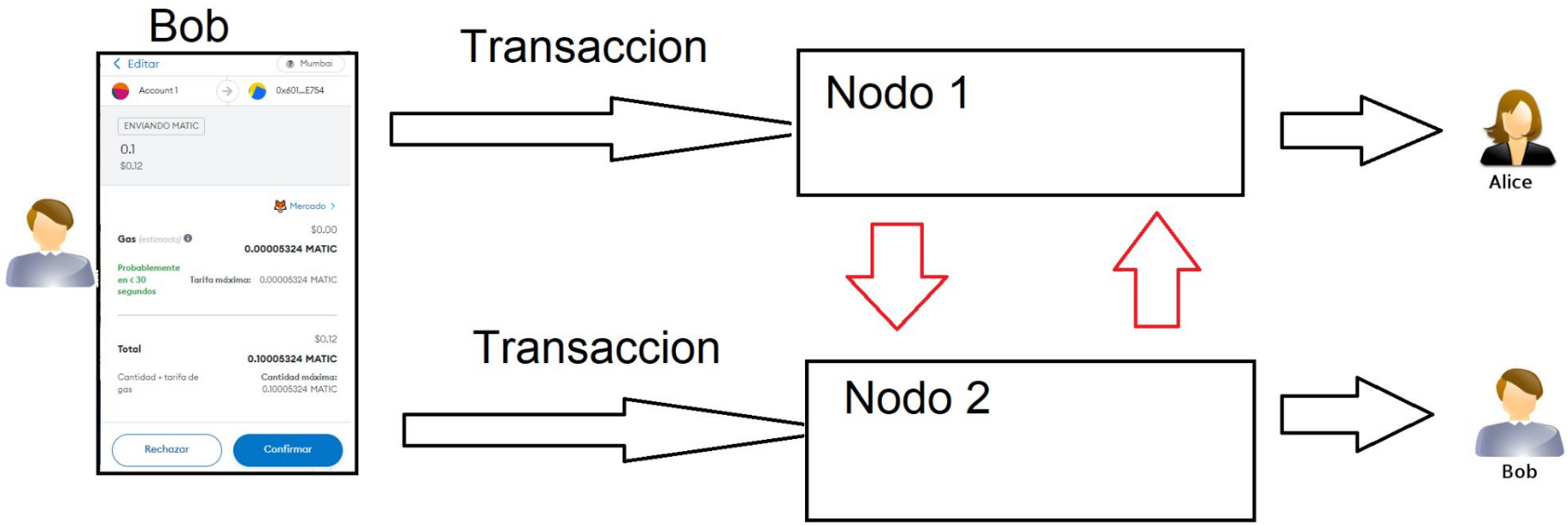
https://andersbrownworth.com/blockchain/public-private-keys/keys

https://andersbrownworth.com/blockchain/hash

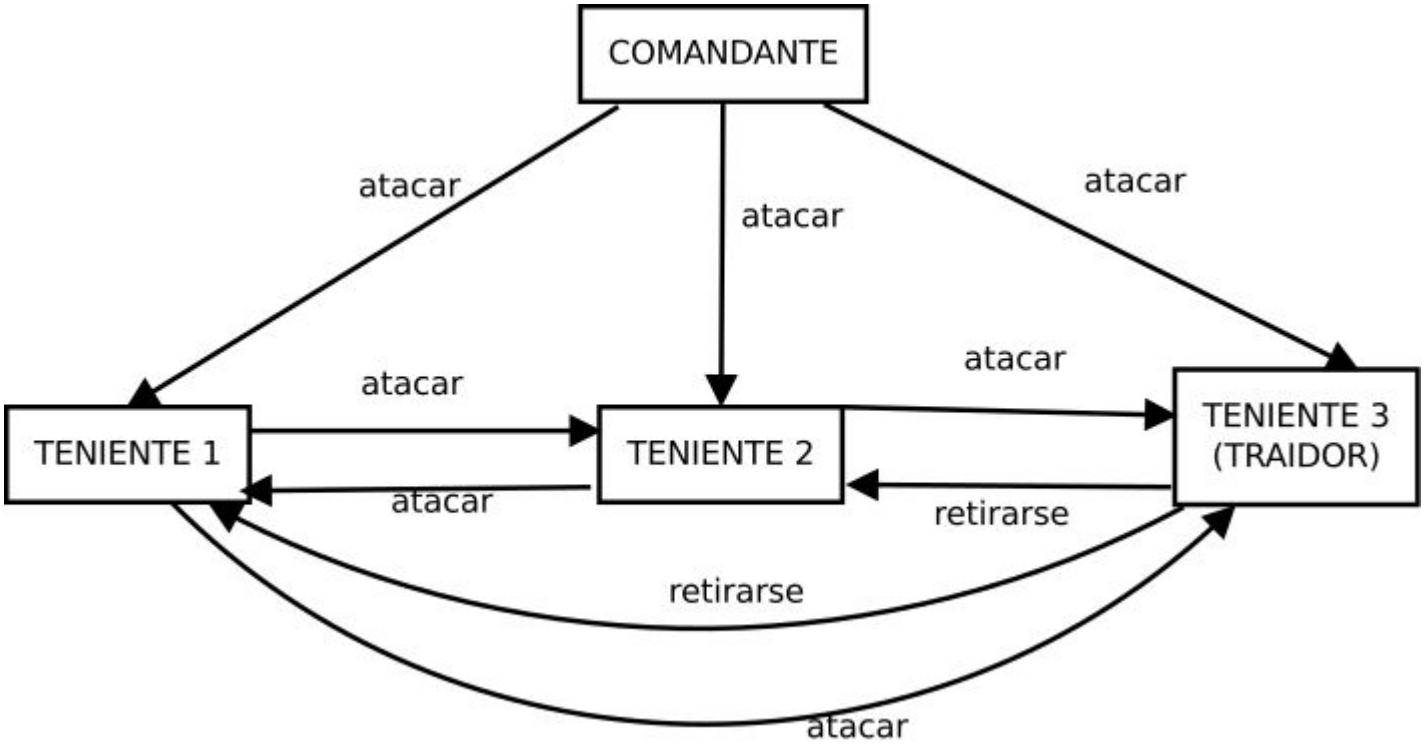
Para ver cómo está conformado un bloque usaremos un explorador de bloque:

https://etherscan.io/block/1704953

Doble Gasto


Bob
Editar
Mumbai
Account 1
0x601...E754
ENVIANDO MATIC
0.1
$0.12
Mercado
Gas (estimada)
$0.00
0.00005324 MATIC
Probablemente en < 30 segundos
Tarifa máxima: 0.00005324 MATIC
Total
$0.12
0.10005324 MATIC
Cantidad + tarifa de gas
Cantidad máxima: 0.10005324 MATIC
Rechazar
Confirmar
Transaccion
Nodo 1
Alice
Transaccion
Nodo 2
Bob

Generales Bizantinos



Ethereum

Esta red funciona de una forma muy similar a Bitcoin para poder así guardar su inmutabilidad y asegurar su transparencia. Por temas ecológicos ha emigrado su método de consenso de PoW a PoS pero sigue el mismo concepto estudiado. La única diferencia es que ahora lo que pone en riesgo no es electricidad y equipos sino dinero que debe apostar, si hace las cosas bien ganará el dinero que mina, si hace las cosas mal perderá lo que tiene apostado. Este cambio lo hizo en el 2022 con “The merge” o ethereum 2.0. Por eso el Nonce ahora lo verán en 0 ya que no realizan PoW.

La otra diferencia con Bitcoin es que las transacciones no necesariamente son de valor de una billetera hacia otra sino que pueden ser programas que conoceremos como Smart Contracts por su inmutabilidad y que poseerá una máquina virtual llamada EVM para hacer estos cómputos. El precio/incentivos a pagar será en Ether (la criptomoneda nativa de la red ethereum)

Bibliografía

Bmoney: http://www.weidai.com/bmoney.txt

PoW: https://nakamotoinstitute.org/finney/rpow/

Bitcoin whitepaper: https://bitcoin.org/bitcoin.pdf

Webs para estudiar blockchain de manera interactiva:

https://andersbrownworth.com/blockchain/public-private-keys/keys

https://andersbrownworth.com/blockchain/hash

Resumen

1) **Bitcoin:** Aunque las criptomonedas fueron concedidas mucho tiempo antes como estudiamos en la historia, la blockchain aún experimentaba problemas por su sistema distribuido como el doble gasto y el problema de los generales bizantinos. Esto bitcoin lo soluciona con su sistema de consenso y el proof of work. Otra cosa que permitió que la blockchain pueda moverse es el diagrama de incentivos económicos que le dan un marco financiero (Nadie invertiría recursos si no obtiene algo a cambio)
2) **Ethereum:** Al igual que Bitcoin, la teoría de los smart contracts se remonta a 1994 (Szabo), pero hasta el invento de la blockchain no existía un marco financiero que sustente la computadora que se necesitaba para que esto pueda operar. (Nadie pondría recursos sin retribución a cambio).
3) **Espíritu:** Si bien comenzó como una criptoanarquía, la tecnología creada se hizo muy poderosa como para ser la tecnología del futuro. (La tecnología no es buena o mala, las personas lo son)

Consultas

¿?

Reto

https://cursoblockchain.com.ar/

Actividad

Contratos

1. Terry se compromete a limpiar el auto de Stacey a cambio de una tarifa de $200.
2. John se compromete a proporcionar a Rory una cantidad fija de 10 kilos de alimentos cada mes a cambio de una tarifa de $500.
3. Nancy se compromete a reparar el televisor de Lee por una tarifa de $300.

Enunciados

1. Minar los 3 contratos en Peer A, B y C. Cada contrato en un bloque. (https://andersbrownworth.com/blockchain/distributed)
2. Verificar que los 3 hashes del bloque 3 sean iguales.
3. ¿Qué pasa si Rory tiene acceso al nodo B y quiere modificar la cantidad de alimentos a su favor y cambia los 10Kg por 11Kg? Minar de vuelta esta versión y comparar los hash de los últimos bloques (el bloque 3). ¿Qué sucedió? ¿Cómo comprobarán los nodos A y C que el nodo B está haciendo trampa?

Enunciados VIP

Dado el siguiente bloque: https://etherscan.io/block/1704956

Verificar:

1) Hash
2) Nonce
3) Timestamp
4) ¿Cuánto fue el block reward?
5) Verificar que el previous hash de este coincida con el hash del bloque anterior: https://etherscan.io/block/1704955

Dado: https://etherscan.io/block/17062859
¿Por qué el Nonce está en 0?