CURSO
BLOCKCHAIN

Módulo 3

Parte 2: 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

Wallets y exploradores de bloques

¿Qué es una cuenta de criptomonedas?

Estas son un **conjunto de 3 números** que nos permitirán guardar valor, así como realizar transferencias y verificar su origen, haciendo uso de la criptografía asimétrica estudiada.

- **Clave Privada** = Me permite crear transacciones
- **Clave Pública** = Me permite verificar la autenticidad de la transacción.
- **Dirección**= Me permite recibir transacciones.

Todas las criptomonedas se basan en estos 3 principios aunque los procesos matemáticos del uno al otro pueden variar.

Cuentas

Clave Privada:

- Sirve para firmar mensaje asegurando autenticidad.
- Numero aleatorio de 256 bit, 32 bytes o 64 digitos hexadecimales.
- Si la pierdo, estoy frito

Clave Publica:

- Sirve para verificar la autoría.
- Derivada de la clave privada mediante ECDSA.
- No sirve para firmar mensajes

Address:

- Sirve para recibir transacciones
- Derivado de la clave publica usando keccak. Bit_96_256(keccak256(clave_publica))
- Aunque a veces la usen como sinonimo de clave publica, son distintas.

Seguridad de cuentas

La seguridad solo se basa en la probabilidad casi nula de que 2 personas escojan el mismo número aleatorio para su clave privada siendo que casi hay una cuenta para cada átomo del universo visible. Esto vuelve inutil la fuerza bruta o rainbow tables dejando solo la ingeniería social para el robo de claves privadas.

Entropía

- Medida de qué tan aleatorio es realmente un número.
- Para que dos números no coincidan, la entropía debe ser alta. Por esto no sirve usar generadores randoms como los que se mostraron sino que debemos usar aleatorizadores a nivel criptográficos.

Problema

Las claves privadas equivalen a 64 números hexadecimales que debemos guardar para poder hacer una transferencia.

¿Qué pasa si copiamos mal 1 de los 64 números al guardar la billetera?

Perdemos todos los fondos de la billetera

Solución

Mnemónico

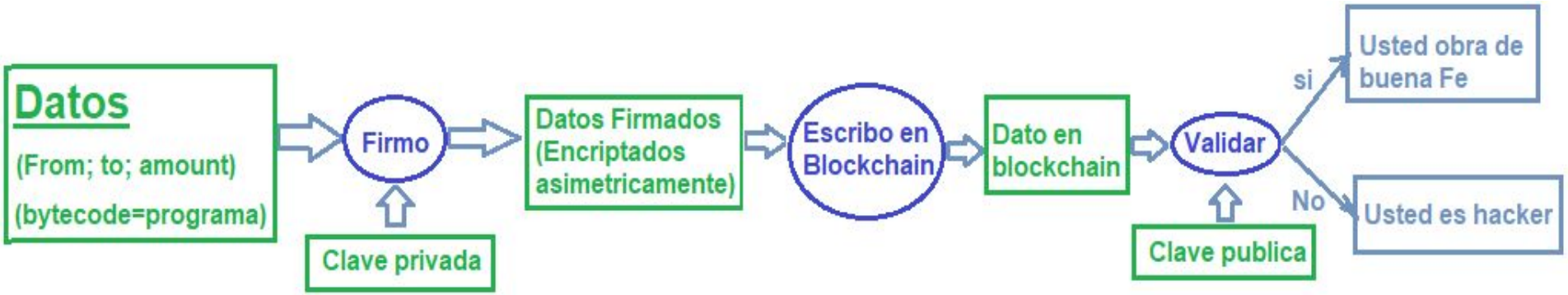
Existe un algoritmo conocido al cual le ingresamos el mnemónico (12 o 24 palabras) y podremos ir generando un conjunto de claves privadas determinísticas, Esto quiere decir que si conocemos el mnemonico siempre crearemos las mismas claves privadas al ejecutar el algoritmo. Este estandar se lo conoce como BIP39.

Pueden verlo en el siguiente enlace: https://iancoleman.io/bip39/

mnemónico= spoon fancy distance clock goose fiber auction daughter birth trim mandate million

Por qué palabras en vez de numeros: Porque las palabras tienen mayor nivel de redundancia. Si alguien escribe Inzect porque copió mal, no le costará mucho trabajo descubrir que la palabra en realidad era insect.

Resumen de funcionamiento



Wallets

Es una **interfaz de usuario**, para proporsionarle un **metodo gráfico** y más sencillo para realizar las operaciones.

Aplicaciones de wallets pueden ser Metamask, trustwallet, la interfaz de un exchange centralizado que tiene una billetera y te provee una interfaz gráfica para que la manejes, etc.

Tipos de Wallets

Segun su conexion a internet:

- Cold Wallets: No conectadas a internet. (Paper wallets, Hardware Wallets)
- Hot Wallets: Conectadas a internet. (Metamask, trustwallet)

Según dueño de las claves privadas:

- Custodias: Alguien más maneja tus claves privadas y por lo tanto tus criptomonedas o tokens. Tu identidad. (Exchanges centralizados como Binance)
- No Custodias: Solo tu conoces tus claves privadas y administras tus tokens y criptomonedas. (Metamask, trustwallet, paper wallets, hardware wallets)

Ventajas y Desventajas

Cold vs Hot Wallets:

- Más seguras por no estar conectadas a internet.
- Más difícil de manejar o más caras.

custodia vs no custodias:

- La seguridad de las custodias es manejada por profesionales.
- Las custodias recibirán más ataques informáticos.
- NYKNYC (Not your keys, not your coins)
- Las no custodias son más difíciles de manejar
- En las custodias puedo recuperar la clave si la pierdo.
- Si la custodia desaparece puedo perder el dinero.

Redes

Cómo explicamos, todas las criptomonedas siguen los mismos principios de criptografía de clave pública, sin embargo la matemática y funciones utilizadas varían de una a otra. Así Bitcoin usa una y Ethereum usa otra y por eso no todas las billeteras sirven para todas las criptomonedas.

Tendremos billeteras de Bitcoin, de Ethereum, de Solana, de Near, de polkadot, etc. Existen wallets multi chain que tienen a más de una, pero en realidad lo que hacen es guardar cuentas distintas dentro de la misma aplicación de usuario.

Por se ethereum la primera en desarrollar smart contracts y luego el resto una copia, muchas se hicieron EVM compatibles (EVM= ethereum virtual machine. Es la computadora que procesa los smart contracts). Todas las que sean EVM compatible podrán ser utilizadas con la misma wallets de ethereum ya que trabajarían de la misma forma, pero hay que agregarles la red.

Algunas de estas redes pueden ser: Binance Smart Chain (BSC), Polygon, Arbitrum, Avalanche, Optimism, Fantom, Cronos y muchas otras.

CURSO BLOCKCHAIN

Wallets Multifirmas

La Billetera Multifirma contiene las direcciones publicas de Billetera 1 y Billetera 2 y solo permitirá la extracción cuando haya comprobado que ambas quieran hacerlo.

Panorama práctico de Wallets

1. Descargar Metamask
2. Agregar red.
3. Obtener dinero de una faucet.
4. Crear otra cuenta.
5. Mandarse dinero de una cuenta a la otra.
6. Verificarlo en el explorador de bloques.

Bibliografía

Creando una paper wallet, Cristian Marchese: https://www.youtube.com/watch?v=psSG8DHTZQM

Ethereum Yellowpaper, Gavin Wood: https://ethereum.github.io/yellowpaper/paper.pdf

Mastering ethereum, Andreas Antonopoulos: https://drive.google.com/file/d/1zlDsf1Ea320IqNXNwaY5V9Z0RHCewHB3/view?usp=sharing

Mastering Bitcoin, Andreas Antonopoulos: https://drive.google.com/file/d/1maYq16-TOumyo4aiGNwU7RUtaIMPJc-8/view?usp=sharing

BIP39: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

Resumen

1) **Cuenta:** Conjunto de una clave privada para firmar una transacción, una clave pública para que las transacciones puedan verificarse y una dirección para poder recibir tokens o criptomonedas.
2) **Wallets:** Aplicación de usuario que guarda cuentas y simplifica el proceso de firma de transacciones de los usuarios. La más conocida es Metamask, la cual es una hot wallet por estar conectada a internet. En el caso de tener mucho dinero se recomienda cold wallets como las hardware wallets.
3) **NYKNYC:** Si no es tu clave, no son tus monedas. Frase muy conocida en el mundo cripto.
4) **Explorador de bloques**: dApps que sirven para ver y estudiar las transacciones y bloques que hay dentro de una blockchain determinada.
5) **Wallets multifirmas:** Contratos Inteligentes que unen voluntades de varias cuentas individuales. Muy usadas en DAOs.

Consultas

¿?

Reto

https://cursoblockchain.com.ar/

Enunciados

1. Mandar a una dirección 1 Matic. ¿Cuántos Matics te devuelve?
2. Decir en qué horario se hizo una cierta transacción.
3. Decir de qué valor fue una determinada transacción.
4. ¿Quién lo mandó?
5. ¿A quién le llegó?
6. En qué bloque se minó dicha transacción.