Seminario Blockchain

Clase Práctica N·2

Profesores:
- Esp. Ing Fernando Boiero

UNIVERSIDAD CATÓLICA DE CÓRDOBA
JESUITAS

Blockchain Demo: Parte 2 - Public / Private Keys & Signing

- Continuaremos con la demo de la clase pasada pero nos adentraremos un poquito más.

- Iremos viendo las partes claves de una llave Pública y Privada, como se asocian y dependen una de otra... así como también la firma.

Coinbase Transactions:

- Habíamos visto la clase anterior sobre transacciones entre personas.
- Ahora veamos lo siguiente, cómo prevenimos una transacción que gasta toda la plata de otra persona para acreditarse a uno mismo? Pareciera que no hay protección para eso en lo que estuvimos viendo.

- Para esto vamos a tener que ver los conceptos de Pares de claves Públicas y Privadas, a las cuales posteriormente las vamos a usar para firmar transacciones… veamos eso ahora…

Public/Private Key Pair:

- La **clave privada** es un número muy muy largo generalmente. Random… sin coherencia alguna en la secuencia de números.

- La clave Privada es muy importante que cada uno como **usuario** y dueño de la misma siempre la **mantenga secreta y no la comparta**… porque es de la que depende toda la seguridad y acceso a las operaciones.

- La **clave Pública** en cambio, es **la que se comparte con todos** y que no hay problema que el resto la sepa… no hay riesgo de que la sepa todo el mundo.

- **No hay forma de derivar de una Public Key a una Private Key**. Es como una versión pública de tu clave privada pero que no revela la clave privada en sí.


Public Key
Private Key
Message
+ = Encrypted
+ = Decrypted
+ = Signed
+ = Authenticated

- Hagamos click en el botón ¨Random¨ así obtenemos una Clave Privada buena, consistente y original. Y sumado a esto surgirá la Clave Pública asociada. La Clave Privada obtenida va a ser la que voy a usar para hacer firmas (Signatures).

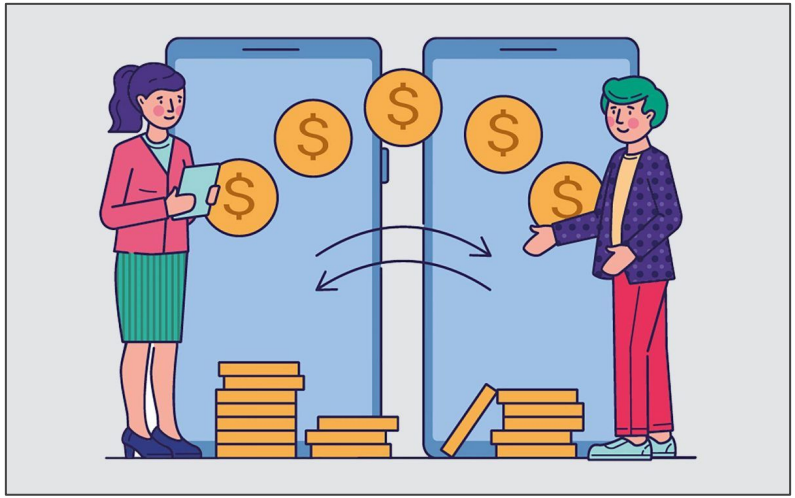
- Hagamos algunas firmas ahora…

Signatures:

- Veamos una **Firma de un mensaje**… (Utilizando la Clave Privada para firmar) al hacer click en Sign, obtenemos el Message Signature. El cual se lo puedo pasar a alguien… y en Verificar, veremos como ese otro puede hacer para verificar el mensaje. Esa otra persona, teniendo la Clave Pública, sumado al mensaje y a la Firma del mensaje… podría ser capaz de verificar la originalidad del mensaje… si le damos click al botón Verificar, veremos que pasa.

¿Que opinan que pasaría si alguno de los datos es alterado?

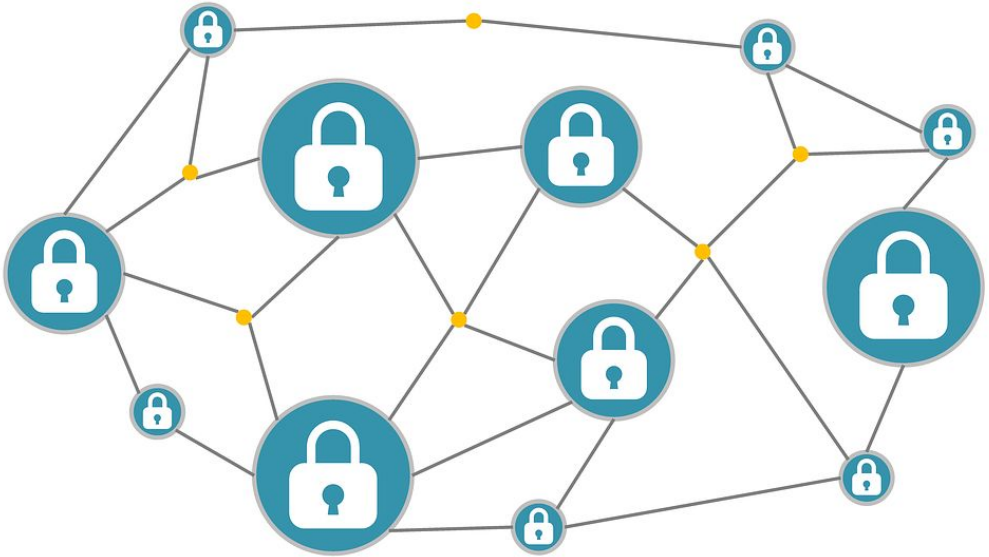
- Ahora pongamos algo de estructura alrededor de esto, **vamos a hacer una transacción de dinero en este caso en vez de un mensaje**… que sería lo que se hace al operar con cripto activos.



Transaction:

- Se va a **enviar un monto de dinero desde una clave pública** (digamos que es la mía) **a otra clave pública de otra persona** (alguna de los alumnos). Esta operación se va a firmar con la Private Key del que está generando la operación, en este caso el que envía el dinero… al hacer click en sign se consigue un ¨Message Signature¨. De acuerdo, se envía la firma del mensaje a alguien más (nodos de la cadena)… Ellos saben que quiero enviar un monto desde mi clave pública a la clave pública de otra persona. Al verificar esto, se ve que es correcto y que no hay alteraciones en la operación.

- Ahora usemos esto en la Blockchain que habíamos visto la clase pasada…

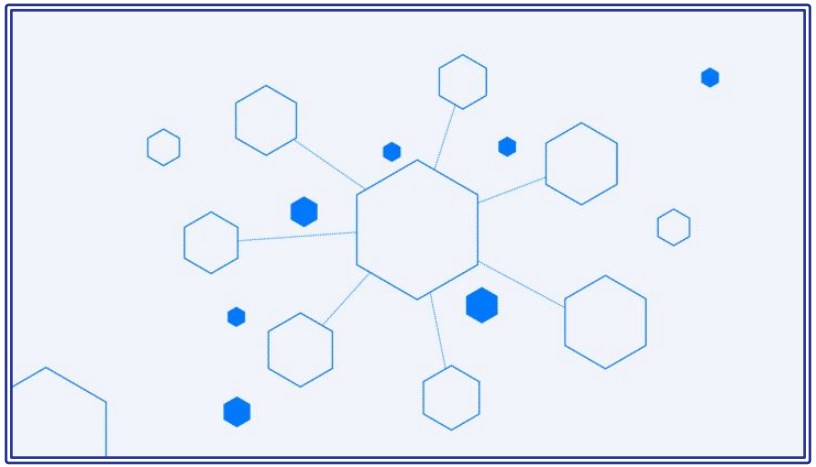


Blockchain:

- Veamos que **no hay más nombres ya**… solo **están las claves públicas** en el ¨From¨ y en el ¨To¨. A su vez se ve que hay una Firma para cada transacción.
- Si modificamos algún monto por ejemplo, veremos que el Bloque se rompe y a su vez se rompe la Firma ya que la misma no está verificada. Podríamos re minar el Bloque y obtener un bloque minado pero con la Firma inválida. El minero no tiene mi Private Key, solo tienen mi Public Key, por lo que no pueden obtener la firma correcta.

- **Esa es la forma de verificar que el mensaje/transacción hecha fue hecha por la persona que tenía la plata y no por cualquier otro!**

- Así es como ¨Public/Private Key Message Signing¨ es usado para proteger transacciones y asegurar que son de las personas que eventualmente las hicieron.



Conclusiones:

- Si pensamos bien en esto, funciona realmente bien ya que si tuviéramos que crear una nueva ¨Address¨ o clave privada lo único que tendríamos que hacer es ir hacia atrás y generar un nuevo número Random o Private Key. **No tendríamos que ir a ninguna entidad centralizada para que nos den una Public/Private Key Pair**, solo la creamos y la usamos nuevamente. Sacamos la Public Key derivada y la usamos para lo que necesitamos hacer, con esta nos podrían pagar por ejemplo o demás opciones que se pueden hacer con esta tecnología.

Así es como funciona básicamente una Blockchain. Ya veremos más en profundidad todo con más ejemplos. Es muy similar a como funciona Bitcoin, la madre de todas las Blockchains.

Consigna:

Levantar el proyecto nuevo en Localhost e interactuar con el mismo:

https://github.com/anders94/public-private-key-demo

Herramientas:

- Git: https://www.hostinger.com.ar/tutoriales/instalar-git-en-distintos-sistemas-operativos
- node.js: https://nodejs.org/en/download/
- npm: https://www.npmjs.com/
- Docker (docker-compose up -d) https://docs.docker.com/compose/reference/up/