educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 3 - Proyecto Integrador - Etapa 2

Etapa 2: Desarrollo del modelo

Escenario

Todos los usuarios, sean pacientes o médicos, pueden formar parte de una red *Blockchain* registrándose en la aplicación de atención médica. Después de verificar las identidades, **cada usuario de *Blockchain* recibirá una identificación única**, representada por un *hash* (también llamado ***dirección de cuenta)***.

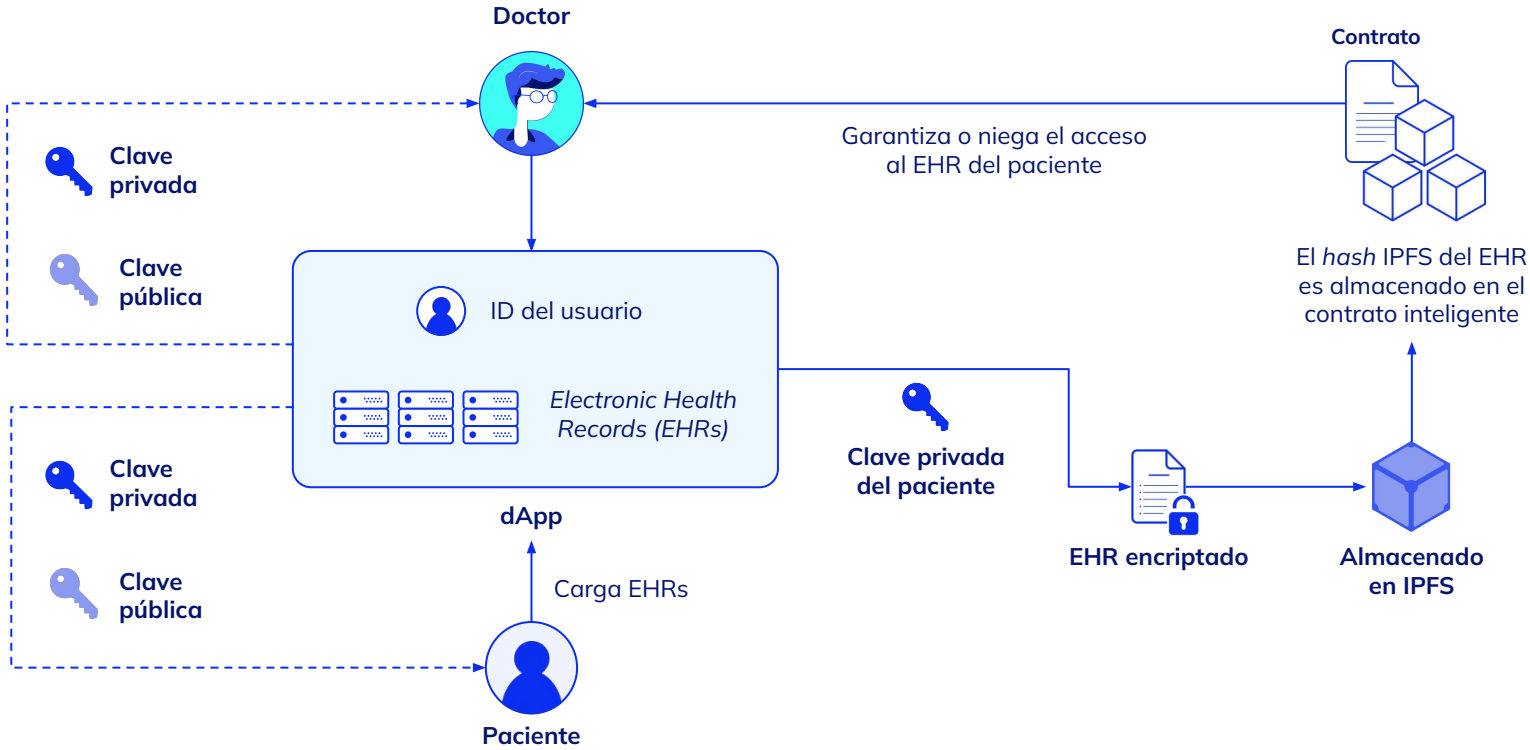
Se generará un **par de claves, pública y privada**. El usuario mantiene la confidencialidad de la clave privada, y la clave pública es la dirección de la cuenta que se puede compartir.

La clave privada debe firmar cualquier transacción relacionada con la dirección de la cuenta. Una ***transacción*** se puede definir como un proceso de carga, actualización, eliminación o intercambio de datos de una ***Historia Clínica Electrónica (HCE)*** (en inglés *Electronic Health Record, EHR*). Todas las transacciones deben **garantizar que las claves públicas y privadas coincidan, antes de que las transacciones se registren en la Blockchain**.

Después de registrarse en la red *Blockchain*, la institución de salud o los pacientes pueden cargar sus registros de salud en la aplicación. Los datos de los EHR de los pacientes, junto con los datos de sus visitas, recetas, facturación, etc., serán encriptados y almacenados en el ***IPFS***.

Una vez que los documentos se cargan en el *IPFS*, la dirección de los documentos almacenados se almacena en los *contratos inteligentes*. Por lo tanto, al usar el *IPFS*, se **reduce el espacio necesario para almacenar en bloques**, lo que en última instancia reduce el costo de cada transacción.

Veamos el esquema del siguiente slide.


Doctor
Contrato
Clave privada
Clave pública
Garantiza o niega el acceso al EHR del paciente
El hash IPFS del EHR es almacenado en el contrato inteligente
ID del usuario
Electronic Health Records (EHRs)
Clave privada
Clave pública
Clave privada del paciente
dApp
EHR encriptado
Almacenado en IPFS
Carga EHRs
Paciente

El ***Sistema de archivos interplanetario*** (**IPFS**, por sus siglas en inglés) es un sistema distribuido utilizado para almacenar y acceder a archivos. Este sistema nos permite almacenar archivos en Internet sin la necesidad de un servidor de *hosting*.

Los archivos que se cargan en la red son almacenados en distintos computadores, asignándole a cada archivo un identificador (*hash criptográfico*). Luego, al buscar un archivo, se le pide a la red que encuentre *nodos* que almacenen el contenido para obtenerlo.

Para subir archivos a IPFS es necesario contar con **un nodo conectado a la red**, que podemos obtener de dos formas:

- Utilizando un **nodo propio**: debemos instalar una implementación de IPFS en nuestra computadora para conectarnos a la red IPFS y transferir nuestros archivos.
- Utilizando un **nodo remoto** (e.g Infura).

En esta etapa del *Proyecto integrador* trabajaremos con el IPFS.

Consigna

1. En la máquina virtual ***Kali Linux***, en el escritorio, encontrarás una carpeta denominada ***EHR-Using-Blockchain***, dentro de la cual se encuentra otra denominada ***EHR***. Encontrarás una plantilla para generar una historia clínica, denominada ***PlantillaHistoricaClinica.pdf.*** No lo edites, haz una copia y renómbrala como ***HCE2.pdf***.

2. Completa la historia clínica ***HCE2.pdf*** y guarda los cambios. Consulta el archivo ***HCE1.pdf*** para ver cómo hacerlo.

3. Abramos una terminal dentro de la carpeta ***EHR*** (***botón derecho > Open Terminal Here***).

4. Mediante el comando **`ipfs help`** podrás ver una ayuda para poder desarrollar el resto de la práctica.

5. Abre una segunda terminal (***File > New Tab***) y conecta nuestro nodo local mediante el comando **`ipfs daemon`**.

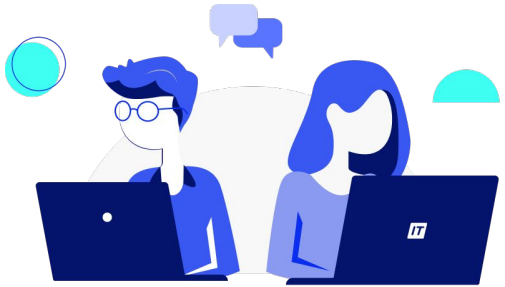
6. Vuelve a la primera terminal y sube el archivo ***HCE2.pdf*** a la red interplanetaria. Copia el valor del *hash* resultante y guárdalo mediante el comando **`echo valor_hash > HCE2.pdf.hash`**.

7. Verifica que el archivo se ha subido correctamente visitando https://gateway.ipfs.io/ipfs/<hash_archivo>

8. Si abre el archivo ***HCE1.pdf.hash*** verá el *hash* del archivo correspondiente. Búscalo en la red interplanetaria.

> **Nota:** La red almacenará nuestro archivo siempre que otros pares accedan a él, por lo que es esperable que después de un tiempo el archivo deje de estar disponible (de manera similar a lo que ocurre con los torrents). De ser así, súbelo nuevamente.

9. Intercambia con tus compañeros de curso el *hash* de la historia clínica generada en ***HCE2.pdf*** y accede a algunos de ellos



¡Sigamos trabajando!