educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 2 - Resolución de la etapa 1

Resolución de la etapa 1

1. Se debería implementar una ***blockchain* privada** que se guíe bajo el concepto de privilegios, ya que en una *blockchain* pública cualquier usuario puede conectarse a la red y acceder a la información.

   Además, se puede adaptar la forma de almacenamiento, la estructura y el contenido de las transacciones según las propias necesidades.

2. Para almacenar los datos se deberían utilizar **algoritmos simétricos**. Dos candidatos serían *AES* y *ChaCha20*. El primero tiene implementación por bloques y el segundo por flujo. El modo de operación por flujo es algo menos seguro, pero más orientado a la transmisión. Como es más importante el almacenamiento, ya que no hay grandes requerimientos de transmisión, usaremos *AES* con clave de 256 bits. En cuanto al modo de operación, lo más recomendable es *GCM*. Para esquemas de cifrado asimétrico, se recomienda *ECDH* de 128 bits.

¡Sigamos trabajando!