Rapport TD2-Blockchain Programming

Le but de ce TD est de coder un wallet.

BIP39 :

• Créer un programme python ou JS interactif en ligne de commande (2pts)

• Créer un entier aléatoire pouvant servir de seed à un wallet de façon sécurisée (2 pts)

Pour la création de cet entier aléatoire nous allons utiliser le module secrets. Avec secrets.bytes on a une série de bytes que l'on vas convertir en binaire. Ensuite on va hasher cette série de bytes.

Notre binaire finale de taille 134 bits sera la concaténation du binaire du début plus le checksum (les 4 dernier bits de mon hash).

• Représenter cette seed en binaire et le découper en lot de 11 bits (2 pts)

• Attribuer à chaque lot un mot selon la liste BIP 39 et afficher la seed en mnémonique (2 pts)

On a importé le fichier french.txt et convertie notre binaire en mots.

• Permettre l'import d'une seed mnémonique (2 pts)

On a fait les chemin inverse, on obtient la seed BIP39 a l'aide des Mnemonic.

• Extraire la master private key et le chain code (2 pts)

On a hashé notre seed avec sha512 et diviser notre hash en deux parties : la private key et la chain. Pour obtenir la clé privée j'ai utilisé SECP256k1 et ecdsa.

• Extraire la master public key (2 pts)

Pour extraire la clé publique j'ai utilisé les mêmes librairies et j'ai rajouté b'04' devant ma clé publique