ANANDARASA Milojan

BICHAT Guillaume

Rapport-TD2

-Créer un repo github et le partager avec le prof .
-Créer un programme python ou JS interactif en ligne de commande.

```
C:\Users\Miloj\TD2-Blockchain>scrypt.py

                              ##################################
                                     Magasin de clés:
                              ##################################
Souhaitez-vous créer une nouvelle graine ou restaurer un portefeuille en utilisant une graine existante ?
                                 1- Créer une nouvelle graine.
                                 2- J'importe ma graine mnémonique.
                                 3- Quitter.
                           ########################################
Tapez votre choix:
```

-Créer un entier aléatoire pouvant servir de seed à un wallet de façon sécurisée

-Représenter cette seed en binaire et le découper en lot de 11 bits

-Attribuer à chaque lot un mot selon la liste BIP 39 et afficher la seed en mnémonique

```
Tapez votre choix:
1

Voici votre graine mnémonique:
['flip', 'infant', 'visual', 'escape', 'surface', 'boring', 'capital', 'mirror', 'child', 'rely', 'winter', 'pelican']
```

-Permettre l’import d’une seed mnémonique

-Importer une seed et vérifier son format (2 pts)

```
Tapez votre choix:
2

Entrez les mots, issue de votre graine mnémonique, un par un (tapez 1 pour acceder à l'ensemble des mots):

mot n°1: flip

mot n°2: abc

Le mot n'appartient pas à la liste bip39.
Retrouvez la liste bip39 en tapant 1.

mot n°2: child

mot n°3:
```

-Extraire la master private key et le chain code

-Extraire la master public key

```
Votre seed mnémonique est donc:
['zoo', 'able', 'cram', 'bus', 'ill', 'subject', 'worry', 'wrap', 'time', 'stay', 'stage', 'spike']

    1- Voir sa master private/public key et sa master chain code .

    2- Générer une clé enfant.

    3- Retour.

1

Votre master private key est:
f1f2285c04474933e3d90d2e23da1246731662fa3734a6b378545dbe396a82e8

Votre chain code est:
b2fe62742a3a04a42949bfada7f2f71e83a72fc47bd3fea9c991d880497a36d5

Votre master public key est:
5cd0e94c88e307f6353ac547a00b5fde2c7cd37edd3438cf0ad1385450b7ec1417



    1- Voir sa master private/public key et sa master chain code .

    2- Générer une clé enfant.

    3- Retour.
```

-Générer une clé enfant

```
2

La  child private key est:
3728409e3c65f23f8060c5ae697c8aa0214ae894dc7aaa71fff407949baa187e

La child chain code est:
c48b5226a2050751f6f551cad54e9d96144266213ac50447ec248c36d773e8bf

    1- Voir sa master private/public key et sa master chain code .

    2- Générer une clé enfant.

    3- Retour.
```