Blockchain Programming

TD2 - Monnaies numériques

BIP 39

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

```
□ Invite de commandes - blockchain_programming_td2.py

1 - Générer un seed aléatoire

2 - Importer un seed

3 - Importer un seed mnémonique

4 - Récuperer la Master Private Key

5 - Récuperer le Master Chain Code

7 - Afficher le seed en mnémonique

θ - Exit

Saisir l'action que vous souhaitez réaliser.

6

Voici la liste de mot associée au seed : path conduct certain toy teach output health monkey collect kit vague win

Press the <ENTER> key to continue...
```

• Permettre l'import d'une seed mnémonique

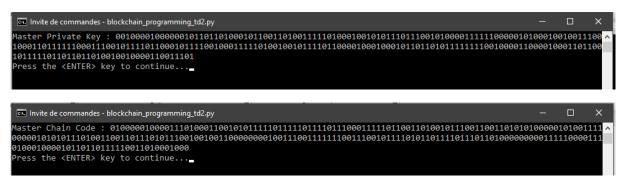
```
Invite de commandes - blockchain_programming_td2.py
Rentrez le mot numéro : 1
path
Index = 1287
Rentrez le mot numéro : 2
conduct
Index = 374
Rentrez le mot numéro : 3
certain
Index = 301
Rentrez le mot numéro : 4
toy
Index = 1843
Rentrez le mot numéro : 5
teach
Index = 1780
Rentrez le mot numéro : 6
output
Index = 1259
Rentrez le mot numéro : 7
health
Rentrez le mot numéro : 8
monkey
Index = 1145
Rentrez le mot numéro : 9
collect
Rentrez le mot numéro : 10
Index = 983
Rentrez le mot numéro : 11
vague
Index = 1925
Rentrez le mot numéro : 12
a4a3096bcf43e49093779085aad803ceb38c23770641f2dcf062df10baec9e3c
0101111111000010111111011010
 ress the <ENTER> key to continue..._
```

BIP 32

• Importer une seed et vérifier son format



• Extraire la master private key et le chain code



- Extraire la master public key
- Générer une clé enfant
- Générer une clé enfant à l'index N
- Générer une clé enfant à l'index N au niveau de dérivation M