

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

```
Invite de commandes - blockchain_programming_td2.py
Le chiffre random est :
213869908266169484350637929157978211069

Le chiffre sous forme binaire (128 bits) :
1010000011100101110110001001011011110011001111011110100100111010011110010010110110001111010111111000010
11111101

Hashage en SHA256 en hex
a4a3096bcf43e49093779085aad803ceb38c23770641f2dcf062df10baec9e3c

Hashage en SHA256 en bin
10100100101000110000100101101011110011110100001111001001000010010011011110111100100001000010110101010110000000011
1100111010110011000110001000110111011100000110010000011110010110111001111000001100010110111100010000101101011101100
1001111000111100

Voici le seed : 10100000111001011101100010010110111100110011110111101001001110101101010001100011110010010110110001111
010111111100001011111011010
Press the <ENTER> key to continue...
```

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

```
Voici le seed : 10100000111001011101100010010110111100110011110111101001001110101101010001100011110010010110110001111
010111111100001011111011010
Press the <ENTER> key to continue...

Saisir l'action que vous souhaitez réaliser.
6
10100000111
00101110110
00100101101
11100110011
11011110100
10011101011
01101010001
10001111001
00101101100
01111010111
11110000101
11111011010
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...
```

- 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 - Récupérer la Master Private Key
5 - Récupérer le Master Chain Code
7 - Afficher le seed en mnémonique
0 - 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
Index = 849
Rentrez le mot numéro : 8
monkey
Index = 1145
Rentrez le mot numéro : 9
collect
Index = 364
Rentrez le mot numéro : 10
kit
Index = 983
Rentrez le mot numéro : 11
vague
Index = 1925
Rentrez le mot numéro : 12
win
Index = 2010
a4a3096bcf43e49093779085aad803ceb38c23770641f2dcf062df10baec9e3c
Format du seed ok

Voici le seed : 10100000111001011101100010010110111100110011110111101001001110101101010001100011110010010110110001111
01011111100001011111011010
Press the <ENTER> key to continue...

```

BIP 32

- Importer une seed et vérifier son format

```
Invite de commandes - blockchain_programming_td2.py
Rentrez votre seed (chaîne de 132 bits) :
10100000111001011101100010010110111100110011110111101001001110010010110110001111010111111000010
11111011010
Format du seed ok

Voici le seed : 1010000011100101110110001001011011110011001111011110100100111001001011011000111101001111
01011111100001011111011010
Press the <ENTER> key to continue...
```

- Extraire la master private key et le chain code

```
Invite de commandes - blockchain_programming_td2.py
Master Private Key : 00100001000000101101101000101100110100111110100010010101110111001010000111110000010100010011100
10001101111110001110010111101100010111100100011111010010010111101000100010110110111111001000011000010001101100
101111011011010010010000110011101
Press the <ENTER> key to continue...
```

```
Invite de commandes - blockchain_programming_td2.py
Master Chain Code : 010000010000111010001100101011111011111011110001111101100110100101110011001101010100000101001111
000001010101110100110011011101011100100100100000001001110011111100111001011110110111101110110100000000111110000111
010001000010110110111110011010001000
Press the <ENTER> key to continue...
```

- 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