Rendu TD2

Créer un repo github

https://github.com/S-uzan/TD2

Créer code en python exécutable en ligne de commande

```
Macintosh-de-sam:~ samuel$ /Library/Frameworks/Python.framework/Versions/3.7/bin
/python3 /Users/samuel/Desktop/A4/S8/Blockchain/TD2.py
Bonjour
Que voulez vous faire?
Taper 0 pour generer une seed
Taper 1 pour importer une seed
0
['slender', 'talent', 'tumble', 'trial', 'spot', 'drum', 'true', 'cable', 'fabri
c', 'scan', 'rigid', 'jungle']
```

Générer un entier aléatoire

```
rand =  bin(random.getrandbits(128))[2:].zfill(128)
```

J'ajoute le cheksum

```
hashed = hashlib.sha256(rand.encode('utf-8')).hexdigest()

bin_result = rand.zfill(128) + bin(int(hashed,16))[2:].zfill(256)[:4]
```

Découpage en lot de 11 bits

```
while i<=11:
    seed.append(bin_result[11*i:(11*(i+1))])
    i=i+1
```

Attribuer à chaque lot un mot et afficher

```
while i<=11:
    seed[i] = liste_bip_39[seed[i]]
    i=i+1
print(seed)
```

```
['hunt', 'caught', 'sell', 'net', 'code', 'cart', 'castle', 'join', 'glance', 'pass', 'allow'
, 'husband']
```

Permettre l'import d'une seed mnémonique(fonction importation_seed())

```
Bonjour
Que voulez vous faire?
Taper 0 pour generer une seed
Taper 1 pour importer une seed
1
mot n°0:science
mot n°1:banner
mot n°2:execute
mot n°3:lottery
mot n°4:identify
mot n°5:dizzy
mot n°6:rich
mot n°7:escape
mot n°8:vote
mot n°9:river
mot n°10:loud
mot n°11:will
Que voulez vous faire?
Taper 1 pour extraire la master private key
Taper 2 pour extraire le chain code
Taper 0 pour quiter
```

Importer une seed et vérifier son format :

Comme on peut le voir sur la capture d'écran précédente la clé a bien étais importer je vais maintenant changer le dernier mot pour avoir un exemple avec un mauvais format

```
mot n°7:escape
mot n°8:vote
mot n°9:river
mot n°10:loud
mot n°11:science
La clé n'est pas valide
```

Extraire la master private key et le chain code

```
Taper 1 pour extraire la master private key
Taper 2 pour extraire le chain code
Taper 0 pour quiter
1
ee0b249d767ce8d3557418ec916bb3f5dc195af45449dcde7d8ee41ed35cec77
Que voulez vous faire?
Taper 1 pour extraire la master private key
Taper 2 pour extraire le chain code
Taper 0 pour quiter
2
4801a86f9a464dfccfe7278af72eabd190a88f921f59c85574eae5db8fe83ed3
```

Je n'ai pas réussi a trouver la relation entre la Master Private keys et la master public keys donc je n'ai pas pu faire la suite