BONAN Alexandre
TRUONG Léo

ESILV A4 FinTech

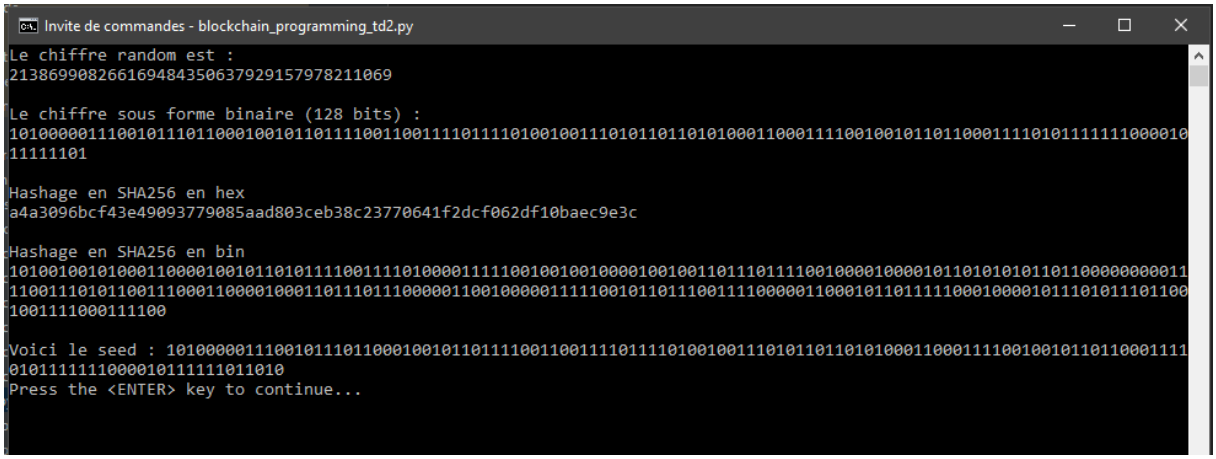
Blockchain Programming

TD2 - Monnaies numériques

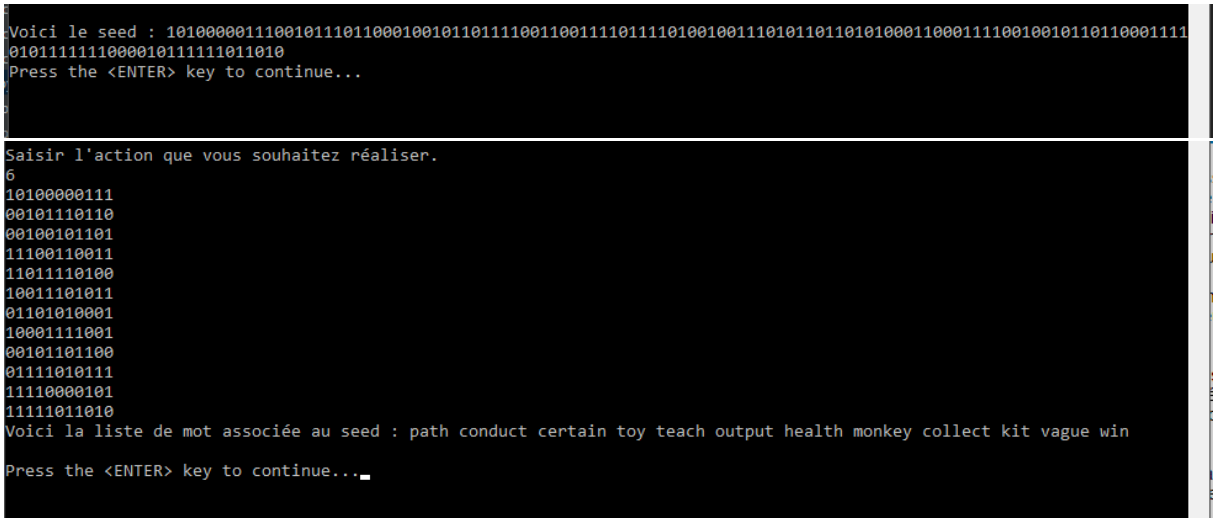
BIP 39

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

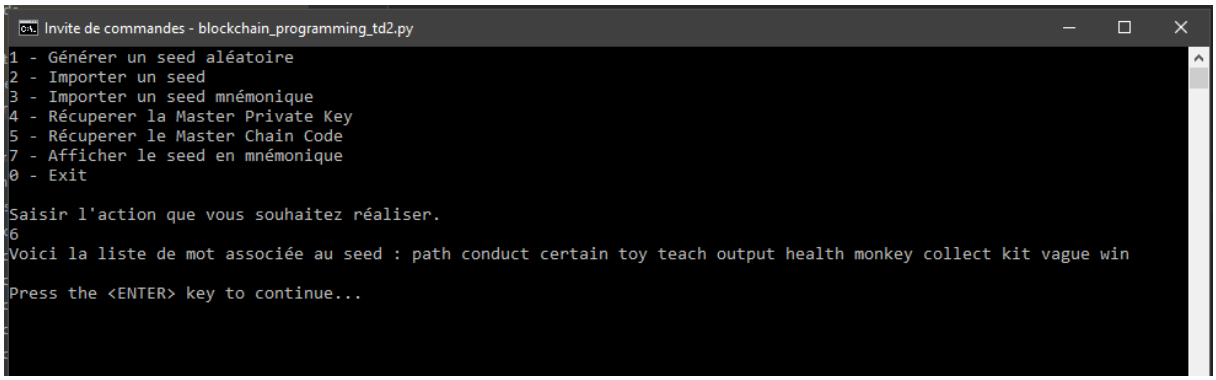
- **Créer un entier aléatoire pouvant servir de seed à un wallet de façon sécurisée**



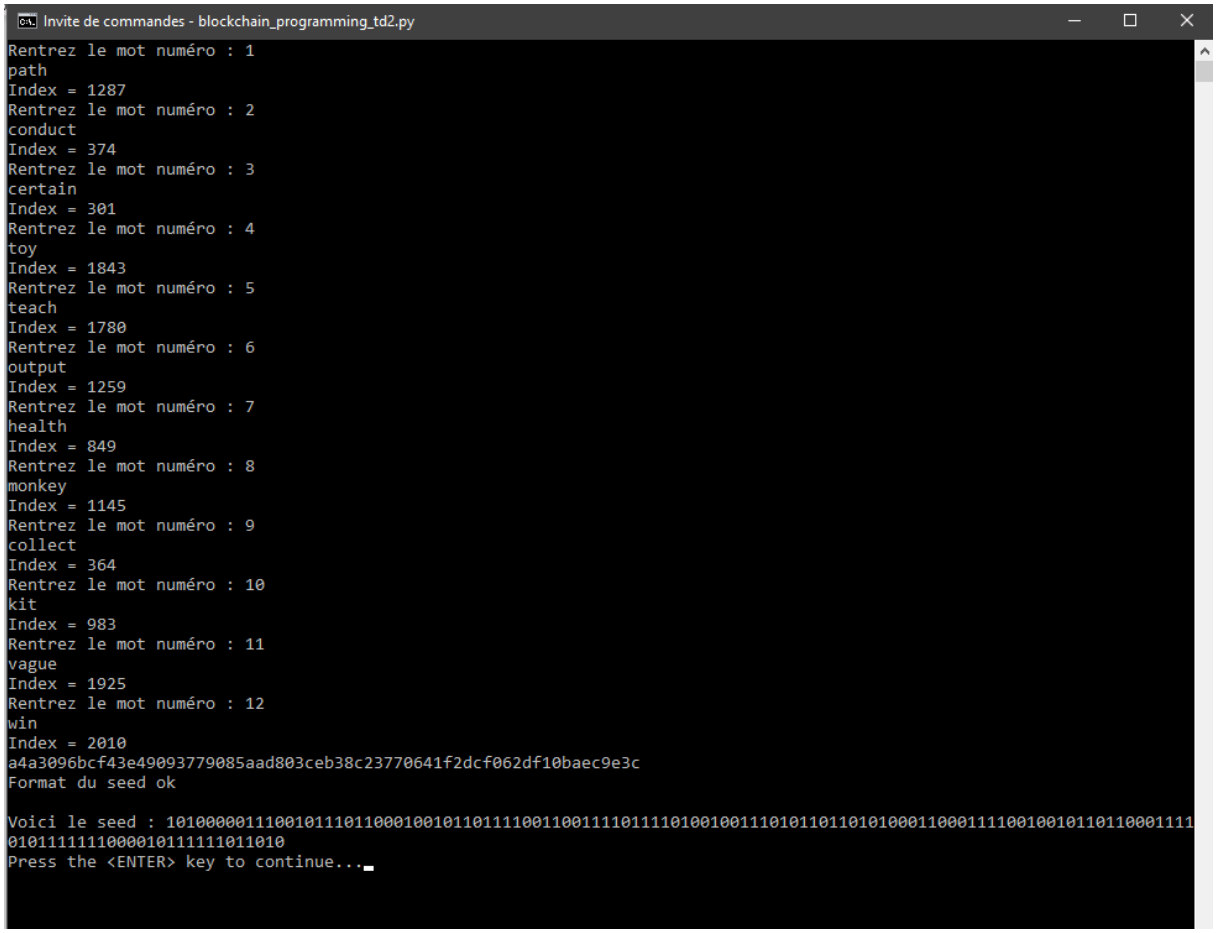
- **Représenter cette seed en binaire et le découper en lot de 11 bits**



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

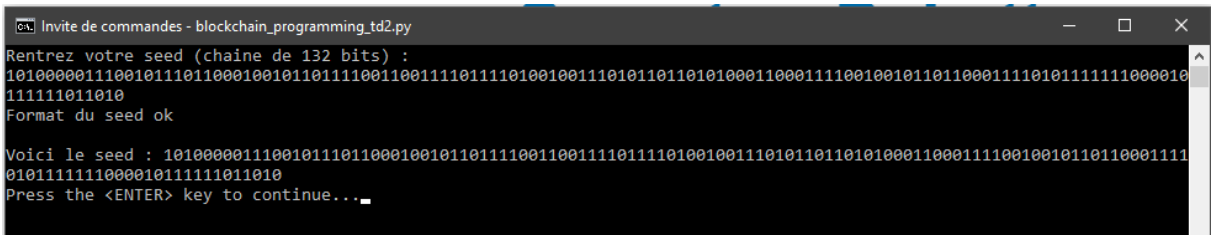


- **Permettre l'import d'une seed mnémonique**

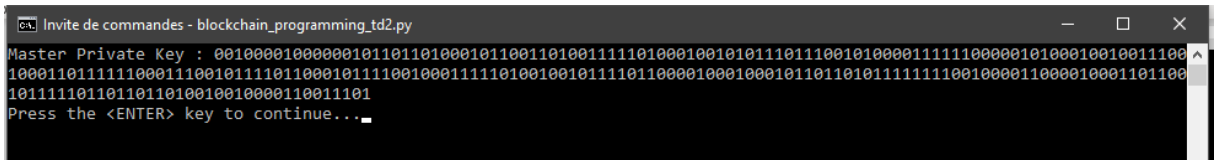


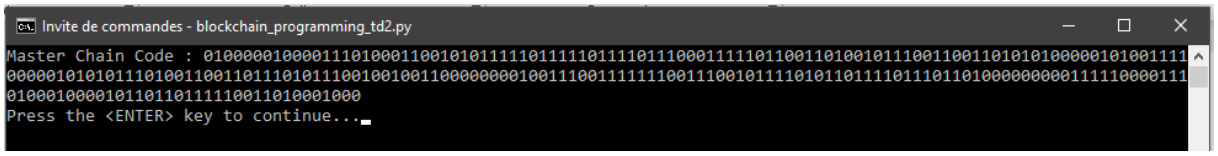
BIP 32

- **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**