Numéro d'inscription: 25575
Léo Renault
Thème: La ville

La blockchain un outil pour concevoir la ville de demain.

Contexte:

-taux d'abstention croissant

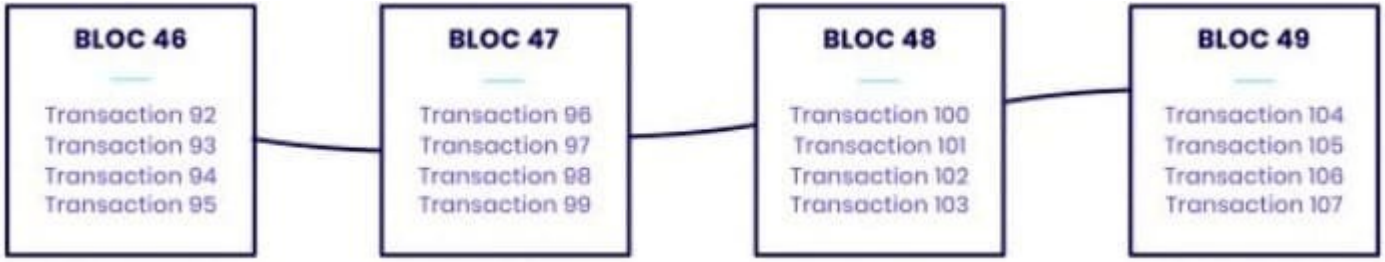
-systéme traditionnel de vote sujet à l'erreur humaine

Objectif: Implémenter un vote sur un réseau blockchain

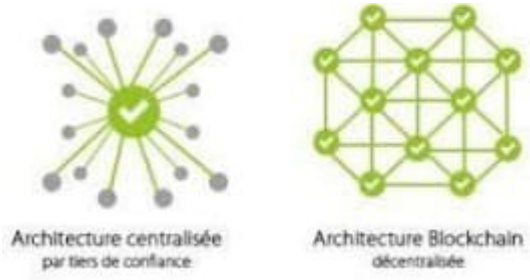
Dans quelle mesure la technologie blockchain permet d'effectuer des votes numériques sécurisés ?

Définitions

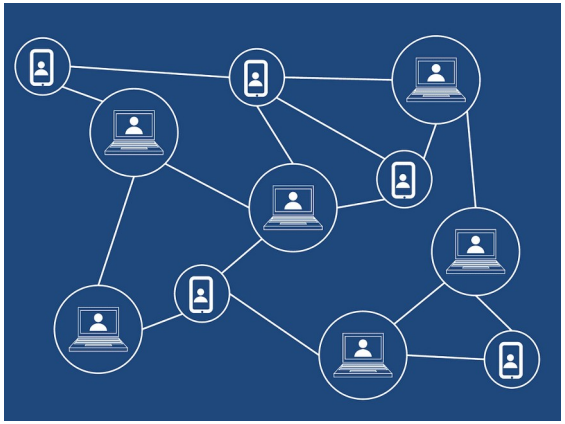
Blockchain:



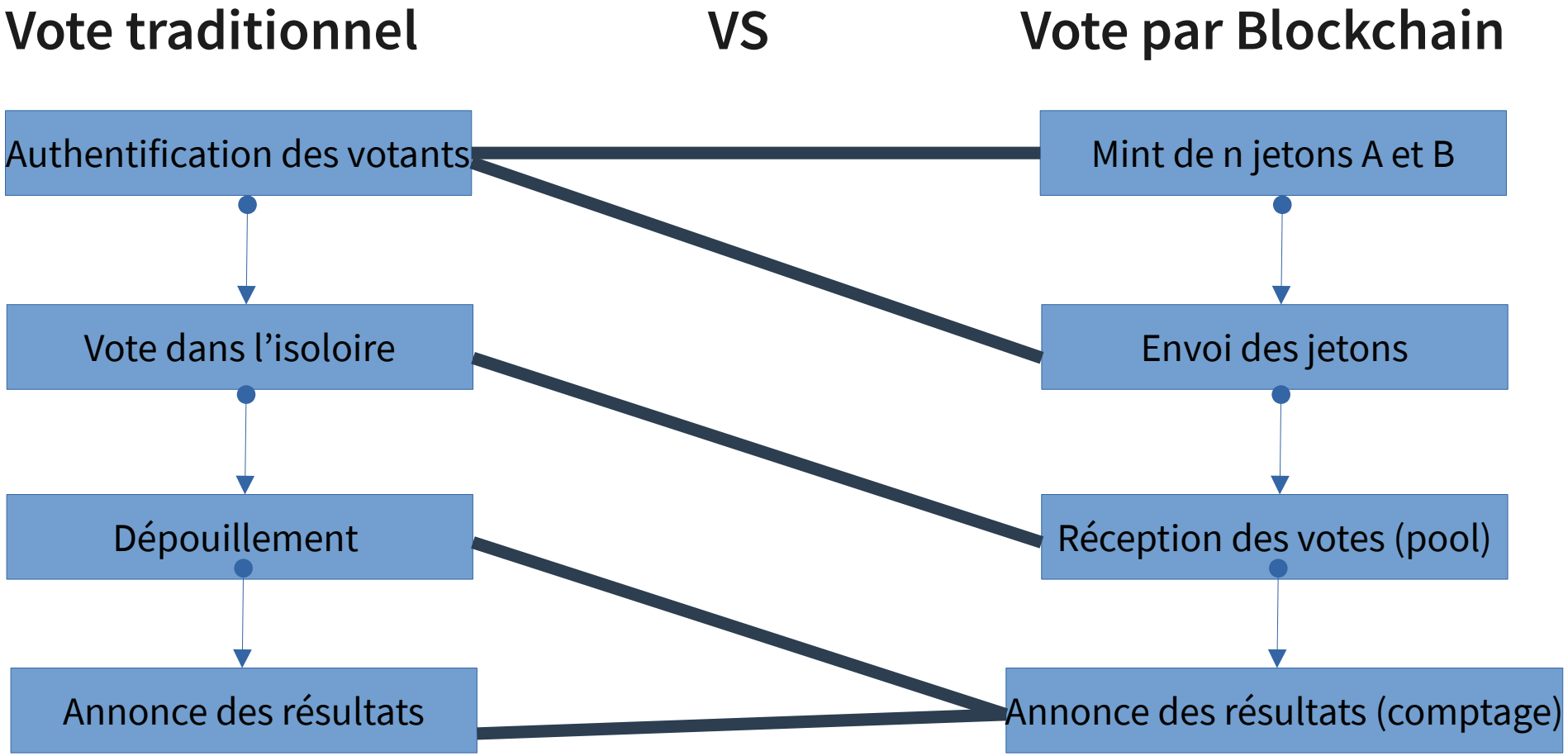
Décentralisation



Réseaux blockchain



Protocole: Vote entre un choix A et B



Première modélisation naïve

Choix de la structure: Liste

Découpage du vote en plusieurs fonctions:

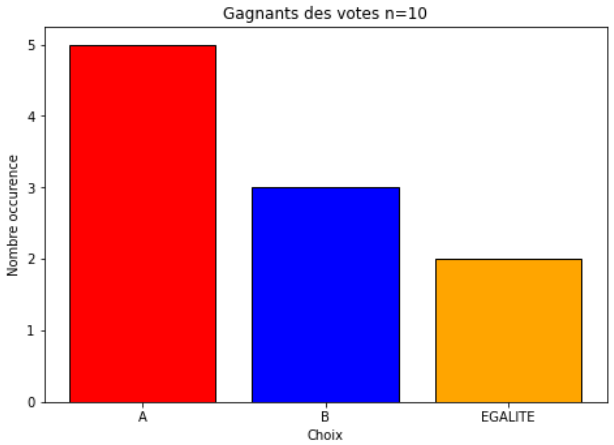
-création des bulletins

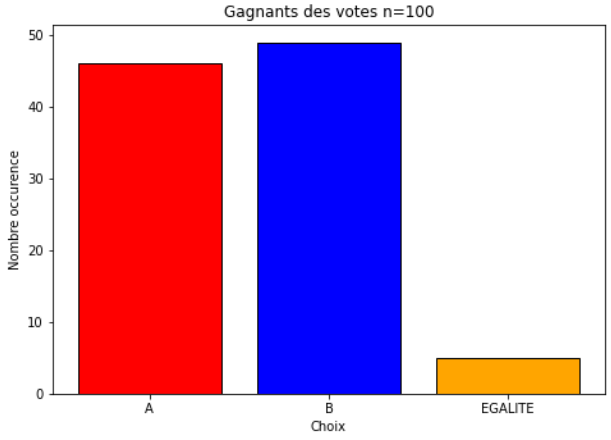
-distribution des bulletins

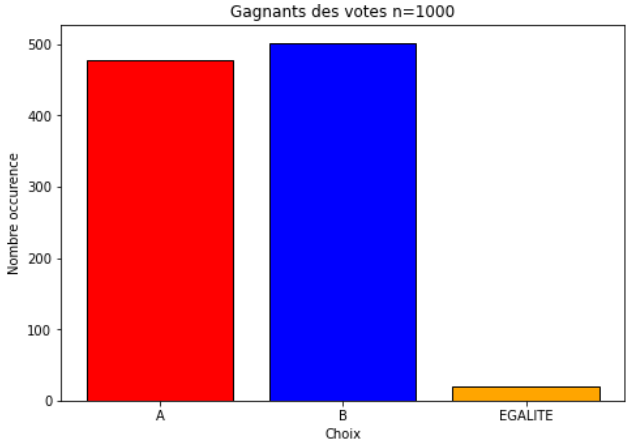
-simulation du vote des citoyens

-dépouillement

-annonce du résultat







Bilan: première modélisation naïve

Avantages:

→ transparence

→ vote à distance

→ rapidité

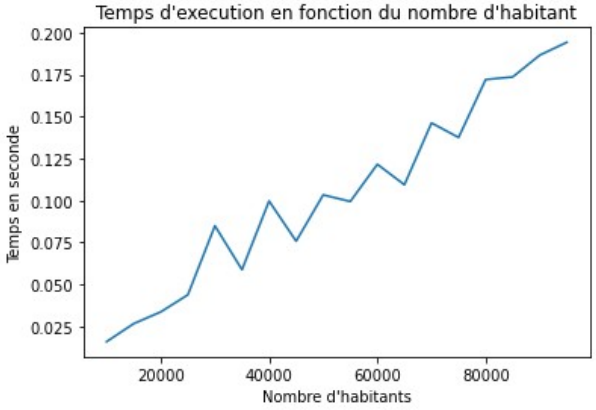
→ complexité linéaire: O(6n)

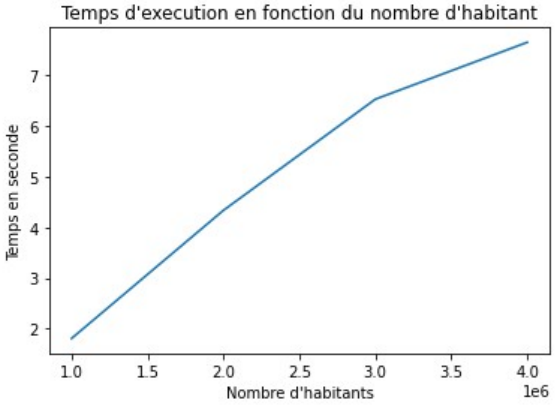
Limites de ma simulation:

→ Authentification du résident (votant)

→ secret de vote

→programme pas sécurisé





Paris (2M habitants): 4,23secondes

Annexe 1

Nouveau modèle: deuxieme modélisation

Hypothèses:

→ Authentification centralisée

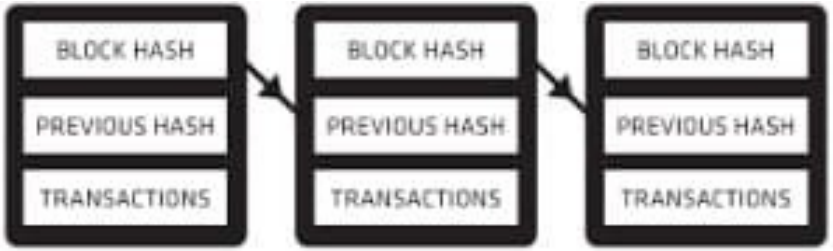
→ Anonymisation des adresses publiques

Améliorations:

→implémentation d'une fonction de hashage (SHA-256)

→création d'une blockchain

→mise en place d'un facteur d'influence

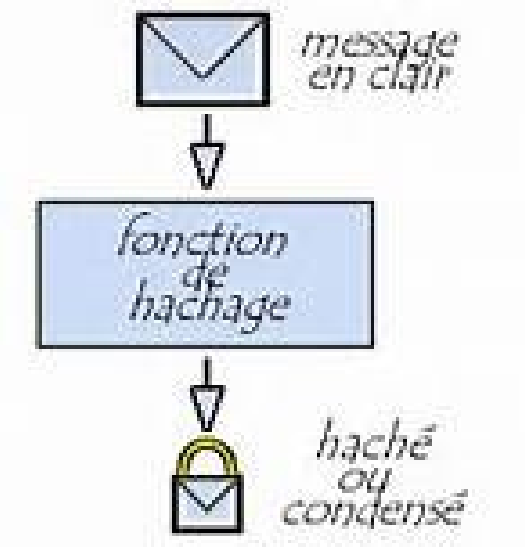


Bilan: deuxième modélisation

Rôle de la fonction de hashage:

→créer une chaîne de bloc

→sécuriser ma blockchain




```
['B', 'B', 'B', 'B', 'B', 'C', 'B', 'A', 'C', 'B', 'B', 'A', 'B', 'C', 'A', 'C', 'A', 'A', 'B', 'B', 'A', 'A', 'A', 'B', 'C', 'C', 'A', 'A', 'B
Data 1: Genesis Block - 0
Hash 1: 39331a6a2ea1cf31a5014b2a7c9e8dfad82df0b0666e81ce04cf8173cc5aed3e

Data 2: 32 jetons ont été crée dans la pool Pool d'envoie - 39331a6a2ea1cf31a5014b2a7c9e8dfad82df0b0666e81ce04cf8173cc5aed3e
Hash 2: 414720d22cebdbcc131d4b04be29664f59e1e3ea4faa3d2154eebe3a5ba33567

Data 3: La pool d'envoie a envoyé 1 bulletin de vote A,B et C au votant 0 - 414720d22cebdbcc131d4b04be29664f59e1e3ea4faa3d2154eebe3a5ba33567
Hash 3: 8f47a3965cd50054f647f69c12cb93036b0469c0ed2af93ff78a3f090fedbc41
```

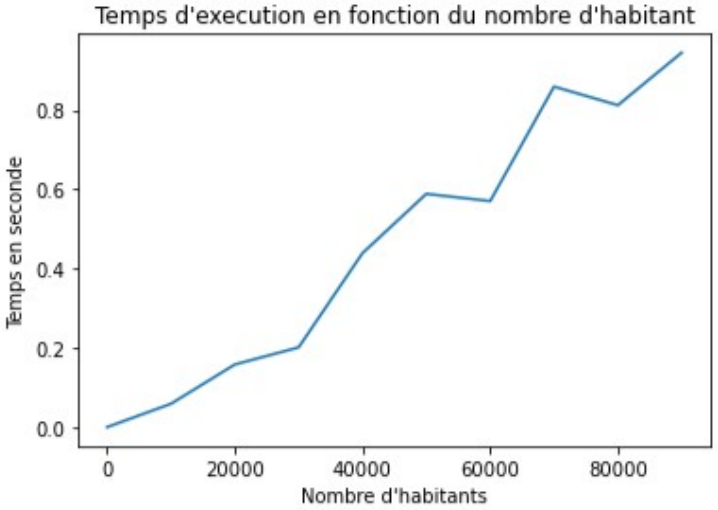

Annexe 2

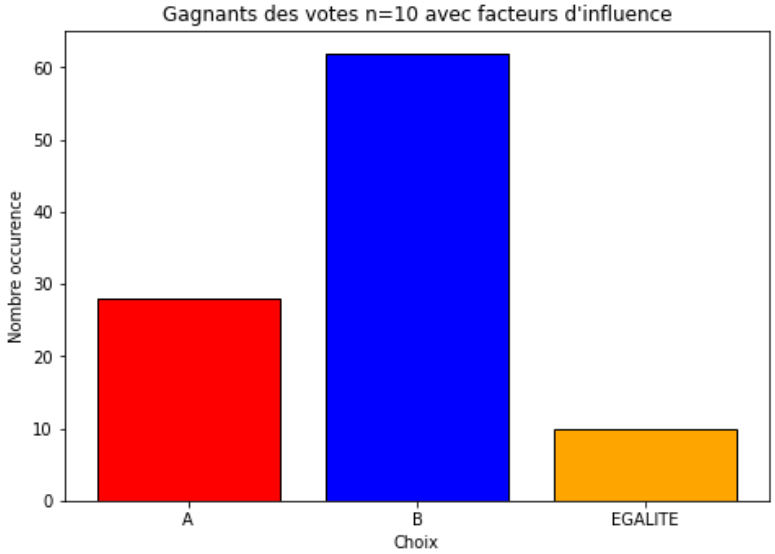
Bilan: deuxième modélisation

Choix de la structure: création de classes

→Block et Blockchain

→Complexité en O(24n)





Remarque:

→ 4 fois plus que lors de la première modélisation

→Paris: 20,75secondes

→la complexité reste linéaire

Annexe 3

Sécurité de la blockchain: Réseau

Attaque sur réseau blockchain: (corruption du vote)

→ attaque à 51% (prise de contrôle du consensus)

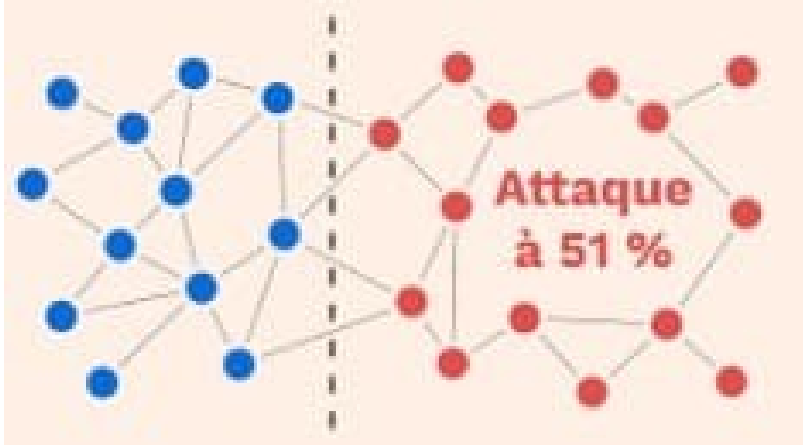
→attaque par inversion de la fonction de hashage

→problème de la double dépense

Nouvelles hypothèses:

→ utilisation d'une blockchain avec beaucoup de noeuds

→utilisation d'une fonction de hashage encore jamais cassée (éviter les collisions)



Nouveau modèle: troisième modélisation

Amèliorations:

→implémentation d'un réseau blockchain: 5 mineurs (=validateurs=noeuds du réseau)

→niveau de difficulté variable en fonction

de la puissance de calcule du réseau

```
mineur1("leo","8535e86c8118bbbb0a18ac72d15d3a2b37b18d1bce1611fc60165f322cf57386",0,True)
```

```
True
```

```
consensus("leo","8535e86c8118bbbb0a18ac72d15d3a2b37b18d1bce1611fc60165f322cf57386",0)
```

```
leo
8535e86c8118bbbb0a18ac72d15d3a2b37b18d1bce1611fc60165f322cf57386

True
```

```
mineur2("","07032003",3,False)
```

```
E
07031c1e646426654cc80fc5f9daf0ccb1c02a187712253a0881fc0001cf2b0f

True
```

```
mineur2("","07032003",4,False) # 4 est le max pour 3 boucle
```

```
zl
07032b5d2755291a1e1c3b00499be9e7091774c37cf5a39e74ca3e81687f76a7

True
```

```
mineur3("","07032003",5,False) #à partir de 6 on ne parvient plus à trouver le message clair, 5 est le max pour 4boucles
```

```
h=
0703203e87e8c89a623b0edeb6f4dda9a3ea48816afc7ca9885bd4f954c4549a

True
```

→chaque mineur à sa propre technique de recherche du message clair

→incertitude sur la possibilité de trouver le résultat: on ne peut pas prédire la sortie

```
mineur5("","07032003",6,False)#une nouvelle fois blocage à partir de 6
```

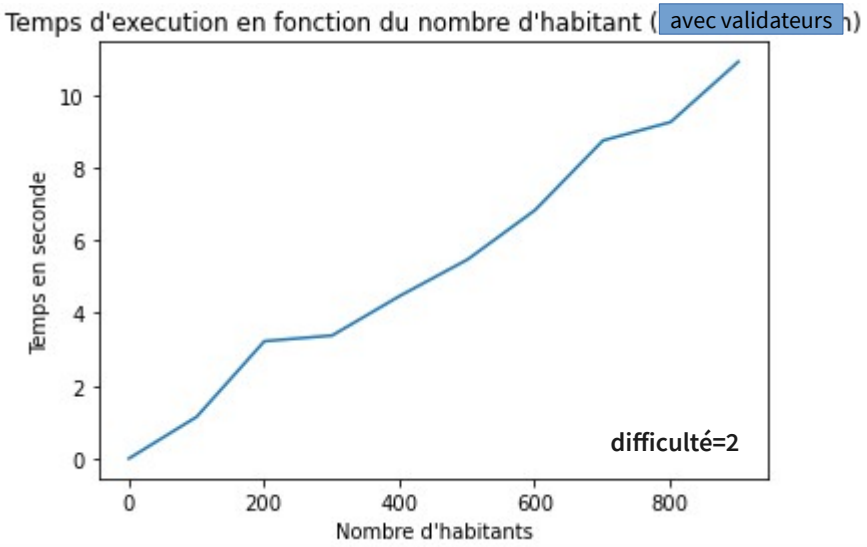
```
---------------------------------------------------------------------------
KeyboardInterrupt                         Traceback (most recent call last)
Cell In[229], line 1
----> 1 mineur5("","07032003",6,False)

Cell In[222], line 13, in mineur5(vote, empreinte, d, mode)
     11 val=True
     12 for k in range(d+1):
---> 13     if hashlib.sha256(str(i).encode()).hexdigest()[k]!=empreinte[k]:
     14         val=False
     15 if val:
```

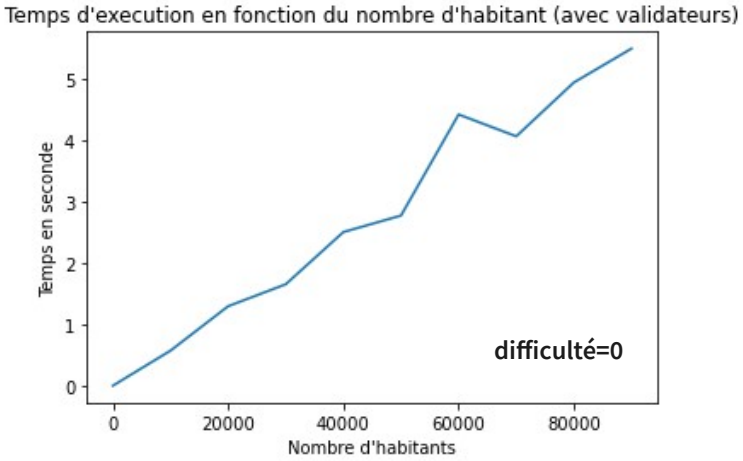

Annexe 4

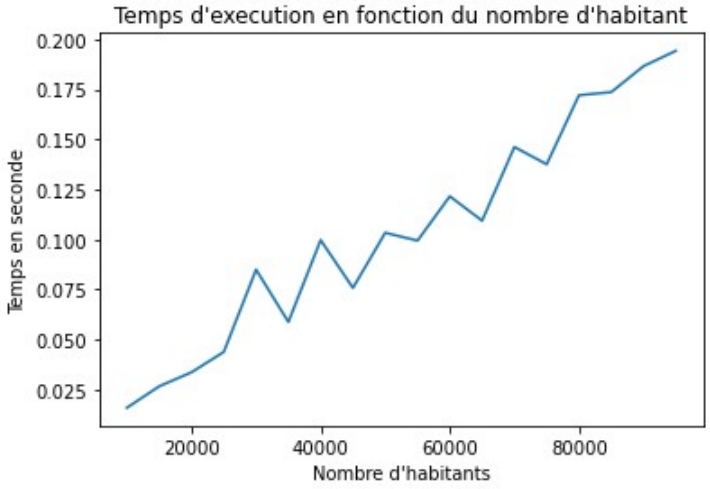
Nouveau modèle: troisième modélisation

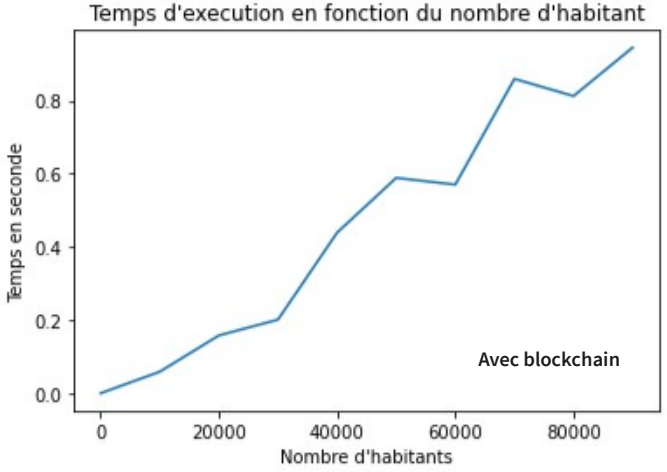
```
empreinte à trouver: cebeaacd2e122c6b000262b007b06692ac91775833c69e96fe80746999cd588a
difficulté:4
mineur_proposition:q_q
mineur_hash:cebea0b7f7ceab291a1aa7901210bb677c748066af76c2676b9005371e143fef
empreinte à trouver: c85fa53be6b0717164b452c2b1c5496ef6eb5a2e7ceab4a45e3580e2098b4ef7
difficulté:3
mineur_proposition:rH
mineur_hash:c85f482447b102b50a7c9375afbfc80ac5730a1c83fabdabb7354e861997de3b
empreinte à trouver: 983d1b3bf13fe73cc8781bfd11eae8684dfd128ff2ddfea95f7116d05474c58d
difficulté:2
mineur_proposition:*'
mineur_hash:9837985ab5c01cce23af80fb7d09b7b4e4e16abf34d342ebc5ff6001c19b2805
empreinte à trouver: 152ab08f7402d31d272c7c6e2a466b77d52fc9baae8289fb2a0c25e4fd28a2eb
difficulté:3
mineur_proposition:tc
mineur_hash:152ae816af11b98a9c84f8fd7fbf49844f45e1a37d8aa2d2ec3ca01d8891d007
```

Comparaison avec les autres modèles









Conclusion

Objectifs atteints ?

→création d'un algorithme de vote (1ère modélisation)

→implémenation d'une blockchain (2ème modélisation)

→implémentation d'un réseau blockchain décentralisé (3ième modélisation)

→sécurité à l'échelle du réseau

→efficience de mon algorithme

Nouvelles perspectives:

→sécurité à l'échelle de l'utilisateur (système asymétrique, RSA)

→implémentation autre que le vote (commerce, mobilité...)