Rapport TP : Sécurité dans le réseau

réalisé par:

- Soufiane KHAMLACH
- Sidali HAMDI
- Najat BAKKI (Scrum Master)
- Soufiane CHAHBOUN

Encadré par:

Mr. Damien SAUCEZ

Sprint n° 3 : Générer un identifiant qui comprend une partie immuable

Introduction:

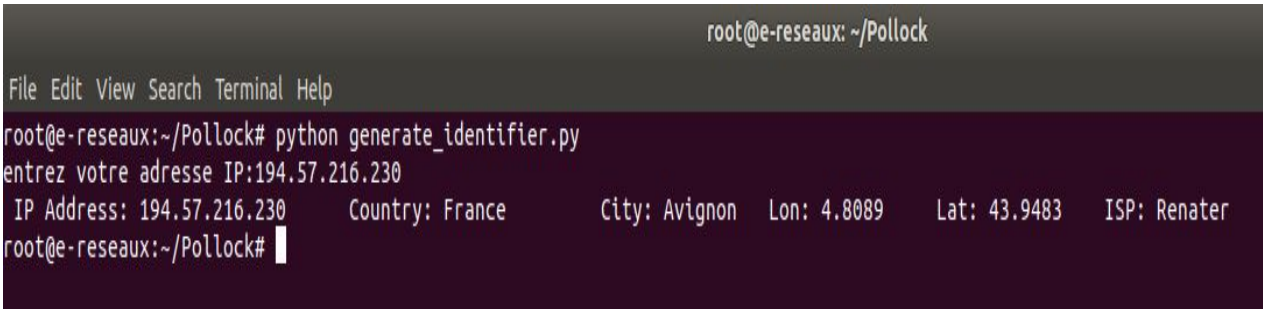
La technologie décentralisée rencontre des problèmes très importants. Lors d'une transaction on ne sait jamais si le client est vraiment le client et le vendeur est bien le vendeur, pour ça on doit réfléchir à une solution pour assurer la sécurité des échanges.
La réflexion nous amène donc à choisir entre deux solutions, La signature électronique et la blockchain.

1. créer une fonction de géolocalisation avec un système d'anonymat pour la sécurité privée de l'utilisateur

Lors de cette étape, on a créer un algorithme qui nous renvoie la localisation exacte d'un utilisateur à partir de l'adresse IP Publique qu'on fournit manuellement.
Ce programme nous fournit le pays, la ville et les coordonnées spatiales.

2. Génération d'un identifiant unique pour chaque noeud qui prend en compte une géolocalisation.

Nous avons pensé dans un premier temps à générer un nombre aléatoire de 32 bits à partir le "uuid" qui divise 128 bits par 4 , puis de faire un hash de ce dernier. Après on demande à l'utilisateur de rentrer une référence (ses initiales, son nom, …) et on l'ajoute au milieu du nombre hashé. On récupère la localisation (ville par exemple) et on concatène avec le message hashé,on obtient donc un identifiant qui porte une référence unique et prend en compte la localisation du noeud.



On entre l'adresse IP Publique du noeud et il nous retourne la localisation.

On affiche l'identifiant finale du noeuds qui est composé de l'identifiant hashé plus le message entré par l'utilisateur qui se place au milieu de la chaîne, tout cela est concaténée avec la localisation.

Pour échanger entre l'émetteur et le récepteur on doit générer une paire de clé Pu/Pr, pour s'assurer de l'identité de chacun on doit procéder par un système de certification, qui peut être une entité intermédiaire de confiance centralisée.