DESTREE Gabriel, RASSU Michael, BENCHRIFA Mohamed Amine, AMINE KHODJA Ahmed Ramy

BlockChain - Identifiants

Contrainte à respecter :

-> Garder l'anonymat de chaque entité.
-> En cas de litige on doit pouvoir retrouver l'identité d'un chauffeur ou d'un utilisateur.

Chauffeurs et utilisateurs:
Identifiant de même format entre chauffeur et utilisateurs.
L'identifiant est composé de son nomPrenom chiffré avec shamir. Qui sera trouvables si 10 chauffeur ou utilisateurs s'allient pour le trouver.

Mise en condition Création de compte:

Un utilisateur ou chauffeur s'inscrit, il rentre alors son nom et son prenom qui forme une chaine de caractère qui sera converti en hexadécimal puis généré un polynôme de shamir d'ordre 24 (avec k=25 et le n = nombre d'utilisateur) puis envoyé à tous les utilisateurs du blockchain un point à chaqu'un, qui a leurs tours généreront un point supplémentaire et leurs enverra en retour. Ce qui à pour conséquence que chaque utilisateurs du blockchain disposera d'un point qui permet de décrypter l'id de chaque utilisateur.
Chaque utilisateurs disposera d'une clé qui permet en association avec 25 autres permet de trouvé le nom et prénom d'un utilisateur/chauffeur.

->On suppose que l'utilisateur ou le chauffeur qui s'inscrit fourni une bonne identité.
->On suppose que un utilisateur/chauffeur ne peut avoir qu'un compte.

Mise en condition course:

Quand un client trouve un chauffeur et valide une course avec lui, un identifiant pour la course est créé. Basé sur l'identifiant du client et du chauffeur ainsi que la date.
La formule est : Identifiant utilisateur * Identifiant chauffeur * date.
La date permet d'identifier la date a laquelle faire la course mais aussi générer des identifiants différents si un utilisateurs fais plusieurs courses avec un même chauffeur.

Mise en condition litige:
Si un utilisateurs (ou chauffeur) désire faire un litige à propos d'une course, disposant de son identifiant utilisateurs , de la date, il permet de prouver que c'est bien lui qui à fais la

course avec ce chauffeur en particulier et trouver son identifiant, qui sera possible de décrypter afin de retrouver l'identité avec l'approbation de 25 utilisateurs du réseau. Chaque personne parmi les 25 va envoyer son g(x) a la personne réclament le litige chiffré avec sa clé publique.

Smart Contracts

Un contrat sera publié et devra être accepté à la création d'un compte utilisateur, qui demande le consentement que ses données (nom et prénom) peuvent être fourni à un utilisateur du réseau en cas de litige s'il réussi à avoir l'approbation de 25 autres utilisateurs.