

ADDA Ahlem Lamia
ALCARAZ Hugo
ISLAHI Chaimae
NDIAYE Samba Oumar

M1 SICOM

VALIDATION D'UN TRAJET

(Blockchain)



TABLE DES MATIÈRES

1. Introduction	3
2. Paiement	3
3. Solution la plus simple	5
4. Différents problèmes possibles : côté utilisateur.	5
UN CHAUFFEUR EN RETARD ?	5
UN POINT DE DÉPOSE NON RESPECTÉ	5
UN AUTRE CHAUFFEUR A EFFECTUÉ LA COURSE ?	5
MON CHAUFFEUR A FAIT UN ARRÊT QUE JE NE LUI AI PAS DEMANDÉ	6
POUR TOUT PETIT PROBLÈME : LA NOTATION FINALE	6
LE CHAUFFEUR ARRIVE AVEC UN VÉHICULE DIFFÉRENT	7
5. Problème côté chauffeur	7
ANNULATION DU PASSAGER	7
6. Sources	7

1. Introduction

Pour commencer, on se basera sur le cas où notre application fonctionne de telle sorte que l'utilisateur définit la position où il souhaite arriver ainsi que le prix qu'il est prêt à payer pour la distance qu'il souhaite faire.

À ce moment-là, une demande est donc envoyée à tous les chauffeurs se trouvant dans une zone proche de celle de l'utilisateur. Le chauffeur a alors le choix d'accepter ou refuser la course. Si la course est acceptée, le chauffeur doit alors se rendre sur le lieu de récupération.

Il n'y aura donc pas de surprises pour l'utilisateur si jamais le chauffeur décide de faire un détour ou de lui faire payer des frais de nettoyage ou de parking comme cela a déjà pu arriver dans l'histoire d'UBER.

Une façon de valider peut-être de générer un **nonce**, le nonce est créé lorsque le chauffeur à accepter le trajet, il est donné qu'à l'utilisateur (passager) et il doit le fournir à la fin du trajet au chauffeur. Ce nonce ne peut être saisi que par le chauffeur qui est prévu pour la course donc si par exemple un autre chauffeur est venu à la place de celui qui devait venir, le nouveau chauffeur ne pourra pas encaisser le paiement.

2. Paiement

Les problèmes de paiement peuvent être bien différents :

- Problème carte bancaire
- Site indisponible car mise-à-jour
- Problème serveur
- Erreur utilisateur saisie chiffre

Pour régler cela notre idée est donc de payer avant, en sécurisant bien sur les données et en se débrouillant pour qu'elle ne soit pas centralisée.

L'idée de fonctionnement d'une crypto monnaie nous est donc venu à l'idée.

Ci-dessous la façon dont pourrait fonctionner cette crypto monnaie.

Les utilisateurs sont identifiés par un identifiant unique : **Chauffeur** et **passager**

Nous devons sécuriser les paiements : sans dévoiler les RIB (portefeuille virtuel ?)

- Il faut s'assurer de l'identification d'une adresse de portefeuille utilisateur et l'intégrité du paiement :
 - Signature électronique et hachage
 - Deux fonctions cryptographiques sont utilisées :
 - Les fonctions de signature électronique et de hachage.

- La signature électronique se basera alors sur le principe d'un jeu de clés : une clé publique / une clé privée. .
 - Cela signifie qu'une personne peut, à partir d'une clé privée, obtenir la clé publique correspondante mais pas l'inverse (La clé est à sens unique). Il est donc techniquement quasi-impossible de trouver le code de la clé privée (connu de son seul propriétaire) à partir de la clé publique.
 - Une empreinte cryptographique est le résultat d'une fonction de hachage appliquée à une donnée initiale.
-
- Comme la signature électronique asymétrique, cette empreinte est à sens unique : il est quasiment impossible de déterminer la donnée initiale à partir de son empreinte. De plus, toute modification des données initiales induira une empreinte différente.
 - Le portefeuille contient des clefs de signature électronique permettant de les utiliser.

Pour réaliser un paiement, l'utilisateur va générer à partir de son portefeuille un jeu de clé (clé privée / clé publique).

- Une adresse de paiement (RIB) est alors créé à partir de la clé publique.
- La signature électronique permet de s'assurer que l'utilisateur est propriétaire d'une adresse de paiement, qu'il possède bien la clé privée associée à cette adresse.

Avant que le paiement soit enregistré, le protocole de vérification réalisé par les nœuds du réseau comporte les étapes suivantes :

➤ **Étape 1**

Établir le lien entre deux adresses utilisateur et un paiement réalisé

➤ **Étape 2**

S'assurer que le passager possède suffisamment de coins sur son adresse pour réaliser le paiement

➤ **Étape 3**

Vérifier l'intégrité du paiement

Cette étape consiste à vérifier la balance financière de chaque utilisateur du réseau, pour éviter les doubles dépenses (comme le ferait une banque dans un système centralisé).

3. Solution la plus simple

Le cas le plus simple est lorsque l'utilisateur et le chauffeur ont tous les deux validé le trajet sans aucun problème. La validation est alors effective, la somme d'argent prévue pour la course est alors envoyée du passager au chauffeur.

4. Différents problèmes possibles : côté utilisateur.

UN CHAUFFEUR EN RETARD ?

- Le passager attend son chauffeur plus de 10 minutes, il n'est pas encore sur place.

Solution :

- Le passager annule sa commande et précise sur la partie évaluation du chauffeur qu'il n'est pas ponctuel.

UN POINT DE DÉPOSE NON RESPECTÉ

- Le chauffeur n'a pas déposé le client au lieu précisé au départ de la course

Solution :

- A la fin d'un trajet l'utilisateur et le chauffeur doivent valider les données, UBER ne recevra que l'heure et la date de validation, et la géolocalisation sera stockée sur les téléphones des deux sans que UBER ne puisse y accéder, si jamais il y a litige, UBER peut demander l'autorisation. Si le temps de validation des deux utilisateurs diffère trop l'un de l'autre, UBER peut tirer une conclusion grâce à ces temps et même imposer une amende au chauffeur s'il n'a pas bien fait son travail.

UN AUTRE CHAUFFEUR A EFFECTUÉ LA COURSE ?

- Lors de l'arrivée de mon chauffeur, je me rends compte que le chauffeur qui m'attend n'est pas le même que celui qui était prévu pour le trajet sur l'application.

Solution :

- Chaque chauffeur UBER a un ID unique disponible sur son application, sur mon application, j'ai son ID d'afficher, je lui demande de me montrer le sien pour vérifier que c'est le même et donc si ce n'est pas le cas j'ai le droit de le prendre en photo comme justification de l'annulation de trajet.
 - Solution valable sauf si le chauffeur officiel à "donner" son compte à une tierce personne, l'ID sera donc le bon.
- Dans le cas on l'on utilise les nonce, ce problème ne peut exister car si un autre chauffeur prend la place de celui qui aurait dû effectuer le trajet il ne pourra pas encaisser le montant.

MON CHAUFFEUR A FAIT UN ARRÊT QUE JE NE LUI AI PAS DEMANDÉ

- Lors du trajet, le chauffeur s'est arrêté à un endroit qui a des conséquences sur mon heure d'arrivée.

Solution:

- Pouvoir interrompre la course en signalant les raisons qui nous porte à le faire

POUR TOUT PETIT PROBLÈME : LA NOTATION FINALE

- Le client doit noter le chauffeur une fois arrivé à destination pour garantir des courses de qualité aux passagers.
- Problèmes fréquents :
 - Chauffeur impoli
 - Non-respect du code de la route
 - Le chauffeur refuse de se rendre à la destination sélectionnée.
 - Autres problèmes avec le chauffeur.
 - Comportement du chauffeur désagréable

Solution:

- Donner la possibilité au client de noter le trajet :
 - Possibilité d'attribuer 1 à 5 étoiles au chauffeur.
 - Possibilité de laisser des commentaires détaillés par le biais de la liste de problèmes fréquents.
 - Les notes sont prises au sérieux donc les chauffeurs qui seront mal notés peuvent se voir refuser l'accès à l'application Uber.

LE CHAUFFEUR ARRIVE AVEC UN VÉHICULE DIFFÉRENT

- Lors de l'arrivée de mon chauffeur je me rends compte que le véhicule est différent à celui que j'avais commandé sur l'application.

Solution:

- Possibilité de changer de véhicule si cela n'a pas de conséquence à mon heure d'arrivée.
- Possibilité d'annuler le trajet, et de choisir un autre chauffeur.

5. Problème côté chauffeur

ANNULATION DU PASSAGER

- Si la fonction « annulation » a été activée par le passager

Solution :

- Si le passager annule la commande moins de 5 minutes avant l'arrivée du chauffeur, il paiera la totalité du coût du trajet.
- Si le chauffeur annule la course après avoir attendu cinq minutes sur le lieu de prise en charge. le passager paiera la totalité.

6. Sources

- ❖ <https://www.numetik-avocats.fr/wp-content/uploads/2018/05/NUMETIK-AVOCATS-Livre-blanc-Blockchain.pdf>
- ❖ <https://help.uber.com/fr-FR/partners/article/comment-sont-facturés-les-frais-da-annulation-dun-passager%C2%A0?nodeId=eebc0564-5228-4d70-997c-0fe63f0753c2>
- ❖ <https://help.uber.com/fr-FR/riders/section/problèmes-liés-à-une-course?nodeId=595d429d-21e4-4c75-b422-72affa33c5c8>
- ❖ <https://help.uber.com/fr-FR/riders/article/noter-un-chauffeur?nodeId=478d7463-99cb-48ff-a81f-0ab227a1e267>
- ❖ <https://help.uber.com/>