IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Projet développement n° 24 - Juin 2018

AUTEURS :
M. Dahoumane, M. El Houicha, F. Hafid et M. Maachou
mehdi.dahoumane@imt-atlantique.net maroua.el-houicha@imt-atlantique.net
hafid.faycal@imt-atlantique.net marouane.maachou@imt-atlantique.net

TUTRICE :
Elsa DUPRAZ
elsa.dupraz@imt-atlantique.fr

Comprendre et implémenter les mecanismes du Bitcoin

RESUME

La plateforme réalisée au cours de ce projet s'adresse principalement à des enseignants souhaitant introduire à leurs élèves les concepts relatifs aux crypto-monnaies ou à des professionnels voulant réaliser des tests de sécurité. En outre, elle permet aux utilisateurs de créer un compte et d'effectuer les diverses opérations qu'on peut retrouver avec une cryptomonnaie

INTRODUCTION

Les crypto-monnaies ont aujourd'hui réussi à s'imposer dans les milieux financiers et à susciter l'intérêt d'une grande partie de la population. Accessibles à tous -des professionnels du domaine aux simples usagers-, elles sont de plus en plus utilisées. C'est la raison pour laquelle nous avons cherché à comprendre et à implémenter les mécanismes du Bitcoin, la crypto-monnaie la plus répandue.

NOS REALISATIONS

```
Bienvenue dans l'application.
Donnez votre ID : Marouane

donnez votre MDP : 1
Vous êtes connectés. Bienvenue :)

Entrez le numéro de votre opération :
1- Consulter votre solde
2- Deconnexion
3-Consulter l'historique de vos transactions
4-Effectuer une transaction
```

Nous avons créé une plateforme utilisateur qui permet l'identification puis diverses opérations (transaction, consulter le solde…)

Nous avons implémenté une BlockChain simplifiée et sécurisée qui traite les transactions et stocke celles qui sont validées

Nous avons implémenté, en orienté objet sous forme de classes, des modélisations du Bitcoin, d'un utilisateur (User) ainsi que d'une Transaction

Nous avons assuré la sécurité et la fiabilité en reproduisant les mécanismes du Bitcoin tels que les fonctions de hashage SHA256 ou l'algorithme ECDSA pour les signatures digitales

RESULTATS

Sous Python, nous avons été capable de développer une plateforme qui permet aux utilisateurs de créer un compte, consulter leur solde et effectuer des transactions en toute sécurité grâce aux protocoles employés et inspirés du Bitcoin.

CONCLUSION ET PERSPECTIVES

Tout au long de l'implémentation, nous avons mené plusieurs séries de tests qui ont permis dans un premier temps de vérifier que les transactions s'effectuaient correctement et que la blockchain s'actualisait convenablement. Par la suite, nous avons axé les tests sur la sûreté de notre crypto-monnaie en simulant des cyber-attaques. Ce projet peut alors servir à long terme à des professionnels souhaitant réaliser des tests de sécurité ou à des enseignants souhaitant aborder le thème des crypto-monnaies avec leurs étudiants.