Achtatou Sean
Sergei Tickomirov

Université du Luxembourg

Bachelor en Science Informatique

La chaine de block

Semestre 2 - 2017-2018

1.Introduction

Ce projet de Bachelier, se penche parmi l'une des branches de la cyber-sécurité présente aujourd'hui, autour d'un système utiliser par plusieurs institutions, et commençant à se faire connaitre par le monde petit à petit : la chaine de block.

Comme son nom l'indique, il s'agit d'un algorithme basé sur une chaine de block ayant pour but le partage d'informations, plus précisément de transactions, entres utilisateurs par « Peer to Peer » signifiant qu'il n'existe pas de serveur centralisé dans le réseau. Le fonctionnement du Block Chain, principalement sa sécurité, fut étudié par différents chercheurs autour du globe, et ces derniers l'on considéré comme étant informatiquement impossible à déjouer. De ce fait, le but premier de ce projet est d'affirmer ces résultats en ayant la possibilité de fournir des exemples pratiques. D'une autre part le fonctionnement détaillé du Block Chain est également à prendre en compte. De ce fait, nous divisons l'algorithme du Block Chain en différentes parties :

● La fonction de hachage
● La signature digitale
● L'arbre de Merkle.

Ces différentes parties sont vérifiés individuellement pour confirmer leur sécurité. Bien sûr, certaines contraintes sont à prendre en compte lors de nos recherches tel que :

● La compréhension mathématique des formules présentes dans les différents algorithmes.

● Une connaissance basique en sécurité informatique principalement pour la signature digitale.

De plus, due à l'utilisation d'exemples pratiques, un langage de programmation ; ici Python 3 ; et une connaissance minime en programmation est fort recommandé.

2.Sommaire

Nous commençons par la fonction de Hachage. Cette dernière permet de « compresser » des données d'une certaine taille à une taille fixe plus petite. Il existe plusieurs fonctions de hachage, ici nous utilisons SHA-256[256 Bits de donnée fixe]. Cette fonction est utilisée pour pouvoir détecter d'éventuelles modifications des données et se doit de respecter plusieurs propriétés lui donnant sa haute sécurité :

● Déterminisme
● La première résistance pré-image
● Deuxième résistance pré-image
● La résistance à la collision.

Nous vérifions ces dernières en mettant en pratique la fonction hachage et en tentant de casser son l'algorithme.

Ensuite, la signature digitale. Permettant de créer une signature à l'utilisateur pour l'identification d'une transaction entres les utilisateurs dans le réseau. Cette dernière, créant une clé publique à partir de la clé privée également créer, va-t'en résulter une signature par l'établissement d'une une fonction de hachage sur la clé privée et les données. Lors de la vérification, l'algorithme s'octroie la clé publique, la signature et les données pour confirmer l'authenticité de la transaction. Tel que la fonction de hachage, la signature digitale se doit de respecter différentes propriétés tel que :

● L'authentification
● La non-réfutation
● Et l'intégrité

Par la suite, nous nous intéresserons à l'arbre de Merkle. Cette opération se passant individuellement dans chaque bloc de la chaine, permet de confirmer l'existence d'une certaine transaction du bloc. Utilisant la fonction de hachage pour son algorithme, son utilité reste optionnelle car ce n'est qu'une simple vérification de la présence d'une transaction .

Pour finir, nous créons, grâce à ces différentes parties citées plus haut, une chaine de block local. Puisque nous ne nous intéressons pas à la partie réseaux, mais plus sécurité, la signature digitale n'est pas à prendre en compte.

3.Conclusion

Nous nous rendons vite compte, grâce à nos différentes observations et tests sur ces fonctions, que ces dernières sont promettantes et confirment bel et bien la haute sécurité que la chaine de block laisse croire. De ce fait, le réseau de la chaine de block pourrait bel et bien devenir dans un avenir proche, l'un des principaux réseaux de transaction digital, voire le seul.