



Méthodes Informatiques Appliquées à la Gestion de l'Entreprise

Mémoire Master 2 Classique

Comment remplacer les banques par les blockchains ?

Auteur :

Sokhna Maimouna SOW

Encadrant :

Mme Marie-Pierre GERVAIS

Année scolaire
2017 - 2018

Présentation

A quoi cela sert-il ? En quoi est-ce un problème lié à l'informatique / qui peut être résolu grâce à l'informatique ?

En quoi votre sujet se différencie-t-il des sujets des années précédentes (par exemple depuis 2014) en M2 MIAGE classique ?

Qu'est ce qui existe ? quelles sont les limites de cet existant ?

Qu'est ce qui pourrait permettre de résoudre le problème ? d'aller au delà des limites ?

Que comptez vous proposer / expérimenter ?

Votre réalisation comprend-elle une part de développement (qu'il s'agisse d'une application en Java, d'un tableau de bord en Excel, de règles pour outil de BI, etc) ?

Est-il possible de valider votre proposition ? aurez-vous accès à des données pour le faire (si applicable à votre sujet) ?

Entre 5 et 10 références (avec au moins 5 références qui ne sont pas des liens de pages Web, mais plutôt des articles ou livres, de préférence à valeur scientifique cad publiés dans une conférence ou journal scientifique)

Une blockchain est une technologie de stockage et de transmission d'information sécurisée. Elle constitue une base de données sécurisée et distribuée qui contient toute l'historique de tous des les échanges entre ses utilisateurs depuis sa création. Cette base est partagée par les différents utilisateurs sans intermédiaire, donnant la possibilité à chacun de vérifier la validité de la chaîne. Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Chaque bloc est validé par les noeuds du réseau appelés les "mineurs", selon des techniques qui dépendent du type de blockchain, qui si elle est publique, fonctionne obligatoirement avec une monnaie programmable. Ici je prendrais Bitcoin qui

est un bon exemple de monnaie. Dans la blockchain du bitcoin cette technique est appelée le “Proof-of-Work”, c’est à dire preuve de travail, et consiste en la résolution de problèmes algorithmiques. Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l’ensemble du réseau. Le caractère décentralisé de cette nouvelle technologie, couplé avec sa sécurité et sa transparence, fait des prouesses aujourd’hui.

Par ailleurs il n’existe pas de banque centrale qui produit cette monnaie bitcoin. En effet, il s’agit d’ordinateurs distincts qui appartiennent au même réseau Bitcoin et qui sont rémunérés contre un service. C’est ce qu’on appelle le **minage de Bitcoin**. Il est sécurisé par le procédé cryptographique, la preuve de calcul. La difficulté pour quiconque de résoudre ces preuves de calcul assure la sécurité de toutes les transactions.

Mais pourquoi utiliser cette monnaie virtuelle alors que nous avons accès à nos comptes bancaires par internet et nous pouvons faire des virements et des paiements en ligne ? Simplement l’anonymat ! La première raison de l’émergence de cette monnaie. Vous pouvez en effet régler vos achats dans l’anonymat le plus complet ce qui vous permet d’éviter tout risque de hacking sur votre compte bancaire courant. Cette monnaie échappe aussi à tout système bancaire mis en place jusqu’ici donc pas de contrôle et personne ne la maîtrise assez pour la réguler.

Pendant ce temps, nous avons un système bancaire qui a un réseau organisé, encadré et centralisé. C’est un système qui est bien construit et trop bien hiérarchisé et qui fonctionne grâce à des dirigeants qui ont la main sur tout et ont toujours le dernier mot.