Blockchain
La confiance distribuée

Rapport Info 910

Par
Thomas Bottollier-Darbelin
Baptiste Diot
Aramais Stepanyan

Pour
Info 910 - Cryptologie

Professeur
M. Pierre Hyvernat

le
04/01/2021

Table des matières

I) Introduction

A notre époque, les échanges et les transactions se déroulent de plus en plus de façon distante et par voie numérique. Une évolution exacerbée depuis le début de l'année 2019 avec les mesures sanitaires de distanciation sociale et de quarantaine mises en place contre la propagation du coronavirus.
Cette situation amène une accélération de la hausse d'une demande déjà grandissante ces dernières années : l'accès à des technologies permettant d'authentifier et de sécuriser les échanges numériques de façon rapide, fiable et transparente pour l'utilisateur.
En effet, si les usages et les besoins évoluent rapidement, les technologies permettant leur sécurisation doivent en faire de même afin d'éviter d'éventuelles failles de sécurité. De telles failles pourraient compromettre la confiance entre les utilisateurs et le gouvernement par exemple.
L'une des technologies les plus prometteuses étant susceptible de répondre à ces besoins d'évolution rapide (tout en maintenant le plus haut niveau possible de sécurité et de fiabilité) est la Blockchain. Cette technologie issue du développement de la cryptomonnaie Bitcoin, a l'avantage d'être décentralisée, en plus d'utiliser des méthodes plus "classiques" de sécurisations par cryptographie.
Nous allons voir à travers deux exemples, l'importance de la confiance dans les nouveaux services rendu possibles par la Blockchain et comment cette confiance est garantie par son caractère décentralisé :

- Projet du MIT d'application mobile pour le tracking de contacts COVID
- IBM Food Trust

II) Présentation Blockchain

La Blockchain est une base de données qui est représentée par des blocs chaînés qui contiennent des données.

Le terme Blockchain est pour la première fois utilisé en 1991 pour l'utilisation dans les signatures électroniques des documents, mais la vraie célébrité de ce terme a été apportée par Satoshi Nakamoto en 2009 avec la création de monnaie numérique « Bitcoin ».

1) Fonctionnement

Chaque bloc contient des données, le hash du bloc lui-même et le hash du bloc précédent. Donc tous les blocs sont reliés entre eux. Une fois que le bloc a été validé et ajouté à la chaîne, il est impossible de le modifier ou de le retirer.

Le hash du bloc permet de vérifier que le bloc n'a pas été modifié. Mais actuellement les ordinateurs possèdent assez de ressources pour parcourir toute la chaîne, modifier chaque bloc et recalculer le hash. Pour éviter ce problème, il a été inventé un système « Proof of Work » qui sert à ralentir la création des nouveaux blocs par la vérification de leurs hashs.

Pour les Bitcoin la création d'un nouveau bloc dans la chaîne peut durer environ dix minutes. Ce mécanisme exclut la possibilité de falsification de bloc mais il est beaucoup critiqué car ça nécessite de grandes capacités de calcul. Et c'est pour cette raison que lors du transfert de bitcoins une commission est facturée. C'est ainsi que s'effectue le paiement pour la puissance de calcul utilisée.

Il existe deux types de Blockchain publique et privée.

La **Blockchain publique** est une base de données ouvertes dans laquelle chaque participant peut lire et écrire les données. Principalement utilisé pour les monnaies numériques.

La **Blockchain privée** possède des restrictions pour la lecture et l'écriture des données. Les blockchains privées sont beaucoup utilisées par les entreprises pour expérimenter en interne.

Les avantages de la Blockchain sont :

- Décentralisation – la chaîne ne possède pas de serveur principal. Chaque participant est le serveur qui contient toutes les données.
- Transparence - toutes les informations des transactions sont dans l'accès public pour tout le monde. Mais ces données restent immuables.
- Illimité - en théorie il est possible d'ajouter un nombre infini de blocs.
- Fiabilité – pour ajouter un nouveau bloc il faut que tous les autres blocs le valident. Ça permet de filtrer les transactions et d'enregistrer seulement les transactions valides. Il est impossible de changer le hash contenu dans un bloc.

2) Utilisation de la Blockchain

Dans la plupart des cas, la blockchain est utilisée dans le secteur de la finance, du commerce et de l'assurance. En plus de ça la Blockchain est employée pour :

Identification d'identité : certains services récents (start-ups) dans le domaine de l'identification d'identité fonctionnent sur la base de la technologie Blockchain. Ils créent l'équivalent numérique d'une carte d'identité.

Droit d'auteur : il existe des plateformes qui permettent aux artistes, musiciens et inventeurs de garder leurs droits d'auteur à l'aide d'identifiants cryptés dans les blocs chaînés.

Élections : jusqu'à présent, la Blockchain n'a été utilisée que pour le vote privé. Cependant, l'Université de Virginie souhaite mettre en œuvre une technologie basée sur la Blockchain. Cela réduira les risques de falsification à zéro.

Gestion et jurisprudence : le potentiel de Blockchain dans ce domaine est infini. Il est possible de créer un système qui pourra stocker des informations sur les données budgétaires ou autres données gouvernementales importantes qui ne pourront être modifiées. Il existe déjà des projets comme « Borderless » qui combinent des services juridiques et économiques.

Charité : la Blockchain, avec sa capacité à enregistrer et stocker des données, est très efficace dans le domaine de la charité. La plateforme « GiveTrack » fournit des informations ouvertes sur les dons aux fondations caritatives ainsi que leurs dépenses.

Immobilier : l'introduction de la Blockchain dans le secteur immobilier peut considérablement l'améliorer. Le processus d'achat et de vente sera accéléré et le stockage des données deviendra beaucoup plus fiable.

Potentiellement, la technologie Blockchain peut être utile partout où il est indispensable d'avoir des rapports, une authentification ou du stockage de données. Le potentiel est illimité.

III) Exemples d'application

1) Projet du MIT – Private Kit : Safe Paths

Projet du MIT pour anonymiser les données dans une application de tracking des contacts COVID.

A) Problématique

L'un des aspects les plus importants de la confiance entre un utilisateur et un service ou une application numérique est la protection des données personnelles de l'utilisateur. Dans le contexte actuel de pandémie mondiale, la confiance qu'un utilisateur a envers une application est d'autant plus cruciale quand elle conditionne l'adoption d'une application permettant d'enrayer la progression du virus et ainsi réduire le nombre de victimes. En effet, les applications mobiles permettant le traçage des personnes contaminées dans le but de notifier les personnes saines avec qui elles sont entrées en contact ont une efficacité proportionnelle au pourcentage de la population qui les utilise.
Il est donc essentiel que ces applications soient sécurisées et qu'elles apportent le plus haut niveau possible de confiance aux utilisateurs.
C'est pour répondre à cette problématique que des chercheurs du MIT ont entrepris de concevoir les bases d'un système permettant de mettre à profit les avantages de la Blockchain pour sécuriser et anonymiser les données utilisateurs.

B) Fonctionnement

Le système conceptualisé par le MIT Media Lab et ses collaborateurs a pour but de proposer une alternative aux applications de suivi des contacts COVID (ou d'autres maladies contagieuses), sans aucun compromis sur la protection des données personnelles des utilisateurs.
Pour réaliser cet objectif, le projet s'appuie dans un premier temps sur des technologies de cryptographie (des fonctions de hachage unidirectionnelle déterministe notamment) et une architecture client-serveur peu complexe.

Première implémentation

Dans cette première configuration, chaque utilisateur de l'application mobile possède un identifiant et un historique de contact.
L'application mobile d'un utilisateur *A* collecte à intervalle régulier des données Bluetooth. Ces données correspondent aux identifiants des autres utilisateurs entrant dans un faible rayon autour de l'utilisateur *A*.
Un timestamp est ajouté, le tout est crypté puis ajouté à l'historique de contact.
Une fois par jour, l'historique de contacts est uploadé sur un serveur géré par un organisme de confiance (gouvernemental ou autre).
Si l'utilisateur *A* contracte le Coronavirus, le serveur stockant les historiques de contacts est notifié. Le serveur notifie à son tour tous les utilisateurs présents dans la liste de contacts de

l'utilisateur *A,* en conseillant un test ou une visite chez le médecin selon la fréquence et la longueur du ou des contacts constatés.

Implémentation améliorée par la Blockchain

Dans la première implémentation, il subsiste une faille de sécurité pour les données utilisateur: le serveur centralisant les historiques de contact et gérant les notifications. En effet, l'organisme contrôlant le serveur peut est compromis :

- L'organisme n'est en fait pas digne de confiance et il accède aux données personnelles des utilisateurs.
- L'organisme n'est pas assez vigilant en termes de cyber-sécurité et le serveur possède des failles de sécurité exploitées par des hackers pour accéder aux données personnelles des utilisateurs.

Cette faille peut être supprimée par l'utilisation d'une Blockchain en lieu et place d'un serveur central.

Si le rôle du serveur central est confié à une Blockchain, les problèmes de sécurisation d'un serveur unique ou de confiance en un organisme tiers disparaissent. La propriété de décentralisation de la Blockchain permet d'avoir une confiance maximale envers le système.

2) IBM Food Trust

Le programme Food Trust est une initiative d'IBM essayant de résoudre plusieurs problèmes liés au secteur agro-alimentaire. Des problématiques telles que l'hygiène alimentaire, l'efficacité de la chaîne d'approvisionnement, la coordination entre les différentes entreprises ou encore le gaspillage alimentaire sont toujours d'actualité et sont des questions que les entreprises et les consommateurs se posent de plus en plus.

Food Trust est un bon exemple d'application utilisant la technologie blockchain pour résoudre ces problèmes. Ce programme est un réseau permettant de connecter les producteurs, les fournisseurs, les fabricants et les revendeurs entre eux à travers des rapports détaillés des processus de la chaîne d'approvisionnement.

A) Problématique

En informatique, on sait que beaucoup d'entreprises ont un retard conséquent en termes de technologie et d'outils numérique pouvant simplifier ou automatiser un processus. Ce retard est d'autant plus visible dans l'industrie pharmaceutique et agro-alimentaire en raison des normes qui leurs sont imposées par la FDA (Food and Drug Administration pour les États-Unis) ou par la EMA (European Medicines Agency pour l'Europe). Par manque de temps ou de moyen, un grand nombre d'entreprises préfèrent continuer leur gestion de leurs procédés avec ce qu'ils connaissent, c'est-à-dire une gestion manuelle.

Efficacité dans la chaîne d'approvisionnement et gaspillage alimentaire

Plusieurs études ont montré un problème d'inefficacité dans la chaîne d'approvisionnement dans le secteur agro-alimentaire. Tous les acteurs de la chaîne en sont responsables. Une mauvaise gestion au sein de l'entreprise ou une mauvaise coordination entre les entreprises peuvent entraîner une perte de profit non négligeable mais également augmenter l'empreinte carbone de l'entreprise et le gaspillage alimentaire. Une perte de profit de $60 milliards a été estimé en raison de l'inefficacité entre les producteurs et les fournisseurs[1]. En termes de gaspillage alimentaire, 1,6 milliards de tonnes de nourriture jeté chaque année ont été estimés par manque de coordination entre les acteurs de la chaîne d'approvisionnement et une mauvaise traçabilité des dates de péremption et de la chaîne du froid.

Confiance des consommateurs

Aujourd'hui, lors d'un achat, 84 % des consommateurs accordent de l'importance sur où et comment un produit a été fabriqué[3]. Ils veulent de plus en plus savoir la provenance d'un produit, s'il vient de commerce équitable, son impact écologique sur la planète, etc.

La qualité et la fraîcheur d'un produit est une question de plus en plus grandissante dans la tête des consommateurs et donne une problématique en plus pour les acteurs de la chaîne d'approvisionnement.

La fraude alimentaire

La fraude alimentaire peut prendre plusieurs formes telles qu'un mauvais étiquetage ou de fausses déclarations destiné à tromper le consommateur ou encore une substitution d'un produit par un autre de nature ou de qualité différente.

Par manque de transparence, de régulations et de responsabilité, la fraude alimentaire a augmenté de 60 % au cours de ces deux dernières années[4]. Beaucoup d'entreprises ne se rendent simplement pas compte qu'ils peuvent être touchés et affectés par de la fraude alimentaire.

B) Solutions apportées grâce à la blockchain

Avec le programme Food Trust, IBM utilise la blockchain pour permettre à tous les acteurs de la chaîne d'approvisionnement de pouvoir tracer la provenance, la localisation en temps réel et le statut de leurs produits.

Avec ce système, les entreprises participant aux programmes peuvent identifier les problèmes éventuels dans la chaîne et peuvent optimiser leur approvisionnement en développant de meilleurs modèles prévisionnels sur l'offre et la demande. Ceci leur permettra d'éviter des dépenses inutiles mais surtout d'éviter de jeter le surplus de nourriture potentiel.

La visibilité de l'ensemble de la chaîne d'approvisionnement ne bénéficie pas qu'aux entreprises, mais également aux consommateurs. Les entreprises proposent ainsi une transparence complète permettant de suivre chaque étape de la chaîne pour assurer aux consommateurs la provenance et la qualité de leurs produits.

IBM Food Trust possède également un module de certifications, permettant aux entreprises de prouver leur qualité en affichant les certificats délivrés par un audit, augmentant ainsi la confiance entre les différents acteurs de la chaîne et avec les consommateurs

Cette preuve de qualité offre un autre avantage pour les entreprises. Un consommateur qui a confiance en la qualité d'un produit d'une certaine marque aura tendance à l'avenir à racheter le même produit ou d'autres produits de cette même marque.

IV) Conclusion

Actuellement, la Blockchain est une technologie encore relativement jeune et ses avantages et limitations ne sont pas encore complètement définies. Les exemples des projets Private Kit et IBM Food Trust nous ont permis d'entrevoir une partie de son potentiel dans le domaine de la confiance entre différents acteurs. Cependant, ses véritables atouts restent encore à prouver.

Nous verrons dans les prochaines années si cette technologie arrive à mûrir et à s'imposer comme une véritable innovation ou si elle reste un "gadget", sans réel intérêt concret dans ses applications.

Sources

Présentation Blockchain

http://bestinvestpro.com/blokchejn-chto-eto-ponyatnym-yazykom/

https://zen.yandex.ru/media/id/5e3d6f47cfae456d3d739836/chto-takoe-blokchein-prostymi-slovami-polnoe-opisanie-5e3dc039f58c3b19c8d963b2

Projet du MIT - Private Kit : Safe Paths

https://arxiv.org/pdf/2003.14412.pdf

https://www.wired.com/story/covid-19-contact-tracing-apps-cryptography/

IBM Food Trust

https://www.ibm.com/downloads/cas/LR8VR8YV - Supply Chain Efficiencies

https://www.ibm.com/downloads/cas/JDKYEKD5 - Brand Trust

https://www.ibm.com/downloads/cas/ZN9EWKRQ - Food Safety

https://www.ibm.com/downloads/cas/QK0MVJNZ - Food Freshness

https://www.ibm.com/downloads/cas/YDKZAB6O - Food Fraud

https://www.ibm.com/downloads/cas/R8VDMJ4Y - Sustainability

https://www.ibm.com/downloads/cas/JLDRRDWQ - Food Waste

https://www.bcg.com/publications/2018/tackling-1.6-billion-ton-food-loss-and-waste-crisis

https://j-sainsbury.co.uk/media/1767151/sainsbury_s_takes_tesco_price_promise_to_judicial_review.pdf

https://www.newfoodmagazine.com/video/74615/combating-global-food-fraud/