IDEMIA

Blockchain : bien plus qu'un buzzword

Par Bruno Letellier, CTO - Mobile Operators chez IDEMIA

 # PAIEMENT
 # IDENTITÉ

POSTÉ LE 26.02.18

- La Blockchain, ou « chaîne de blocs », est un concept plus simple qu'il n'y paraît : formation accélérée sur le sujet
- Le transfert des clés, du Cloud vers un élément physique sécurisé, permet d'envisager de nouvelles applications de la blockchain au quotidien

Depuis l'apparition de la blockchain en 2009, la technologie a souvent fait parler d'elle en raison de son ingéniosité et de son potentiel révolutionnaire pour d'innombrables secteurs. Loin de n'être qu'un mot à la mode, cette innovation fait entrer nos vies digitales dans une nouvelle dimension. Mais comment fonctionne-t-elle ? Prêts au décollage pour découvrir cette innovation ?

Fragmentation bloc par bloc

Imaginons que, pour le dîner, vous souhaitiez préparer un hamburger avec de la viande biologique issue de l'agriculture responsable. Le concept à l'origine de la blockchain, une chaîne d'informations immuable, consiste à vous permettre de toujours savoir parfaitement quels produits atterrissent dans votre assiette. Ainsi, d'un simple coup d'œil, vous pourriez connaître l'alimentation quotidienne de la vache, ses conditions d'élevage, le mode de transformation de la viande et son processus de vente. Une fois déclarés par l'éleveur, le boucher et le transporteur, tous ces « blocs » d'informations sont horodatés et liés à leurs auteurs. Ils ne peuvent ensuite être modifiés par personne d'autre. Jamais. Bien sûr, vous pouvez déjà obtenir toutes ces informations aujourd'hui mais, pour cela, il vous faudrait mener une étude ou vous rendre sur place, à la ferme, tandis que la blockchain peut fournir des informations immédiates, fiables et infalsifiables en temps réel.
Bien que la blockchain ne concerne pas encore les hamburgers, elle est devenue un « registre » d'informations largement accepté pour les transactions bitcoin, les dossiers médicaux et la gestion de l'identité.

Une forteresse de confiance

Par nature, la blockchain est une base sécurisée pour les données qui nous permet de partager des informations partout et avec tout le monde. Un registre détaillé des activités est certes déjà un avantage, mais comment pouvons-nous avoir la certitude que ses informations sont fiables ? Les clés privées prennent ici tout leur sens. Seuls les utilisateurs en possession de la bonne clé peuvent contribuer à leurs blocs d'informations. Ainsi, l'agriculteur de notre analogie ne peut enregistrer que des informations relatives à sa ferme et non au traitement, au conditionnement ni au transport de la viande. Grâce à la transparence offerte par la base de données, l'ensemble de l'activité est suivi et peut être analysé par toutes les personnes ayant accès à la blockchain, sans oublier que tous les utilisateurs sont aussi responsables de leurs contributions.

Le gardien des clés

L'utilisation de clés privées est un véritable facteur différenciateur de la blockchain car elle permet une gestion autonome et centralisée des données. Mais, en contre-partie, elle ouvre la porte à d'éventuelles corruptions. En effet, bien que le verrouillage de l'accès à la blockchain renforce certainement son niveau de sécurité, il crée aussi un objet de toutes les convoitises : la clé. Et si la clé privée est volée, le pirate peut écrire de manière irréversible dans le registre au nom du propriétaire de celle-ci. Or aujourd'hui, les clés privées sont toutes très commodément stockées dans le Cloud et leur regroupement dans un seul et même endroit en fait une cible très alléchante pour les hackers.

IDEMIA, le leader mondial des identités de confiance, transfère ces clés du Cloud vers un élément sécurisé afin de les stocker dans un coffre-fort physique sécurisé et s'assurer que seul son propriétaire légitime peut les utiliser pour intervenir dans la blockchain. Une fois la clé dans le coffre, son accès peut être protégé avec les données biométriques de l'utilisateur. Ensuite, il suffit d'associer la clé à une identité vérifiée et le propriétaire contrôle tout, sans aucun risque de voir son identité usurpée. De plus, la dispersion de toutes les clés complique considérablement la tâche des malfaiteurs. En effet, il ne leur suffit plus de pirater une plate-forme pour accéder directement à toutes les clés stockées, ils doivent s'attaquer à chaque utilisateur individuellement.

Blockchain IRL *(in real life)*

Outre l'avantage d'augmenter le niveau de sécurité des clés privées, leur transfert dans un élément physique sécurisé facilite la procédure et fait entrer la blockchain dans notre monde physique. Aujourd'hui, la cryptomonnaie ne peut être utilisée qu'en ligne car c'est là que sont stockées les clés. La promesse d'une clé physique sécurisée nous permettra d'utiliser cette monnaie pour régler nos achats dans la vraie vie. Demain, nous pourrons ainsi acheter une tasse de café à un distributeur automatique connecté. Cette machine enregistrera l'achat dans le registre et un simple geste de notre smartphone nous suffira pour payer notre café en toute sécurité. Plus sûre, la cryptomonnaie simplifie la vie, pour le bonheur de tous.

Chez IDEMIA, la gestion et la vérification de l'identité sont ancrées dans notre ADN. Sécuriser votre identité est un défi que nous sommes prêts à relever afin de garantir que vous seul puissiez être vous. Dans le monde de la blockchain, une identité à toute épreuve authentifie toute la chaîne d'information et ouvre les portes à des applications illimitées. Suite au prochain épisode !