

La Blockchain : Une révolution aussi importante qu'Internet ?

3 questions à Sam Guilaumé, ingénieur diplômé de l'ESEO, Directeur de EnerBee et Co-fondateur de TwinPeek¹

Beaucoup ont entendu parler de la monnaie virtuelle Bitcoin, mais probablement peu de personnes sont familiers avec la technologie sous-jacente, la « Blockchain », qui est pourtant en passe de révolutionner nombre de secteurs de la société.

A l'occasion de son intervention lors d'une conférence-débat sur la Blockchain organisée par l'ESEO le 22 juin dernier, Sam Guilaumé, entrepreneur, fin connaisseur du secteur des nouvelles technologies et usager de la Blockchain, nous aide à comprendre les fondamentaux de cette révolution à venir.

1. Qu'est-ce que la Blockchain ? En quoi est-ce utile ?

Sam Guilaumé : La Blockchain (ou « chaîne de blocs ») est un registre numérique d'informations, une base de données qui permet d'enregistrer des informations de façon séquentielle, infalsifiable et perpétuelle. Ces données peuvent être par exemple des transactions financières, comme dans la monnaie virtuelle Bitcoin, ou toute autre type de transaction : commerciale par exemple, ou encore administrative.

Une particularité de la Blockchain est d'être répliquée en de multiples copies, ce qui contribue à sa sécurité : pour modifier des données enregistrées il faudrait contrôler l'ensemble ou une large majorité des copies de la Blockchain. Cette distribution s'effectue sans contrôle centralisé, ce qui a permis par exemple d'établir, dans le cas de la monnaie virtuelle Bitcoin, un registre mondial et sécurisé de transactions financières sans aucune banque au centre ; la Blockchain devient elle-même le « tiers de confiance » qui garantit la propriété et la valeur des bitcoins.

2. Quels pourraient être les avantages de l'utilisation de la Blockchain pour notre société ?

Sam Guilaumé : Les usages de la Blockchain sont multiples car la notion de registre d'information est au centre de très nombreuses activités dans la société. Ses applications sont si nombreuses et son impact potentiel si important qu'on évoque actuellement une possible « quatrième Révolution industrielle ». A terme, la Blockchain peut ainsi permettre de se passer d'intermédiaires dans les échanges commerciaux ou administratifs. Elle pourrait court-circuiter certaines activités d'établissements

¹ Le projet TwinPeek a pour objectif de permettre aux internautes d'avoir une existence anonyme et sécurisée en ligne grâce à des « jumeaux virtuels ».

financiers (banques, assurances) ou de plateformes collaboratives (Uber, Airbnb, Le Bon Coin...). D'une part, ces intermédiaires sont actuellement vulnérables aux cyberattaques. D'autre part, ils se rémunèrent en prélevant une commission sur les échanges financiers ou en capturant les données personnelles des utilisateurs. Avec la blockchain, les échanges sont directs, sans intermédiaire et surtout sécurisés.

Pour de nombreuses filières économiques la Blockchain peut aider à éviter la fraude et contribuer à la traçabilité des produits à travers de multiples acteurs. Prenons l'exemple de la filière automobile qui voudrait suivre la vie d'un véhicule (vente- revente, entretien...) dans les réseaux de professionnels comme de particuliers. Le fait d'avoir un outil qui enregistre toutes les caractéristiques et les événements de la vie des véhicules permet de fiabiliser le système et garantit une description correcte du véhicule. La Blockchain ferait alors office de carnet de suivi et d'entretien dématérialisé des véhicules. On ambitionne de l'utiliser dans le secteur de l'énergie avec l'émergence de multiples sources de production : la production individuelle d'électricité (grâce à des panneaux solaires situés sur le toit d'une habitation par exemple) pourrait être vendue directement au réseau sans administrateur centralisé tel que EDF.

Il existe aussi des déclinaisons en termes de démocratie numérique. L'Estonie développe actuellement le concept de « e-citoyenneté ». Des cadastres distribués et participatifs voient le jour. Néanmoins, il n'est pas sûr que la Blockchain serve de support au vote, événement ponctuel par nature qui ne nécessite pas obligatoirement d'en constituer un historique perpétuel.

L'un des principaux enjeux que la Blockchain pourrait contribuer à résoudre, et sur lequel je travaille, est celui de la maîtrise des données personnelles, garantissant à la fois l'anonymisation et le droit à l'oubli, tout en donnant aux opérateurs économiques des garanties sur l'existence ou la solvabilité d'un client.

3. La technologie Blockchain présente-t-elle des limites ?

Sam Guilaumé : Comme pour toute technologie récente, il existe plusieurs contraintes techniques à lever pour optimiser son utilisation. Une Blockchain ne fait que grandir et peut atteindre une taille gigantesque, il est donc de plus en plus difficile de synchroniser les nouveaux acteurs entrant dans le système. La récupération de l'historique enregistré prend énormément de temps. La performance n'est pas encore à son niveau maximal, la vitesse d'insertion de nouvelles données est actuellement faible car limitée par la puissance du réseau auquel sont connectés les utilisateurs ; cette vitesse peut être insuffisante pour des applications qui nécessitent des enregistrements à très haute fréquence.

On s'interroge aussi sur le modèle de cohérence de l'historique partagé. Si plusieurs acteurs écrivent dans une mémoire partagée, que faire lorsque les informations saisies sont contradictoires, voire concurrentes ?

La question la plus sensible reste cependant le contrôle et l'intégrité des informations enregistrées. Lorsque des transactions doivent être enregistrées, des acteurs de la Blockchain (les mineurs) codent et vérifient les transactions. Le pouvoir d'écriture sur cet historique intègre est entre les mains des mineurs. Ils pourraient donc censurer des informations ou les utiliser de manière malveillante.