Blockchain Technologie

En ces temps de mondialisation du marché où la productivité, l'efficacité, et surtout la sécurité sont des aspects primordiaux de notre société, nous avons un besoin croissant de les garder à l'esprit lorsque nous considérons le développement de nouvelles technologies. De ce fait, parmi toutes les technologies émergentes, celle qui mérite le plus de retenir notre attention au niveau de la sécurité est la Blockchain. En effet cet outil permet de faciliter et de sécuriser sur plusieurs aspects les échanges tout en réduisant ses coûts.

Tout d'abord qu'est-ce que la blockchain ? C'est une base de données décentralisée qui permet le stockage et les transmissions d'information ultra sécurisée grâce à une écriture cryptée. Etant décentralisée, elle n'est pas stockée sur un serveur central mais possédée par plusieurs utilisateurs qui la stocke, ce sont les nœuds dans le réseau de blockchain. Ces nœuds peuvent vérifier entre eux la validité de la chaine. Ainsi les échanges se font sans avoir besoin d'une personne tierce ou d'avoir constamment accès à un serveur spécifique. Prenons par exemple un pêcheur, après avoir ramené une prise, il enregistre les données pertinentes telles que l'espèce, le poids, l'heure et la date de la prise, et l'envoie au marché. Il crée ainsi un bloc avec les données de l'origine du poisson. Au marché, le marchand enregistrera l'heure et la date, et l'état dès la réception. Il créera ainsi un autre bloc adjacent mais basé sur l'original. Lorsqu'il vendra le poisson, il enregistrera ensuite l'heure et la date de la vente mais aussi les informations de l'acheteur sur un 3ème bloc, basé sur le 2nd créant ainsi une chaine d'information qui matérialisera le parcours concret de la denrée. C'est donc une base de données crée et maintenue par les utilisateurs.

Au niveau de la sécurité, une fois les informations enregistrées, il n'y a aucun moyen de les altérer sans avoir à changer toute la chaine. De ce fait, dû à l'immuabilité des données stockées, les nœuds au sein d'un réseau de blockchain s'accordent sur leur état réel et leur validité. Cet accord collectif permet aussi de protéger contre les éventuelles attaques et les modifications étant donné que les informations existent en plusieurs exemplaires.

La sécurité des blockchains est assurée par une méthode cryptographique appelée hachage. Le hachage est un algorithme conçu pour recevoir une entrée de donnée de n'importe quelle taille, et renvoyer une valeur déterminée de longueur fixe. La blockchain Bitcoin© par exemple renvoie un hachage de 64 caractères. Quelle que soit la quantité de donnée entrée, le hachage sera de la même longueur. Si l'on rentre des informations différentes, le hachage résultant sera différent. Mais si on entre les mêmes informations identiques, le hachage sera toujours le même, c'est un identificateur unique de ce bloc d'information. Lorsqu'on ajoute ou modifier des informations, on va créer un 2nd bloc avec son hachage unique mais basée sur le bloc précédent. Etant donné que le hachage dépend des informations du bloc, toute modification de ces informations nécessitera de changer toute la chaine. De ce fait il est impossible de trafiquer les informations sans créer une incohérence facilement détectable. C'est ce qui contribue à l'immutabilité des informations.

Un autre aspect de la sécurité du réseau de blockchain réside dans la crypto-économie. C'est l'étude de l'économie dans l'environnement créé par les protocoles des blockchains. Cette

étude est basée sur la théorie de jeu qui analyse et prédit les comportements des acteurs signifiants dans un environnement donné. Les nœuds qui détiennent les blockchains sont, par nature des protocoles de ces dernières, incités à agir de manière honnête dans leurs propres intérêts. Les Bitcoins© par exemple, utilisent un algorithme nommé Proof of Work (preuve de Travail) qui illustre bien cet incitation a agir de manière honnête. Le minage du Bitcoin© est extrêmement coûteux et nécessite beaucoup de ressources financières beaucoup de temps. Il en résulte donc un système de comportement collectif qui récompense les nœuds honnêtes et expulse immédiatement du réseau les nœuds malveillants.

En résumé, la technologie de blockchain est parmi les plus intéressantes de notre époque étant donné les besoins grandissants de sécurisation et transfert des données. Elle est assurée par non seulement son cryptage et son immuabilité mais aussi par l'environnement qui pousse ses responsables à agir de manière honnête. De plus, les données étant stockées et dupliquées par les utilisateurs, il n'y a pas de risques d'attaques sur un serveur unique. La technologie de la blockchain est émergente et il n'y a aucun doute sur le fait qu'elle jouera ²un rôle prépondérant dans l'avenir de notre société.

SOURCES/VIDEO

https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application

https://www.journaldunet.com/economie/finance/1195520-blockchain-definition-et-application-de-la-techno-derriere-le-bitcoin-juin-2021/

https://www.ibm.com/fr-fr/topics/blockchain-security#:~:text=La%20s%C3%A9curit%C3%A9%20de%20la%20blockchain%20est%20un%20syst%C3%A8me%20complet%20de,d'attaque%20et%20de%20fraude.

https://academy.binance.com/fr/articles/what-makes-a-blockchain-secure