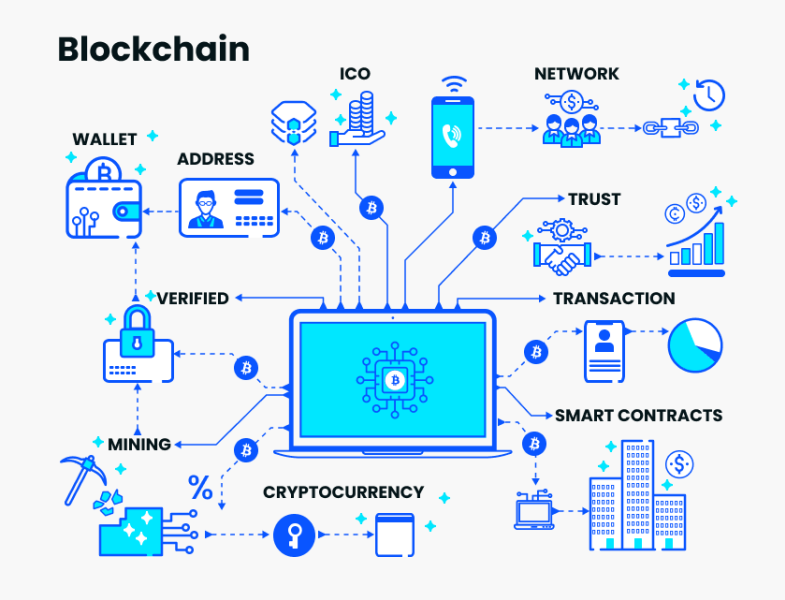
BLOCKCHAIN TECHNOLOGIE



1. Qu'est-ce que la blockchain ?

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. Chacun pourrait le consulter à volonté, mais sans pouvoir modifier son contenu une fois écrit.

2. Origines de la technologie

La Blockchain est née lors de la création du bitcoin en 2009. Le bitcoin est certifié 'non-duplicable', traçable et infalsifiable, tout ceci garanti par une technologie appelée blockchain. Les échanges et les transferts de bitcoins sont visibles par tous, il est donc impossible de créer de faux bitcoins sans que cela se voie dans le registre décentralisé. Cette technologie permet également de réaliser des paiements et d'éviter le double paiement (c'est-à-dire qu'une personne ne peut pas utiliser un même bitcoin dans deux transactions différentes).

Elle permet aussi de mettre en place un système de paiement immédiat et sans avoir besoin de passer par un tiers. Nous faisons souvent la confusion entre bitcoin et blockchain. Le bitcoin est une application particulière de la blockchain, qui repose sur une valeur monétaire : c'est une crypto-monnaie. Dans ce domaine, la blockchain technologie est utilisée pour assurer la traçabilité des transactions, puisque chaque bitcoin a un code de cryptage propre.

3. Les promesses de la technologie

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 modifie 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.

Le gain de transparence est également important et nous offre de nouvelles manières de travailler. Par défaut, l'échange de données est crypté. Toutefois, en fonction de l'implémentation de blockchain, il est possible soit de tout cacher et ne révélé que l'essentiel, soit, plus intéressant encore, de cacher une information, tout en assurant la conformité. Des mesures portant sur de la propriété intellectuelle peuvent être cryptées. Toutefois, la réponse certifiée à une exigence réglementaire peut, elle, être affichée uniquement aux personnes

autorisées. Cela ouvre des horizons inespérés et une amélioration des échanges entre acteurs aux intérêts divergents.

Nombre d'usages consistent également à s'assurer qu'une opération a bel et bien été réalisée, sans risque que l'information n'ait été altérée dans le temps par une autorité particulière, ce qui est notamment utile pour réduire les désaccords entre deux entreprises, par exemple lors de l'envoi de documents importants.

Enfin, un autre avantage de la blockchain réside dans le fait qu'il s'agit d'une technologie push, et non pull. Cela signifie que, pour qu'un contrat puisse avoir accès à une information, il faut que celle-ci soit explicitement disponible. Par opposition, par exemple, la technologie Visa ou MasterCard utilise une démarche pull, c'est-à-dire que dès l'instant où le numéro de carte est donné, toute application ou tout système peut avoir accès à toutes les données associées à la carte. Dans le cadre d'une carte de paiement, les données sont usuellement les coordonnées bancaires de la personne et la somme disponible sur le compte. Une telle démarche serait trop dangereuse avec la technologie Blockchain, puisque les données associées au contrat sont beaucoup plus nombreuses. Sans entrer dans le détail, il serait possible d'identifier une personne par recoupement de données et d'habitudes d'utilisation des contrats en question.

Les promesses sont nombreuses. Dans le futur proche, la blockchain peut avoir un impact social, économique, monétaire, législatif et même politique.

4. Le cryptage de la blockchain

La nature sécurisée de la blockchain signifie que le cryptage de la technologie blockchain est une mesure de sécurité renforcée. Le chiffrement de la chaîne de blocs empêche les informations sensibles de tomber entre de mauvaises mains et d'être utilisées à mauvais escient ou falsifiées. Parce que la nature de la blockchain réside en grande partie dans le fait que les données ne peuvent pas être modifiées ou supprimées, elles doivent donc être très protégées. Toutes les données sont vérifiées, téléchargées et sécurisées par cryptage. Le fonctionnement de la sécurité de la blockchain et du cryptage repose sur un algorithme qui doit être résolu afin de vérifier une donnée lorsqu'elle est ajoutée à une blockchain. Cela garantit que des mesures de sécurité sont prises avant même que le séjour ne soit stocké.

Le cryptage lui-même, en ce qui concerne la blockchain, réside dans les mathématiques derrière le réseau minier. Le cryptage est le processus de conversion d'informations ou de données en un code, en particulier pour empêcher tout accès non autorisé. Le chiffrement utilise des techniques plus mathématiques ainsi que des mots de passe et des clés utilisés pour déchiffrer les informations et s'appuie fortement sur un algorithme pour rendre les informations originales illisibles. Le processus lui-même convertit les informations et les données d'origine en texte brut, qui est un texte alternatif qui lui permet d'être crypté et sécurisé. Lorsqu'un utilisateur autorisé a besoin d'accéder ou de lire les données d'une blockchain, il peut les déchiffrer à l'aide d'une clé. Cela reconvertira ensuite le texte en clair en texte original auquel il sera possible d'accéder, et c'est tout à fait le cas avec la blockchain.

Le fonctionnement du cryptage est basé sur la force d'une clé de sécurité de cryptage. Dans la dernière partie du 20e siècle, les développeurs Web utilisaient un cryptage 40 bits qui était facilement percé. Au fil des ans, les couches et la sécurité du cryptage sont devenues de plus en plus compliquées pour protéger les données encore plus loin que jamais. De nombreuses entreprises, dans le passé, n'ont pas réussi à chiffrer leurs données d'une manière qui signifie qu'elles ont laissé leurs bases de données ouvertes à des informations sensibles et ont causé la chute de leur entreprise. L'utilisation de la blockchain et du cryptage qu'elle contient se concentre sur l'utilisation du cryptage et des blocs pour protéger les données de la manière la plus sécurisée possible.

Il existe plusieurs méthodes de chiffrement, c'est ce qu'on appelle la cryptographie à chiffrement symétrique et ce type de chiffrement utilise la même clé secrète pour chiffrer un message brut à la source, puis envoyer la version chiffrée au destinataire qui est déchiffrée une fois qu'il atteint sa destination. L'utilisation de chiffres et de combinaisons pour représenter les lettres de l'alphabet permet au récepteur de décrypter ce que dit n'importe quel message. Par exemple, '01' pourrait être 'A', '02' pourrait être 'B' et continuerait ainsi pour pouvoir être déchiffré. Le mot « bonjour » serait crypté sous la forme « 0805121215 » et le destinataire devrait connaître la méthodologie de cryptage pour pouvoir comprendre tout ce qui lui a été envoyé ou récupéré à partir d'une blockchain. Il existe de nombreuses variantes complexes de la méthodologie de chiffrement et présente l'inconvénient de partager largement la clé.

Une autre forme de cryptage est la cryptographie à cryptage asymétrique qui utilise deux clés différentes, l'une publique et l'autre privée. Les deux clés distinctes sont utilisées à la fois pour le chiffrement et pour déchiffrer les données. L'utilisation de la clé privée n'est connue que du propriétaire et tout ensemble de données peut être déchiffré à l'aide de la clé privée du récepteur. Ceci est considéré comme une version encore plus sécurisée de la blockchain que la cryptographie à chiffrement symétrique, car moins de personnes ont accès à la clé nécessaire pour pouvoir déchiffrer quelque chose.

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 cette incitation à 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.

5. Pourquoi utilisons-nous Blockchain ?

La blockchain, telle qu'elle est, est un moyen intéressant de stocker des données afin qu'elles puissent être utilisées de différentes manières. La nature de la blockchain elle-même signifie

que les données fournissent un moyen précis de montrer quelles transactions et actions opérationnelles ont eu lieu, étant entendu qu'elles ne peuvent pas être modifiées. C'est pourquoi de plus en plus d'entreprises optent pour la blockchain et maintiennent la sécurité de leurs données. Le terme blockchain est presque devenu un appariement avec la crypto-monnaie, mais on oublie que la blockchain était avant tout une forme de stockage de données.

Crypto-monnaie

L'utilisation de la crypto-monnaie est l'un des principaux moyens d'utilisation de la blockchain. Comme la blockchain enregistre chaque transaction via une entreprise, l'utilisation de cette forme de stockage des séjours est utilisée pour la crypto-monnaie. La crypto-monnaie telle que Bitcoin a fourni une plate-forme pour que la blockchain devienne élevée et considérée dans différents secteurs et types d'entreprises. L'utilisation de la blockchain dans la crypto-monnaie fonctionne en garantissant que la technologie est sécurisée et anonyme. La transparence de la blockchain signifie que le bitcoin peut très bien fonctionner sur une base anonyme et fournir des transactions sécurisées de son utilisation. Il s'agit d'un outil avancé de tenue de registres, ce qui en fait le logiciel transactionnel idéal à utiliser pour une crypto-monnaie ou une entreprise ou un produit transactionnel.

Vote numérique

Le vote numérique est un moyen de réduire la fraude électorale en utilisant la technologie blockchain d'une nouvelle manière. La blockchain offre la possibilité de voter numériquement et est plus efficace que les autres méthodes standard de vote numérique car elle est plus transparente et serait vraiment précise en raison de sa nature immuable. Les régulateurs seraient en mesure de voir tous les changements apportés si un type de fraude avait été tenté.

La sécurité alimentaire

La sécurité alimentaire est une autre façon dont la technologie blockchain pourrait être sous-utilisée. L'utilisation de la blockchain serait capable de détecter et de retracer votre nourriture jusqu'à la source. Cela inclurait la façon dont les aliments et les produits étaient transportés vers les zones de préparation qui auraient pu être utilisées pour créer un produit que vous pourriez consommer. Ce serait une excellente méthode et un moyen de suivre et de retracer tout virus, maladie ou contaminant d'origine alimentaire. Cela permettrait à l'industrie de la production alimentaire de rationaliser les problèmes qu'elle pourrait rencontrer avec une certaine gamme de produits et de les corriger rapidement.

Suivi de la chaîne d'approvisionnement et de la logistique

L'utilisation de la technologie blockchain avec la chaîne d'approvisionnement et la logistique permettra de rationaliser et de rendre plus précises certaines structures opérationnelles. La nature en bloc de ce type de stockage de données signifie que tout type de changement dans la logistique sera vu par toutes les personnes qui ont accès aux données et bien sûr, signifie que s'il y a des problèmes d'approvisionnement ou le côté logique d'une opération il peut alors être identifié quant à ce qui a causé ce problème et donc le résoudre plus rapidement.

Protection des droits d'auteur

Une autre façon dont la technologie blockchain peut être sous-utilisée est la protection des droits d'auteur et des redevances. Alors que l'accès des gens à Internet devient de plus en plus facile, la propriété de certains contenus a traversé l'essor. Avec la technologie blockchain, la véritable identité de qui écrit un certain contenu peut être établie. Cela garantirait qu'un artiste obtienne ce qu'il tire d'un contenu qu'il a créé et qu'il ne soit pas discrédité parce que la propriété ne peut être prouvée. La technologie Blockchain supprimerait toute ambiguïté et tout problème à ce sujet.

6. Conclusion

En résumé, le cryptage de la blockchain est extrêmement important pour maintenir la nature sécurisée des données qu'il protège. D'ailleurs, 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 un 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
- https://academy.binance.com/fr/articles/what-makes-a-blockchain-secure
- « Les Blockchain : de la théorie à la pratique, de l'idée à l'implémentation » 2e édition, les auteurs : Billal CHOULI, Frédéric GOUJON, Yves-Michel LEPORCHER, publié par *Edition ENI*