



# La blockchain

## Qu'est-ce que la blockchain ?

La **blockchain** ou chaîne de blocs en français, est une **technologie numérique permettant** aussi bien le **stockage et la transmission d'informations** que **diverses transactions sans une autorité centrale à titre de vérificateur** mais plusieurs informaticiens appelés des mineurs. Ces derniers vont, aux travers de logarythmes, **analyser l'exactitude et l'authenticité de l'action** par la prevue de travail ou Proof Of Work en anglais. Losqu'un nombre défini de mineurs ont vérifié l'action, celle-ci est validée et **enregistrée définitivement dans un bloc**.

Si la blockchain est apparu avec le Bitcoin en 2008, elle est utilisée aujourd'hui pour des transactions autres que monétaires. Cet article ne traitera volontairement pas des cryptomonnaies pour mettre en valeur les autres fonctionnalités de la blockchain.

## Fonctionnement de la blockchain

Un **bloc est une petite base de données qui contient toutes les informations d'une transaction** qui sont validées par la communauté de mineurs faisant fonctionner le réseau. Ces informations sont hachées, c'est à dire que **le texte est transformé en "valeur hash"** qui ne peut plus revenir à une forme de texte.

Chaque bloc contient un nombre défini de hash ainsi que le hash du précédent bloc (voir schema 1 page 2). Le fait de **contenir le hash du précédent bloc, relie les blocs entre eux et les rendent non modifiables** car modifier une valeur hash, modifierait toute la chaîne, les mineurs en seraient immédiatement avertis et trouveraient instantanément le contrevenant. **Chaque bloc contient les données précises des personnes qui ont validé les informations et leur rémunération mais aussi la date et l'heure exacte de chaque action dans le bloc. Le hash peut être comparé à une empreinte digitale ce qui le rend unique et garantit l'authenticité du bloc.** C'est ce système de hash qui rend la blockchain si sûr.

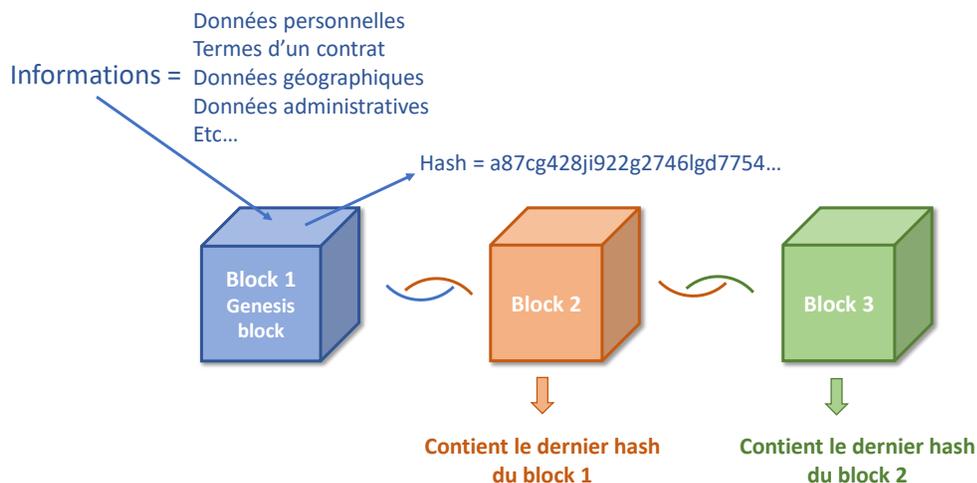
Une fois que le nombre défini de mineurs a validé les informations, le bloc est ajouté à la blockchain. Lorsque le bloc a atteint son contenu maximal, par exemple 12 MB, un autre est créé et c'est ainsi que se forme une blockchain.

### La blockchain

Qu'est-ce que la blockchain ? .....	1
Fonctionnement de la blockchain....	1
Les smart-contracts .....	2
Les registres partagés .....	3
Pour qui et pour quoi ? .....	3
Le Web décentralisé .....	4
Internet Of Things .....	5
Investir dans la blockchain ?.....	5
Conclusion.....	6

### Les points à retenir

- La blockchain sauvegarde de manière définitive et hautement sécurisée.
- L'automatisation des contrats fera gagner du temps et de l'argent.
- Le consommateur aura accès à toutes les informations concernant la chaîne d'approvisionnement.
- Les Etats pourraient stocker les données de la population sur des registres partagés.



**Schéma 1** : fonctionnement simplifié d'une blockchain : les informations sont cryptées en hash et chaque block est lié au précédent par le dernier hash. Le premier block s'appelle genesis car il ne contient pas de hash d'un autre block.

*“Le smart-contract permet la confidentialité, la limitation des erreurs, et la suppression des vérifications intermédiaires, souvent coûteuses...”*

## Les smart-contracts

Comment les blockchains peuvent-elles nous être utiles au quotidien ?

Nous avons vu précédemment que les **blockchains** garantissent une sécurité accrue en terme de gestion des données. Elles **peuvent aussi assurer la simplification et la réduction des parties prenantes** dans un grand nombre de situations.

Actuellement, lorsque nous signons un contrat, que ce soit un contrat d'assurance, de vente d'un bien immobilier ou d'une voiture, plusieurs parties prenantes sont actives pour assurer la bonne exécution du contrat. Plus il y a de parties prenantes et plus le prix de la transaction sera élevée car chacun sera rémunéré selon son implication.

Dans le cas d'un **smart-contract**, **seules les parties contractantes seront impliquées dans l'exécution des termes du contrat**. Le smart-contract fonctionne sur le principe de "si... alors" et **exécute automatiquement les termes du contrat** lorsque les conditions sont vérifiées par les mineurs.

Il **permet la confidentialité, la limitation des erreurs et la suppression des vérifications intermédiaires** qui sont souvent coûteuses. Plusieurs plateformes de blockchain permettent d'enregistrer des contrats et

leurs conditions d'exécution comme par exemple : Side Chains, NXT, Ethereum, etc.

Dans le cadre d'une assurance, par exemple, l'assuré serait automatiquement indemnisé selon les critères établis. **En cas de sinistre, il suffirait à l'assuré, de remplir un formulaire électronique** avec le détail de la situation. Le cas serait vérifié par **la blockchain qui validerait l'authenticité du fait et enclencherait le remboursement du sinistre** à l'assuré selon les termes de son contrat d'assurance.

**AXA Assurance a créé AXA Fizzi et testé pendant deux ans les smart-contracts auprès de ses assurés.** Les entreprises de transport maritime travaillent elles aussi sur cette nouvelle technologie pour gagner du temps sur les formalités administratives et de ce fait réduire le temps de livraison des marchandises (voir page 3, les cas concrets d'utilisation de la blockchain).

1 Smart-contract : contrat intelligent, identique à un contrat papier à la différence qu'il exécute automatiquement les termes conclus entre les parties contractantes

## Les registres partagés

Si les smart-contracts permettent l'exécution automatique d'ordres, **les registres partagés quant à eux, permettent le stockage d'information.**

Ce dernier est **un document informatique enregistré sur un réseau, visible et modifiable par les personnes ayant un accès à ce dernier.** Le document a la possibilité d'enregistrer toutes les modifications de façon définitive si bien que chacun peut voir l'historique du document.

Dans le cadre du registre foncier, par exemple, la Confédération met en place la digitalisation des données foncières. Aujourd'hui, **la plupart des cantons tiennent leur registre foncier sous forme électronique.** Cependant ces registres ne sont pas enregistrés sur une blockchain ce qui **les rend vulnérables à d'éventuels hackers** qui pourraient rançonner les cantons. Dans une interview du 20.02.2019, Ueli Maurer reconnaissait **"une certaine réticence dans l'administration à l'égard des nouvelles technologies"**. Mais il a tout de même invité "quelques étudiants à rédiger un mémoire sur l'utilisation de la blockchain dans l'administration". **D'ici quelques années** l'administration aura compris les avantages et la sécurité que procurent les blockchains et de **nombreuses données civiles seront enregistrées sur des registres partagés.**

**Les registres partagés peuvent être privés ou publiques.** Le registre foncier pourrait être un registre partagé publique. Ses données ne sont pas confidentielles et tout citoyen a le droit de consulter le plan d'occupation des sols.

**Un registre partagé privé** pourrait être utilisé **dans le cadre d'une entreprise dont les informations propres à la société pourraient être consultées uniquement par les employés.** Ou dans le cadre d'un hôpital, **les données des patients seraient consultables uniquement par les médecins et infirmières en charge du patient.**

Les avantages sont multiples : d'une part, **seules les personnes autorisées ont accès au registre ;** d'autre part, **les informations sont disponibles sur un seul support et sont modifiées en temps réel. Il n'y a donc pas la possibilité de croisement d'informations** et spécifiquement dans le cadre d'un hôpital, aucun risque de désinformation du personnel soignant qui n'aurait pas été informé d'un changement de dernière minute.

## Pour qui et pour quoi ?

Le principe de la blockchain permet l'enregistrement de transactions financières mais **aussi la mise en mémoire d'écritures telles que les brevets, la traçabilité des marchandises, les diplômes ou les titres de propriété.** Un des plus grands avantages de cette technologie est **la transparence de chaque action.** Tout un chacun peut avoir accès aux données enregistrées pour peu qu'il s'enregistre dans la blockchain concernée.

Certaines entreprises de **la grande distribution sont en test pour vérifier la traçabilité de leurs marchandises et mettre les informations à disposition de leurs clients.** L'entreprise Carrefour, par exemple, utilise une douzaine de blockchains pour la traçabilité de ses produits. Ses concurrents Auchan et Casino en font de même. **En temps normal pour obtenir les informations d'un produit** comme un poulet par exemple, **il faut quinze jours alors qu'avec les données sur la blockchain il ne suffit que de quelques secondes.**

Le grand public pour qui la blockchain est un mot inconnu, va bientôt pouvoir bénéficier de cette technologie pour mieux choisir ses produits.

Si aujourd'hui **le consommateur** a des possibilités restreintes pour vérifier les déclarations des marques sur la qualité de leurs produits, demain il **pourra contrôler par lui-même toute la chaîne de production et d'acheminement de son produit.** Cette technologie permettra d'éviter les nombreux scandales sanitaires auxquels les consommateurs ont dû faire face par le passé.

Si **la blockchain** semble compliquée à utiliser, elle **sera disponible sous forme d'applications pour smartphone** et les utilisateurs ne seront pas conscients qu'ils utilisent une blockchain.

## Cas concrets d'utilisation de la blockchain

Les assurances utilisent déjà la blockchain car elle simplifie la vérification des modalités d'obtention de remboursement en cas de sinistre. Par exemple, Axa Fizzy, a mis en place une assurance pour les voyageurs. Lorsque le vol a eu un retard de plus de 2 heures, le passager est indemnié automatiquement.

Les armateurs de porte-conteneurs tels que Maersk, ont mis en place une blockchain où toutes les informations telles que la position du bateau, les différends eaux internationales, les zones de conflit, sont recensées et à l'aide des données GPS la société est informée en temps réel sur l'évolution de son chargement. En cas de problème, les informations sont directement traitées et les logarythmes mettent en place les solutions nécessaires à chaque situation.

## Le Web décentralisé

Lorsque le Web a été créé, l'objectif était de rendre accessible à tous l'information, les produits et de pouvoir communiquer facilement à travers la planète entière. Aujourd'hui, ce résultat est atteint et une très large majorité de la population mondiale a accès à de l'information gratuite, des cours en ligne à des prix réduits voir gratuits et aussi à des marchandises qu'ils ne trouveraient pas près de chez eux.

Malheureusement, cette nouvelle technologie est plus ou moins sous contrôle des GAFAs (Google, Amazon, Facebook et Apple). Ces multinationales collectent toutes les données personnelles des utilisateurs pour les revendre ou faire du ciblage marketing. Lorsqu'un utilisateur Facebook poste une photo sur son compte, celle-ci devient la propriété de Facebook qui peut l'utiliser comme bon lui semble. Tim Berners-Lee, le fondateur du Web a demandé en mars 2018, via Twitter, que "toutes les données personnelles appartiennent et doivent rester sous le contrôle de son détenteur".

Avec la blockchain chaque utilisateur pourra gérer ses données et

les protéger. L'utilisateur pourra donner accès à ses informations aux personnes qu'il choisira mais il pourra aussi révoquer ces acteurs car sans la clé d'accès ils ne pourront plus utiliser ces dernières. C'est un progrès non négligeable pour le respect de la vie privée de chacun. Nous sommes tous traqués sur le net. Il suffit de voir comment les publicités s'adaptent en fonction des sites visités. Suivant les réseaux sociaux il est possible de donner un descriptif psychologique de l'utilisateur et lui envoyer des offres commerciales qui répondent à son profil. Chez les jeunes utilisateurs ces pratiques peuvent inciter à l'achat alors qu'il n'y avait pas de volonté au départ.

A l'avenir l'utilisation de la blockchain devrait redonner au consommateur un certain contrôle sur sa vie privée et ne plus être influencé par des acteurs commerciaux ultra-puissants.

*"L'utilisation de la blockchain devrait redonner au consommateur un certain contrôle sur sa vie privée..."*

**Le Web décentralisé va aussi présenter des bénéfices pour les personnes qui font commerce de leur créativité.**

Comme nous l'avons vu précédemment, l'utilisation de la blockchain permet de réduire les intermédiaires. Dans le cas de l'industrie de la musique, la blockchain pourrait résoudre les conflits entre les plateformes de téléchargement et les compositeurs. La liste des intermédiaires est longue et l'artiste perçoit au final seulement environ 1.35% du prix du téléchargement et doit souvent attendre plusieurs mois avant de recevoir l'argent.

En revanche, en utilisant une blockchain comme Ujo Music sur Ethereum par exemple, l'artiste fixe lui-même les conditions

**d'accèsibilité, il garde le contrôle sur les droits d'auteur et peut suivre les revenus des ventes en directe.**

Les utilisateurs ne sont pas fréquents pour l'instant car il y a certains freins tels que la technologie qui est adaptée à quelques acheteurs et non pour des téléchargements de masse ; les dispositions légales car pour l'instant aucun texte officiel ne régit la blockchain ; et l'aspect compliqué des blockchain pour les utilisateurs dont une grande majorité ignorent l'existence même de telles infrastructures.

## Internet Of Things

L'utilisation des blockchains se fera principalement au travers des smartphones qui permettent de contrôler une grande partie du quotidien.

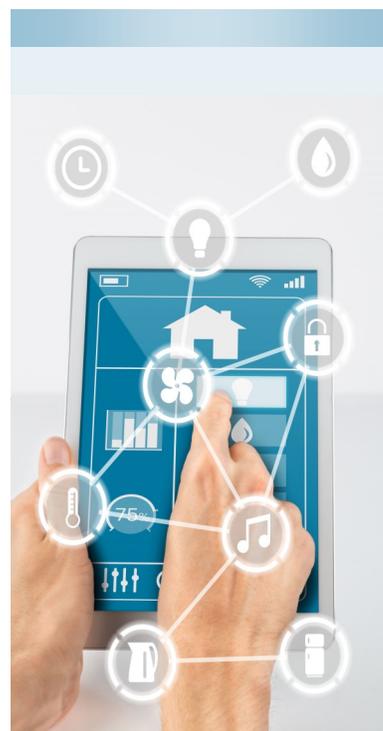
L'Internet des objets ou IdO, représente tous les objets qui se connectent aux smartphones ou à des ordinateurs. Il s'agit entre autres de la domotique qui gère les intérieurs des lieux de vie mais aussi au domaine de l'e-santé, des automobiles, des jouets pour les enfants, etc.

Dans le futur, des milliards d'appareils vont se connecter entre eux et des milliards de données personnelles vont être échangées.

Si ces objets connectés rendent de précieux services et facilitent la vie de leurs utilisateurs,

ils les **vulnérabilisent en transmettant des données sensibles**. Par exemple, lorsque nous démarrons des appareils électro-ménagers à distance, des données informatiques sont envoyées par le réseau internet. Suivant qui intercepte ces informations, elles pourraient être utilisées pour vendre de l'information privée à des fins marketing mais plus dangereusement, elles pourraient renseigner sur notre présence ou non à notre domicile.

Pouvoir enregistrer des données personnelles sur une blockchain et les rendre accessibles par une clé cryptée permettra de protéger la vie privée des utilisateurs d'IdO.



*“Pouvoir enregistrer des données personnelles sur une blockchain et les rendre accessibles par une clé cryptée permettra de protéger la vie privée des utilisateurs d'IdO.”*

## Comment investir dans la blockchain ?

Pour les investisseurs, la blockchain est une technologie plutôt floue que beaucoup disent très prometteuse en termes de ROI mais qui en réalité présente une volatilité démesurée. Si la volatilité est appréciée pour les gains qui peuvent s'en dégager, les fluctuations brutales sont réhabilitées, d'autant plus si l'investisseur ne connaît pas très bien le produit.

Comment pouvoir bénéficier des promesses d'investissement sur une technologie naissante sans prendre de risques inconsidérés ? Comme il est mentionné au début de l'article, nous n'allons pas encourager l'investissement dans les crypto-monnaies car leurs indices sont trop aléatoires.

Les opportunités d'investissement se trouveront plutôt du côté du private equity qui va devenir accessible à des investisseurs intéressés par l'art ou l'immobilier par exemple, et dont les parts de capitaux seront plus abordables.

Les financements de projets vont se faire aux travers de plateformes blockchains qui accueilleront des montants d'investissements variés car les processus de capitalisation seront simplifiés. C'est le même principe que les plateformes de crowdfunding qui permettent à de tous petits investisseurs de financer un projet à hauteur de leurs moyens financiers.

La galerie d'art Dadiani s'est associée à la plateforme Maecenas pour vendre un tableau d'Andy Warhol. Plus de 800 enchérisseurs ont participé à la vente pour un montant de 1,7 million de dollars. Chaque acheteur a reçu un certificat numérique du montant de token investi. Cette nouvelle forme d'investissement va ouvrir de nouvelles perspectives pour le private equity et pourquoi pas un nouvel essor économique car de nombreux projets pourront être financés sans attendre un hypothétique prêt des banques.

## Conclusion

Depuis la révolution industrielle au XIX siècle notre société a connu une profonde métamorphose et le quotidien des êtres humains a considérablement changé.

**Le Web a été inventé en 1989 en Suisse au CERN. Et c'est en 1993 que le premier navigateur Web a été publié alors que le Web ne comptait que 200 sites internet** à travers le monde. Au tout début des années 2000 très peu de personnes faisaient des recherches sur le Web et encore moins avaient une connexion internet à la maison et quasiment personne ne pouvait imaginer que **20 ans plus tard, la très grande majorité de la population serait connectée** et aurait la possibilité de commander et payer une pizza sur un téléphone portable qui se rapprocherait plus d'un ordinateur de poche tant la fonctionnalité de téléphonie n'est quasi plus utilisée.

**Il en va de même pour la blockchain.** C'est une technologie dont le fonctionnement et ses applications dans notre quotidien sont difficiles à imaginer aujourd'hui mais **d'ici quelques années nous ne pourrions plus fonctionner sans elle car elle sera adaptée au**

**mode de vie de notre société.**

Les échanges commerciaux entre les nations vont continuer de se développer, **les consommateurs seront de plus en plus concernés par leur implication dans les circuits d'approvisionnement et l'impact sur l'environnement.** La complexité administrative ne cessera de croître et seule **une technologie blockchain pourra nous aider dans notre quotidien**, qu'il soit privé ou professionnel, **tout comme le Web nous rend service aujourd'hui.**

*“...d'ici quelques années nous ne pourrions plus fonctionner sans la blockchain car elle sera adaptée au mode de vie de notre société.”*

