

Qu'est-ce qu'une crypto-monnaie (définition) ? Qu'est-ce que la blockchain ? Quel est l'intérêt des crypto-monnaies ? Comment et pourquoi créer une crypto-monnaie ? Légalité de la blockchain et des cryptos ?

La blockchain c'est quoi, comment ça marche ?

La **blockchain** signifie en français chaîne de blocs, c'est une base de données transparente, sécurisée et décentralisée qui utilise la cryptologie (cryptage des transactions). Cette base de données distribuée est protégée contre la falsification et possède tous les échanges effectués entre ses utilisateurs depuis sa création. Partagée par ses différents utilisateurs et sans intermédiaire chacun vérifie la validité de la chaîne. Une blockchain peut être publique, privée ou bien les deux et peut être comparable à un grand livre comptable public anonyme et infalsifiable. Plusieurs types de technologie et de consensus prédominent au sein d'une blockchain :

- **POW** (proof of work) : preuve de travail. Utilise le minage (puissance de calcul des processeurs et cartes graphiques d'ordinateur) pour valider les transactions.
- **POS** (proof of stack) : preuve de participation ou d'enjeu. Utilise une certaine quantité de crypto-monnaie pour valider les transactions.

Certaines variantes peuvent exister en fonction de la crypto-monnaie. Ce qui différencie principalement POW de POS est que POW demande beaucoup plus de ressource que POS notamment au fur et à mesure que la crypto-monnaie se développe et que de nouveaux blocs sont créés. En effet, le hachage devient de plus en plus complexe dans le temps si le nombre de transaction augmente. Cela consomme donc évidemment beaucoup plus d'énergie.

Les deux principaux algorithmes de hachage utilisés sont :

- **SHA-256**
- **Scrypt**

Les blockchains pourraient remplacer la plupart des « tiers de confiance » centralisés comme pour les métiers de banques, notaires, assurances, etc.

L'utilisation de la blockchain peut se distinguer en trois catégories :

- Applications de transfert d'actifs (monétaire, titres, votes, actions, obligations, etc.).
- Applications de la blockchain en tant que registre (traçabilité des produits et des actifs).
- Smart contracts (programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans intervention humaine une fois démarrés).

Le processus de transaction sur la blockchain varie de **quelques secondes à quelques minutes** en fonction de la blockchain utilisée ce qui est beaucoup plus rapide qu'un virement SEPA.

Beaucoup de crypto-monnaie utilise le principe du "wallet" c'est à dire un portefeuille numérique qui est proposé par la blockchain en question depuis leur propre site Internet généralement. Ce portefeuille est souvent décliné pour les différents systèmes d'exploitation : Windows, Mac, Linux. Une fois l'application installée sur votre système d'exploitation une clé publique et privée est automatiquement générée sous forme d'un fichier wallet.dat (sauvegardez bien ce fichier car si vous le perdez vous aurez alors tout perdu). Une fois que toute la blockchain sera téléchargée sur votre disque dur, votre portefeuille sera synchronisé et vous pourrez dès lors effectuer des transactions depuis ce même portefeuille (émission/réception). Pensez à le verrouiller si vous ne l'utilisez pas.

Nous pouvons donc dire que posséder des unités (jetons) d'une crypto-monnaie est comme être actionnaire de celle-ci. Il est toujours possible de revendre ou d'échanger les unités stockées dans votre portefeuille en passant par des plateformes en ligne sécurisées et spécialisées qui convertiront vos unités soit vers une autre crypto-monnaie désirée soit directement en euro via un virement SEPA (sauf si la crypto-monnaie disparaît des radars du jour au lendemain car il n'y a aucune garantie). Le processus d'achat fonctionne de la même manière. **A noter que très peu de crypto-monnaies permettent la conversion en monnaie FIAT (€, \$, etc.), Bitcoin le permet.**

IMPORTANT : Pensez à **sécuriser vos cryptos-actifs** car ceux-ci sont vulnérables, notamment sur les plateformes d'échanges (piratage informatique de [Mt. Gox](#)). Vous pouvez par exemple sécuriser vos crypto-monnaies en utilisant un [Ledger Nano S](#) (portefeuille numérique) dont un **certain nombre de crypto-monnaies** sont prises en charge. Sinon, vous pouvez détenir vos propres **clés publiques & privés** mais attention à ne pas les perdre car sans celles-ci vous ne pourrez plus réaliser de transactions et vos fonds seront bloqués à tout jamais !

Quand, pourquoi et comment est apparue la blockchain ?

La blockchain est apparue avec la création de **Bitcoin** (*système monétaire autonome limité à 21 millions d'unités*), la première crypto-monnaie **créé en 2008** dont son auteur "*Satoshi Nakamoto*" n'a toujours pas été identifié.

Elle fut lancée en 2008 suite la crise financière et annoncée comme une alternative au système bancaire classique et centralisé.

Quel cadre juridique pour la blockchain ? Est-ce légal ?

Bien que la blockchain se soit démocratiser au cours de ses dernières années, aucun cadre juridique n'existe autour de celle-ci. Cela ne veut pas dire pour autant que son utilisation et la participation à l'environnement blockchain en est interdite car elle représente pour de très nombreux acteurs un avenir certain. Avenir technologique déjà présent et utilisé par des centaines entreprises et startups. Cette technologie commence à s'intégrer dans les systèmes informatiques, bancaires et d'information. Ceci est comparable à l'arrivée d'Internet dans les années 1990 via le "World Wide Web".

Certains pays et états commencent d'ailleurs a accepter l'utilisation de la crypto-monnaie ou comme le Bitcoin en lui donnant un **cadre légal**. *Ce phénomène devrait s'intensifier dans les années futures.*

Je vous invite à lire ce rapport sur l'[encadrement des monnaies virtuelles](#).

Nous entendons aujourd'hui parler de plus en plus de crypto-actifs et non de crypto-monnaies preuve que le marché s'oriente vers la reconnaissance du jeton ou token comme un actif financier.

Ce sujet est d'ailleurs actuellement traité au **Sommet du G20** à Buenos Aires en Argentine et en pourparler à l'assemblée nationale via une mission d'information. Le rapporteur de la mission d'information est le député parisien [Pierre Person](#).

Puis-je alors créer un nouveau concept de blockchain ?

Oui bien entendu, cependant ce n'est pas si facile. Actuellement quelques milliers de personnes travaillent dans l'univers de la blockchain ; cela peut paraître beaucoup mais sur l'ensemble de la planète ce n'est pas si énorme. C'est aussi l'affaire de spécialistes, de cryptologues ayant des connaissances très spécifiques et très pointues en terme de cryptologie.

Si vous estimez avoir les connaissances nécessaires ainsi qu'un environnement adéquat vous pouvez tenter l'aventure en créant votre société, start-up ou lancer une **ICO (levée de fonds réalisé principalement en crypto-monnaies [BTC](#) - [ETH](#))**.

*Cependant, pour l'heure, le marché n'étant pas régulé, de nombreux risques vous attendent. Le parcours de création, le développement de votre société peut s'avérer très complexe et risqué. Nous entendons tout et son contraire même de la part des professionnels et experts du milieu donc **VIGILANCE oblige !***

Quels acteurs sur le marché français ?

A ce jour, nous comptons quelques acteurs français actifs dans l'univers de la blockchain comme :

- **iExec** (jeton [RLC](#)) un cloud décentralisé basé sur la blockchain
- **Ark** (jeton [ARK](#)) une plateforme de solutions blockchain tout-en-un
- **Tezos** (jeton [XTZ](#)) une nouvelle plateforme pour les contrats intelligents et les applications décentralisées, concurrent d'[Ethereum](#) (jeton [ETH](#))

Quelle conclusion ?

Le monde de la cryptologie, de la blockchain (crypto-monnaies, crypto-actifs) est un secteur encore de niche ou de belles opportunités sont à prévoir. Son utilisation et sa compréhension se font rares en Europe comparé aux Etats-Unis et au Japon qui ont une bonne longueur d'avance. Il faudra donc suivre attentivement ce que cet environnement technologique blockchain nous réserve tant d'un point de vue juridique (politique, législatif) que technologique. Un nouvel horizon se dessine et peut être que certaines start-up et entreprises françaises en seront le fer de lance.

Mais... peut être et sûrement que certaines cryptos-monnaies disparaîtrons ! Cependant la technologie elle même ne devrait pas tomber dans les oubliettes et les meilleurs projets continueront à se développer !

À l'heure actuelle le marché de la crypto-monnaie pèse plus de **200 milliards d'euros** avec plus **2000 crypto-monnaies** identifiées selon [coinmarketcap](#), la plateforme de capitalisation des crypto-monnaies avec leurs cours. Les crypto-monnaies alternatives au Bitcoin sont appelées "**altcoins**" et représentent 60% de la capitalisation totale du marché soit 40% pour Bitcoin. Un Bitcoin aujourd'hui s'approche des 6000 euros alors qu'il ne représentait que quelques centimes à son lancement. De nouveaux millionnaires sont nés sur ce nouveau marché car ils ont osés l'aventure blockchain à ses tout premiers balbutiements.

De nouvelles crypto-monnaies naissent fréquemment avec leurs technologies et améliorent ainsi la

technologie blockchain dans son ensemble.

A noter : Le marché des crypto-monnaies, crypto-actifs est très spéculatif dû principalement au fait qu'il ne soit pas régulé. C'est aussi un marché qui ne dort jamais car on peut trader sur différents échanges comme [binance.com](https://www.binance.com) 24h/24, 7j/7 et dans le monde entier.

**Et vous, quel avenir pensez-vous de la blockchain notamment en France et en Europe ?
Pensez-vous que la France peut en être le fer de lance ? Avez-vous envie de tenter
l'aventure ?**

N'hésitez ci-dessous pas à partager vos avis et expériences sur ce sujet passionnant.