
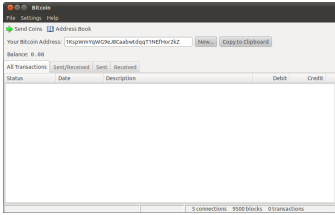


# Bitcoin

Bitcoin	
	
	
Bitcoin sur Ubuntu	
<b>Développeurs</b>	Satoshi Nakamoto, Gavin Andresen
<b>Première version</b>	4 février 2009
<b>Dernière version</b>	0.7.1 (17 octobre 2012)
<b>Écrit en</b>	C++
<b>Environnements</b>	Windows, Linux, Mac OSX
<b>Langues</b>	Anglais, Français, Allemand, Espagnol, Néerlandais, Portugais, Italien, Russe
<b>Type</b>	Monnaie électronique
<b>Licence</b>	MIT License
<b>Site web</b>	bitcoin.org <sup>[1]</sup>

**Bitcoin**<sup>[2]</sup> est une monnaie électronique décentralisée conçue en 2009 par le pseudonyme Satoshi Nakamoto. Son utilisation passe par un protocole informatique implémenté par un logiciel libre portant le même nom, écrit en C++ et publié sous licence MIT.

Fonctionnant de façon entièrement distribuée, la gestion de la monnaie est répartie sur tous les nœuds du réseau, de façon à ce que le bon fonctionnement du système dépende non pas de l'intégrité ou de la compétence d'un émetteur central, mais uniquement de la robustesse des procédés cryptographiques employés.

Le symbole monétaire, non officiel, est ₿ ou ₮<sup>[3]</sup>, et le sigle correspondant est BTC.

Le projet Bitcoin est un des systèmes informatique parmi les plus puissants au monde<sup>[4]</sup>.

## Origine du concept

Bitcoin est une amélioration significative d'un concept imaginé par Wei Dai, appelé b-money dans un document d'avril 1999<sup>[5]</sup> et du concept "bitgold" décrit en 2005 par Nick Szabo. Bitcoin résout en particulier le problème crucial du modèle de confiance : les serveurs "honnêtes" votent avec leur puissance de calcul pour déterminer la chaîne de transaction légitime (portant la plus grande preuve de calcul). Dans b-money, les serveurs étaient supposés verser un dépôt de garantie dans un mécanisme peu explicite. L'idée d'utiliser une chaîne de preuves de calcul fut avancée dans le projet bitgold bien que Nick Szabo ne proposait d'utiliser qu'une majorité d'adresses pour établir la légitimité d'une chaîne de transactions, ce qui laissait entier le problème de contrôler le nombre des adresses.

## Principes techniques

Les participants forment un réseau informatique communiquant à travers Internet. Lorsqu'un ordinateur cherche à se connecter au réseau, sa première tâche consiste à trouver d'autres ordinateurs actuellement connectés. Dans les premières versions du logiciel, cette étape était réalisée en se connectant à un réseau IRC. Par la suite, cette méthode est devenue uniquement une solution de rechange, car la méthode privilégiée consiste désormais (en 2012) à utiliser une liste d'adresses IP statiques écrites directement dans le code source du logiciel.

Une fois l'ordinateur connecté, la deuxième étape consiste à télécharger la base de données de toutes les transactions effectuées depuis le lancement du projet. Une transaction consiste en un transfert d'un certain montant de bitcoins d'un certain compte à un autre. Un compte est identifié par une *adresse bitcoin*, qui en simplifiant est l'analogue d'un numéro de compte en banque. Pour être valide, chaque transaction doit être signée, au sens cryptographique du terme. Pour cela, la cryptographie asymétrique est utilisée, ce qui est rendu possible par le fait qu'une adresse bitcoin est aussi l'empreinte cryptographique d'une clef publique. Une transaction prend en entrée la référence d'une transaction précédente qui justifie que les fonds nécessaires sont bien possédés, et présente en sortie une ou plusieurs adresses bitcoins avec les montants attribués correspondants. Une transaction épuise toujours entièrement le montant en entrée, car cela simplifie les calculs de balance totale.

Une fois la base de données téléchargée, le logiciel fonctionne en mode nominal : il communique alors continuellement avec les autres ordinateurs du réseau, avec lesquels il échange des informations sur les adresses IP du réseau et sur les nouvelles transactions apparaissant au fur et à mesure que des utilisateurs s'échangent des bitcoins. Quand une nouvelle transaction est reçue, elle n'est pas considérée comme valide tout de suite. Elle doit d'abord être incorporée dans ce qu'on appelle un bloc de transactions. Il s'agit d'un regroupement de transactions récentes qui attend pour être validé de subir un traitement cryptographique appelé preuve de travail. Effectuer cette preuve de travail requiert du temps de calcul, et en général un seul ordinateur du réseau y parvient dans un intervalle de temps d'environ dix minutes. La difficulté est d'ailleurs régulièrement adaptée pour maintenir cet intervalle.

Cette idée de regrouper les transactions en blocs et de ne valider ces blocs qu'à l'issue d'une preuve de calcul est le point le plus original du système. C'est la solution au problème du double paiement, car les différences dans la connaissance des transactions sur le réseau, différences inévitables ne serait-ce qu'à cause des latences de communication, sont alors arbitrées par ce processus de détermination du bloc, qui joue le rôle d'un tirage au sort. Lorsqu'un ordinateur remporte ce tirage au sort, il reçoit des bitcoins ne provenant pas d'une transaction précédente. Cette attribution de bitcoins permet l'introduction initiale de bitcoins dans la base, et prend la forme d'une transaction spéciale située en tête de bloc. Selon l'ordinalité du bloc, le montant de bitcoins attribué est variable et diminue géométriquement de telle sorte que la somme totale de bitcoins en circulation ne pourra jamais excéder vingt et un millions de bitcoins.

Pour transmettre des bitcoins, chaque ordinateur doit signer une transaction faisant référence en entrée à une transaction précédente dont le montant de sortie est suffisant. La clef privée doit correspondre à la clef publique avec laquelle a été créée l'adresse bitcoin en sortie de la transaction précédente. L'ordinateur doit donc stocker toutes ces clefs privées localement, sans bien sûr partager ces informations. Le fichier correspondant s'appelle *wallet.dat*, et c'est ce fichier qui doit être conservé et sauvegardé par l'utilisateur, et de façon confidentielle. La perte de ce portefeuille électronique entraînerait de façon irréversible la disparition des bitcoins correspondant, qui resteraient éternellement dans la base sans jamais pouvoir changer d'adresse.

La cryptographie est utilisée pour permettre le tirage au sort décrit plus haut, ainsi que la signature des transactions. A aucun moment le système ne chiffre des données transmises sur le réseau. Toutes les transactions sont *en clair*, et leur anonymat n'est protégé que par le fait que le logiciel n'utilise aucune données personnelles sur l'utilisateur. Un utilisateur ne peut trahir son identité que s'il le fait volontairement, si son adresse IP est traçable, où éventuellement à la suite d'une méticuleuse et complexe étude statistique sur la base de données des transactions.

## Technologies employées

- bitcoin utilise le concept de preuve de travail, initialement imaginé pour résoudre le problème du spam, et implémenté par exemple dans le système Hashcash ;
- Les algorithmes de hashage sont SHA-256 et RIPEMD-160. Un double hash en SHA-256 est utilisé pour obtenir le hash des blocs et donc la preuve de travail, tandis qu'un SHA-256 suivi d'un RIPEMD-160 est utilisé pour construire les adresses bitcoins ;
- Les signatures de transactions sont effectuées en utilisant la cryptographie à courbes elliptiques, dite ECDSA. En l'occurrence, la courbe employée est *secp256k1* ;
- Le logiciel originel écrit par Nakamoto utilise Berkeley DB pour la gestion de ses bases de données ;
- Au sein d'un bloc, les transactions sont stockées sous la forme d'un arbre de Merkle ;
- La validation des transactions fait appel à un langage de script interne conçu par Nakamoto. Ce langage, volontairement minimaliste et non Turing-complet, doit permettre au logiciel de s'adapter aisément à des évolutions ultérieures et permettre des fonctionnalités avancées comme les Smart contract (en).

## Format d'une adresse bitcoin

Une adresse bitcoin est fabriquée à partir du RIPEMD-160 du SHA-256 de la clef publique que l'adresse identifie. Il existe donc un maximum de  $2^{160}$  adresses bitcoins possibles, soit environ  $10^{48}$  (à titre de comparaison il y a environ  $10^{47}$  molécules d'eau sur Terre<sup>[6]</sup>). Une adresse bitcoin possède un préfixe identifiant le numéro de version (0 par défaut) et une somme de contrôle de quatre octets. En tout, une adresse bitcoin occupe donc 25 octets.

Une adresse est représentée au format ASCII grâce à un encodage dédié sur 58 caractères alphanumériques: les chiffres et les lettres majuscules et minuscules, à l'exception des lettres et chiffres l, I, 0 et O, que Nakamoto a exclues car ces lettres se ressemblent dans certaines fontes.

Voici un exemple d'adresse bitcoin (on montre ici volontairement une adresse invalide, c'est-à-dire avec une mauvaise somme de contrôle) : 175tWpb8K1S7mH4Zx6rewF9wQrcPv245W

Une adresse bitcoin est la seule information nécessaire pour recevoir des bitcoins. Il n'est pas nécessaire de faire tourner le logiciel bitcoin pour la réception, il suffit de communiquer une adresse. Seule la personne qui paie communique la transaction complète au reste du réseau à travers le logiciel client.

## Principes économiques

### Transaction

Une transaction correspond à l'envoi d'une certaine somme d'une adresse vers une autre adresse. Une transaction est prise en compte par le système au bout de 10 minutes environ.

### Frais

Chaque transaction peut être gratuite ou bien accompagnée de frais. On retrouve le même fonctionnement dans les monnaies nationales : par exemple les paiements en espèces sont gratuits alors que les paiements par carte bleue sont taxés par les banques. Dans le cas des bitcoins, c'est l'émetteur de la transaction qui décide du montant éventuel des frais payés. Ces frais permettent à la transaction d'être prise en compte prioritairement par le système.

## Sous-unités

Actuellement chaque bitcoin est divisible jusqu'à la 8ème décimale, c'est à dire en sous-unités de 0.00000001 bitcoin. Il est possible de parler de milibitcoins ou de microbitcoins pour représenter des sommes inférieures au bitcoin.

## Bourses d'échanges

Les bitcoins peuvent être échangés contre d'autres monnaies (USD, EUR, ...) sur différentes bourses d'échanges sur internet. Il n'est pas possible actuellement de payer par des moyens grands public comme la carte bleue ou le système Paypal. Par contre il est possible d'accéder aux bourses d'échange par virement bancaire.

## Taux de change

En date du 11 novembre 2012 :

- Un bitcoin peut être acheté pour 8,55 €<sup>[7]</sup>, soit 10,84 \$US<sup>[8],[9]</sup>,
- Un total de 10,375 millions de bitcoins sont en circulation,
- Cela donne une valorisation totale d'environ 90 M d'€.



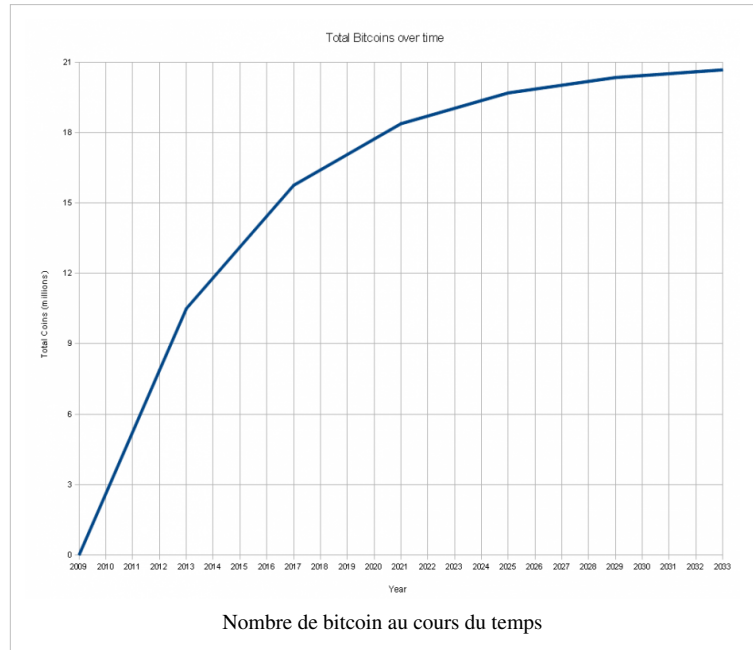
Date	cours en euros <sup>[10][11]</sup>
7 février 2011	4,15 €
9 août 2011	5,36 €
2 octobre 2011	3,76 €
25 novembre 2011	1,83 €
10 décembre 2011	2,3 €
25 janvier 2012	4,34 €
3 août 2012	8,51 €
15 août 2012	10,84 €
22 octobre 2012	8,94 €

Un pic a eu lieu en juin 2011 où les bitcoins s'échangeaient pour plus de 30 USD.

Le taux de change n'est qu'un indicateur de la valeur du bitcoin. Il faut aussi prendre en compte ses différentes utilisations, comme par exemple l'épargne, la spéculation boursière, l'envoi d'argent à l'étranger, l'achat de biens et de services<sup>[12],[13]</sup>, etc.

## Distribution

La monnaie bitcoin n'est pas contrôlée par une autorité centrale, comme par exemple la banque centrale pour une monnaie nationale, mais par le logiciel pair à pair Bitcoin écrit par la communauté. Le logiciel prévoit l'émission de monnaie d'après une règle mathématique (de type série géométrique). Pour simplifier : 50 BTC sont émis toutes les 10 minutes pendant les 4 premières années du système. Ensuite, le montant est divisé par 2 pour passer à 25 BTC pendant les 4 années suivantes et ainsi de suite, jusqu'à atteindre la sous unité maximum et donc le nombre maximum de bitcoin émis au delà de 2033. On obtiendra donc un maximum de 21 millions de bitcoins émis au total. Il faut noter que les 10 minutes et 4 ans sont des valeurs approximatives qui dépendent d'autres facteurs.



## Théorie économique

Toutes les monnaies nationales connaissent une inflation, faible à forte selon les politiques menées par leur banque centrale. À l'inverse, la monnaie Bitcoin va finir par connaître la déflation, car la quantité de bitcoins générée est prévue à l'avance dans le logiciel et le nombre maximum ne dépassera pas 21 millions d'unités. De plus les bitcoins perdus par les utilisateurs ne seront jamais remplacés. C'est pourquoi le projet bitcoin est vu par la communauté comme une expérience originale en termes économiques, constituant une sorte de mise à l'épreuve de l'école autrichienne d'économie. Son succès ou son échec est difficile à prévoir.

## Risques et critiques

Dès l'origine, bitcoin a fait l'objet de critiques souvent véhémentes, à l'encontre d'aspects aussi bien techniques qu'économiques ou même politiques. Nombre de ces critiques ne sont pas propres à bitcoin, et pourraient être adressées à d'autres systèmes de paiement ayant des caractéristiques similaires (anonymat pour le cash, montant fixe pour l'or, etc..)

Les risques les plus souvent mentionnés pour les utilisateurs de Bitcoin sont les suivants :

- Risque lié à l'irréversibilité des transactions, essentiellement liée à l'anonymat même relatif du système, qu'on retrouve aussi avec toute forme de paiement en espèce ;
- Risques liés au logiciel et à l'environnement informatique (fichier wallet mal protégé, bande passante requise pour charger les blocs, possibilité d'attaques de déni de service...). Ce risque se retrouve avec toute forme de paiement électronique ou même avec les cartes bancaires dont une simple photocopie peut parfois être utilisée par les malfaiteurs ;
- Risque de change par rapport aux monnaies fiduciaires. Ce risque est lié au fait que bitcoin est une monnaie à part entière, particulièrement jeune et donc sujette à de fortes variations de son cours ;
- Risque technologique: il est souvent avancé que le réseau bitcoin ne pourrait pas monter en puissance pour traiter toutes les transactions en mode pair-à-pair. La croissance exponentielle de la taille de la base de données deviendrait ingérable. Cependant, il faut noter que, pour économiser de l'espace disque, cette base est stockée à l'aide d'un arbre de Merkle qui pourra être "élagué" au fil du temps. D'autre part, si les nœuds du réseau peinent à

suivre l'augmentation de la taille de la base de données, des "super-nœuds" bitcoin sont déjà envisagés, comparables aux processeurs de paiement qu'on trouve sur les réseaux bancaires actuels. On peut noter aussi que, la loi de Moore aidant, et la population mondiale n'étant finalement que de quelques milliards d'individus, la totalité des activités économiques humaines, même à l'échelle mondiale, est probablement à la portée de calcul et de stockage mémoire des ordinateurs personnels modernes.

D'autres critiques<sup>[14]</sup> portent sur le concept même d'une telle monnaie, en comparaison avec les monnaies étatiques ou l'étalon-or :

- La création de la monnaie consomme du temps machine<sup>[réf. nécessaire]</sup> (alors que la monnaie étatique peut être créée à partir de rien). Il est alors souvent rétorqué que ce temps machine assure la sécurité du traitement des transactions (les réseaux bancaires consomment aussi du temps machine pour traiter les transactions, ainsi que de l'énergie pour la construction et le fonctionnement de l'infrastructure logistique). Par ailleurs, la difficulté de traitement des blocs n'a rien de figé: elle s'adapte au nombre de personnes cherchant à obtenir des bitcoins par cette méthode. Elle résulte donc d'un choix volontaire des participants, et non d'une donnée extrinsèque à laquelle ils devraient se plier ;
- Le concept favorise les premiers créateurs de monnaie (« *early adopters* ») : cette critique, allant jusqu'à assimiler bitcoin à un schéma de Ponzi<sup>[15]</sup>, peut être adressée à toute matière première rare qui serait utilisée comme moyen d'échange comme l'or ou à toute innovation technologique qui ne serait pas adoptée universellement dès son introduction ;

## Évènements notables

- 3 janvier 2009 : création du bloc *genesis*<sup>[16]</sup>
- Février 2009 : Annonce sur le site P2Pfoundation et publication d'une première version du logiciel
- 12 décembre 2010 : Dernier message posté par Nakamoto sur le principal forum
- 9 février 2011 : Le bitcoin atteint la parité avec le dollar.<sup>[17]</sup>
- Février 2011 : Lancement de Silk road
- Utilisation de cartes graphiques (GPU) pour miner les bitcoins<sup>[Quand ?]</sup>
- Juin 2011 : Le taux de change dépasse les 30 USD, et redescend sous les 4 USD en décembre
- Utilisation de cartes FPGA pour miner les bitcoins<sup>[Quand ?]</sup>
- 27 septembre 2012 : Création de la Fondation Bitcoin<sup>[18]</sup>
- 16 novembre 2012 : Wordpress accepte les bitcoins pour ses services payants<sup>[19]</sup>
- 28 novembre 2012 : Division de la récompense de minage, de 50 à 25 BTC

## Liens externes

- Site officiel du projet Bitcoin, en anglais<sup>[20]</sup>
- Le document initial publié par Satoshi Nakamoto, en anglais<sup>[21]</sup>
- Partie française du forum officiel Bitcoin, en français<sup>[22]</sup>
- e-ducate.fr - blog en français<sup>[23]</sup>
- bitcoin.fr - blog en français<sup>[24]</sup>
- blockexplorer.com<sup>[25]</sup>, site permettant de consulter la base de données en ligne
- Vidéo de présentation à La Cantine<sup>[26]</sup>
- Article paru<sup>[27]</sup> dans linuxfr.org, autres articles<sup>[28]</sup>
- Vidéo de la conférence sur bitcoin aux Rencontres Mondiales du Logiciel Libre 2012<sup>[29]</sup>
- Article d'introduction au bitcoin<sup>[30]</sup>, sur le Framablog par le blogueur Lionel Dricot, auteur de plusieurs articles de promotion du bitcoin<sup>[31]</sup>
- Avec Bitcoin, payer et vendre sans les banques<sup>[32]</sup>, article explicatif sur le site *Lemonde.fr*, daté du 1er décembre 2012.

- (en) *Virtual currency schemes* <sup>[33]</sup>, rapport de la banque centrale européenne, au sujet des monnaies virtuelles, se concentrant bitcoin et sur les Linden dollars, monnaie utilisée sur le jeu second life.

## Notes et références

- [1] <http://www.bitcoin.org/>
- [2] Une francisation possible de la prononciation est /bitkwɛ/, comme dans les mots bit et coin
- [3] unicode caractère 0x0243
- [4] (en) ([http://en.wikipedia.org/wiki/List\\_of\\_distributed\\_computing\\_projects](http://en.wikipedia.org/wiki/List_of_distributed_computing_projects)) Liste des projets de calcul distribué
- [5] (en) b-money (<http://weidai.com/bmoney.txt>) sur le site de Weidai, le 19 avril 1999
- [6] Voir l'article Ordre de grandeur (nombres)
- [7] Site officiel (<http://www.bitcoin.fr>).
- [8] Mt Gox - Bitcoin Exchange (<http://mtgox.com>)
- [9] The Bitcoin 4 Cash Service (<http://www.bitcoin4cash.com>)
- [10] Évolution de la valeur du bitcoin en € (<https://docs.google.com/spreadsheets/ccc?key=0Av8Pq5-AyB1wdENrTFNWZHZ3OXAZeGICR2JCbl9wOWc#gid=0>)
- [11] Données financières et techniques du réseau Bitcoin (<http://bitcoincharts.com/>)
- [12] Services and Goods (<http://fr.bitcoin.it/wiki/Trade>)
- [13] Que faire avec mes bitcoins (<http://www.bitcoin.fr/post/2010/12/30/Que-faire-avec-mes-bitcoins>)
- [14] Bitcoin va-t-il sauver l'humanité ? (<http://www.madore.org/~david/weblog/2011-05.html#d.2011-05-16.1883>), Is the cryptocurrency Bitcoin a good idea? (<http://www.quora.com/Bitcoin/Is-the-cryptocurrency-Bitcoin-a-good-idea>)
- [15] Bitcoin: de la révolution monétaire au Ponzi 2.0 (<http://owni.fr/2011/06/15/bitcoin-revolution-monetaire-ponzi/>), *Owni.fr*, juin 2011
- [16] On sait que le bloc n'a pas été créé avant cette date car il contient le titre de la une d'un quotidien anglais.
- [17] (en)<http://www.nostate.com/4044/bitcoin-history-us-dollar-parity-on-9-february-2011/>
- [18] (en) (<https://bitcoinfoundation.org/blog/?p=28>) Premier post du blog de la Bitcoin Foundation.
- [19] (en) (<http://en.blog.wordpress.com/2012/11/15/pay-another-way-bitcoin/>) Annonce sur le blog de Wordpress.
- [20] <http://www.bitcoin.org>
- [21] <http://www.bitcoin.org/bitcoin.pdf>
- [22] <https://bitcointalk.org/index.php?board=13.0>
- [23] <http://www.e-ducat.fr>
- [24] <http://www.bitcoin.fr>
- [25] <http://blockexplorer.com>
- [26] <http://lacantine.ubicast.eu/videos/webinar-02-10-2011-155256/>
- [27] <http://linuxfr.org/2010/09/30/27430.html>
- [28] <http://linuxfr.org/tags/bitcoin/public>
- [29] <http://video.rml1.info/videos/bitcoin-monnaie-complementaire-et-logiciel-libre/>
- [30] <http://www.framablog.org/index.php/post/2011/08/08/bitcoin>
- [31] <http://ploum.net/tag/bitcoin>
- [32] [http://www.lemonde.fr/sciences/article/2012/11/29/payer-et-vendre-sans-les-banques\\_1798066\\_1650684.html](http://www.lemonde.fr/sciences/article/2012/11/29/payer-et-vendre-sans-les-banques_1798066_1650684.html)
- [33] <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

# Sources et contributeurs de l'article

**Bitcoin** *Source:* <https://fr.wikipedia.org/w/index.php?oldid=86050264> *Contributeurs:* Alco, Arkanosis, AsTeRfr, Brunohbrassard, Coyau, Coyote du 86, David Latapie, Dilbert, Domsau2, DuoSRX, Dwarfpower, Ecureuil espagnol, Elfix, EricDeschamps, Expertom, Fauve, Floxit, Frakir, Grondilu, Grégoire12, Jboillot, Jerome Charles Potts, Jmax, Johngeek, Jrcourtois, Kimory, Love Sun and Dreams, Lylvic, M0tty, MOut, Marc Mongenet, Marin M., Melksoft, PAC2, Popolon, Pro virus, S0l0xal, SF007, Sirk390, SniperMaské, Sodatux, Sofian, Stanjourdan, Superjuju10, ThisIsNotReal, Tobovs, TrAsHeR, Visite fortuitement prolongée, Vituzzu, Yoha, Zawer, 80 modifications anonymes

# Source des images, licences et contributeurs

**Image:Bitcoin logo.svg** *Source:* [https://fr.wikipedia.org/w/index.php?title=Fichier:Bitcoin\\_logo.svg](https://fr.wikipedia.org/w/index.php?title=Fichier:Bitcoin_logo.svg) *Licence:* Copyrighted free use *Contributeurs:* bitboy  
**Fichier:Bitcoin screenshot.png** *Source:* [https://fr.wikipedia.org/w/index.php?title=Fichier:Bitcoin\\_screenshot.png](https://fr.wikipedia.org/w/index.php?title=Fichier:Bitcoin_screenshot.png) *Licence:* Public Domain *Contributeurs:* hacktolive (?)  
**File:Bitcoin exchange.png** *Source:* [https://fr.wikipedia.org/w/index.php?title=Fichier:Bitcoin\\_exchange.png](https://fr.wikipedia.org/w/index.php?title=Fichier:Bitcoin_exchange.png) *Licence:* Creative Commons Attribution-Sharealike 3.0 *Contributeurs:* 0x0F, 99of9, Aleš Janda  
**File:Total bitcoins over time.png** *Source:* [https://fr.wikipedia.org/w/index.php?title=Fichier:Total\\_bitcoins\\_over\\_time.png](https://fr.wikipedia.org/w/index.php?title=Fichier:Total_bitcoins_over_time.png) *Licence:* Creative Commons Attribution 3.0 *Contributeurs:* Insti

# Licence

Creative Commons Attribution-Share Alike 3.0 Unported  
[//creativecommons.org/licenses/by-sa/3.0/](https://creativecommons.org/licenses/by-sa/3.0/)