# Bitcoin, c'est quoi ?

Bitcoin est une nouvelle devise numérique pour des transactions en ligne sans tiers de confiance : c'est de l'argent liquide sur internet.
Comment présenter Bitcoin à celles et ceux qui ne sont pas passionnés par la technologie ?
Le plus simple est de partir d'une application d'internet que tout le monde peut utiliser : le web.

Le web est un protocole libre (« open source »), comme bitcoin.
Sur le web, il y a des sites (les nœuds du réseau) et des gens qui surfent en utilisant un explorateur (browser) comme Internet Explorer, Chrome, Safari, etc..
Tout le monde peut éditer un site et tout le monde peut surfer sur le web.
Bitcoin fonctionne de manière similaire : il y a des vérificateurs (les nœuds du réseau, que les initiés appellent des « mineurs ») et des gens qui effectuent des transactions en utilisant un porte-monnaie (wallet).
Tout le monde peut être vérificateur (« mineur ») et tout le monde peut envoyer ou recevoir des bitcoins.


Fondamentalement, Bitcoin est une nouvelle application sur internet qui permet de payer un correspondant par voie électronique mais sans passer par une banque : l'usage de cette nouvelle « monnaie » électronique est donc comparable à celui que nous faisons des billets de banque et des pièces de monnaie dans le monde physique.
Un bitcoin est donc une sorte de jeton numérique qui peut être divisé à l'infini en fractions plus petites et s'échanger sur internet aussi simplement qu'un message électronique.
Comme il peut s'échanger contre un bien ou un service dont le prix est exprimé en bitcoin, il peut aussi s'échanger contre des euros auprès d'un bureau de change en ligne.


Un porte-monnaie électronique rempli de bitcoin est un simple fichier enregistré sur un ordinateur : il doit être protégé comme un porte-monnaie traditionnel contre le même risque de vol, simplement avec des moyens différents.
Il peut être copié à volonté. Evidemment la sauvegarde ne crée pas de nouveaux bitcoins, pas plus que sauvegarder votre carnet d'adresses ne crée de nouveaux contacts: la sauvegarde permet seulement de le retrouver plus facilement en cas de besoin.

En tant que tel, Bitcoin peut être considéré comme la première devise complémentaire (non-étatique) universelle, disponible sur internet.

Cependant la réponse à cette première question de définition n'est pas si simple car Bitcoin est une invention protéiforme.

L'invention consiste précisément à réunir dans un même système trois fonctionnalités et des caractéristiques qu'on trouve généralement dans plusieurs organisations : un protocole d'échanges sur internet, une devise numérique et un registre public de transactions.
La réponse la plus complète et la plus simple est pourtant celle-ci : bitcoin est un protocole d'échanges sur internet avec une application de « porte-monnaie » électronique accessible pour tous.
Bitcoin est donc un nouveau « réseau » de paiement de pair-à-pair sur internet. Les paiements en Bitcoins sont des paiements en liquide car il n'y a pas d'intermédiaire bancaire entre le payeur et le receveur.
Cette caractéristique définit aussi Bitcoin, par extension, comme une nouvelle devise, complémentaire, indépendante des Etats, circulant sur internet.
Le protocole Bitcoin peut donc exercer dans le domaine monétaire un pouvoir de transformation comparable à celui du Web dans le domaine de l'édition.

Bitcoin est aussi un grand livre comptable de transactions, groupées dans une base de données publiques : pour chaque transaction, le montant en bitcoin, l'adresse électronique du payeur et celle du destinataire sont connus de tous les participants au réseau.
A chaque adresse électronique bitcoin correspond une clé privée, similaire au mot de passe correspondant à une adresse de courrier électronique. La principale différence tient au fait que l'adresse de courrier et son mot de passe doivent être mémorisés par l'utilisateur : dans le cas de bitcoin, c'est l'ordinateur personnel qui se charge de mémoriser ces données.
Clé privée et adresse

En fait, une adresse bitcoin et sa clé privée seraient quasiment impossible à mémoriser du fait de leur longueur (34 caractères pour une adresse bitcoin et 50 caractères pour sa clé privée) : la sélection d'une adresse se fait par un simple « clic » dans un carnet d'adresses, de même que la signature d'une transaction avec une clé se fait en cliquant le mot « envoyer » ou « payer ».
A chaque montant en bitcoin reçu sur une adresse correspond donc une clé secrète dont la connaissance permettra à son propriétaire de le dépenser auprès d'un futur destinataire.
La propriété d'un bitcoin se résume donc à la connaissance de la clé secrète permettant de le dépenser.
Ce secret est lié mathématiquement à l'adresse électronique du destinataire : le couple adresse bitcoin/clé privée peut être compris par analogie comme un coffre « bancaire » muni de sa clé.
L'adresse bitcoin représente l'adresse de la banque où se trouve le coffre et le numéro du coffre.
La clé privée permet d'ouvrir le coffre.
Vous disposez d'autant de « coffres » que vous voulez et vous pouvez transférer l'argent entre ses coffres. Vous pouvez aussi payer quelqu'un en lui envoyant de l'argent vers son coffre.

Join the discussion…

**alexandre** • il y a 3 ans
c'est le future.. nos petits enfants pourrons se payer une coupe de cheveux en Bitcoins... hemmm ah wé mmm... wéééé
1 • Reply • Share ›

**Neko Desu !** alexandre • il y a 2 ans
Et même un Bescherelle !
• Reply • Share ›

**Bitcoin ? s'faire enculer** • il y a 10 mois
J'ai toujours rien compris
• Reply • Share ›

**jarod26** • il y a un an
j'y comprends rien
• Reply • Share ›


**MrVideogames94** • il y a 2 ans
*Se fait des sous avec bitcoin* putain j'ai 200 € !
• Reply • Share ›

**totolemito** • il y a 2 ans
C'est vrai que c'est pas facile de comprendre mais c'est un peut il me semble comme un certificat rsa ssl/tls émis par une autorité de confiance bon je continue d'apprendre :)
• Reply • Share ›

**riviere** • il y a 3 ans
je comprend rien bouhouhou help me
• Reply • Share ›

**sophie watkins** riviere • il y a 2 ans
moi non plus on est deux :))!!!
• Reply • Share ›

**oulaoula** sophie watkins • il y a 2 ans
Qui peut traduire svp?
• Reply • Share ›

**yayel** • il y a 3 ans
Merci de cet article, je comprends mieux comment ça marche.
• Reply • Share ›