Les places de marché Bitcoin, ça sert à quoi et ça marche comment ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 décembre 2013

http://www.bortzmeyer.org/bitcoin-marches.html

Il y a plein d'aspects rigolos dans le système Bitcoin et je ne vais pas répéter sur ce blog les très bonnes choses qu'on trouve partout. Cet article se focalise sur un seul aspect, les **places de marché**. Quel est leur rôle dans le système ? Que font-elles exactement ?

La présentation dans les médias de ces places de marché ("*bitcoin exchanges*" dans la langue de Warren Buffett) est souvent trompeuse : elles sont souvent décrites comme un acteur indispensable, nécessaire au fonctionnement du système et, dans ce cas, on en vient forcément à les comparer aux banques traditionnelles, et à se demander si elles sont meilleures ou pires que ces banques et si on a vraiment gagné au change (ah, ah) à remplacer sa banque par une place de marché Bitcoin.

La vérité est que ces places ne sont nullement indispensables. C'est une des beautés de Bitcoin : les intermédiaires ne sont pas indispensables. Vous pouvez parfaitement avoir vos bitcoins dans un ou plusieurs portefeuilles installés sur votre ordinateur et envoyer ou recevoir des bitcoins avec d'autres volontaires, sans passer par une place de marché. Échanger des bitcoins, c'est simplement publier une nouvelle transaction dans la chaîne de transactions publique et cela ne nécessite pas d'intermédiaire entre votre logiciel (comme Electrum <http://electrum.org/> ou Multibit <https://multibit.org/>) et la chaîne. Les intermédiaires peuvent jouer un rôle utile (j'ai personnellement un compte sur deux de ces places de marché) mais ne sont pas nécessaires. Le rôle d'une de ces places de marché est double : stocker votre argent, qu'il soit en euros ou en bitcoins, et le changer d'euros en bitcoins ou réciproquement.

Le premier rôle est proche de celui d'une banque classique : votre argent n'est pas chez vous, il est dans le "*cloud*". À vous de voir si vous trouvez cela plus sûr ou pas. Des places de marché ont déjà été piratées et les bitcoins volés (les voleurs vont là où est l'argent...) Mais des PC individuels à la maison ont déjà été victimes de logiciels malveillants qui ont volé les bitcoins. Ou de panne ou de destruction <http://ecrans.liberation.fr/ecrans/2013/11/28/il-jette-son-disque-dur-qui-vaut-55-millio
962764>.

Si on peut se passer de la première fonction, en gardant les bitcoins chez soi, pour la seconde, c'est plus difficile. Bien sûr, rien n'empêche d'échanger des bitcoins contre des euros avec des copains, ou avec des inconnus rencontrés sur BitcoinMeet <http://www.bitcoinmeet.com/> ou LocalBitcoins <https://localbitcoins.com/>. Pour des petites sommes « pour voir », je ne pense pas que cela cause un problème. Au delà, je ne me prononcerai pas sur la légalité de l'opération. En effet, le bitcoin lui-même n'est pas légal ou illégal. Il est « a-légal » dans la mesure où il n'est pas traité par une loi. Son échange entre acteurs économiques ne me semble pas poser de problème (je ne suis pas juriste, attention, prenez mes appréciations avec des pincettes). En revanche, sa conversion en euros (ou le contraire) fait intervenir la monnaie officielle et c'est là que s'exerce le pouvoir de l'État, à des fins d'imposition ou de lutte contre certains trafics. Donc, l'achat ou la vente de bitcoins avec des euros ne peut probablement pas se faire simplement, d'un commun accord. Vous devez passer par une place de marché (ou par un distributeur automatique <http://www.bortzmeyer.org/premiers-bitcoins.html>), et celles-ci sont fortement régulées. (À noter qu'aussi bien les partisans du Bitcoin, pour s'en féliciter, que ses adversaires, pour le déplorer, affirment souvent que le Bitcoin échappe à toute loi et toute régulation. C'est tout à fait faux, au moins quand on l'échange avec la monnaie officielle.)

Donc, quelles sont les places de marché disponibles, et leurs caractéristiques ? Les médias, qui ne font en général rien d'autre que de se recopier les uns les autres, n'en citent quasiment qu'une seule, Mt.Gox. Enregistrée au Japon, ce n'est pourtant pas forcément la solution la plus naturelle pour quelqu'un qui vit en France, comme moi. Il existe pourtant de nombreuses autres places de marché, et je vais citer les deux où j'ai un compte, Bitcoin Central <https://www.bitcoin-central.net/> et Kraken <https://www.kraken.com/>. Elles sont entièrement en ligne (pas de guichets physiques). Dans les deux cas, on se crée un compte en ligne mais, au contraire de tant de services sur le Web, on ne peut pas s'en servir tout de suite, un certain nombre de vérifications sont faites. Ces vérifications dépendent de la politique de la place de marché mais aussi des lois et réglements qui s'appliquent à elles. Si le Bitcoin lui-même peut être décrit comme planant dans un espace virtuel, ces places de marché sont, elles, fermement ancrées dans un espace légal national.

Du point de vue de cet ancrage national, Bitcoin Central est français <https://www.bitcoin-central.net/page/legal-notes> (et doit donc appliquer la loi française <http://www.numerama.com/magazine/28077-bitcoin-utilise-par-les-douanes-pour-pieger-un-trafiquant.html>), et Kraken états-unien <https://www.kraken.com/about/contact> (avec une adresse d'une banque allemande en Grande-Bretagne pour les virements... On peut noter que leur site Web n'est pas excessivement bavard en informations). Les vérifications demandées sont bien plus détaillées pour Bitcoin Central (il faut donner des détails personnels et envoyer un fichier numérisé d'un certain nombre de papiers officiels) et plus longues (il m'a fallu seize jours pour être validé). Il est difficile de comparer avec les conditions de Kraken, car, alors que Bitcoin Central est binaire (on est validé ou on ne l'est pas), Kraken a un système de niveaux ("*tiers*"), cinq au total. Pour passer au niveau supérieur, il faut fournir plus d'informations et se prêter à plus de vérifications. Et les actions qu'on peut faire sont limitées en fonction du niveau. Pour ma part, je suis actuellement au niveau Deux (le troisième, puisque cela part de zéro), ce qui me permet de déposer ou retirer 2 000 $ par jour (avec une limite de 10 000 par mois). La validation à ce niveau a pris deux jours mais il est difficile de dire ce qui a été exactement vérifié (je ne pense pas que quelqu'un soit venu voir en bas de l'immeuble si mon nom était bien sur une des boîtes aux lettres).

Une fois qu'on est validé, que peut-on faire ? L'interface de Bitcoin Central est très simple, n'offrant que peu de possibilités, ce qui est certainement un avantage pour les débutants :

Sans vérifier la documentation, on trouve tout de suite comment déposer des euros ou des bitcoins, changer de l'argent, ou retirer des euros ou des bitcoins. Dans mon cas, j'ai alimenté mon compte Bitcoin Central avec des euros par un simple virement bancaire SEPA vers l'IBAN indiqué. Ensuite, j'ai pu changer ces euros en bitcoins et retirer ensuite des bitcoins, en les envoyant à l'adresse Bitcoin indiquée. On voit donc qu'on peut utiliser une place de marché juste pour le change et ne pas laisser son argent

ensuite. (Mais attention, avant de retirer des bitcoins, assurez-vous que le portefeuille de destination est sécurisé, à la fois contre le piratage, et contre la perte accidentelle. Vérifiez la sécurité de la machine qui l'héberge, et les sauvegardes. N'oubliez pas que Bitcoin a une sémantique proche de l'argent liquide : si vous envoyez à une mauvaise adresse, l'argent est perdu. Si votre disque dur vous lâche, même chose.) Un autre piège avec Bitcoin Central (documenté mais, comme je l'ai écrit, je n'avais pas lu la documentation) : pour des raisons de sécurité, des tas de choses sont stockées hors-ligne et ne sont extraites du coffre-fort qu'à certains moments. Vous n'aurez donc pas vos bitcoins tout de suite.

L'interface de Kraken est très différente. Par défaut, pour passer un ordre, vous avez la version simple :

Et il y a une version plus riche :

Beaucoup plus riche qu'avec Bitcoin Central, l'interface est même franchement effrayante pour des débutants qui ne connaissent pas le monde de la finance. On vous y propose de faire plein de choses. Suivez un conseil de bon sens : si vous ne connaissez pas ces instruments financiers, tenez-vous à l'écart et contentez-vous, comme dans le paragraphe précédent, d'échanger des bitcoins contre des euros (toujours avec un virement bancaire pour alimenter le compte originalement). L'interface de Kraken étant riche, consulter la documentation, même pour des tâches simples, est recommandée.

Je ne suis pour l'instant qu'un tout petit utilisateur, expérimentant avec des petites sommes. Je ne peux donc pas encore donner d'affirmation solide sur la meilleure place de marché. Je ne peux notamment rien dire sur la qualité du support utilisateurs chez Kraken, je n'ai pas encore eu à l'utiliser. Mais je note que, pendant la grande panne de Kraken du 12 décembre 2013 (apparemment due à une attaque par déni de service), le "*community manager*" n'a donné aucune information sur Twitter. En revanche, chez Bitcoin Central, je peux dire que le support est aimable, assez rapide, et répond en général de manière pertinente. Je le sais car j'ai eu souvent besoin de faire appel à eux, chaque opération nécessitant au moins un appel au support, en raison du nombre de choses qui ne fonctionnaient pas encore (virements qui n'arrivent pas, courrier de demande de confirmation qui ne part pas, etc). Leur logiciel semble encore très jeune. Mais, à chaque fois, ça a fini par marcher donc, si vous devenez client de Bitcoin Central, vous profiterez du déboguage fait grâce aux premiers utilisateurs :-)

Sur Kraken, un chose est à noter : on peut enregistrer sa clé publique PGP et les messages de Kraken vers vous sont alors en PGP. Excellente idée et j'aimerai bien que les autres banques suivent ! Deux petits bémols toutefois, le sujet du message est en clair et Kraken le fait très informatif, donc cela diminue l'intérêt de chiffrer. Et Kraken met le texte chiffré directement dans le corps du message au lieu d'utiliser le RFC 3156 [1].

Kraken et Bitcoin Central disposent d'autres mécanismes de sécurité rigolos. Par exemple, l'authentification de base est faite par un mot de passe mais on peut demander des mécanismes plus sûrs (mais aussi plus complexes). Pour l'instant, comme je ne manipule que de petites sommes, j'ai juste activé une option astucieuse de Kraken : celle qui bloque toute modification du compte pendant une période qu'on choisit. Ainsi, même si je me fais piquer mon mot de passe, l'attaquant devra attendre quelques jours avant de changer les paramètres d'authentification, ce qui me permettra de détecter le problème et de donner l'alarme.

Ah, et si vous vous demandez ce que veulent dire les termes financiers mystérieux de l'interface de Kraken, Vincent Archer a fait un excellent travail d'explication, que je copie/colle ici avec mes remerciements. "*Leverage*", en économie, c'est le taux d'endettement. Par extension, c'est l'emprunt pour

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc3156.txt`

investissement, lorsqu'on emprunte pour investir dans quelque chose qui rapportera plus que le taux d'intérêt à payer, par opposition à l'emprunt de financement ("*borrowing*"), pour financer un achat. Utilisé aussi pour indiquer le taux d'endettement ; quand on te demande le niveau de "*leverage*", c'est que tu veux emprunter une partie du montant pour acheter tes bitcoins. Ce n'est pas une distinction absolue, mais plutôt un usage. On utilise beaucoup en adjectif l'expression "*leveraged buyout*" qu'on voit dans le rachat d'entreprise. Elle signifie qu'une partie du rachat de la boite est fait avec un emprunt (et pas en trésorerie ou en échange d'actions).

"*Margin*", c'est la partie de ton achat qui est financée par le prêt.

Et la position, dans la bourse, c'est quand tu dois forcément vendre ou acheter quelque chose, en général parce que tu as acheté ou vendu à découvert (ou en "*margin*", comme on vient de dire). Si tu as choisi un pourcentage d'emprunt, tu te places dans une position d'obligation où tu devras revendre la partie que tu as financée via le prêt. Sinon, c'est juste que tu as fait une opération de change et tu peux tout garder.

Et bien sur, "*closed*" signifie dérouler l'obligation de revente... Et réaliser (matérialiser en vrai) le bénéfice ou la perte. Fin des explications financières de Vincent.

Les idées sur le caractère a-légal du bitcoin et sur le fait que c'est l'échange en euros qui l'amène sous les projecteurs de la régulation viennent d'une publication de la Banque de France, Focus n° 10, disponible en ligne <https://www.banque-france.fr/publications/documents-economiques/focus.html>.

Merci à Vincent Archer et Laurent Penou pour la relecture, mais je garde le "*copyright*" sur toutes les fautes et erreurs de cet article.