Bitcoin libérera-t-il la monnaie à l'échelle d'Internet ?

« Papa, tu faisais quoi quand les crédits Facebook sont devenus l'unique moyen de paiement sur internet ? »

C'est par cette phrase cinglante que s'achève le billet de notre ami Ploum, qui nous a fait l'honneur d'un article original sur le Framablog.

Le propos se divise en deux parties.

La première nous explique très clairement pourquoi nous avons urgemment besoin d'un système d'échange monétaire libre et décentralisé, à fortiori lorsqu'il s'agit de micropaiements ou de microdons.

La seconde est consacrée à **Bitcoin** (cf cette vidéo) qui semble potentiellement d'ores et déjà répondre au besoin mais qui n'est pas sans poser questions et problèmes[1].

Je ne sais si Bitcoin s'imposera, mais celui qui réussira lui ressemblera.

Et ce jour-là Papa sera fier d'annoncer à son rejeton qu'on pourra non seulement se passer des crédits Facebook mais qu'on n'aura plus à trembler servilement lorsque les bourses mondiales se mettent à tousser.

Décentralisation monétaire

Ploum – juillet 2011
Licence Creative Commons By-Sa

Quelle que soit votre motivation profonde, vous êtes beaucoup, parmi les lecteurs

de Framasoft, à voir dans l'Internet un espace de liberté, d'expression, de communication, d'échanges, d'entraide et bien d'autres.

Afin que cette liberté soit garantie, il est nécessaire d'éviter à tout prix une centralisation qui mettrait le pouvoir absolu d'un service donné dans les mains d'une seule personne, entreprise ou gouvernement. En effet, un service décentralisé assure non seulement la pérennité du réseau mais permet également une indépendance d'un client par rapport à un fournisseur de service.

C'est pour cette raison qu'à Framasoft nous sommes de fervents défenseurs de l'email, que nous utilisons XMPP à la place de MSN, que nous préférons identi.ca à Twitter et que nous suivons avec impatience les progrès de Diaspora pour proposer une alternative à l'omniprésent Facebook.

Mais si l'entraide, la communication et l'échange sont de très belles choses, ils ne sont malheureusement pas entièrement suffisants et la majorité d'entre nous, Framasoft inclus, a encore terriblement besoin d'argent.

Alors que le troc est entièrement décentralisé, chacun troquant selon ses convenances, l'argent est un service totalement centralisé fourni par les états. D'ailleurs, ne parle-t'on pas de « banque centrale » ?

Ce système est, de plus, complètement opaque, les citoyens devant entièrement faire confiance à l'état central qui, lui-même, délègue une partie de ce pouvoir aux banques privées.

Le fait que ce soit un bien ou un mal reste sujet à interprétation. Néanmoins, en regard de la crise économique de 2008, il faut bien admettre que le résultat de l'actuelle politique économique centralisée est relativement mitigé. C'est d'ailleurs une des raisons pour laquelle certaines collectivités ont développé des systèmes d'échange locaux (SEL), en temps qu'alternative locale et auto-gérée à l'économie traditionelle.

Sur le réseau la situation n'est guère meilleure. Quelques acteurs centralisés comme Visa et Paypal monopolisent les transferts entre monnaie réelle et monnaie virtuelle. Cette situation d'oligopole leur est, bien entendu, fortement profitable : taxes à l'entrée d'argent dans le système, taxe à la sortie d'argent du système, commission sur chaque transaction. Sans compter que toutes vos dépenses, représentant une grande part de votre vie privée, sont fichées et

archivées entre les mains d'entreprises pas toujours scrupuleuses.

Au final, il s'ensuit un véritable racket de l'internaute : afin que votre correspondant puisse recevoir 1€ au bout de la ligne, il n'est pas rare de devoir verser 1,20€, 1,50€ voire 1,80€, sous forme de frais fixes et de pourcentage sur la transaction. Ces frais, négligeables pour les grosses sommes, empêchent tout développement réel des petits transactions, des microdons, des micro-achats. Ces entreprises acquièrent également un pouvoir politique, s'octroyant le droit de « geler » ou de supprimer des comptes, comme ce fut le cas pour Wikileaks.

Le transfert de petites sommes est pourtant un moteur de notre économie. Si l'on hésite à acheter un album de musique à 14€, acheter une chanson à 1€ peut se faire sur un coup de tête. Les grandes entreprises ont donc développé des systèmes de « comptes » ou d'abonnements. Vous versez une somme importante en une fois que vous pourrez dépenser petit à petit. L'Apple Store ou les crédits Facebook fonctionnent sur ce principe. Mais outre le fait que ces systèmes sont centralisés, ils nécessitent d'immobiliser une grosse somme d'un seul coup et ne sont bien sûr pas interopérables. Une fois vos 25€ versés sur Facebook, ils sont irrécupérables et non-transférables en dehors des applications Facebook.

Quelques alternatives tentent également de proposer un modèle original, comme Flattr. Flattr offre en effet de déterminer une somme mensuelle fixe qui sera divisée par le nombre de dons faits chaque mois. Néanmoins, cela reste centralisé et avec des frais prohibitifs. Ainsi, Framasoft ne touche que 90% des dons faits via Flattr.

Une solution idéale serait de proposer un système d'échange monétaire libre et décentralisé. Un tel système existe et a un nom : Bitcoin.

Techniquement, le fonctionnement de Bitcoin est relativement complexe, se basant sur des algorithmes cryptographiques et le peer-to-peer. Le gros problème d'une monnaie virtuelle est d'éviter la « double dépense ». Par essence, une information virtuelle peut être répliquée à l'infini, problème qui tracasse l'industrie musicale depuis plusieurs années.

Bitcoin résout ce problème en utilisant le peer-to-peer. Lorsque Alice donne un bitcoin à Bob, elle rend la transaction publique. Les participants au réseau bitcoin (les « mineurs ») vérifient que la transaction est légitime en s'assurant que, dans leur historique des transactions, Alice est bien la dernière personne à avoir reçu

ce bitcoin précis, chaque bitcoin étant unique. Les « mineurs » annoncent sur le réseau que la transaction est confirmée. Quand suffisamment de « mineurs » ont confirmé la transaction, Bob peut considérer que Alice ne pourra plus dépenser son bitcoin et qu'il en est donc le propriétaire. Si Alice tente de redépenser son bitcoin, les « mineurs » refuseront la transaction, arguant que, d'après l'historique, Bob est le légitime propriétaire du bitcoin.

Pour encourager les « mineurs » à faire ce travail de vérification, le réseau gratifie le premier mineur à vérifier chaque bloc de transactions d'un bonus. Ce bonus, qui est pour le moment de 50 bitcoins, décroît avec le temps et a pour conséquence de distribuer la monnaie graduellement à travers le réseau.

Le nombre de bitcoins ainsi générés étant une fonction décroissante, on a pu calculer que le nombre total de bitcoins ne dépasserait jamais 21 millions.

Intrinsèquement, le bitcoin n'a aucune valeur. C'est juste la preuve qu'un échange a été fait. Mais n'en est-il pas de même pour n'importe quelle monnaie ?

Afin de garantir l'anonymat, les transactions ne se font pas directement entre Alice et Bob mais entre deux adresses du type 1GTkuikUyygRtkCy5H6RMuTMGA1ypqLc1X, qui est la partie publique d'une clé de cryptage asymétrique. Bob donne à Alice son adresse et seul eux deux savent à qui appartient l'adresse. Le réseau ne possède aucun moyen de lier l'adresse réceptrice à Bob. Bob, de son côté, possède la partie privée de la clé, lui permettant de prouver qu'il est bien le destinataire de tous les bitcoins envoyés à cette adresse. Bob peut générer autant d'adresses qu'il le désire et l'usage est de générer une adresse par transaction.

La facilité d'échange et la rareté du bitcoin en font un candidat idéal pour une monnaie électronique décentralisée. Des sites de vente en ligne acceptant les bitcoins sont donc apparus sur le net. Beaucoup de personnes, tablant sur un succès futur des bitcoins, on décidé d'en acheter une certaine quantité, ce qui a fait monter le prix du bitcoin. Une véritable économie parallèle s'est développée, principalement basée sur la spéculation. La valeur du bitcoin est passée de 0,01€ en novembre 2010 à 25€ en mai 2011, avant de redescendre aux alentours de 10€ en juin 2011.

Si Richard Stallman n'a pas encore pris de position publique au sujet du bitcoin, le fait qu'il s'agisse d'un logiciel libre, décentralisé et permettant des paiements

anonymes en fait la coqueluche de certains libristes. La Free Software Foundation elle-même accepte dorénavant les donc en bitcoins. Après moins de deux jours, plus de 270 bitcoins avaient été envoyés anonymement, l'équivalent de près de 700€ de dons à l'époque et 2700€ actuellement !

Mais tout n'est pas rose au pays des bitcoins et les critiques sont nombreuses.

Beaucoup s'étonnent notamment au fait d'attacher de la valeur à quelque chose qui n'en a pas. À ce sujet, le bitcoin ne diffère pas d'un bout de papier ou même d'un morceau de métal jaune brillant. La valeur attachée à un objet est en effet liée à la confiance que le possesseur a de pouvoir échanger cet objet. Mais entre accorder sa confiance à un gouvernement et l'accorder à un réseau P2P décentralisé, il y a un pas que beaucoup hésitent à franchir.

Le bitcoin est anonyme et permet de gros échanges d'argent sans aucun contrôle, tel la vente de drogue ou de services illicites. Les partisans du bitcoin répliquent que bitcoin n'est qu'un outil, comme l'est la monnaie papier. Beaucoup d'outils facilitent les activités illégales: Internet, la cryptographie, le réseau Tor. Il est d'ailleurs déjà possible d'acheter de la drogue en ligne en payant en bitcoins. Faut-il bannir ces outils pour autant ? Une chose est certaine: le bitcoin opère dans une zone encore floue de la légalité. Même les activités parfaitement licites sont confrontées à un problème de taille: comment déclarer des revenus en bitcoins ? Faut-il payer des impôts ? À ce titre, Bitcoin peut être considéré comme un gigantesque SEL à l'échelle d'Internet.

Nombreux, également, sont ceux qui pointent l'inégalité de Bitcoin. En effet, les premiers bitcoins étaient très faciles à générer. Les tous premiers entrants ont donc, sans effort, récolté des milliers de bitcoins. Est-ce que le fait d'avoir cru en bitcoin avant tout le monde est suffisant pour justifier leur nouvelle richesse ? Le bitcoin n'est-il pas une gigantesque pyramide de Ponzi ? De manière amusante, cette critique semble typiquement européenne. Dans un monde où la richesse est un signe de succès, les Américains ne semblent en effet pas y voir le moindre inconvénient, surtout dans la mesure où cet enrichissement entièrement virtuel ne s'est pas fait au détriment d'autres personnes.

Économiques, philosophiques, morales, techniques ou politiques, Bitcoin interpelle et soulève de nombreuses questions à propos du système dans lequel nous vivons, ne laissant personne indifférent. À tel point que certains se

demandent si le prix actuel du bitcoin n'est pas entièrement artificiel et créé par l'enthousiasme des spéculateurs. Sa difficulté d'utilisation et l'apparent amateurisme des sites acceptant les bitcoins ne semblent pas plaider en faveur du bitcoin.

En Juin 2011, MtGox.com, le principal site d'échange de bitcoin contre des dollars, a été piraté et des opérations ont été réalisées de manière frauduleuse, plongeont l'économie du bitcoin dans l'incertitude pendant une semaine complète. La valeur du bitcoin n'en a que peu souffert mais, pour certains, l'évênement a été un signal d'alarme: le bitcoin est encore très expérimental et sa valeur peut tomber à zéro en quelques heures.

Mais, malgré tout, Paypal, les crédits Facebook et les pièces d'or de World of Warcraft nous ont démontré que la généralisation des monnaies virtuelles est une évolution inéluctable. Si elle n'est pas exempte de critiques, Bitcoin semble à ce jour la seule alternative libre et décentralisée utilisable.

Bitcoin disparaitra-t-il comme une bulle spéculative après quelques mois ? Transformera-t-il durablement la société ? J'avoue ne pas en avoir la moindre idée mais je sais que mon plus grand cauchemar est de me réveiller un matin avec une petite tête blonde me demandant auprès de mon lit: « Papa, tu faisais quoi quand les crédits Facebook sont devenus l'unique moyen de paiement sur internet ? »

Notes

[1] Crédit photo : TraderTim (Creative Commons By-Sa)