

The Internet of money

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 décembre 2016

<https://www.bortzmeyer.org/internet-of-money.html>

Auteur(s) : Andreas Antonopoulos

ISBN n°9781537000459

Éditeur : Merkle Bloom

Publié en 2016

Ce petit livre rassemble le texte de plusieurs conférences d'Andreas Antonopoulos au sujet de Bitcoin. Les textes ont été édités, les erreurs corrigées, mais le ton reste celui des conférences de l'auteur, passionnantes et brillantes. Sa thèse principale est que le Bitcoin n'est pas juste une monnaie, c'est un mécanisme sur lequel on va pouvoir bâtir plein de nouvelles relations économiques, c'est l'"*Internet of money*". Et les vieux dinosaures du monde actuel peuvent toujours critiquer, et prétendre que le Bitcoin n'a pas d'avenir, Antonopoulos démonte tous leurs arguments. (Les conférences elles-mêmes sont visibles en ligne <<https://www.youtube.com/user/aantonop>>.)

C'est donc vraiment le bouquin à faire lire aux gens qui expliquent doctement que le Bitcoin n'est pas une monnaie réelle, ou bien que ce n'est qu'une expérience d'une poignée de gusses dans leur garage. Antonopoulos est très pédagogue... et très militant.

Il n'a pas de mal à rappeler que les arguments contre le Bitcoin sont à peu près les mêmes que ceux employés par les messieurs sérieux et les experts médiatiques contre l'Internet (ou, puis-je ajouter, contre Unix et contre le logiciel libre) : c'est juste une expérience, ce n'est pas sérieux, c'est un truc de hippies libertariens, cela ne durera pas. Pourquoi croirait-on aujourd'hui ces mêmes experts ? D'où le titre du livre, qui fait allusion au fait que l'auteur prédit au Bitcoin le même succès que l'Internet : déranger les systèmes en place, permettre de nouvelles possibilités, reposer les questions. « Dire que le Bitcoin est une monnaie numérique, c'est aussi réducteur que dire que l'Internet est un téléphone amélioré. »

Un concept intéressant dans une des conférences est celui d'**inversion de l'infrastructure**. Au début, la nouvelle technologie utilise une infrastructure conçue pour la technologie précédente, et a donc bien du mal. Les premières voitures roulaient sur des routes prévues pour les chevaux. Ceux-ci ont quatre pattes et un bon équilibre, les trous ne les dérangent pas trop, alors qu'ils étaient redoutables pour les voitures. Petit à petit, les choses ont changé, l'infrastructure s'est inversée, et ce sont aujourd'hui les chevaux qui marchent sur une route goudronnée conçue pour les voitures. De même, l'Internet à ses

débuts devait emprunter une infrastructure conçue pour le téléphone (et on avait besoin de modems, pour faire passer IP pour de la voix) alors qu'aujourd'hui, l'infrastructure s'est inversée, c'est la voix qui n'est plus qu'une des nombreuses applications qui utilisent l'infrastructure de l'Internet.

De la même façon, estime Antonopoulos, les services bancaires traditionnels continueront à exister, mais seront simplement des applications au-dessus de Bitcoin.

L'auteur est bien conscient que les adversaires du Bitcoin ne vont pas se contenter de le ridiculiser ou de le critiquer. Ils vont activement tenter de l'interdire. Il est très optimiste sur les chances du Bitcoin de résister à cette censure (dans le pire des cas, les transactions seront encodées en "smileys" dans les discussions des articles Wikipédia et ne pourront donc pas être stoppées...) Après tout, Bitcoin a déjà été testé au feu, d'innombrables attaques ont déjà visé cette monnaie, et le Bitcoin a toujours survécu. (Voir à ce sujet l'hilarant site « *Bitcoin Obituaries* » <<https://99bitcoins.com/bitcoinobituaries/>> » et l'amusante vidéo « Not this time » <<https://www.youtube.com/watch?v=-h1N2ne15HI>>.)

Antonopoulos insiste sur le caractère « sans permission » du Bitcoin. Il n'y a pas de Président du Bitcoin, chacun avec une idée peut la mettre en œuvre sur la chaîne de blocs tout de suite, sans demander de permission. En tant que « *programmable money* », Bitcoin n'a pas seulement un usage (payer) mais tous les usages qu'on peut imaginer. (Le Bitcoin est neutre, au sens de « neutralité du réseau » <<https://www.bortzmeyer.org/neutralite.html>> ».)

Antonopoulos fait remarquer que toutes les innovations ont été la cible d'innombrables critiques à leur début. (Il oublie de dire que certaines critiques étaient justifiées. Par exemple, il cite des déclarations anti-voiture des débuts de l'automobile, pointant les dangers mortels de cette technologie, dangers qui existent toujours.) Ces critiques semblent bien ridicules avec le recul, comme celles contre le Bitcoin sonneront moyenâgeuses dans le futur. Antonopoulos remarque avec justesse que ces critiques portaient souvent sur des points de détail, qui allaient évoluer avec le temps. Ainsi, les premières critiques des automobiles portaient sur la difficulté à les faire démarrer, problème réel mais qui a été vite résolu avec l'invention du démarreur. (Personnellement, je me souviens bien des premières démonstrations de l'Internet que je faisais au début des années 1990, où la plupart des remarques des gens portaient sur le caractère « peu convivial » des logiciels utilisés. Peu de gens étaient capables de voir l'intérêt de cette technologie, au-delà de problèmes ergonomiques temporaires.)

Dans une autre conférence, Antonopoulos revient sur la monnaie : de quand date t-elle ? Et, d'ailleurs, qu'est-ce qu'on appelle « monnaie » ? (Beaucoup de messieurs experts refusent de considérer le Bitcoin comme une monnaie car ils donnent de la monnaie une définition arbitraire et anti-historique du genre « la monnaie est le moyen de paiement décidé par un État, et régulé ».)

L'auteur insiste aussi sur l'importance pour les acteurs du monde Bitcoin de ne pas copier bêtement le vocabulaire du passé. Ainsi, il s'énerve (à juste titre) contre les articles mentionnant le Bitcoin et qui sont illustrés par... des pièces de monnaie. Il reconnaît que c'est d'ailleurs en partie la faute du terme « bitcoin » qui est trompeur. De même, le terme de « portefeuille », souvent utilisé pour les logiciels de gestion de ses bitcoins, est erroné : on ne peut pas copier un portefeuille traditionnel, alors qu'il n'y a aucun problème à le faire avec un portefeuille Bitcoin (il ne stocke pas d'argent, mais des clés).

Autre exemple de l'erreur qu'il y a à copier aveuglément les anciennes techniques, les places de marché Bitcoin. Ces places n'ont rien de Bitcoin, ce sont des établissements financiers traditionnels et, notamment, leur modèle de sécurité n'est pas du tout celui de Bitcoin.

Compte-tenu de la marée médiatique anti-Bitcoin (et anti-cryptomonnaies en général), on a bien besoin d'un livre comme celui-ci, qui redresse la barre. Par contre, il ne faut pas y chercher une analyse balancée. On ne voit aucune critique sur les aspects problématiques du Bitcoin. Il faudra un autre livre pour cela. Un volontaire pour écrire une critique sérieuse du Bitcoin ? (Qui ne se limite pas à des points de détail spectaculaires comme l'identité de Nakamoto, ou à du simple conservatisme du genre « les banques n'en veulent pas » ?) En attendant, lisez le livre, et écoutez les conférences d'Andreas Antonopoulos, vous ne le regretterez pas.