Bitcoin - métamorphoses

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 décembre 2018

https://www.bortzmeyer.org/bitcoin-metamorphoses.html

Auteur(s) : Jacques Favier, Benoît Huguet, Adli Takkal Bataille
ISBN n°9-782-100-784646
Éditeur : Dunod
Publié en 2018

———————-

Le Bitcoin suscite toujours autant de passions, et les informations à son sujet varient toujours de l'enthousiasme délirant aux enterrements prématurés <https://99bitcoins.com/bitcoin-obituaries/>. Il est amusant de noter que les uns comme les autres utilisent souvent les mêmes arguments qu'il y a dix ans, au moment du lancement de la cryptomonnaie. Au contraire, le livre de Favier, Huguet et Bataille se demande « où en est le Bitcoin aujourd'hui ? » Certainement pas au même point qu'en 2008.

J'avais déjà parlé du précédent livre <https://www.bortzmeyer.org/bitcoin-acephale.html> de ces auteurs. Celui-ci est destiné à un public plus informé, qui connait déjà le Bitcoin et souhaite s'informer sur les derniers développements.

Comme dans leur livre antérieur, les auteurs n'hésitent pas à nager à contre-courant du discours dominant. Depuis deux ou trois ans, la mode est à dire « le Bitcoin, c'est pas bien mais la chaîne de blocs, c'est la solution à tous les problèmes de l'humanité ». Pour eux, au contraire, le Bitcoin reste la meilleure solution à bien des problèmes pour lesquels on crée de nouvelles chaînes de blocs, et ils sont très confiants dans sa capacité à évoluer pour répondre aux défis d'aujourd'hui. Les auteurs suggèrent que ce discours bruyant sur la chaîne de blocs sert à évacuer le caractère disrupteur du Bitcoin et à ramener le torrent des cryptomonnaies dans son lit, un lit bien contrôlé et bien régulé.

Les auteurs notent bien que la grande majorité des articles sur le Bitcoin sont très médiocres, juste une compilation de clichés (Law, les tulipes <https://www.smithsonianmag.com/history/there-never-was-real-> et Ponzi). Parfois, la malhonnêteté intellectuelle va plus loin, comme le reportage de France 2 sur le Bitcoin se terminant par…un envol de pigeons. Comme le notent Favier, Huguet et Bataille, « illustre-t-on un reportage sur une banque centrale par des photos de poulets en batterie ? »

Un autre exemple de la propagande contre les cryptomonnaies concerne les ICO, un mécanisme de financement où une entreprise débutante vend des jetons d'une cryptomonnaie…qui n'existe pas

encore. Les ICO sont systématiquement diabolisés dans les médias, qui ne parlent que du risque de perdre son argent, si l'entreprise se casse la figure. Mais, comme le disent les auteurs « pourquoi est-il admis qu'on puisse perdre de l'argent avec la Française des Jeux et pas avec les ICO ? »

À juste titre, les auteurs sont hostiles au concept de « chaîne de blocs privée » (ou « chaîne de blocs à permission ») en notant qu'il s'agit soit de banales bases de données partagées, rebaptisées chaîne de blocs pour des raisons marketing, soit d'erreurs techniques où on utilise une chaîne de blocs pour un problème où elle n'est pas la meilleure solution. En effet, tout l'intérêt de Bitcoin est de fournir de la confiance dans un état alors même que les participants ne se connaissent pas. Si les participants se connaissent et ont déjà une structure en place ou, pire, si le seul participant est une entreprise spécifique, la chaîne de blocs n'a guère d'intérêt.

Et pendant ce temps, Bitcoin ne reste pas inactif : si le logiciel et le protocole n'évoluent qu'avec prudence, la communauté autour du Bitcoin, elle, a beaucoup changé et, au milieu de nombreuses crises, a prouvé sa faculté à s'adapter, dans un environnement impitoyable.

Le gros du livre tourne autour d'un enjeu technique essentiel pour toute chaîne de blocs : le passage à l'échelle. Vu que la taille de blocs de Bitcoin est limitée (notamment pour éviter certaines attaques par déni de service) et que l'écart de temps entre deux blocs est fixe, Bitcoin ne peut pas traiter un nombre illimité de transactions. Une chaîne de blocs qui ne mettrait pas de limite aurait d'autres problèmes, notamment la croissance illimitée de la chaîne, que tous les pairs doivent charger. Bref, on ne peut pas envisager, avec le Bitcoin classique, un monde où chacun paierait son café à la machine avec des bitcoins. Il faut donc améliorer le passage à l'échelle. Ce sujet est bouillonnant en ce moment dans le monde Bitcoin. (Le livre remarque que cela évoque l'époque où les experts auto-proclamés répétaient que l'Internet n'avait pas d'avenir, qu'il s'écroulerait dès qu'on essaierait de s'en servir vraiment, pendant que les vrais experts travaillaient à améliorer l'Internet, afin qu'il puisse assurer le service qu'en attendaient les utilisateurs.)

Les auteurs décrivent donc les solutions comme les « chaînes de côté » ("*sidechains*", comme par exemple Blockstream ou RootStock) où une chaîne ayant moins de limites sert pour les transactions courantes, et son état final est mis de temps en temps sur une chaîne principale, par exemple celle de Bitcoin. Ainsi, la chaîne de côté croît vite mais on n'a pas besoin de la garder éternellement. Autre possibilité, les échanges hors-chaîne mais reportés sur la chaîne comme avec le Lightning Network. Cette partie du livre est plus difficile à lire, reflétant le caractère très mouvant de ces innovations.

Le livre couvre également en détail le cas des scissions, notamment la plus grosse qui a affecté Bitcoin depuis deux ans, et qui est toujours en cours, Bitcoin Cash (sans compter Bitcoin SV.)

Le cas des contrats automatiques est aussi traité, en exprimant un certain scepticisme quant à la possibilité d'en produire sans bogues. Mais, surtout, le livre note que la plupart des problèmes « intéressants » qu'on pourrait traiter avec des contrats automatiques nécessitent de l'information sur le monde extérieur à la chaîne. Si le déroulement d'un contrat automatique d'assurance dépend du temps, par exemple, il faudra bien accéder à des informations météorologiques, et cela ne sera plus pair-à-pair, cela ne pourra pas se faire entièrement sur la chaîne de blocs. (Il faudra utiliser ce qu'Ethereum appelle des oracles, qui ne sont pas pair-à-pair, donc posent un problème de confiance.)

Le monde Bitcoin, sans même parler des autres cryptomonnaies, est très actif en ce moment et des nouvelles propositions émergent tous les jours et d'innombrables essais sont lancés. Ce livre est donc un document utile pour avoir une vision relativement synthétique de l'état actuel de Bitcoin et de ses dernières évolutions. J'ai apprécié le côté ouvert de ce livre, qui présente des changements en cours, sans essayer d'imposer une vision unique.

Note : j'ai reçu (sans engagement) un exemplaire gratuit de ce livre par l'éditeur.
