Bitcoin : un prochain fork agité

Le 16 novembre prochain, au matin, un événement secouera le petit monde des monnaies cryptographiques : Bitcoin subira un nouveau fork, c'est-à-dire une nouvelle séparation en deux chaînes de blocs distinctes. Pourquoi ? Comment ? Est-ce bien nécessaire ?

Avec
H16

Le débat qui agite la communauté Bitcoin fait rage depuis deux ans et porte sur la méthode que la monnaie cryptographique doit suivre pour croître aussi harmonieusement que possible. Cette croissance passe par l'augmentation du nombre de transactions que le réseau peut supporter à chaque nouveau bloc, produit une fois toutes les 10 minutes environ.

Deux grandes écoles s'affrontent : la première vise à augmenter le nombre de transactions dans chaque bloc ce qui revient à augmenter la taille des blocs. La seconde entend faire porter la plupart des transactions en dehors de ces blocs et de ne reporter dans les blocs effectivement produits que des transactions de règlement global (settlement). Tout se résume donc à savoir si Bitcoin peut grossir en accroissant la taille de ses blocs ou en déportant une partie de plus en plus importante des transactions dans une seconde couche protocolaire (appelée Lightning Network).

Si, il y a deux ans, les deux options étaient ouvertes et le débat animé, les positions des uns et des autres se sont progressivement cristallisées et endurcies à tel point que les deux factions semblent maintenant irréconciliables.

La première école, tenante des « gros blocs », a déjà réalisé un premier fork en Août dernier que j'évoquais dans un précédent billet et qui a donné naissance au Bitcoin Cash. De façon intéressante, une partie des mineurs qui sécurisent la chaîne Bitcoin a rejoint les équipes de Bitcoin Cash et parallèlement, une majorité des mineurs sur le marché semble indiquer vouloir augmenter la taille des blocs aussi sur la chaîne historique.

La seconde école, dite Bitcoin Core, s'y refuse maintenant catégoriquement au point que les dissensions s'accumulent entre les mineurs (tenant d'un doublement de la taille des blocs) et les développeurs de Core.

Dans ce contexte et du point de vue extérieur d'un investisseur lambda, mettre de l'argent (ou laisser de l'argent) dans Bitcoin actuellement, c'est prendre de fait un pari risqué sur la capacité de tout un écosystème à surmonter ces dissensions internes d'autant que les deux familles ont des positions par nature antinomiques et ont un autre souci : les développeurs assurent la maintenance de l'applicatif, les mineurs assurent la sécurisation du réseau.

Autrement dit, on ne peut guère se passer ni des uns, ni des autres sur le plan technique.

Sur le plan économique, cependant, c'est plus complexe encore : les développeurs sont, par nature, achetables (même si un paquet de ceux travaillant sur Core sont maintenant millionnaires puisque bénéficiant des récentes montées de cours du Bitcoin). Les mineurs, par nature, ont lourdement investi pour leur infrastructure. Changer complètement de chaîne ou de méthode de travail leur coûterait potentiellement une fortune, ce qui leur impose un pragmatisme économique implacable. S'ajoutent à ces acteurs les échanges (plateformes de trading et d'achat/vente de bitcoin ou de cryptomonnaies) qui peuvent faire un choix politique en donnant ou non la possibilité aux acteurs de marché d'échanger ou non les cryptos produites ainsi qu'attribuer des tickers (des noms) à ces cryptos. Ainsi, un échange qui déciderait de donner le ticker « BTC » à la chaîne produite par les mineurs (Segwit2X) donnerait directement la possibilité aux acteurs de marché d'échanger ce bitcoin spécifique plutôt que le « bitcoin Core », et inversement.

Les autres acteurs économiques (traders, consommateurs lambda, commerçants) n'ont en réalité pas leur mot à dire puisque leurs échanges et leurs « votes économiques » ne sont comptés que lorsqu'ils font des transactions, transactions qui sont prises en compte par les échanges et enregistrées in fine par les mineurs. Restent les nœuds du réseau pair-à-pair, ceux qui ne minent pas et qui se contentent de valider les transactions : ces derniers peuvent choisir d'accepter ou non les bitcoins des uns ou des autres, mais en définitive ils n'ont pas d'impact réel tant qu'il existe au moins un nœud de chaque parfum donné, connecté à un ou plusieurs échanges.

Économiquement, les seuls acteurs pertinents du tableau sont donc les mineurs et les échanges qui déterminent quasiment à 100% dans quel sens le marché se comportera vis-à-vis de tout nouveau fork. Les autres acteurs seront obligés de suivre.

Concrètement, c'est actuellement une belle confusion entre les différents échanges et les mineurs : une super-majorité de ces derniers veulent S2X (c'est en tout cas ce qu'ils signalent), et les échanges semblent tendre à considérer que la nouvelle chaîne produite par ces derniers sera libellée B2X et non BTC, ce qui impactera directement son prix (l'acheteur/vendeur lambda voulant du BTC et pas autre chose).

Cette confusion signifie aussi que le fork sera potentiellement un moment de grande volatilité. Dans ce genre de situation, il faut être sûr de pouvoir acheter ou vendre rapidement, **ce qu'aucun échange ne pourra garantir** ; pire, cette situation pourrait durer le temps que les deux chaînes issues du fork se sécurisent correctement. Si 80% du hashrate (la puissance de calcul fournie par les mineurs) disparaît de la chaîne Core, la production du bloc de transactions suivant sera 5 fois plus lente, par exemple. Si le prix chute sur l'une des deux chaînes, les mineurs devront faire des choix économiques rapides pour rediriger leur puissance vers la chaîne la plus rentable. Les variations de cette puissance pourraient ajouter à la confusion, sans compter que, pour un mineur, basculer d'une chaîne B2X vers une chaîne Core ou même vers une chaîne Bitcoin Cash ne représente guère d'effort technique, mais seulement un pari économique.

Tous les ingrédients sont réunis pour une belle panique, ou, en tout cas, une volatilité importante du cours du Bitcoin. Si elle est temporaire, ceux qui seront sortis avant cette période pourront très bien se repositionner plus tard en rachetant à moindre coût les Bitcoins devenus meilleurs marchés lorsque la poussière retombera…

On devra donc agir avec prudence dans les prochaines semaines.

Sur le plan philosophique à présent, si on observe les comportements précis des communautés derrière les mineurs d'un côté et Core de l'autre, on remarque un autre souci : ce sont des communautés qui s'adressent à des publics très différents, et particulièrement étanches.

Les premiers sont essentiellement des business-men qui recherchent le profit et qui seront tenus, économiquement, de s'adapter à la donne, quelle qu'elle soit. Les seconds, en revanche, peuvent très bien faire fi des réalités économiques et se concentrer sur les aspects purement techniques. Ce n'est pas forcément gênant en soi, mais cela induit des pratiques qui ralentissent à l'évidence la pénétration du Bitcoin en tant que produit sur un marché particulièrement concurrentiel (à titre d'exemple, on pourra noter que le logiciel principal n'a pas évolué en ergonomie sur les sept dernières années).

Autrement dit : la communauté des mineurs vise à rendre le système capable de répondre à des demandes croissantes de transactions, ici & maintenant. En cela, ils rejoignent Bitcoin Cash, à tort ou à raison, qui cherche à fournir un système capable de traiter un nombre progressivement plus grand de transactions, directement sur la blockchain, sans passer par des inventions technniques supplémentaires.

A contrario, Core cherche à pousser les petites et nombreuses transactions en dehors de la chaîne principale (via Lightning Network), ce qui ne permet absolument pas de répondre aux besoins exprimés ici & maintenant, mais seulement à des besoins futurs, éventuellement, si les développements se passent bien et si le réseau se comporte comme prévu. Core propose dans le futur des réponses techniques fort complexes à des problèmes actuels dont la solution simple et rapide a déjà prouvé qu'elle fonctionnait (au moins sur les sept précédentes années de croissance du Bitcoin). De surcroît, pour l'utilisateur lambda, les techniques proposées sont particulièrement complexes à comprendre et à utiliser (je vous mets au défi d'expliquer les side-chains et Lightning Network à votre grand-mère).

On peut ergoter des heures sur les avantages comparés des techniques d'un côté et de l'autre. Il reste néanmoins que la vision initiale de Nakamoto consistait à créer une monnaie électronique sans tiers de confiance, utilisable par tout le monde. Un tel but nécessite d'apporter des réponses technologiques dont la sécurité et la facilité d'usage soient au moins égales à celle de l'argent liquide et des moyens de paiement électroniques qu'on connaît actuellement.

Or, depuis l'arrivée du Bitcoin, d'autres cryptos continuent à rechercher ce but. Bitcoin qui bénéficie jusqu'à présent de son avantage de premier arrivé et de son effet réseau, se fait progressivement grignoter des parts de marché. Les deux années écoulées sur ce débat trop animé, qui se terminent par ce fork délicat ont laissé du temps aux concurrents pour se solidifier. Peut-être ce fork permettra-t-il de clarifier les positions.

En tout état de cause, ces éléments imposent à mon sens la plus grande prudence concernant Bitcoin et les investissements qu'on pourra y faire dans les prochaines semaines.