Publié sur *CNRS Le journal* (https://lejournal.cnrs.fr)



Point de vue
Sociétés
Numérique
Économie

# Bitcoin, bien plus qu'une monnaie

22.02.2018, par Nicolas Houy et François Le Grand

Au-delà des transactions financières dématérialisées, la cryptomonnaie se distingue par son organisation expérimentale. Fondée sur une totale décentralisation, celle-ci lui a permis, jusqu'ici, de se développer. Lui permettra-t-elle de survivre ?

**Une fois par mois, retrouvez sur notre site les Inédits du CNRS, des analyses scientifiques originales publiées en partenariat avec Libération [8].**

Si vous avez entendu parler de Bitcoin récemment, c'est sûrement entouré d'autres mots comme *blockchain*, *smart contract*, une combinaison de trois lettres (XRP, BCH, ETH, etc.) ou un autre anglicisme plein de promesses de technologie indépassable… ou bien de faillite imminente doublée d'un gouffre énergétique. Or Bitcoin et les cryptomonnaies constituent avant tout une grande expérience économique, informatique et sociale.


Tout comme Ripple ou Bitcoin Cash, Ethereum et Litecoin font partie des 1500 cryptomonnaies apparue dans le sillage de Bitcoin



## Un protocole pour se passer de confiance

Créé en 2008 et utilisé dès 2009, Bitcoin – avec une majuscule - désigne un protocole informatique : une liste de règles et de normes permettant à des ordinateurs et à leurs utilisateurs de communiquer entre eux. De nombreux protocoles informatiques existent déjà et vous les utilisez quotidiennement. Ainsi, POP vous permet d'aller chercher vos courriels, HTTP vous permet de consulter des pages internet...

*Bitcoin est considéré par une grande partie de ses utilisateurs comme une expérience*

Le protocole Bitcoin a pour objet de garantir des droits de propriété exclusifs sur des unités de compte, les bitcoins - sans majuscule. La particularité de Bitcoin est que cette garantie ne vient pas d'une entité tierce mais repose au contraire sur un principe très fort : les utilisateurs doivent pouvoir ne faire confiance à personne et en particulier à aucune entité centrale.

Comment réaliser une telle prouesse dans un réseau numérique où les données peuvent facilement être dupliquées ? Bitcoin y parvient en mettant en œuvre une combinaison complexe d'algorithmes de cryptographie, d'incitations, et de contraintes économiques. A ce titre, la blockchain – le livre de compte numérique enregistrant toutes les transactions effectuées depuis la création du premier bitcoin - ne constitue qu'un aspect de cette machinerie complexe et est indissociable des autres éléments du protocole.

## Bitcoin et ses clones

Conséquence du principe d'absence de confiance a priori : le fonctionnement de Bitcoin doit être transparent et toute personne souhaitant le faire doit pouvoir vérifier sa mise en œuvre. Concrètement, cela signifie que Bitcoin doit reposer sur des règles ouvertes et accessibles à tous. A l'inverse, utiliser un protocole et un logiciel propriétaires, comme par exemple Skype, demande de faire a priori confiance à son développeur ou à son éditeur.

Comme le protocole est ouvert, celui-ci peut être copié, modifié et remis en circulation à volonté et par n'importe qui. Avec un peu d'aisance technique, créer votre propre version de Bitcoin ne vous demanderait que quelques heures. Aujourd'hui, derrière le terme générique de *cryptomonnaies*, on a la plupart du temps des protocoles dérivés de Bitcoin. Si certaines de ces cryptomonnaies, comme Ethereum par exemple, proposent une approche technologique différente, beaucoup de celles-ci ne sont que de simples clones, voire des arnaques. Cette génération spontanée de centaines ou de milliers de cryptomonnaies est donc une conséquence inévitable des principes de base qui régissent Bitcoin.


A l'intérieur d'une ferme de minage située au Canada. Les fermes de minage sont des sortes de data center dédiés aux calculs permettant de générer (miner) les cryptomonnaies.

© Christinne Muschi/Bloomberg via Getty Images

Même s'il pourrait sembler préférable de concentrer les efforts sur un seul protocole, cette ouverture est selon nous indispensable. En effet, en contribuant à la profusion de cryptomonnaies concurrentes, elle favorise l'amélioration continue de Bitcoin, constamment sous la menace de perdre sa position dominante. Bitcoin est d'ailleurs considéré par une grande partie de ses utilisateurs comme une expérience. Tout d'abord comme une expérience informatique dont la viabilité technique n'est pas encore acquise. Une expérience sociale également, dans laquelle les conflits au sein de la communauté ne se résolvent pas forcément par le consensus. L'ouverture du protocole permet que les désaccords se tranchent par la mise en circulation d'un protocole dérivé concurrent – on parle alors de *hardfork* - et ce sont finalement aux utilisateurs de choisir. Ainsi, l'année dernière, d'importantes différences de points de vue sont apparues autour des solutions à l’engorgement du réseau Bitcoin face à une utilisation croissante. Deux nouveaux protocoles implémentant des solutions techniques différentes, Bitcoin Cash et Bitcoin Gold, se sont séparés de la blockchain du

protocole Bitcoin principal : chaque utilisateur a alors pu choisir sa solution préférée, sans intervention d'une autorité supérieure.

## Une décentralisation créatrice

Cette volonté de décentralisation pourrait ainsi expliquer l'anonymat persistant de Satoshi Nakamoto, le créateur de Bitcoin.  Cette caractéristique conforte l'absence d'entité de référence et constitue un avantage unique -- certainement voulu par Satoshi lui-même. En effet, le développement de Bitcoin n'est ainsi plus soumis à l'approbation de son créateur, dont l'aura aurait pu influencer certaines décisions de la communauté quant à l'évolution du protocole, risquant de mettre à mal la décentralisation de la gouvernance de Bitcoin. Le contraste est d'ailleurs saisissant avec le protocole Ethereum dont le fondateur intervient toujours beaucoup dans le projet ; ce qui peut être interprété comme une rupture partielle du principe d'absence de confiance a priori.

Que penser de l'évolution et des mutations des multiples cryptomonnaies ? De nombreux scénarios sont envisageables. On peut imaginer une coexistence de quelques-unes de ces monnaies, chacune occupant une niche correspondant à un usage spécifique : réserve de valeur, transfert de micro-paiements, monnaie pour objets connectés, etc.

*Derrière le terme générique de cryptomonnaies on a la plupart du temps des protocoles dérivés de Bitcoin*

Toutefois, il est probable que beaucoup disparaitront lentement -faute d'utilisateurs désireux de les acquérir-, ou bien plus violemment, comme dans le cas de Coiledcoin, détruit en 2012 par des mineurs de Bitcoin. Dans tous les cas, chaque investisseur doit être conscient que l'argent investi dans une cryptomonnaie peut disparaître avec celle-ci. Après la phase de grande diversification que vient de connaître dans l'écosystème des cryptomonnaies, il faut nous attendre à une prochaine extinction de masse.

Nous pensons néanmoins que Bitcoin a plusieurs atouts qui devraient lui permettre de ne pas connaître le sort des dinosaures et de rester la cryptomonnaie de référence. Tout d'abord, les expériences passées - et les défis ont été nombreux !- ont montré son excellente résilience, démontrant à l'occasion la qualité des développeurs qui accompagnent sa croissance. Ensuite, Bitcoin est pour l'instant le seul protocole à avoir dû se poser la question de la montée en charge de son utilisation. Ainsi, pour des raisons de fiabilité, de sécurité et de stabilité, Bitcoin pourrait constituer la colonne vertébrale d'un futur système cryptomonétaire. Néanmoins, l'expérience Bitcoin est trop récente pour savoir si elle évoluera vers ce modèle ou bien disparaîtra à jamais.

*Les points de vue, les opinions et les analyses publiés dans cette rubrique n'engagent que leur auteur. Ils ne sauraient constituer une quelconque position du CNRS.*

---