COMPRENDRE BITCOIN et les CRYPTO-MONNAIES ALTERNATIVES

Cyril Fiévet

Cyril Fiévet

Comprendre Bitcoin et les crypto-monnaies alternatives

ISBN numérique : 979-10-262-0104-5

librinova

Courriel : contact@librinova.com

Internet : www.librinova.com

Avant-propos

A qui s'adresse ce livre ?

Les crypto-monnaies sont un sujet à la fois récent et complexe. Et, si l'on admet que c'est un phénomène, il est loin d'être parvenu à maturité, à tous les égards. L'immense majorité des gens sont donc encore dans une phase d'ignorance, d'apprentissage et de découverte.

On peut ainsi identifier quatre catégories de personnes, en fonction de leur niveau de familiarisation avec Bitcoin et les crypto-monnaies :

1. Les gens qui en ignorent tout, ou en ont vaguement entendu parlé mais sans savoir ce dont il s'agit.

2. Les gens qui ont une connaissance de base du sujet, via des articles de presse ou des articles sur Wikipedia, mais qui n'ont jamais utilisé Bitcoin ; ils savent que cela existe, mais ne comprennent pas forcément l'intérêt de Bitcoin et des crypto-monnaies.

3. Les gens qui utilisent Bitcoin en se limitant à un usage basique : ils ont "testé" la chose, possèdent un porte-monnaie, ont acheté du Bitcoin, et effectué avec quelques transactions ; ils comprennent l'intérêt et les avantages des crypto-monnaies, mais demeurent incertains quant à leur avenir.

4. Les gens qui font un usage avancé de Bitcoin et d'autres crypto-monnaies : ils sont "convaincus", possèdent plusieurs porte-monnaie, participent à la génération de ces monnaies (cf. ***Mining***), suivent l'actualité du domaine et achètent/vendent en permanence des crypto-monnaies alternatives sur les places de marché.

Ce livre s'adresse en priorité aux deux premières catégories de personnes, mais aussi aux gens de la troisième catégorie qui souhaitent évoluer vers la quatrième (si vous êtes dans la 4e catégorie, ce livre ne vous apprendra pas grand chose). Le contenu de ce livre est toutefois insuffisant pour réellement devenir un utilisateur avancé de Bitcoin et des crypto-monnaies. Mais il apporte un "vernis", ou une culture générale, destinés à aider celles et ceux qui voudraient aller plus loin qu'une utilisation basique de Bitcoin.

Pour le dire autrement, ce livre n'est pas destiné à former des experts sur le sujet, mais contient les informations nécessaires pour jauger de l'intérêt de Bitcoin et des crypto-monnaies, et progresser vers leur utilisation avancée – tout en sachant qu'il dépasse déjà largement les connaissances minimales nécessaires, et donc les besoins, de la plupart des utilisateurs de base de Bitcoin.

Comment lire ce livre ?

Il n'est pas nécessaire de lire ce livre de façon linéaire. On peut le faire, mais on peut aussi y piocher les réponses aux questions que l'on se pose, en fonction des besoins.

L'ouvrage comporte deux parties :

- une liste de questions fondamentales, dont les réponses apportent un éclairage général ;

- un lexique encyclopédique, qui ne se contente pas de fournir des définitions, mais apporte des détails plus avancés ou plus techniques,

tout en comportant une sélection de 150 sites Web permettant d'en savoir davantage.

Chaque réponse aux questions renvoie vers des mots du lexique, les entrées correspondantes étant identifiées par des mots en ***italique gras***.

1. Pourquoi s'intéresser à Bitcoin et aux crypto-monnaies ?

"Bitcoin fonctionne ! Il y aura d'autres monnaies similaires qui pourraient même être meilleures mais, en attendant, il s'est créé une vaste industrie autour de Bitcoin. Des gens ont fait fortune avec cette monnaie, d'autres ont perdu beaucoup d'argent, mais elle fonctionne dès à présent." – Richard Branson, PDG de Virgin, septembre 2014

Il y a deux ou trois ans, la plupart des articles de presse consacrés à Bitcoin étaient essentiellement négatifs. On évoquait un dispositif obscur, au mieux sans grand intérêt, au pire potentiellement dangereux. Beaucoup estimaient que Bitcoin était seulement une *"arnaque"*, évoquant les *"systèmes pyramidaux"* ou les *"systèmes de Ponzi"*, des mécanismes financiers frauduleux. D'autres soulignaient *"qu'on ne peut rien acheter en Bitcoin"* et qu'il s'agissait davantage *"d'un amusement pour informaticiens"* que d'une véritable monnaie.

Au fil du temps, un changement presque palpable s'est opéré. Au fur et à mesure que la popularité de Bitcoin grandissait, beaucoup se sont intéressés de plus près au fonctionnement et à la philosophie de Bitcoin, y découvrant des principes novateurs et un potentiel bien réels. De nombreuses entreprises spécialisées, proposant de nouveaux produits et services autour de Bitcoin sont apparues, partout dans le monde, participant à une forme "d'évangélisation" pour faire comprendre l'intérêt et la puissance de la crypto-monnaie. Gouvernements et banques centrales ont d'ailleurs dû prendre position et les déclarations officielles, même si elles demeurent souvent mitigées, attestent d'une prise de conscience quant à l'importance prise par Bitcoin – et sa réalité.

Cette réalité peut se mesurer. La capitalisation de Bitcoin, c'est-à-dire la valeur cumulée des *bitcoins* en circulation, représente à ce jour 5 milliards de dollars. L'un des fournisseurs de porte-monnaies électroniques Bitcoin, Coinbase, a dépassé en 2014 le cap des deux millions de clients, et il est admis qu'il existe aujourd'hui plus de 5 millions de gens possédant un porte-monnaie Bitcoin dans le monde. Il est probable que tous ces gens ne sont pas des utilisateurs acharnés de Bitcoin, mais il est facile d'admettre que des centaines de milliers le sont. Chaque jour, environ 85.000 transactions sont effectuées en Bitcoin, soit une transaction par seconde, représentant en cumul l'équivalent de plus de 50 millions de dollars échangés quotidiennement sous cette forme[1]. Sur Internet, le forum sur lequel se réunissent les utilisateurs les plus passionnés de Bitcoin et des crypto-monnaies, pour en débattre et s'échanger conseils et opinions, compte plus de 350.000 membres.

De nombreux commerces (plus de 70.000), qu'il s'agisse de magasins physiques ou en ligne, acceptent les paiements en Bitcoin. Un café dans un bar, une paire de chaussures dans une boutique physique, ou un billet d'avion acheté sur Internet peuvent être réglés avec Bitcoin, exactement comme on le ferait avec des billets en Euro ou une carte bancaire. Dans plusieurs grandes villes, aux Etats-Unis, aux Pays-Bas, en Espagne ou ailleurs, apparaissent aussi des "Boulevards Bitcoin", c'est-à-dire des rues dans lesquelles tous les commerçants, qu'il s'agisse de restaurants ou de magasins, ont décidé d'accepter Bitcoin. De même, les distributeurs automatiques de *bitcoins*, des machines se présentant comme les traditionnels distributeurs automatiques de billets, se généralisent dans la plupart des grandes villes. Il en existe dans une vingtaine de pays, y compris en France, en Belgique et en Suisse, et plusieurs constructeurs ont annoncé mi-2014 des plans de déploiement prévoyant l'installation de centaines de distributeurs, que ce soit aux Etats-Unis, en Europe ou en Asie. Et ces distributeurs, installés dans des bars, restaurants et lieux publics, n'ont rien de gadgets. Le tout premier distributeur Bitcoin installé dans le monde, fin 2013 à Vancouver, au Canada, a délivré en *bitcoins* l'équivalent de plus d'un million de dollars canadiens – en seulement 29 jours d'exploitation.

Certaines entreprises, notamment aux Etats-Unis ou en Irlande, commencent aussi à payer une partie des salaires de leurs employés en *bitcoins*[2]. Les investisseurs privés de s'y trompent pas et, rien qu'au deuxième trimestre 2014, les sociétés de capital-risque ont investi plus de 70 millions de dollars dans d'innombrables jeunes entreprises, qui se créent presque quotidiennement pour proposer des produits et services autour de Bitcoin.

Tout cela peut se résumer simplement : qu'on le veuille ou non, Bitcoin est une réalité, Bitcoin fonctionne et Bitcoin est en train de prendre une ampleur considérable.

Quand l'histoire se répète

Par bien des aspects, nous sommes en train de revivre ce que s'est produit à la fin des années 1990, quand le monde a découvert l'intérêt et le potentiel d'Internet, et de sa partie la plus visible, le World Wide Web. L'histoire avait démarré lentement et, en 1995, nous n'étions qu'une poignée, surtout en France, à nous intéresser à ce réseau bizarre qui permettait d'afficher – lentement – sur son ordinateur des pages en anglais, physiquement hébergées au bout du monde, le plus souvent sans image et uniformément grises. A l'époque, l'immense majorité des gens ignoraient tout d'Internet et ceux qui en avaient entendu parler le traitaient au mieux avec circonspection, au pire avec dédain.

Presque vingt ans plus tard, je me souviens avec un certain amusement des regards narquois de certains hauts représentants de l'élite économique et médiatique française, quand j'évoquais devant eux la future "révolution Internet", à laquelle j'avais d'ailleurs consacré mon tout premier livre. On m'expliquait volontiers qu'Internet était *"un truc d'informaticiens américains"*, qui *"ne marcherait jamais en France"*, et qui *"en aucun cas ne pourrait remplacer notre bon vieux Minitel"*. Quelques années plus tard, tandis que standards et protocoles s'affinaient, que la puissance des

modems augmentait et que, par milliers, de nouvelles entreprises produisaient du contenu, des produits et des services uniquement destinés au Web, on comprenait qu'Internet était là pour durer – et qu'il allait bien changer à tout jamais la diffusion d'information, l'organisation du travail, le commerce et les échanges de personnes à personnes. En en mot, qu'il allait transformer, en profondeur, la société mondiale.

Bien sûr, Bitcoin n'est pas le Web. Mais, quand on s'y intéresse, on perçoit la même excitation, la même énergie, la même volonté d'innover et de transformer l'existant qui animaient le petit monde de l'Internet entre 1995 et 1998. Et, bien sûr, on constate la même méfiance et le même scepticisme de la part de celles et ceux qui en ignorent tout – ou feignent d'en ignorer le potentiel par crainte de voir se métamorphoser, ou s'écrouler, le monde qu'ils connaissent.

Le bon moment

Pour les observateur attentifs de l'évolution d'Internet, dont beaucoup soufrent de voir ce qu'il est devenu, Bitcoin arrive au bon moment. Car, tandis que l'actualité financière des ces dernières années était marquée par des faillites de banques et une crainte généralisée quant à des systèmes bancaires que beaucoup jugent archaïques, Bitcoin et les autres crypto-monnaies font souffler un vent de renouveau sur un Internet qui a peu à peu perdu de son sens.

Internet et le Web ont beaucoup changé ces dernières années, mais pas forcément en bien. Les véritables innovations s'y font rares. De nouvelles start-ups, développant de nouveaux services et applications y apparaissent bien, mais ne proposent souvent que des copies de modèles existants. Une grande majorité des sites d'information cherchent moins à innover, ou à produire de la qualité, qu'à générer du *buzz*. Les réseaux sociaux ont bien apporté quelque chose, mais leur multiplication et leur démocratisation conduisent à un sentiment de saturation, tout en érigeant la procrastination

en vertu. Le Web – et ses utilisateurs – a sombré dans la facilité.

Ce faisant, Internet s'est abandonné aux affres de le centralisation, du monopole, du traçage et de la surveillance. Comme l'a révélé le scandale Snowden, les internautes et leur vie privée sont devenus quantités négligeables. Traités comme de simples "marchandises", ils sont échangés, épiés, manipulés même, tandis que la moindre de leur action en ligne – tout message, tout partage, toute photo, tout *"like"*, le moindre clic, en fait – est dûment enregistrée, stockée, comparée, analysée et, bien sûr, commercialisée.

Internet n'est plus, et depuis longtemps, cet espace de liberté qu'on nous avait promis, un réseau décentralisé et démocratique, un lieu "transparent" mis à disposition de tout citoyen. Au contraire, le Net est désormais totalement dominé par une poignée de "géants", qui en contrôlent les arcanes et en surveillent les utilisateurs. Il ne s'agit pas de fustiger ces entreprises, qui sont toutes des réussites formidables sur leurs marchés respectifs, mais de constater que, alors qu'on peut énumérer leurs noms sur les doigts d'une seule main, leur poids a dépassé la taille critique.

Internet s'apparente désormais davantage à une poignée de puissants monopoles qu'à un espace libre. Même si vous le souhaitiez, il vous serait quasiment impossible aujourd'hui d'utiliser Internet (ou votre téléphone mobile, du reste) – sans faire appel à aucun moment à un service appartenant à Google, Microsoft, Apple, Facebook ou Amazon. Dans une large mesure, ces cinq entreprises décident de la façon dont nous accédons aux réseaux, de ce que l'on peut y faire, de ce que l'on y voit (ou pas), de ce qu'on peut y acheter – et à quel prix. C'est un étrange paradoxe de constater qu'un réseau qui avait précisément été pensé et construit pour être totalement décentralisé s'est transformé quelques décennies plus tard en un système hiérarchique et quasi pyramidal.

Dans ce contexte, Bitcoin n'est pas seulement utile, mais pourrait s'avérer salutaire. Car les crypto-monnaies représentent un mouvement qui "vient du bas", c'est-dire des utilisateurs eux-mêmes. Bitcoin et les crypto-monnaies ne sont pas créées par des entreprises puissantes, imposant leurs produits à grands coups de marketing, mais par des individus qui cherchent

à innover en collaborant les uns avec les autres. Ces individus ne sont que des initiateurs, qui mettent des codes informatiques à disposition de tous, et s'appuient ensuite sur la communauté des internautes pour les faire connaître, les faire évoluer et les amener à se transformer en des systèmes qui fonctionnent. Et ces systèmes visent principalement un but unique : redonner le pouvoir aux utilisateurs d'Internet, en leur permettant d'échanger – des biens, des services, de l'information, de l'argent – en toute sécurité et sans utiliser d'intermédiaires inutiles.

Bitcoin n'est pas un service centralisé proposé par une multinationale. Il n'existe que par et pour les internautes qui l'utilisent. Bitcoin n'est pas non plus le nouveau site "branché" ou "à la mode", et encore moins l'appli "qu'il faut avoir" sur son smartphone dernier-cri pour ne pas paraître ringard. Ce n'est pas un énième Twitter, Instagram ou Tinder. Bitcoin est un concept. Et ce concept est si novateur que l'on ne peut aujourd'hui qu'en effleurer l'impact potentiel. Mais cet impact, qui se concrétise déjà sous des formes très diverses – à commencer par une monnaie comme il n'en a jamais existé dans l'histoire humaine –, sera profond et bien réel.

Bitcoin, un arbre devant une forêt

L'essentiel de la littérature consacrée aux crypto-monnaies se concentre sur Bitcoin. C'est naturel, car Bitcoin est la plus ancienne, la plus importante (en capitalisation) et la plus répandue des monnaies électroniques. Mais c'est un tort, car l'intérêt de Bitcoin ne réside pas tant dans la monnaie qu'il représente, que ce à quoi il a donné naissance.

La révolution (car c'est en une) qui se produit actuellement est la libéralisation et la démocratisation du concept de monnaie. Bitcoin est, pour l'instant, la partie la plus visible de cette révolution. Mais de nombreuses autres monnaies, souvent directement inspirées de Bitcoin et reposant sur des technologies parfois similaires, parfois bien distinctes, apparaissent sans relâche et sont également dignes d'intérêt.

Plusieurs milliers de ces "Altcoins", ou crypto-monnaies alternatives, ont été lancées ces dernières années, et plusieurs centaines d'entre elles sont toujours actives — et parfois très actives. Quelques-unes de ces monnaies, y compris créées tout récemment, témoignent d'une forte maturité conceptuelle, apportant de réelles innovations, destinées à améliorer ou enrichir les principes de base de Bitcoin. Si toutes ne survivront pas à moyen ou long terme, elles forment néanmoins un écosystème riche et vaste, duquel pourraient émerger de nouvelles plate-formes de paiement et d'échange très novatrices.

Car il faut comprendre que les principes clés mis en oeuvre par Bitcoin et les crypto-monnaies servent principalement à garantir la sécurité ou la confidentialité d'échanges entre personnes. Dès lors, rien n'oblige à limiter ces principes à des applications financières et monétaires. Pourquoi ne pas utiliser les mêmes procédés pour créer d'autres types d'applications, qui n'ont rien à voir avec des monnaies, comme des messageries électroniques, des services d'échange de fichiers, des dispositifs de stockage partagé, voire des réseaux sociaux d'un genre nouveau ?

De fait, toutes ces applications (et d'autres) sont en gestation, et certaines commencent à apparaître, laissant entrevoir un renouveau sur Internet d'une ampleur considérable. Qu'on ne s'y trompe pas, ce qui se déroule actuellement dans l'univers encore confidentiel des crypto-monnaies revient bel et bien à repenser l'Internet au travers de la technologie mise en oeuvre par Bitcoin, en particulier le principe de "chaîne de blocs", via des services et des applications décentralisés, maintenus et contrôlés par les utilisateurs eux-mêmes – et uniquement par eux.

Il faudrait être fou, ou outrageusement pessimiste, pour penser que toute cette énergie, ces idées, ces technologies innovantes et éprouvées, ces centaines de milliers d'utilisateurs, ces milliers d'informaticiens et d'entrepreneurs, travaillant de concert dans un même but, n'auront été qu'un feu de paille et ne débouchent sur rien.

Au contraire, il faut s'attendre à des changements multiples et profonds, tant dans les outils dont nous disposons au quotidien, que dans les mécanismes – financiers, juridiques, économiques, politiques même –

établis de longue date. Et il est facile d'admettre que tout cela fasse grincer des dents. Bitcoin et les crypto-monnaies menacent les monopoles en place. Et c'est d'ailleurs bien l'intention des artisans de cette transformation, qui entendent changer l'existant, bousculer les privilèges, s'affranchir des intermédiaires et redonner le pouvoir aux internautes.

Pour toutes ces raisons, Bitcoin et les crypto-monnaies alternatives méritent qu'on s'y intéresse de près. C'est un univers fascinant, en pleine évolution, dont surgiront sans aucun doute des innovations qui transformeront en profondeur non seulement Internet, mais les règles et systèmes établis dans l'organisation de notre société.

Bien sûr, Bitcoin est complexe. On peut en expliquer l'intérêt en une phrase, mais un livre entier ne suffit pas à en détailler le fonctionnement et les mécanismes sur lesquels il s'appuie. Même si l'on peut devenir utilisateur d'une crypto-monnaie quelconque en quelques minutes, il faut y investir du temps pour en comprendre les arcanes. Mais l'enjeu est à la hauteur de l'effort car, pour la toute première fois dans l'Histoire, nous – individus, citoyens, internautes – pouvons disposer de monnaies, de dispositifs et d'applications dont nous – et uniquement nous – sommes les maîtres.