getabstract
compressed knowledge

Classement ?
8

Caractéristiques clés ?
Pratique
Complet
Bien structuré

Acheter le livre ou le livre audio

Bitcoin & cryptomonnaies faciles

Comprendre les monnaies numériques et leurs enjeux économiques et politiques

Claire Balva, Gwendal Fossois et Alexandre Stachtchenko • First Éditions © 2022 • 192 pages

Conseils de vie / Retirement / Argent
Économie / Marchés financiers / Cryptomonnaies

Points à retenir

- Notre système monétaire mondial a connu un bouleversement majeur au lendemain de la Seconde Guerre mondiale.
- La naissance de Bitcoin est auréolée de mystère. L'identité de son créateur, Satoshi Nakamoto, reste inconnue à ce jour.
- Première monnaie numérique décentralisée, Bitcoin repose sur deux concepts fondamentaux.
- D'autres cryptomonnaies, telles que Ethereum, Litecoin, Solana et Avalache concurrencent Bitcoin.
- Les particuliers et les entreprises investissent de plus en plus dans la cryptoéconomie.
- En proposant des solutions décentralisées et plus résilientes, les cryptomonnaies sont à même de répondre aux problématiques actuelles de notre monde.

Commentaires

Parfois appelées cryptoactifs, cryptodevises ou actifs virtuels, les cryptomonnaies suscitent tout autant la méfiance que la curiosité. Malgré tout, une chose est sûre : l'intérêt pour la monnaie virtuelle ne cesse de croître. Alexandre Stachtchenko et Claire Balva, tous deux spécialistes des cryptomonnaies, nous invitent à découvrir l'univers de la monnaie virtuelle, ses enjeux politiques et économiques ainsi que les défis auxquels elle est confrontée. Un livre utile pour démystifier les cryptomonnaies et répondre à une question fondamentale : faut-il avoir peur des cryptoactifs ou sont-ils au contraire porteurs d'espoir ?

Résumé

Notre système monétaire mondial a connu un bouleversement majeur au lendemain de la Seconde Guerre mondiale.

Jusqu'au XX^{e} siècle, le système monétaire mondial était indexé sur les métaux précieux. Les États et les banques devaient disposer de suffisamment de réserves d'or et d'argent pour inspirer confiance et éviter que le système déraille. Mais les accords de Bretton Woods de 1944, au lendemain de la Seconde Guerre mondiale, mettent fin à l'étalon-or et instaurent un système monétaire mondial centré sur le dollar américain. Désormais, seul le dollar américain est convertible en or, les autres monnaies, elles, devenant uniquement convertibles en dollars. En 1971, Nixon met fin à la convertibilité du dollar en or, de nombreux États s'étant insurgés contre un système monétaire fortement discutable et contre le « privilège exorbitant » dont disposaient les Américains. Néanmoins, le dollar, jouissant d'une « confiance par défaut », reste l'étalon monétaire mondial.

> *« Depuis la fin de la guerre froide, le dollar ne représente ni ne vaut rien, si ce n'est lui-même, mais sa garantie par la puissance américaine soutient son statut de monnaie de référence. »*

Aujourd'hui, nos monnaies nationales ne sont plus frappées en or, le billet de banque est devenu une monnaie fiduciaire et sa valeur repose sur l'assurance qu'il sera accepté comme moyen de règlement par les différentes parties prenantes. Ainsi, toute transaction effectuée de manière numérique ou en liquide dépend d'un intermédiaire – ou tiers de confiance. La valeur de notre argent est donc dépendante d'une autorité centralisée, et c'est là que le bât blesse. En effet, plus les moyens de paiement se diversifient et plus le nombre de ces tiers de confiance augmente, ce qui coûte non seulement du temps et de l'argent, mais génère également des doutes quant à la fiabilité de ces derniers. L'avènement d'Internet et du numérique a accentué ces doutes, car nos échanges sont désormais traçables et nos comptes consultables en ligne. Par ailleurs, la surabondance d'intermédiaires s'accompagne de risques tels que l'exclusion financière, si l'accès au système bancaire n'est pas garanti, et d'une surveillance accrue par les banques et les États.

> *« La monnaie, donc, dans son fonctionnement actuel, repose sur une sorte de pacte faustien : en échange de la rapidité et de la simplicité des paiements, nous offrons aux intermédiaires, et en particulier aux banques commerciales, une fenêtre directe sur l'ensemble de notre vie privée […]. »*

C'est dans ce contexte que Bitcoin a émergé, non seulement en tant que réponse à un système monétaire à la dérive et des crises financières dévastatrices, mais également comme un rempart contre les assauts répétés – nourris par le développement d'Internet – à l'encontre de notre vie privée. C'est donc grâce à l'idéologie d'un petit groupe d'individus férus de cryptographie, les « cypherpunks » qu'apparaît Bitcoin en 2008. C'est en anticipant les dangers liés au développement du web que le mouvement cypherpunk a formulé son idéologie reposant sur des thèmes tels que la défense de la liberté d'expression et d'information, la mise en garde sur les risques des systèmes actuels et des solutions pour protéger la sphère privée.

La naissance de Bitcoin demeure auréolée de mystère. L'identité de son créateur, Satoshi Nakamoto, reste inconnue à ce jour.

Le réseau Bitcoin est né dans le contexte de la crise financière de 2008, qui a mis en lumière la fragilité structurelle des banques et les risques toxiques sur l'économie en cas de défaillance bancaire. La cryptomonnaie (bitcoin avec un « b » minuscule) est présentée comme la solution à des problèmes qui soulèvent de vives préoccupations tels que la centralisation, les cyberattaques et la surveillance.

> *« Cet "or numérique", [Bitcoin] comme il est parfois qualifié, esquisse les bases de la monnaie de demain en redonnant du pouvoir à ses utilisateurs et ouvre la voie à un renversement du système monétaire mondial largement basé sur le dollar depuis le siècle dernier. »*

Une aura de mystère entoure la naissance de Bitcoin. Impossible de savoir précisément qui l'a créé, quels étaient les objectifs visés ou les grands axes de l'idéologie qu'il défend. Toutefois, la légende en attribue la paternité à un certain Satoshi Nakamoto, qui aurait publié en 2008 un livre blanc intitulé *Bitcoin : un système de paiement électronique pair-à-pair* faisant suite à l'enregistrement deux mois plus tôt du nom de domaine bitcoin.org. Une première version du logiciel Bitcoin est conçue en janvier 2009 et la première transaction en cryptomonnaie a lieu entre Satoshi Nakamoto et Hal Finney, un développeur cypherpunk. Une deuxième, puis une troisième version du logiciel est développée, ainsi qu'une plateforme de jeu permettant d'échanger des bitcoins. Alors que le phénomène bitcoin prend de l'ampleur, son inventeur, Satoshi Nakamoto, publie un dernier message en décembre 2010 et disparaît purement et simplement, entretenant davantage le mystère autour de son personnage.

> *« Aujourd'hui encore, cette inconnue persiste et contribue à la sécurité de Bitcoin : sans fondateur identifié, la gouvernance peut être réellement décentralisée. »*

Le livre blanc publié par Satoshi Nakamoto en 2008 entendait répondre à une problématique : comment contourner le phénomène de « double dépense » lié aux transactions effectuées par le biais d'une monnaie numérique ? En d'autres termes, comment garantir, sans l'intervention d'un tiers de confiance, qu'une unité de compte n'est pas – frauduleusement – dupliquée ? Pour Satoshi Nakamoto, cette démarche n'est possible qu'à plusieurs conditions. Il faut d'abord que les transactions soient enregistrées dans un registre numérique infalsifiable (la « blockchain »). De plus, le système doit être résilient et indépendant de toute autorité ou entité. Ensuite, comme ces transactions sont publiques et vérifiables par tous, il n'y a plus lieu de faire appel à un tiers de confiance. Néanmoins, la confidentialité est respectée grâce à la cryptographie « asymé-

trique », qui garantit l'intégrité de la transaction sans révéler l'identité des participants. Enfin, les bitcoins sont soumis à une émission monétaire maximale (21 millions) et dégressive (la limite sera atteinte en 2140).

Première monnaie numérique décentralisée, Bitcoin repose sur deux concepts fondamentaux.

Le premier concept propre au réseau Bitcoin est la *blockchain* (ou « chaîne de blocs ») qui désigne un grand livre comptable numérique dans lequel sont enregistrées toutes les transactions en bitcoins. Ce registre est dupliqué sur de nombreux serveurs à travers le monde et se met à jour de manière automatisée. Il est constitué de blocs numériques « chaînés » les uns aux autres par ordre chronologique, le premier datant du 3 janvier 2009. Les transactions sont inscrites dans ces blocs (les « pages » du grand livre), un bloc de transactions s'ajoutant toutes les dix minutes. Hébergé sur des serveurs aux quatre coins de la planète, le registre numérique est décentralisé et accessible à tous, ce qui garantit son indépendance.

> *« La gouvernance de Bitcoin est ainsi décentralisée, ce qui garantit son indépendance vis-à-vis des États, des entreprises et des institutions. »*

Le deuxième concept sur lequel repose Bitcoin est le concept de « minage ». Pour garantir la décentralisation, l'enregistrement des transactions est effectué par la communauté ou des « mineurs », qui remplacent le tiers de confiance. Chaque mineur crée un nouveau bloc à partir des transactions en attente de confirmation, puis s'attache à résoudre une équation mathématique pour valider le bloc, une démarche désignée par le terme de « preuve de travail » (PoW ou *Proof-of-Work*). Les mineurs sont donc en concurrence, et celui qui résout le premier l'équation est rétribué en bitcoins et peut ajouter le bloc de transaction à la blockchain. Pour éviter que l'appât du gain ne pousse les mineurs à accaparer plus de 50 % de la puissance de calcul grâce à un équipement informatique surdimensionné – ce qui contribuerait à recréer un système centralisé –, le système Bitcoin envoie un signal de défaillance (et donc une chute du cours de la cryptomonnaie) s'il détecte qu'une majorité de bitcoins est minée par la même communauté d'individus.

D'autres cryptomonnaies, telles que Ethereum, Litecoin, Solana et Avalache, concurrencent Bitcoin.

Bitcoin a fait de nombreux émules. En effet, on dénombre pas moins de 20 000 cryptomonnaies différentes en 2022, même si Bitcoin représente près de la moitié de la valeur du marché. Son grand rival, le protocole Ethereum créé en 2015 par Vitalik Buterin pour gérer des opérations financières plus élaborées que les simples transferts, a permis le développement de la tokenisation ainsi que d'autres applications décentralisées. Ethereum fonctionne selon le même principe de blockchain et de minage par la puissance de calcul que Bitcoin, mais il s'en distingue malgré tout de manière significative. D'abord parce que les blocs de transactions peuvent être créés à des intervalles plus courts. Ensuite, parce que le protocole Ethereum ne fixe aucune limite sur la quantité des « ethers » à miner et enfin, parce qu'il est possible, via des tokens, de créer d'autres cryptomonnaies, telles que les jetons stables (*stablecoins*) ou les jetons non fongibles (*Non Fongible Tokens*) sur sa blockchain. Litecoin, Solana et Avalache sont d'autres cryptomonnaies qui tentent de concurrencer Bitcoin et Ethereum.

> *« La DeFi peut améliorer l'accès à des services financiers pour tous, où que vous vous trouviez sur la planète : il suffit de disposer d'une connexion Internet. L'enjeu est de taille, quand on se rappelle que 1,7 milliard de personnes n'ont pas accès aux services financiers de base. »*

L'essor des cryptomonnaies a contribué au développement du concept de « finance décentralisée », (DeFi ou *Decentralized Finance*). Cet écosystème financier alternatif fonctionne de manière automatisée, décentralisée, transparente, sans intermédiaire et permet à tout un chacun de le consulter, de l'utiliser ou de le développer. La DeFi est composée de services, ou applications décentralisées (les Dapp), qui « répliquent les usages financiers classiques » et qui sont accessibles à partir d'un portefeuille numérique (un *wallet*). Malgré son succès la DeFi n'a pas encore réussi à détrôner la finance classique et centralisée, notamment en raison de sa complexité technique, de problèmes inhérents de liquidités ainsi que du flou réglementaire qui règne dans ce domaine.

Les particuliers et les entreprises investissent de plus en plus dans la cryptoéconomie.

Si le nombre de détenteurs de cryptos dans le monde reste marginal, il continue en revanche d'augmenter chaque année. Selon Brian Armstrong, directeur de Coinbase, « un milliard de personnes devraient avoir adopté ou essayé des cryptos » d'ici 2032 et celles-ci pourraient à terme représenter une part importante du PIB mondial. Aux États-Unis, 16 % des habitants ont déjà investi dans la cryptoéconomie et en France, ils sont 8 % à avoir franchi le pas. Il s'agit en général de jeunes hommes adultes instruits et, en ce qui concerne la France, près de la moitié des détenteurs ont entre 18 et 35 ans. Les entreprises ne sont pas en reste et investissent dans les cryptomonnaies afin de diversifier leur trésorerie.

> *« Signe de son dynamisme exceptionnel, ce secteur se développe énormément, et en peu de temps : 30,5 milliards de dollars ont été investis en 2021 à travers différentes levées de fonds, soit un bond énorme par rapport à l'année précédente (+ 450 %). »*

L'industrie des cryptomonnaies est aujourd'hui caractérisée par trois acteurs clés :

1. Les mineurs/validateurs : aujourd'hui la puissance de calcul nécessaire au minage (200 millions de TH/s en 2022) et les coûts qu'elle implique en termes d'équipements fait qu'il est impossible pour des particuliers de devenir mineurs. Cette tâche s'est professionnalisée et est désormais prise en charge par des entreprises telles que Bitmain ou Bitfury, de véritables géants dans leur domaine.
2. Les plateformes d'échange : ces plateformes, telles que Coinbase, FTX et Binance, gèrent l'achat et la vente de cryptomonnaies et constituent le « lien privilégié entre le monde crypto et le système monétaire traditionnel ».
3. Les solutions de conservation : ces sociétés proposent des solutions de stockage de clés privées pour accéder à votre portefeuille de cryptomonnaies. Elles sont divisées en deux catégories : celles qui proposent des « solutions d'autoconservation » (c'est vous qui détenez vos fonds) et celles qui proposent des solutions de conservation par un tiers.

En proposant des solutions décentralisées et plus résilientes, les cryptomonnaies sont à même de répondre aux problématiques actuelles de notre monde.

Le Covid-19 a remis en question le fonctionnement même de nos sociétés. L'économie mondialisée, fortement centralisée et spécialisée, a montré ses limites et son incapacité à trouver des solutions lorsque les masques et les médicaments sont venus à manquer en pleine pandémie, par exemple. Les cryptomonnaies, qui proposent des solutions décentralisées et plus résilientes, semblent aujourd'hui bien placées pour répondre à ces problématiques. Par ailleurs, la forte dépendance à l'État et aux banques pose la question du respect des libertés individuelles, comme on a pu le voir lors de l'imposition du pass sanitaire. Les cryptomonnaies sont, dans ce contexte, idéalement positionnées, car elles sont totalement indépendantes des États et des institutions. Enfin, les cryptomonnaies apportent également une réponse à la création excessive de monnaie, qui s'est traduite par un retour de l'inflation. En effet, l'émission de Bitcoin étant limitée et transparente, les cryptomonnaies peuvent ainsi proposer une solution d'épargne dotée d'une politique monétaire « programmée, transparente et prévisible ».

> *« La crise a été une nouvelle occasion de questionner certains piliers de nos modèles de société, et par là même de rendre les cryptos plus attractives. »*

Les transactions en cryptomonnaies progressent avec l'entrée en scène d'acteurs financiers traditionnels, comme les banques centrales, qui proposent leurs propres monnaies numériques – les MNBC (monnaies numériques de banque centrale). Les MNBC de détail sont destinées au grand public, alors que les MNBC de gros s'adressent principalement aux banques. Toutefois, ces MNBC, développées essentiellement pour contrer la concurrence des cryptomonnaies, soulèvent de nombreuses interrogations. La question de la confidentialité est au centre de ces préoccupations, puisqu'un compte en MNBC permettrait à une banque centrale d'accéder à toutes les transactions d'un individu. Se pose également la question de la faisabilité au niveau technique. Quant aux cryptomonnaies, même si elles sont fortement critiquées pour leur impact environnemental – en raison de la consommation énergétique excessive qu'implique leur fonctionnement –, elles représentent une alternative intéressante pour les pays dont la monnaie est fréquemment dévaluée et où les populations sont particulièrement peu bancarisées.

À propos des auteurs

Alexandre Stachtchenko et **Claire Balva** ont cofondé en 2015 Blockchain Partner, un cabinet d'expertise et de conseil aux entreprises spécialisé dans les cryptomonnaies, désormais intégré chez KPMG France. Ils sont également cofondateurs de l'ADAN, l'association des professionnels cryptos en France. Reconnus pour leur expertise et leur pédagogie, ils prennent régulièrement la parole dans les médias et lors de conférences pour expliquer le fonctionnement et les enjeux de ces nouveaux actifs.