Jean-Guillaume DUMAS • Pascal LAFOURCADE • Etienne ROUDEIX
Ariane TICHIT • Sébastien VARRETTE

LES NFT

EN 40 QUESTIONS

–

Comprendre les Non Fungible Tokens

DUNOD

Couverture : Studio Dunod

© Dunod, 2022
11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-083304-7

Table des matières

Avant-propos

En 2022 et pour la plupart des citoyens, le quotidien monétaire est fait de monoculture : une seule monnaie, émise par un seul type d'institutions (les grandes banques commerciales), selon un seul critère (le crédit), concentrant toutes les fonctions (unité de compte, moyen d'échange et de paiement, réserve de valeur et objet de spéculation), avec des unités n'ayant pas de marques spécifiques ou de données particulières qui leur sont attachées. Elles sont donc indistinguables les unes des autres (équivalentes et donc *fongibles*) et cela depuis des centaines d'années. L'unicité et la fongibilité de la monnaie semblent tant procéder d'un ordre naturel qu'il s'avère épineux et délicat de les remettre en question. Il est dès lors difficile de se figurer à quoi pourrait ressembler un monde fait de diversité et quelles en seraient les conséquences.
Toutefois, depuis les années 2000 et en particulier depuis la crise de 2008 qui a révélé la fragilité d'un système monétaire monoculturel, de nombreux projets monétaires alternatifs ont vu le jour. Ceux-ci sont très variés et vont des systèmes d'échanges locaux (SEL) et autres clubs de trocs, jusqu'aux cryptomonnaies, en passant par les monnaies locales et régionales. Au total ce sont plus de 10 000 monnaies alternatives qui circulent en 2022 dans le monde. Parmi tous ces projets, les plus nombreux sont ceux concernant les cryptomonnaies.

En effet, depuis l'apparition de Bitcoin et de la technologie **blockchain** en 2008, plus de 6 700 cryptomonnaies ont désormais vu le jour. Bien évidemment afin d'en tirer profit, certaines reprennent simplement des codes déjà implémentés et bien rodés et surfent simplement sur la vague sans vraiment apporter de contributions. Mais parmi les développements récents, il en est un qui attire tout particulièrement l'attention en semblant à la fois prometteur et porteur de changements majeurs dans la structure même de nos sociétés et de ses institutions : les **NFT** (*Non Fongible Tokens*). Ces objets sont issus de l'utilisation et de la démocratisation des contrats intelligents (*smart contracts*), un des concepts innovants émanant des développements de la blockchain Ethereum. Non contents de remettre en question la monoculture monétaire, ces objets viennent également bousculer la notion de fongibilté, en proposant des jetons numériques qui, par les caractéristiques qui leur sont associées, sont uniques.

Apparus en 2017, ils connaissent depuis une croissance phénoménale qui ne cesse de s'accélérer et concentrent l'attention des médias et des individus qui s'en sont très vite emparés. Le public ne s'y trompe pas : leurs applications potentielles sont énormes et couvrent des domaines de plus en plus divers. Nous ne sommes en réalité qu'aux prémices de leur déploiement et de leur généralisation. Toutefois, si beaucoup d'informations circulent auprès du grand public, peu d'éléments sont donnés sur leurs fondements techniques et leurs caractéristiques véritables, ce qui ne permet pas toujours de saisir toute la mesure de ces innovations comme de leurs potentialités.

Dès lors, l'objectif de cet ouvrage, construit en 40 questions, est dans un premier temps de faire comprendre comment fonctionnent les technologies de registres distribués, les blockchains et les contrats intelligents qui sont à la base des NFT. Le second objectif est d'expliquer comment les NFT fonctionnent véritablement aussi bien d'un point de vue technique que de l'usage concret qui en est fait actuellement.

Dans cette optique, la première partie de cet ouvrage aborde les grands principes fondateurs des blockchains, des cryptomonnaies et des contrats intelligents. Dans la deuxième partie, les caractéristiques spécifiques des NFT sont exposées, avant d'aborder, dans une troisième partie, leurs utilisations dans différents domaines (art, sport, mode, paris, etc.) La quatrième partie explore ensuite les éléments économiques, financiers et juridiques que génèrent les NFT. Enfin, la dernière partie revient sur les outils et concepts techniques utiles à la compréhension détaillée des mécanismes sous-jacents aux NFT.

Les auteurs remercient chaleureusement Frédéric Hayek et Corentin Élissé pour leurs contributions à l'élaboration du contenu de ce livre.

Les auteurs expriment également leur gratitude à Jean-Luc Blanc et Maxine Pouzet pour leurs commentaires et suggestions de modifications constructifs, à la suite de leurs relectures assidues.

Grenoble, Clermont-Ferrand, Luxembourg, le 24 mars 2022.
Jean-Guillaume Dumas, Pascal Lafourcade,
Étienne Roudeix, Ariane Tichit, Sébastien Varrette.

1

Blockchains et cryptomonnaies

1 Qu'est-ce qu'une blockchain ?

Au plus fort de la crise économique de 2008, une nouvelle façon de concevoir la monnaie a été proposée au sein d'un article posté sur Internet et intitulé *Bitcoin : A Peer-to-Peer Electronic Cash System* [13]. Dans cet article, un certain Satoshi Nakamoto décrivait un nouveau système d'émission et de gestion d'unités monétaires, appelé *bitcoin*, qui reposait sur une structure de données de type *a Distributed Ledger Technology (DLT)* et appelée *blockchain* [5, Q. 2].

Par analogie avec les registres classiques dans lesquels les transactions sont regroupées sur des pages, les transactions sont ici agrégées au sein de *blocs* digitaux chaînés entre eux, d'où le terme de blockchains qui désigne dans la suite de cet ouvrage une chaîne de blocs. Dans cette structure de données, les transactions *confirmées* (ou validées) sont intégrées dans des blocs bénéficiant d'un identifiant « unique » dépendant de son contenu, signature * qui est obtenue par une empreinte de hachage ◇. Chaque bloc contient la signature de l'empreinte du bloc précédent de la chaîne, ce qui permet de garantir l'intégrité de l'ensemble des enregistrements et des données de la blockchain à partir du premier bloc, appelé bloc « *Genesis* ».

Les mineurs valident les transactions

Lorsqu'une nouvelle transaction est émise, elle doit être validée. Pour cela, elle est propagée aux les participants dans un ensemble de transactions *non confirmées*. Certaines de ces transactions sont choisies par un *mineur* ↯ pour intégrer un nouveau bloc. Les mineurs valident ces transactions selon des techniques dépendant du type de blockchain. Cette orchestration est illustrée dans

* Une signature électronique (*cf.* question **34**) est utilisée pour prouver l'identité du signataire.

◇ Une empreinte de hachage permet d'obtenir à partir de n'importe quelle entrée une sortie de taille fixe (*cf.* question **33**). L'empreinte ainsi créée ne permet pas d'être inversée pour revenir au message initial.

↯ Un mineur est un participant à la création de nouveaux blocs sur une blockchain. Dans le cas de la *preuve de travail,* utilisée au sein du bitcoin, le mineur va mettre à disposition sa puissance de calcul afin d'être rémunéré par l'émission de nouvelle monnaie (amenée par l'action de minage) et/ou les éventuels frais de commission (*cf.* question **3**).

la figure 1.1. Chaque bloc ne contient pas nécessairement un nombre fixe de transactions. Une fois validé, un bloc est horodaté et ajouté à la blockchain.

Il y a plusieurs modèles de déploiement de ce type de structure, mais c'est une implémentation distribuée au-dessus d'un réseau pair-à-pair, en anglais *Peer-to-Peer (P2P)*, comme celle proposée dans l'article fondateur de bitcoin qui permet d'obtenir un DLT tel que défini précédemment [13]. Ainsi, chaque nœud du réseau possède et maintient une copie cohérente et identique de la blockchain. Il convient alors de définir les mécanismes décentralisés permettant de :

1. distribuer de nouveaux blocs à tous les nœuds impliqués ;
2. valider les transactions et plus généralement les blocs ;
3. assurer la cohérence éventuelle de toutes les copies de la blockchain.

Ces mécanismes dépendent du système de blockchain considéré. Grâce à eux, une blockchain constitue une **base de données publique**, **distribuée**, c'est-à-dire partagée par ses différents utilisateurs, **sans autorité centrale**, **fiable et inviolable**. Ainsi elle peut être assimilée à un grand livre des comptes, *public*, *infalsifiable* et *vérifiable*.

La blockchain est infalsifiable car toute modification d'un bloc dans la chaîne la rend incohérente. En effet, tout bloc est référencé dans le bloc suivant de la chaîne, lui-même référencé dans le bloc suivant, etc. Cette référence est entièrement déterminée par le contenu du bloc et est différente pour chaque variation, même infime : ceci est assuré par l'utilisation d'une empreinte de hachage cryptographique de ce bloc. Pour altérer une partie de la chaîne, il faudrait donc être capable de modifier la totalité des blocs à partir de la modification et cela tellement rapidement que l'ensemble du réseau mondial (qui scrute, vérifie et augmente la chaîne constamment) ne peut s'en apercevoir.

Les raisons du succès des blockchains

Les technologies de type blockchain sont devenues populaires avec le succès grandissant de bitcoin et le développement d'autres systèmes dérivés tels que Ethereum (*cf.* question **7**), Ripple, ou Litecoin. Néanmoins, cette technologie ne se limite pas seulement au domaine économique et monétaire. L'utilisation de la blockchain se répartit principalement en trois domaines :

1. les applications pour le transfert d'actifs, dans le cadre d'une utilisation monétaire *via* les cryptomonnaies (*cf.* question **2**), des titres, des actions ou des obligations ;
2. les applications de la blockchain en tant que DLT, assurant ainsi une bien meilleure traçabilité des produits et des actifs ;

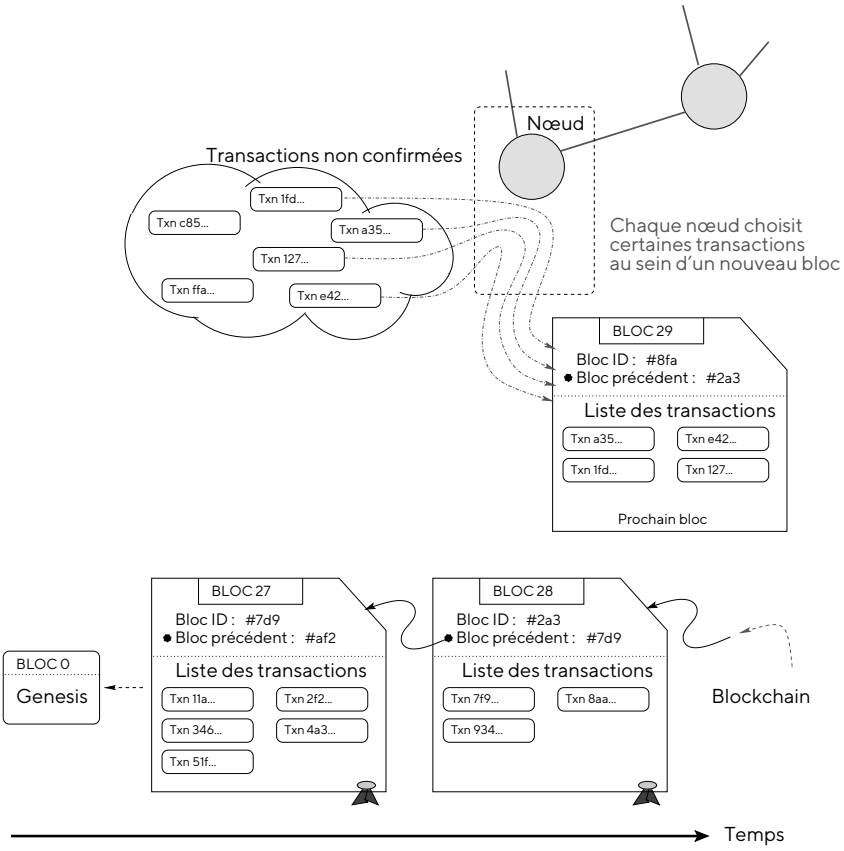

Figure 1.1 – Exemple simplifié d'une structure de données de type blockchain. Les transactions confirmées sont agrégées en blocs certifiés qui sont ajoutés en bout de chaîne à travers un pointeur vers l'empreinte du bloc précédent, formant ainsi une seule et unique chaîne répliquée à travers tout le réseau. Les participants sont aussi appelés des nœuds du réseau distribué que forme la blockchain.

3. les contrats intelligents (*cf.* question **6**) *i.e.*, des programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés. C'est ce dernier cas qui a donné naissance aux jetons non fongibles – *Non-Fungible Token (NFT)* –, le sujet principal de ce livre (*cf.* **parties 2**, **4** et **5**).

Les types de blockchains

Il existe plusieurs types de blockchains : les blockchains publiques, les blockchains privées ou, entre les deux, les blockchains de consortium.

Les *blockchains publiques* sont par définition ouvertes et accessibles à tous. En particulier, tout le monde peut participer aux transactions (et ainsi espérer les voir incluses dans la blockchain sous réserve de validité), mais aussi collaborer aux opérations de *consensus* de la blockchain, permettant de déterminer quel bloc peut être ajouté à la chaîne et à l'état courant, et cela sans besoin d'une autorisation particulière de la part d'une autorité de contrôle (éventuellement distribuée).

Enfin, de telles blockchains sont souvent *permissionless* : les nœuds comme les utilisateurs n'ont pas besoin d'autorisation ni d'authentification.

L'autre grand type de blockchains est celui des *blockchains privées*. L'accès et l'utilisation y sont limités à un certain nombre d'acteurs qui, par ailleurs, ne se font pas nécessairement entièrement confiance. Ici, il convient de dissocier les blockchains **complètement privées**, dans lesquelles les droits d'écriture sont restreints et centralisés au sein d'une seule institution, des blockchains dites de **consortium** où le processus de consensus est contrôlé par un sous-ensemble de nœuds et de participants pré-sélectionnés (selon une approche centralisée ou non) et disposant ainsi d'un rôle privilégié pour la gestion de la blockchain.

Dans les deux cas, l'accès en lecture de la blockchain peut être entièrement public ou restreint, que ce soit au niveau des participants ayant été autorisés ou du nombre de requêtes effectuées. Éventuellement, certains systèmes permettent de limiter l'accès aux preuves cryptographiques à seulement une partie de la blockchain. Enfin, une blockchain privée est dite *permissioned*, si les nœuds du réseau, tout comme les utilisateurs, sont authentifiés et autorisés selon des critères prédéfinis, comme sur la figure 1.2.

Modèles de consensus

L'une des caractéristiques essentielles des blockchains est d'assurer la cohérence des copies du registre distribué construites indépendamment par un grand nombre d'acteurs (les nœuds du réseau) n'ayant *a priori* aucune raison de

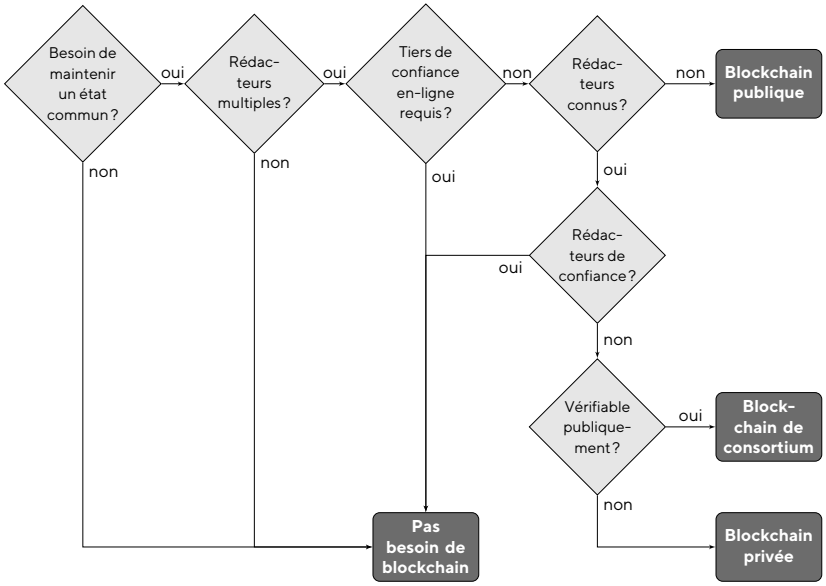

Figure 1.2 – Comment choisir son type de blockchain ? [21]

se faire confiance, ni même de collaborer. Dans un tel contexte, les blockchains reposent sur un algorithme de *consensus* permettant de s'accorder sur l'état et donc l'ordre des blocs de la chaîne, une propriété primordiale pour assurer la cohérence des transactions et éviter les doubles dépenses dans le cadre des cryptomonnaies (*cf.* question **2**).

Le problème vient du fait que les communications dans un réseau P2P ne sont pas instantanées. Ainsi certains nœuds du réseau peuvent être temporairement isolés, ce qui peut conduire à l'apparition de blockchains concurrentes émanant de l'ajout de blocs différents, par des nœuds n'ayant pas conscience l'un de l'autre. De telles duplications sont rares, mais normales. Différemment, rien n'exclut qu'une part des utilisateurs ne cherche à corrompre la blockchain en envoyant des informations erronées ou malveillantes, par exemple pour tenter d'enregistrer des transactions illégales. En pratique, ce problème est connu depuis longtemps [12] sous le nom de « problème des généraux byzantins ». Les fautes dites *byzantines* voient d'ailleurs leur nom tiré de ce problème et caractérisent un comportement arbitraire erroné, éventuellement malveillant, qui

peut s'avérer transitoire ou définitif. C'est précisément de cette façon qu'il convient de modéliser les nœuds du réseau et les utilisateurs de la blockchain dont le comportement dévie du protocole attendu. Ainsi, toute approche tolérante aux fautes byzantines (*Byzantine Fault Tolerance (BFT)* en anglais) offre une base pour un modèle de consensus sur les blockchains. Au-delà des approches BFT (et de ses nombreuses dérivées), d'autres modèles de consensus sont traditionnellement déployés. Parmi les plus courants, il convient de citer :

- **preuve d'autorité** ou *Proof-of-Authority (PoA)* : les transactions et les blocs ne sont validés que par des comptes approuvés qui sont donc en quelque sorte les « administrateurs » de la blockchain ;
- **preuve de travail** ou *Proof-of-Work (PoW)* : la résolution d'un problème mathématique ou d'un puzzle dont la solution est *difficile à trouver* (et donc gourmande en ressources de calcul voire de stockage) est requise pour tout nouveau bloc et cela peut être *vérifié facilement* par d'autres nœuds du réseau. Si de plus toutes les transactions de ce bloc sont valides et que celui-ci est légitime pour être placé en tête de chaîne, il est accepté localement. Si une majorité de nœuds en font autant, le bloc est définitivement accepté et celui qui a trouvé la solution est rétribué ;
- **preuve de participation** ou *Proof-of-Stake (PoS)* qui revient à prouver qu'on possède un certain nombre de jetons associés à la blockchain et créés au lancement de celle-ci. Chaque nœud est invité à miser tout ou partie de ses jetons (*stake*) dans un dépôt en vue d'un tirage au sort qui déterminera le vainqueur pour le tour courant. Le gagnant devient le *validateur* chargé de former un nouveau bloc, qui sera attesté par les autres participants de la loterie. Tout bon comportement est rémunéré, que ce soit pour proposer un nouveau bloc correct ou pour en attester la validité. Au contraire, tout acte malveillant est pénalisé (par exemple en confisquant des jetons). Il existe diverses extensions de ce modèle qui modifient typiquement la distribution régissant le choix du valideur. Dans le cadre d'une *Leased Proof of Stake (LPoS)*, les « petits » propriétaires disposant d'un faible nombre de jetons peuvent les louer (*lease*) afin de faire grossir la contribution d'un nœud particulier dans le dépot. Si celui-ci est choisi comme validateur, les primes et autres frais de transactions sont partagés proportionnellement. Étendant cette approche, une *Delegated Proof-of-Stake (DPoS)* consiste à élire proportionellement au nombre de jetons possédés un délégué en fonction de sa réputation qui participera à la loterie afin de devenir validateur.

De nombreux autres modèles de consensus existent et sont détaillés dans l'ouvrage [5, Q. 5].

2 Qu'est-ce qu'une cryptomonnaie ?

Une monnaie est généralement considérée comme un objet qui concentre simultanément les trois fonctions suivantes :

1. réserve de valeur ;
2. unité de compte ;
3. intermédiaire et moyen d'échanges de biens et services entre les individus (passage par une monnaie au lieu d'un troc direct par exemple).

Avec l'avènement de la cryptographie moderne, il est possible d'assurer ces fonctions à travers des moyens numériques, en créant des monnaies digitales. Une monnaie digitale peut remplir quelques fonctionnalités complémentaires :

- elle doit être non falsifiable (*non-forgeable*) : un utilisateur non habilité dans le système ne doit pas pouvoir créer de la monnaie ;
- il ne doit pas être possible d'effectuer une double dépense : une monnaie dématérialisée étant plus facile à dupliquer, il faut interdire la possibilité de dépenser plusieurs fois la même unité ;
- il faut également pouvoir identifier le fraudeur si cela se produit et s'assurer qu'une personne honnête ne puisse pas être accusée à tort ;
- la vie privée doit être respectée *.

Le premier protocole cryptographique visant à assurer la sécurité des transactions et le respect de la vie privée des utilisateurs dans le cadre d'une monnaie digitale a été proposé par David Chaum en 1983 [3]. Baptisée *ecash*, cette monnaie dépend d'un système monétaire centralisé. Tout l'enjeu était alors de contourner cette dépendance. Ainsi pendant de nombreuses années, et en dépit de quelques autres tentatives comme « b-money », l'utilisation d'un tiers de confiance comme une banque semblait inéluctable. La création du bitcoin par

* Il existe deux versions de ce principe. L'anonymat *faible* garantit qu'il n'est pas possible de savoir qui a effectué une transaction. L'anonymat *fort*, en plus de l'anonymat faible, assure qu'il n'est pas possible de savoir si deux transactions différentes ont été faites par la même entité.

Satoshi Nakamoto [13] a cependant permis un changement radical de paradigme en proposant pour la première fois un système décentralisé garantissant l'intégralité des principes ci-dessus sans autorité centrale et assurant la création de la monnaie et la gestion des transactions. La question **4** détaille les liens entre monnaie et cryptomonnaie.

NewLibertyStandard, le premier fonds monétaire de bitcoin

Le forum Bitcoin a ouvert ses portes courant 2009. Parmi ses utilisateurs assidus, un certain *NewLibertyStandard* a commencé à évoquer l'idée d'une place de marché où il serait possible d'échanger des bitcoins contre des dollars. Décider d'un taux de change BTC/$US devenait alors une question centrale et *NewLibertyStandard* proposa une approche originale pour évaluer ce montant[a]. Soit T ce taux de change pour le mois courant. L'idée était d'estimer T à partir de la consommation électrique annuelle de son ordinateur ($C_{ordi} = 1\,331{,}5$ kWh), du prix du kWh tel qu'évalué depuis sa dernière facture d'électricité (en particulier, $P_{elec} = 0{,}1136$ $US) et du nombre de bitcoins générés au cours du dernier mois b. La formule utilisée était alors :

$$T = \frac{C_{ordi} \times P_{elec}}{12} \times \frac{1}{b}$$

Pour initier ce fonds, une première transaction fut opérée par un utilisateur (appelé *Martti*) qui proposa d'envoyer à *NewLiberty Standard* la somme de 5 050 BTC. En échange, il reçut 5,02 $US par Paypal.

[a] Dans les premières génération des cryptomonnaies : `newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate`

Cette étape marque le point de départ d'un essor phénoménal des monnaies qu'il convient d'appeler *virtuelles* afin de pouvoir les distinguer des monnaies électroniques ou numériques qui, elles, ne sont qu'une version dématérialisée des devises traditionnelles. Ainsi, la Banque centrale européenne (BCE), dans son rapport 2012, définit les monnaies virtuelles de la façon suivante :

> *Une monnaie virtuelle est un type de monnaie dématérialisée non régulée, créée et généralement contrôlée par ses développeurs, et utilisée et acceptée au sein des membres d'une communauté virtuelle spécifique. Parmi celles-ci, seront considérées celles qui sont convertibles avec d'autres monnaies et qui reposent souvent sur un principe de création et de gestion décentralisé et sur des mécanismes cryptographiques, comme bitcoin.*

Pour cette raison, elles sont en général qualifiées de *monnaies virtuelles décentralisées (MVD)* ou de *cryptomonnaies*. Legifrance (JORF numéro 0121 du 23 mai 2017) propose même le terme *cybermonnaie*. En revanche, et contrairement à l'euro en France par exemple, ce type de monnaie n'a pas de cours légal puisque personne n'est tenu légalement de l'accepter en paiement. Les cryptomonnaies sont souvent opposées aux monnaies dites « fiat ». *Fiat* est un mot latin signifiant « qu'il soit fait ». En anglais, le terme est utilisé pour désigner un ordre ou un décret émanant d'un roi ou d'un président. L'expression « monnaie fiat » vient donc de l'anglais car il s'agit d'une copie directe du terme *fiat money* (ou *fiat currency*) qui est une devise d'échange établie par un gouvernement. Présentées de cette manière, les cryptomonnaies semblent très éloignées d'autres monnaies dites « alternatives » telles les systèmes d'échanges locaux (SEL) (comme les clubs de troc) ou les monnaies locales complémentaires (MLC). Le tableau 2.1 résume les principales différences entre ces trois types de monnaies alternatives telles que proposées dans [18].

Caractéristique	MLC	SEL	MVD
Convertibilité avec les monnaies standard	oui	non	oui
Création d'unités adossées aux monnaies standard	oui	non	non
Circulation dans la sphère marchande, fiscalisation	oui	non	oui
Circulation sous forme dématérialisée	oui	non	partiellement
Variabilité de la valeur par rapport aux monnaies standard	non	n/a	oui
Valeurs sociales, environnementales, solidaires, ou à but non lucratif	oui	oui	oui (en 2021) (À l'origine : non)

Tableau 2.1 – Tableau comparatif des cryptomonnaies avec les autres types de monnaies alternatives (« n/a » : non applicable).

C'est le premier critère proposé dans le tableau 2.1 (la convertibilité avec les monnaies standard) qui a permis l'essor du bitcoin et des cryptomonnaies. En effet, après des débuts confidentiels, le bitcoin a commencé à prospérer car un fonds monétaire permettait de convertir les bitcoins créés en devises classiques (le premier taux de change bitcoin/dollar fut publié le 5 octobre 2009).

Le cours du bitcoin, d'abord totalement dérisoire en 2009 ($\simeq$ 0,001 $US, soit environ 0,00071 €), a par la suite pris son envol pour lui permettre de s'inscrire de façon pérenne dans l'environnement économique et d'attirer l'attention des fonds d'investissements. Le bitcoin atteindra une notoriété mondiale en 2013

avant de voir son taux exploser à partir de mi-2016 pour atteindre des sommets en 2021, comme le montre clairement la figure 2.1.

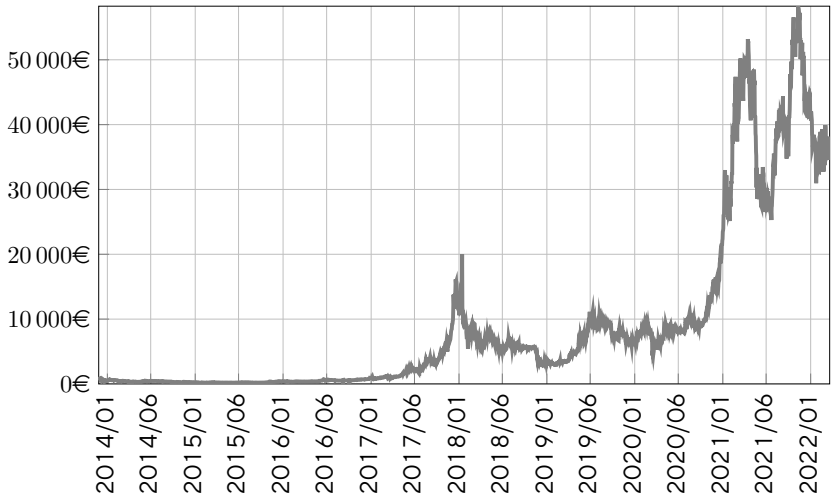

Figure 2.1 – Évolution du cours du bitcoin en euros entre fin 2013 et 2021.

L'arrivée du bitcoin vue comme une escroquerie

L'arrivée du bitcoin coïncidant avec les révélations de « l'affaire Madoff », certains ont pu présenter les cryptomonnaies comme des pyramides de Ponzi, c'est-à-dire comme une escroquerie enrichissant ceux qui sont au sommet de la pyramide et qui ont mis en place le système, au détriment de ceux qui sont situés plus bas dans la hiérarchie et qui se retrouvent ruinés lorsque la pyramide s'effondre.

Ce n'est pas le cas : à travers les registres distribués et les blockchains qui les soutiennent, rien ne prédestine les cryptomonnaies à un écroulement inéluctable. Par ailleurs, l'ensemble des transactions (y compris celles à l'origine de la blockchain) sont publiques. Enfin, et s'il est avéré que les premiers mineurs de bitcoins (dont sans doute Satoshi Nakamoto qui posséderait au moins 5 % de l'ensemble les bitcoins en circulation) ont acquis pour des sommes dérisoires des quantités de bitcoins qui valent