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

11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-084136-3

Table des matières

Avant-propos **vii**

1 Blockchains & cryptomonnaies **1**

1 Qu'est-ce qu'une blockchain ? 3
2 Qu'est-ce qu'une cryptomonnaie ? 9
3 Qu'est-ce que le bitcoin ? 17
4 Les cryptomonnaies sont-elles des monnaies ? 21
5 Qu'est-ce qu'une monnaie virtuelle décentralisée ? 25
6 Qu'est-ce qu'un contrat intelligent ? 31
7 Qu'est-ce que Ethereum ? 37
8 Qu'est-ce qu'une ICO ? 47
9 Qu'est-ce que la finance décentralisée (DeFi) ? 53

2 Jetons non fongibles : NFT **59**

10 Quels sont les jetons fongibles et non fongibles ? 61
11 Quelles différences entre un NFT et d'autres monnaies ? 65
12 Quel a été le premier NFT ? 71
13 Est-ce que les NFT sont interchangeables ? 77
14 Est-il possible de se faire voler un NFT ? 79
15 Pourquoi utiliser un système de fichier distribué comme IPFS ? . . 83
16 Comment créer un nouveau NFT ? 85

3 Utilisations des NFT **91**

17 Qu'est-ce qu'un CryptoKitty ? 93
18 Comment sont utilisés les NFT dans l'art ? 99
19 Comment sont utilisés les NFT dans les jeux vidéo ? 105
20 Comment sont utilisés les NFT dans les jeux de cartes à collectionner ? 117
21 Comment sont utilisés les NFT dans le sport ? 123
22 Comment sont utilisés les NFT dans la mode ? 129
23 Comment les NFT révolutionnent les titres de propriété ? 131
24 Comment peut-on utiliser les NFT pour parier ? 137

4 NFT, droit, économie et finance **139**

25 Y a-t-il un cours des NFT ? 141
26 Comment investir dans des NFT ? 147
27 Quelles sont les principales places de marché NFT ? 153
28 Qu'apportent les NFT à la finance décentralisée (DeFi) ? 159
29 Comment sont réglementés les NFT ? 161
30 Quels sont les apports des NFT au droit ? 165
31 Quelles sont les solutions aux limites du développement des NFT ? 169

5 Les normes techniques des NFT **179**

32 Qu'est-ce qu'une paire de clefs privée/publique ? 181
33 Qu'est-ce qu'une fonction de hachage cryptographique ? 187
34 Qu'est-ce qu'une signature électronique ? 193
35 Qu'est-ce qu'un portefeuille electronique ? 199
36 Comment peut-on créer et programmer son propre type de NFT ? 205
37 Qu'est-ce que la norme ERC-20 pour les jetons fongibles ? 211
38 Qu'est-ce que la norme ERC-721 pour les NFT sur Ethereum ? . . 219
39 Qu'est ce que la norme ERC-1155 pour les jetons hybrides ? 223
40 Quelles sont les normes NFT alternatives ? 227

Annexes **235**
Liste des figures 235
Liste des tableaux 236
Liste des abréviations 237

Bibliographie **239**

Index **241**

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 ;