Préface

2022-03-04

# Préface

# Écrire le livre sur Bitcoin

Je suis tombé sur bitcoin pour la première fois à la mi-2011. Ma réaction immédiate a été plus ou moins "Pfft ! Nerd money !" et je l'ai ignoré pendant encore six mois, n'en saisissant pas l'importance. C'est une réaction que j'ai vue se répéter chez bon nombre des personnes les plus intelligentes que je connaisse, ce qui me réconforte un peu. La deuxième fois que je suis tombé sur bitcoin, lors d'une discussion sur une liste de diffusion, j'ai décidé de lire le livre blanc écrit par Satoshi Nakamoto pour étudier la source faisant autorité et voir de quoi il s'agissait. Je me souviens encore du moment où j'ai fini de lire ces neuf pages, quand j'ai réalisé que le bitcoin n'était pas simplement une monnaie numérique, mais un réseau de confiance qui pouvait aussi fournir la base de bien plus que de simples devises. La prise de conscience que "ce n'est pas de l'argent, c'est un réseau de confiance décentralisé", m'a lancé dans un voyage de quatre mois pour dévorer toutes les informations sur le bitcoin que j'ai pu trouver. Je suis devenu obsédé et captivé, passant 12 heures ou plus par jour collé à un écran, lisant, écrivant, codant et apprenant autant que possible. Je suis sorti de cet état de fugue, plus de 20 livres en moins à cause du manque de repas réguliers, déterminé à me consacrer au travail sur le bitcoin.

Deux ans plus tard, après avoir créé un certain nombre de petites entreprises en démarrage (start-ups) pour explorer divers services et produits liés au bitcoin, j'ai décidé qu'il était temps d'écrire mon premier livre. Bitcoin était le sujet qui m'avait poussé dans une frénésie de créativité et consommé mes pensées; c'était la technologie la plus excitante que j'avais rencontrée depuis Internet. Il était maintenant temps de partager ma passion pour cette technologie incroyable avec un public plus large.

# Public visé

Ce livre est principalement destiné aux codeurs. Si vous pouvez utiliser un langage de programmation, ce livre vous apprendra comment fonctionnent les monnaies cryptographiques, comment les utiliser et comment développer des logiciels qui fonctionnent avec elles. Les premiers chapitres conviennent également comme une introduction approfondie au bitcoin pour les non-codeurs, tel ceux qui veulent comprendre le fonctionnement interne du bitcoin et des cryptomonnaies.

# Pourquoi y a-t-il des insectes sur la couverture ?

La fourmi coupeuse de feuilles est une espèce qui présente un comportement très complexe dans un super-organisme de colonie, mais chaque fourmi individuelle fonctionne selon un ensemble de règles simples dictées par l'interaction sociale et l’échange d'odeurs chimiques (phéromones). Par Wikipedia : "À côté des humains, les fourmis coupeuses de feuilles forment les sociétés animales les plus grandes et les plus complexes sur Terre." Les fourmis coupeuses de feuilles ne mangent pas réellement les feuilles, mais les utilisent plutôt pour cultiver un champignon, qui est la principale source de nourriture de la colonie. Imaginez, ces fourmis cultivent !

Bien que les fourmis forment une société basée sur les castes et aient une reine pour produire une progéniture, il n'y a pas d'autorité centrale ou de chef dans une colonie de fourmis. Le comportement hautement intelligent et sophistiqué présenté par une colonie de plusieurs millions de membres est une propriété émergente de l'interaction des individus dans un réseau social.

La nature démontre que les systèmes décentralisés peuvent être résilients et peuvent produire une complexité émergente et une sophistication incroyable sans avoir besoin d'une autorité centrale, d'une hiérarchie ou de parties complexes.

Bitcoin est un réseau de confiance décentralisé hautement sophistiqué qui peut prendre en charge une myriade de processus financiers. Pourtant, chaque nœud du réseau Bitcoin suit quelques règles mathématiques simples. L'interaction entre de nombreux nœuds est ce qui conduit à l'émergence du comportement sophistiqué, et non une complexité inhérente ou une confiance dans un seul nœud. Comme une colonie de fourmis, le réseau Bitcoin est un réseau résilient de nœuds simples suivant des règles simples qui, ensemble, peuvent faire des choses incroyables sans aucune coordination centrale.

# Conventions utilisées dans ce livre

Les conventions typographiques suivantes sont utilisées dans ce livre :

*Italique*

Indique de nouveaux termes, URL, adresses e-mail, noms de fichiers et extensions de fichiers.

Largeur constante

Utilisé pour les listes de programmes, ainsi que dans les paragraphes pour faire référence à des éléments de programme tels que des noms de variables ou de fonctions, des bases de données, des types de données, des variables d'environnement, des instructions et des mots-clés.

**Largeur constante en gras**

Affiche les commandes ou tout autre texte qui doit être saisi littéralement par l'utilisateur.

*Largeur constante en italique*

Affiche le texte qui doit être remplacé par des valeurs fournies par l'utilisateur ou par des valeurs déterminées par le contexte.

Cette icône signifie un conseil ou une suggestion.

Cette icône signifie une note générale.

Cette icône indique un avertissement ou une mise en garde.

# Exemples de codes

Les exemples sont illustrés en Python, C++, et en utilisant la ligne de commande d'un système d'exploitation de type Unix tel que Linux ou macOS. Tous les extraits de code sont disponibles dans le référentiel GitHub (<https://github.com/bitcoinbook/bitcoinbook>) dans le sous-répertoire *code* du référentiel principal. Fourchez le code du livre, essayez les exemples de code ou soumettez des corrections via GitHub.

Tous les extraits de code peuvent être répliqués sur la plupart des systèmes d'exploitation avec une installation minimale de compilateurs et d'interpréteurs pour les langages correspondants. Si nécessaire, nous fournissons des instructions d'installation de base et des exemples étape par étape de la sortie de ces instructions.

Certains des extraits de code et des sorties de code ont été reformatés pour l'impression. Dans tous ces cas, les lignes ont été séparées par un caractère barre oblique inverse (\), suivi d'un caractère de saut de ligne. Lors de la transcription des exemples, supprimez ces deux caractères et rejoignez les lignes à nouveau et vous devriez voir des résultats identiques comme indiqué dans l'exemple.

Tous les extraits de code utilisent des valeurs réelles et des calculs lorsque cela est possible, de sorte que vous pouvez construire d'exemple en exemple et voir les mêmes résultats dans n'importe quel code que vous écrivez pour calculer les mêmes valeurs. Par exemple, les clés privées et les clés et adresses publiques correspondantes sont toutes réelles. Les exemples de transactions, de blocs et de références de chaîne de blocs ont tous été introduits dans la chaîne de blocs Bitcoin réelle et font partie du grand livre public, vous pouvez donc les consulter sur n'importe quel système Bitcoin.

# Utilisation des exemples de code

Ce livre est là pour vous aider à faire votre travail. En général, si un exemple de code est proposé avec ce livre, vous pouvez l'utiliser dans vos programmes et votre documentation. Vous n'avez pas besoin de nous contacter pour obtenir une autorisation, sauf si vous reproduisez une partie importante du code. Par exemple, écrire un programme qui utilise plusieurs morceaux de code de ce livre ne nécessite pas d'autorisation. La vente ou la distribution d'un CD-ROM d'exemples tirés des livres d'O'Reilly nécessite une autorisation. Répondre à une question en citant ce livre et en citant un exemple de code ne nécessite pas d'autorisation. L'incorporation d'une quantité importante d'exemples de code de ce livre dans la documentation de votre produit nécessite une autorisation.

Nous apprécions, mais n'exigeons pas, l'attribution. Une attribution comprend généralement le titre, l'auteur, l'éditeur et l'ISBN. Par exemple : « *Mastering Bitcoin* par Andreas M. Antonopoulos (O'Reilly). Copyright 2017 Andreas M. Antonopoulos, 978-1-491-95438-6.

Certaines éditions de ce livre sont proposées sous une licence de source libre, comme [CC-BY-NC](https://creativecommons.org/licenses/by-nc/4.0/), auquel cas les termes de cette licence s'appliquent.

Si vous pensez que votre utilisation d'exemples de code ne respecte pas l'utilisation équitable ou l'autorisation donnée ci-dessus, n'hésitez pas à nous contacter à permissions@oreilly.com.

# Adresses et transactions Bitcoin dans ce livre

("codes QR", "avertissements et mises en garde")Les adresses Bitcoin, les transactions, les clés, les codes QR et les données de chaîne de blocs utilisées dans ce livre sont, pour la plupart, réelles. Cela signifie que vous pouvez parcourir la chaîne de blocs, regarder les transactions proposées en exemple, les récupérer avec vos propres scripts ou programmes, etc.

Cependant, notez que les clés privées utilisées pour construire les adresses sont soit imprimées dans ce livre, soit ont été "radiées". Cela signifie que si vous envoyez de l'argent à l'une de ces adresses, l'argent sera perdu pour toujours ou, dans certains cas, tous ceux qui peuvent lire ce livre peuvent le prendre en utilisant les clés privées imprimées dans celui-ci.

N'ENVOYEZ PAS D'ARGENT AUX ADRESSES DANS CE LIVRE. Votre argent sera pris par un autre lecteur, ou perdu à jamais.

# O’Reilly Safari

Safari (anciennement Safari Books Online) est une plate-forme de formation et de référence basée sur l'adhésion pour les entreprises, le gouvernement, les éducateurs et les particuliers.

Les membres ont accès à des milliers de livres, de vidéos de formation, de parcours d'apprentissage, de didacticiels interactifs et de listes de lecture sélectionnées par plus de 250 éditeurs, dont O'Reilly Media, Harvard Business Review, Prentice Hall Professional, Addison-Wesley Professional, Microsoft Press, Sams, Que , Peachpit Press, Adobe, Focal Press, Cisco Press, John Wiley & Sons, Syngress, Morgan Kaufmann, IBM Redbooks, Packt, Adobe Press, FT Press, Apress, Manning, New Riders, McGraw-Hill, Jones & Bartlett et Course Technology, entre autres.

Pour plus d'informations, rendez-vous sur https://oreilly.com/safari.

# Comment nous contacter

Veuillez adresser vos commentaires et questions concernant ce livre à l'éditeur :

O’Reilly Media, Inc.

1005 Gravenstein Highway North

Sebastopol, CA 95472

800-998-9938 (aux États-Unis ou au Canada)

707-829-0515 (international ou local)

707-829-0104 (fax)

Pour commenter ou poser des questions techniques sur ce livre, envoyez un courriel à l'adresse suivante bookquestions@oreilly.com.

Pour plus d'informations sur nos livres, cours, conférences et actualités, consultez notre site Web au lien : https://www.oreilly.com[].

Retrouvez-nous sur Facebook : <https://facebook.com/oreilly>

Suivez-nous sur Twitter : <https://twitter.com/oreillymedia>

Regardez-nous sur YouTube : <https://www.youtube.com/oreillymedia>

# Contacter l'auteur

Vous pouvez me contacter, Andreas M. Antonopoulos, sur mon site personnel : <https://aantonop.com/>

Des informations sur *Maîtriser Bitcoin (Mastering Bitcoin en anglais)* ainsi que l'Édition Ouverte et les traductions sont disponibles sur : <https://bitcoinbook.info/>

Suivez-moi sur Facebook: <https://facebook.com/AndreasMAntonopoulos>

Suivez-moi sur Twitter: <https://twitter.com/aantonop>

Suivez-moi sur LinkedIn : <https://linkedin.com/company/aantonop>

Un grand merci à tous mes mécènes qui soutiennent mon travail par des dons mensuels. Vous pouvez suivre ma page Patreon ici : <https://patreon.com/aantonop>

# Remerciements

Ce livre représente les efforts et les contributions de nombreuses personnes. Je suis reconnaissant pour toute l'aide que j'ai reçue d'amis, de collègues et même de parfaits inconnus, qui m'ont rejoint dans cet effort pour écrire le livre technique définitif sur les crypto-monnaies et le bitcoin.

Il est impossible de faire une distinction entre la technologie bitcoin et la communauté bitcoin, et ce livre est autant un produit de cette communauté qu'un livre sur la technologie. Mon travail sur ce livre a été encouragé, applaudi, soutenu et récompensé par toute la communauté bitcoin du tout début jusqu'à la toute fin. Plus que tout, ce livre m'a permis de faire partie d'une merveilleuse communauté pendant deux ans et je ne vous remercierai jamais assez de m'avoir accepté dans cette communauté. Il y a beaucoup trop de personnes à mentionner par leur nom - des personnes que j'ai rencontrées lors de conférences, d'événements, de séminaires, de rencontres, de pizzas et de petits rassemblements privés, ainsi que beaucoup qui ont communiqué avec moi par Twitter, sur reddit, sur bitcointalk. org, et sur GitHub qui ont eu un impact sur ce livre. Chaque idée, analogie, question, réponse et explication que vous trouverez dans ce livre a été à un moment donné inspirée, testée ou améliorée grâce à mes interactions avec la communauté. Merci à tous pour votre soutien; sans vous ce livre n'aurait pas vu le jour. Je suis éternellement reconnaissant.

Le voyage pour devenir auteur commence bien avant le premier livre, bien sûr. Ma première langue (et ma scolarité) était le grec, j'ai donc dû suivre un cours de rattrapage en anglais écrit lors de ma première année d'université. Je dois remercier Diana Kordas, mon professeur d'écriture d'anglais, qui m'a aidé à développer ma confiance et mes compétences cette année-là. Plus tard, en tant que professionnel, j'ai développé mes compétences en rédaction technique sur le thème des centres de données, en écrivant pour le magazine *Network World*. Je dois remercier John Dix et John Gallant, qui m'ont donné mon premier travail d'écriture en tant que chroniqueur à *Network World* et à mon éditeur Michael Cooney et mon collègue Johna Till Johnson qui ont édité mes chroniques et les ont rendues aptes à la publication. Écrire 500 mots par semaine pendant quatre ans m'a donné suffisamment d'expérience pour éventuellement envisager de devenir auteur.

Merci également à ceux qui m'ont soutenu lorsque j'ai soumis ma proposition de livre à O'Reilly, en fournissant des références et en examinant la proposition. Plus précisément, merci à John Gallant, Gregory Ness, Richard Stiennon, Joel Snyder, Adam B. Levine, Sandra Gittlen, John Dix, Johna Till Johnson, Roger Ver et Jon Matonis. Remerciements particuliers à Richard Kagan et Tymon Mattoszko, qui ont révisé les premières versions de la proposition et à Matthew Taylor, qui a révisé la proposition.

Merci à Cricket Liu, auteur du titre O'Reilly *DNS et BIND*, qui m'a présenté O'Reilly. Merci également à Michael Loukides et Allyson MacDonald de O'Reilly, qui ont travaillé pendant des mois pour aider à la réalisation de ce livre. Allyson a été particulièrement patiente lorsque les délais ont été manqués et les livrables retardés alors que la vie intervenait dans notre échéancier. Pour la deuxième édition, je remercie Timothy McGovern d'avoir guidé le processus, Kim Cofer d'avoir patiemment édité et Rebecca Panzer d'avoir illustré de nombreux nouveaux diagrammes.

Les premières ébauches des premiers chapitres ont été les plus difficiles, car le bitcoin est un sujet difficile à démêler. Chaque fois que je tirais sur un fil de la technologie bitcoin, je devais tirer sur le tout. Je me suis retrouvé coincé à plusieurs reprises et un peu découragé alors que je luttais pour rendre le sujet facile à comprendre et créer un récit autour d'un sujet technique aussi dense. Finalement, j'ai décidé de raconter l'histoire du bitcoin à travers les histoires des personnes utilisant le bitcoin et tout le livre est devenu beaucoup plus facile à écrire. Je dois remercier mon ami et mentor, Richard Kagan, qui m'a aidé à démêler l'histoire et à surmonter les moments de blocage de l'écrivain. Je remercie Pamela Morgan, qui a révisé les premières ébauches de chaque chapitre de la première et de la deuxième édition du livre, et a posé les questions difficiles pour les améliorer. Merci également aux développeurs du groupe San Francisco Bitcoin Developers Meetup ainsi qu'à Taariq Lewis et Denise Terry pour avoir aidé à tester le premier matériel. Merci également à Andrew Naugler pour la conception infographique.

Pendant le développement du livre, j'ai rendu les premières ébauches disponibles sur GitHub et j'ai invité les commentaires du public. Plus d'une centaine de commentaires, suggestions, corrections et contributions ont été soumis en réponse. Ces contributions sont explicitement reconnues, avec mes remerciements, dans &lt<github\_contrib>>. Surtout, mes sincères remerciements à mes éditeurs bénévoles de GitHub, Ming T. Nguyen (1ère édition) et Will Binns (2e édition), qui ont travaillé sans relâche pour organiser, gérer et résoudre les demandes d'extraction, publier des rapports et effectuer des corrections de bogues sur GitHub.

Une fois le livre rédigé, il est passé par plusieurs séries d'examens techniques. Merci à Cricket Liu et Lorne Lantz pour leur examen approfondi, leurs commentaires et leur soutien.

Plusieurs développeurs de bitcoins ont fourni des échantillons de code, des critiques, des commentaires et des encouragements. Merci à Amir Taaki et Eric Voskuil pour les extraits de code par exemple et de nombreux excellents commentaires ; Chris Kleeschulte pour sa contribution à l'annexe Bitcore ; Vitalik Buterin et Richard Kiss pour leur aide avec les mathématiques des courbes elliptiques et leurs contributions au code ; Gavin Andresen pour les corrections, les commentaires et les encouragements ; Michalis Kargakis pour les commentaires, les contributions et la rédaction de btcd ; et Robin Inge pour les soumissions d'errata améliorant la deuxième impression. Dans la deuxième édition, j'ai de nouveau reçu beaucoup d'aide de la part de nombreux développeurs de Bitcoin Core, dont Eric Lombrozo qui a démystifié le Témoin Séparé, Luke Dashjr qui a aidé à améliorer le chapitre sur les transactions, Johnson Lau qui a revu le Témoin Séparé et d'autres chapitres, et bien d'autres. Je dois remercier Joseph Poon, Tadge Dryja et Olaoluwa Osuntokun qui ont expliqué Lightning Network, revu mes écrits et répondu aux questions lorsque je suis resté bloqué.

Je dois mon amour des mots et des livres à ma mère, Theresa, qui m'a élevé dans une maison avec des livres tapissant tous les murs. Ma mère m'a également acheté mon premier ordinateur en 1982, bien qu'elle se décrive comme une technophobe. Mon père, Menelaos, un ingénieur civil qui vient de publier son premier livre à 80 ans, est celui qui m'a enseigné la pensée logique et analytique et l'amour de la science et de l'ingénierie.

Merci à tous de m'avoir soutenu tout au long de ce parcours.

## Version préliminaire (contributions GitHub)

De nombreux contributeurs ont proposé des commentaires, des corrections et des ajouts à la première version préliminaire sur GitHub. Merci à tous pour vos contributions à ce livre.

Voici une liste des contributeurs notables de GitHub :

Unresolved directive in for\_translation\_mastering-bitcoin\_preface\_fr\_CA.asciidoc - include::github\_contrib.asciidoc[]