Mastering Bitcoin

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 novembre 2016

https://www.bortzmeyer.org/mastering-bitcoin.html

Auteur(s) : Andreas Antonopoulos
ISBN n°978-1-449-37404-4
Éditeur : O'Reilly
Publié en 2015
———————-

Vous voulez connaitre tous les détails techniques sur Bitcoin ? Voici un livre recommandé. À la fin, vous en saurez davantage que vous ne vouliez.

Le livre a été écrit par Andreas Antonopoulos, personnage connu dans le monde Bitcoin, et qui écrit de nombreux articles et donne plein de conférences (celle qu'il a donné à Paris le 11 octobre est en ligne <https://www.youtube.com/watch?v=ve0uCmnOFcI>, vous pouvez aussi voir les nombreux tweets que cela a entrainé <https://twitter.com/hashtag/mconf?f=tweets&vertical=default&src=hash> et une excellente « storifycation de ces tweets <https://twitter.com/benjaltf4_/status/800362998946791425>). Son livre commence de manière très pédagogique, à travers des scénarios d'utilisation. Alice utilise Multibit <https://multibit.org/> pour acheter un café à Bob à Palo Alto, Bob fait refaire le site Web de son café à Gonesh, à Bangalore, et Jing mine du bitcoin à Shanghai. Au début, l'auteur fait peu de technique, se focalisant sur les applications.

Ensuite, cela devient plus technique, en commençant par l'installation d'un nœud Bitcoin (le livre n'est pas destiné à M. Michu). Andreas Antonopoulos explique le fonctionnement du client en ligne de commande qui permet de parler à son nœud Bitcoin. De la commande la plus triviale, permettant de savoir à quel bloc en est la chaîne locale :

```
 % bitcoin-cli getblockcount
439785
```

à des commandes plus complexes, ici pour voir l'achat du café d'Alice :

```
% bitcoin-cli gettransaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
```

(Si vous obtenez le message d'erreur "*Invalid or non-wallet transaction id*", c'est que vous n'avez pas bien lu le livre et les instructions qu'il donne pour accéder à toutes les transactions.)

À noter que les exemples ont été réellement faits sur la chaîne publique Bitcoin, et peuvent donc être vérifiés. L'adresse d'Alice est `1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK` et on peut donc voir toutes ses transactions en ligne <`https://blockchain.info/address/1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK`> de sa première obtention de 0,1 bitcoin auprès de son ami Joe (transaction `7957a35fe64f80d234d76d83a2a8f1a0c` à l'achat du café à Bob (transaction `0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c` Le code QR de la demande de bitcoins de Bob, dans le livre, est également un vrai, et on peut le lire (`bitcoin:1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA?amount=0.015&label=Bob%27s%20Cafe&message=`

L'auteur pense aussi aux programmeurs et leur explique comment accéder aux données Bitcoin et les manipuler depuis un programme. Par exemple, en Python, avec la bibliothèque pycoin <`https://github.com/richardkiss/pycoin`>.

Je l'ai dit, ce livre, malgré ses premières pages très pédagogiques sur Bitcoin, est prévu pour les techniciens. Vous y trouverez même une explication de la cryptographie sur courbes elliptiques, permettant de décrire ensuite les différents formats de clés.

Les utilisateurs de l'autre chaîne de blocs Ethereum savent qu'une adresse Ethereum ne désigne pas forcément un compte mais peut référencer un programme qui sera exécuté lorsqu'on enverra quelque chose à cette adresse. Mais peu savent que cette possibilité existe dans Bitcoin depuis longtemps. Antonopoulos décrit donc en détail les différents types d'adresses Bitcoin, notamment les P2SH ("*Pay To Script Hash*") où le paiement va déclencher l'exécution d'un programme qui pourra, par exemple, demander plusieurs signatures pour valider un paiement (la grande différence entre Ethereum et Bitcoin n'est pas la présence ou l'absence de programmes stockés dans la chaîne, elle est dans le fait que seul Ethereum a un langage de Turing ; au passage, le livre contient un court chapitre présentant rapidement quelques chaînes de blocs concurrentes). Il y a même un peu d'assembleur Bitcoin dans le livre (mais pas un cours complet sur ce langage).

Les gens du réseau aimeront également le chapitre sur le fonctionnement pair à pair de Bitcoin et sur la façon dont les nœuds Bitcoin échangent. Un petit coup de `bitcoin-cli getpeerinfo` et je vois que ma machine Bitcoin a 124 pairs, dont 11 se connectent en IPv6. 86 font tourner le logiciel de référence Bitcoin Core et 30 sont basés sur BitcoinJ (ce sont surtout des clients utilisant Multibit <`https://multibit.org/`>).

Je l'ai dit plus haut, ce livre n'est pas du tout nécessaire pour utiliser Bitcoin, ni même pour comprendre comment il fonctionne. En revanche, il est indispensable si vous voulez comprendre les points les plus délicats du fonctionnement de Bitcoin, comme les UTXO <`https://bitcoin.org/en/glossary/unspent-transaction-output`>, la structure de la chaîne avec les arbres de Merkle, le fonctionnement de SPV... Difficile de trouver une question technique sur Bitcoin qui n'aurait pas de réponse dans ce livre.

Avertissement : j'ai acheté ce livre en payant en euros, pas en bitcoins. J'en profite pour rappeler que, si vous aimez ce blog, je veux bien des bitcoins <`https://www.bortzmeyer.org/bitcoin-blog.html`>.

`https://www.bortzmeyer.org/mastering-bitcoin.html`