NEEL MEHTA
ADI AGASHE
PARTH DETROJA

BLOCKCHAIN

BULLE OU RÉVOLUTION ?

MEILLEURE VENTE AUX ÉTATS-UNIS

QUEL AVENIR POUR LE BITCOIN ET LES CRYPTOMONNAIES ?

BLOCKCHAIN

BULLE

OU

RÉVOLUTION ?

Neel Mehta
Aditya Agashe
Parth Detroja

BLOCKCHAIN

BULLE OU RÉVOLUTION ?

Traduction de Bernard Desgraupes

Pour toute information sur notre fonds et les nouveautés dans votre domaine de spécialisation, consultez notre site web : **www.deboecksuperieur.com**

Rue du Bosquet, 7 – B-1348 Louvain-la-Neuve

Dépôt légal :
Bibliothèque nationale, Paris : mars 2021
Bibliothèque royale de Belgique, Bruxelles : 2021/13647/034 ISBN 978-2-8073-3166-2

À mes amis et à ma famille, pour leur soutien,
quelle que soit la folie de mes rêves. —Neel

À ma famille et à mes amis, merci de soutenir ma passion pour les affaires
et de m'aider à surmonter mes craintes à devenir entrepreneur. —Adi

À mes amis et à ma famille pour leur soutien indéfectible
dans mes efforts apparemment ridicules. —Parth

Table des matières

Introduction

Le Bitcoin est un outil pour libérer l'humanité des oligarques et des tyrans, déguisé en méthode pour s'enrichir rapidement.

— Naval Ravikant, fondateur de AngelList [1]

Le bitcoin est probablement du poison pour rat à la puissance deux.

— Warren Buffett, PDG de Berkshire Hathaway [2]

C'était en 2017 et les Nations Unies avaient un problème. En raison de la guerre civile sanglante en Syrie, dix mille réfugiés syriens avaient fui vers un camp de réfugiés en Jordanie voisine [3]. Le Programme Alimentaire Mondial (PAM) des Nations Unies avait installé, dans le camp, des supermarchés où les réfugiés pouvaient acheter des articles tels que l'huile d'olive et les lentilles, et pour acheter ces articles il fallait donner aux réfugiés un peu d'argent. [4]

Le problème était que donner des cartes de crédit prépayées aux réfugiés ne fonctionnerait pas. Cette approche avait coûté des millions de dollars au PAM par le passé à cause des frais de transaction et de la nécessité de nouer des partenariats avec des banques locales – de l'argent qui aurait pu être utilisé pour financer des millions de repas [5]. Fournir aux réfugiés des cartes d'identité qui leur donneraient droit à des biens ne fonctionnerait pas mieux ; lorsque le PAM avait tenté cela dans le passé, les chefs de tribus locaux s'étaient emparés des cartes et avaient commencé à les utiliser comme monnaie d'échange [6].

Le PAM s'est donc tourné vers une technologie naissante appelée blockchain, rendue célèbre pour être la technologie qui sous-tend la monnaie numérique Bitcoin. Le « compte » de chaque réfugié était crédité d'un peu d'argent, et lorsqu'un réfugié se rendait dans un magasin, on vérifiait son identité avec un scanner d'iris, puis il pouvait échanger son crédit contre de la nourriture et des fournitures – le tout sans ouvrir son portefeuille [7]. Les magasins pouvaient ensuite revendre les coupons collectés à l'ONU [8].

Ce projet, appelé *Building Blocks*, a connu un succès retentissant. Il a permis de réduire les frais de transfert d'argent de 98 % [9], de faire baisser la fraude et de simplifier radicalement le processus d'aide aussi bien pour le PAM que pour les réfugiés [10]. L'ONU a rapidement développé ce programme pour servir 100 000 réfugiés [11], avec pour objectif de l'étendre à tous les réfugiés de Jordanie [12].

Les avantages pour l'ONU se situent au-delà de l'aide : l'ONU a annoncé qu'elle serait un jour en mesure de suivre l'identité et l'historique des réfugiés à l'aide de la blockchain, aidant ainsi les réfugiés à obtenir des emplois et des prêts dans de nouveaux pays pour le cas où leurs passeports ou leurs dossiers scolaires auraient été détruits. (13)

Dans le monde entier, on observe un incroyable engouement pour les blockchains et pour leur technologie sœur, les *cryptomonnaies* (comme le Bitcoin mentionné précédemment). La *Harvard Business Review* s'est demandé si les blockchains pouvaient bouleverser le secteur bancaire (14), le célèbre capitaliste d'entreprise Marc Andreessen a déclaré que les blockchains étaient « l'invention la plus importante depuis Internet » (15) et les analystes du monde entier pensent que les cryptomonnaies vont révolutionner la finance et la technologie telles nous les connaissons (16).

D'un autre côté, ces mystérieuses nouvelles technologies ont également acquis une sinistre réputation. Les parrains de la drogue utilisent le Bitcoin pour faire du narcotrafic en ligne de façon anonyme (17), les cryptomonnaies ont été accusées de contribuer au réchauffement climatique (18), et les pirates informatiques exigent des paiements en Bitcoin afin que les forces de l'ordre ne puissent pas les traquer (19). Le battage médiatique positif autour de ces technologies semble souvent poussé trop loin : une entreprise de thé glacé, Long Island Iced Tea, a ajouté le mot « blockchain » à son nom (20) et a vu le cours de son action presque quadrupler (21).

Alors qu'y a-t-il de vrai ? Les blockchains et les cryptomonnaies sont-elles une bulle alimentée par le battage médiatique, des technologies sans cas d'utilisation légitimes ? Ou sont-ce des trouvailles révolutionnaires qui vont transformer les gouvernements, les entreprises, les économies et les sociétés à leur image ? En d'autres termes, s'agit-il d'une bulle ou d'une révolution ?

L'objectif

Comme le montrent les histoires ci-dessus, les blockchains et les cryptomonnaies – collectivement regroupées sous le nom de *crypto* – sont parmi les nouvelles technologies les plus importantes et les moins bien comprises de notre temps. La plupart des conversations publiques sur la crypto sont dominées par des passionnés affirmant qu'elle anéantira banques et gouvernements ou des experts disant que la crypto n'est rien d'autre qu'une arnaque. Peu de gens prennent le temps d'analyser le fonctionnement exact de ces technologies et leur potentiel réel.

Dans *Bulle ou Révolution*, nous voulons changer cela. À travers des exemples concrets, des explications simples et des analyses impartiales, nous voulons vous apprendre comment fonctionne la crypto, où elle est utile et où elle ne l'est pas. Nous vous dirons ce que nous pensons du débat bulle-ou-révolution, en outre nous vous donnerons également les outils nécessaires pour décider par vous-même.

Contenu de l'ouvrage

Dans *Bulle ou Révolution*, vous découvrirez les éléments constitutifs des chaînes de blocs et des cryptomonnaies, vous explorerez leurs forces et leurs faiblesses à travers des études de cas, vous approfondirez leurs implications sociales, politiques, économiques et techniques et vous aurez un aperçu de leur avenir grâce aux entretiens exclusifs que nous avons eus avec des dizaines de leaders de l'industrie technologique.

Voici quelques-uns des sujets que nous couvrirons :

- L'économie du Bitcoin mining
- Les piratages et les failles de cryptomonnaies célèbres
- Les blockchains Xbox pour les jeux vidéo
- La réglementation de la SEC sur les startups crypto
- La tokenisation des devises et l'avenir de la finance
- Les cryptomonnaies émergentes de Facebook

Notre premier livre

Lorsque nous avons écrit tous les trois le best-seller commercial *Swipe to Unlock : The Primer on Technology and Business Strategy*, nous cherchions à enseigner aux lecteurs tout ce qu'ils avaient besoin de savoir sur le monde de la technologie, depuis les mécanismes internes de l'algorithme de recherche de Google jusqu'aux stratégies commerciales de haut niveau de Facebook.

Chaque section de *Swipe to Unlock* était une étude de cas concret, abordant une question que vous vous posez peut-être vous-mêmes – comment Spotify recommande les chansons, comment fonctionnent les voitures sans conducteur et pourquoi Amazon propose la livraison gratuite même si elle y perd de l'argent. Nous avions couvert un large éventail de technologies, de la sécurité à l'informatique en nuage (*cloud computing*) en passant par l'apprentissage automatique.

Mais depuis que nous avons écrit *Swipe to Unlock*, les cryptomonnaies et les chaînes de blocs ont explosé dans la conscience publique comme peu d'autres technologies l'avaient fait auparavant. Il est essentiel que les acteurs du monde technologique, les entrepreneurs, les patrons d'entreprise et même les observateurs occasionnels comprennent ces technologies. Nous avons donc décidé d'écrire un livre sur ce sujet.

Ce livre sera une plongée en profondeur dans un des fondements clés de la technologie ; si vous souhaitez élargir votre compréhension du paysage technologique, acquérir des structures pour en comprendre la stratégie commerciale et une boîte à outils mentale pour évaluer ces nouvelles technologies, vous voudrez peut-être également jeter un coup d'œil à *Swipe to Unlock*. Découvrez-le sur swipetounlock.com ou trouvez-le sur Amazon.

Qui sommes-nous ?

Avant de nous lancer dans le sujet, voici un peu d'information sur chacun de nous.

Neel Mehta est chef de produit chez Google et a auparavant travaillé pour Microsoft et le gouvernement américain, où il a créé le premier programme de stages technologiques du gouvernement fédéral.

Adi Agashe est chef de produit chez Microsoft et ancien fondateur et PDG de Belle Applications.

Parth Detroja est chef de produit chez Facebook et a auparavant occupé des postes de produit et marketing chez Microsoft, Amazon et IBM.

Merci et bonne lecture !

Merci encore d'avoir choisi de lire *Bulle ou Révolution*. Nous espérons que vous trouverez ce livre à la fois informatif, intéressant et peut-être même distrayant. Profitez bien de votre lecture !

Neel Mehta
namehta.com
linkedin.com/in/neelmehta18

Aditya Agashe
adityaagashe.com
linkedin.com/in/adityaagashe
quora.com/profile/Adi-Agashe

Parth Detroja
parthdetroja.com
linkedin.com/in/parthdetroja

Chapitre 1 :

Bitcoin et la Blockchain

Le bitcoin donne, pour la première fois, à un internaute le moyen de transférer une propriété numérique unique à un autre internaute, de telle sorte que le transfert est garanti sûr et sécurisé, que tout le monde sait que ce transfert a eu lieu, et que personne ne peut en contester la légitimité. Les conséquences de cette percée sont difficiles à surestimer.

—Marc Andreessen, co-fondateur
de Andreessen Horowitz [1]

Les tierces parties de confiance constituent des failles de sécurité. J'aimerais que chacun dans le domaine des blockchains ait bien cela en tête. C'est fondamentalement la clé de tout le concept.

—Nick Szabo, créateur du Bit Gold
(précurseur du Bitcoin) [2]

Le jour d'Halloween 2008 [3], un informaticien se faisant appeler Satoshi Nakamoto a publié un livre blanc présentant Bitcoin, une monnaie numérique qui devait permettre aux gens d'échanger de l'argent sans passer par une banque, un gestionnaire de cartes de crédit ou toute autre institution financière. [4] Personne ne savait qui était vraiment Satoshi, mais tout le monde sur la liste de diffusion où il a publié son papier l'a remarqué.
En un seul email, Satoshi présentait au monde les blockchains et les cryptomonnaies, une paire de technologies qui sont devenues des noms familiers. Mais pour bien comprendre ces technologies, nous devons commencer par faire la lumière sur l'invention de ce mystérieux scientifique.

Le problème de l'argent

Tout au long de l'histoire humaine, il y a eu deux façons de détenir de l'argent : posséder des objets physiques (argent liquide, pièces d'or, bétail, sel, etc.) ou avoir une institution de confiance, comme une banque ou une autorité, pour établir combien d'argent vous avez.

Ces deux formes d'argent comportent des problèmes.

Les défauts des formes d'argent physiques ou tangibles, comme l'argent liquide ou les vaches, sont assez clairs : c'est facile à voler, ça ne peut pas être utilisé pour des transactions en ligne ou à longue distance (essayez d'acheter quelque chose en liquide à quelqu'un dans un pays étranger), ça peut souvent être contrefait, et c'est parfois difficile à stocker et à transporter.

Argent médiatisé par des intermédiaires

Pour résoudre ces problèmes, l'humanité a inventé l'argent par l'intermédiaire d'une institution de confiance comme une banque ou un chef local. De nombreuses formes d'argent et de paiements relèvent de ce modèle : comptes bancaires, prêts bancaires, cartes de crédit, chèques et beaucoup d'autres outils financiers que nous utilisons de nos jours. En faisant confiance à une institution centrale, ou à un intermédiaire, vous pouvez résoudre la plupart des problèmes de l'argent tangible.

- Vous pouvez faire confiance à une banque pour que votre argent soit plus en sécurité que si vous le gardiez à la maison (comparez un compte bancaire à de l'argent liquide stocké sous votre matelas).
- Vous pouvez effectuer rapidement des paiements numériques en ligne, car payer quelqu'un est aussi simple que de demander à votre banque et à sa banque de mettre à jour les soldes de vos comptes (qui ne sont que des chiffres dans une base de données quelque part).
- Il est plus difficile de fabriquer de la fausse monnaie quand une autorité de confiance suit exactement combien d'argent chacun possède. (Comme il n'existe pas d'enregistrement central de la somme d'argent dont chacun dispose, le seul moyen de repérer un faux-monnayeur est d'espérer que vous pourrez distinguer les faux billets des vrais.)
- Si vous faites confiance à un intermédiaire pour détenir votre argent, vous n'avez pas besoin d'en transporter avec vous.

Ce genre d'argent géré par des intermédiaires est vraiment remarquable. Mais il y a une raison pour laquelle les gens continuent d'utiliser de l'argent liquide et que certains magasins acceptent uniquement les espèces : l'argent médiatisé par des intermédiaires (désigné sous le sigle *M3*) a son lot de défauts qui, pour la plupart, proviennent du fait même qu'il existe un intermédiaire.

Le premier problème est que, lorsque votre argent passe par des intermédiaires, vous devez respecter leurs règles, ce qui signifie souvent que vous devez payer des frais. Lorsque vous payez quelque chose avec une carte de crédit, le marchand ne reçoit pas toute la somme ; il doit payer des frais au gestionnaire de cartes de crédit (environ 1,5 à 2,5 % pour Visa, Mastercard et Discover, et 2,5 à 3,5 % pour American Express)[1]. (5)

1. Ces frais plus élevés sont l'une des raisons pour lesquelles de nombreux magasins n'utilisent pas American Express.

Envoyer de l'argent à l'international avec PayPal vous coûtera environ 3 % de frais, et si vous êtes un commerçant, accepter un paiement avec PayPal vous coûtera également environ 3 % [6]. Et les frais d'envoi d'argent à l'étranger avec Western Union, MoneyGram, Xoom, ou d'autres sociétés d'envoi de fonds peuvent également représenter quelques pour cent [7].

Vous pouvez maintenant comprendre pourquoi de nombreux magasins acceptent uniquement des espèces ou imposent des montants minimaux pour utiliser les cartes de crédit.

Un autre problème avec M3 est que vous ne pouvez l'utiliser que si les intermédiaires vous y donnent accès. Concrètement, cela signifie que les deux milliards de personnes non bancarisées dans le monde [8] ne peuvent pas utiliser d'argent impliquant un compte bancaire (c'est-à-dire la plupart du M3), et que les personnes avec un mauvais crédit ou pas de crédit du tout ne peuvent pas utiliser de cartes de crédit.

Le dernier gros problème avec M3 est que vous leur confiez votre argent et, de nos jours, vos données. Les banques sont plutôt douées pour ne pas perdre votre argent, mais les antécédents des institutions financières en matière de sécurité des données sont loin d'être aussi bons. Des pirates ont volé des données concernant 100 millions de clients de JPMorgan en 2014 [9] et des informations sensibles (dates de naissance, adresses, etc.) relatives à 100 millions de clients de Capital One ont été dérobées en 2019 [10]. Sans parler du piratage le plus infâme de tous : quand les données personnelles (y compris les numéros de sécurité sociale) de près de 150 millions d'Américains ont été volées à Equifax [11].

En bref, l'argent tangible n'est pas sûr, il est peu pratique, facile à contrefaire et impraticable pour des paiements numériques. L'argent médiatisé par des intermédiaires, ou M3, résout ces problèmes, mais introduit des problèmes de frais, de manque d'accessibilité et une forme différente d'insécurité. Du coup, nous devons choisir ce qui nous empoisonne le moins.

Intangibilité

Cependant si vous y réfléchissez, vous vous rendrez compte que ce dont nous avons surtout besoin avec l'argent, c'est l'intangibilité. M3 vous procure l'intangibilité en introduisant des intermédiaires : si vous faites confiance aux institutions pour gérer et déplacer votre argent à votre place, vous n'avez plus à détenir d'argent tangible. Mais, bien sûr, les intermédiaires ont leur propre lot d'inconvénients. Existe-t-il un moyen d'éliminer les intermédiaires tout en conservant l'intangibilité ? En d'autres termes, peut-on avoir une forme d'argent à la fois intangible *et* sans intermédiaire ?

Vous voyez probablement où nous voulons en venir. Mais il s'avère que des gens ont déjà inventé une forme d'argent intangible et sans intermédiaire il y a des siècles, bien avant que Satoshi ne présente publiquement Bitcoin. Pour découvrir ces gens, il faut rendre visite à la minuscule île micronésienne de Yap au milieu de l'océan Pacifique.

Pierres de Rai

La monnaie traditionnelle de Yap est constituée d'anneaux de pierre géants connus sous le nom de pierres de rai. Ces pierres sont massives : certaines atteignent dix pieds de large [(12)] et pèsent le poids d'une camionnette [(13)]. Chaque village de Yap a des dizaines de pierres de rai éparpillées dans la ville [(14)].

Une pierre de rai, une forme de monnaie traditionnelle sur l'île de Yap, dans le Pacifique. Source : Wikimedia [(15)]

Comme vous pouvez l'imaginer, les gens ne peuvent pas trimbaler ces pierres autour de l'île pour payer avec. Au lieu de cela, les Yapais gardent en mémoire collectivement à qui appartient chaque pierre et tiennent un journal mental des transactions passées. Par exemple, si la fille du chef veut acheter un bateau au charpentier, elle pourrait annoncer aux villageois qu'une pierre de rai qu'elle contrôle (par exemple, celle de la plage) appartient désormais au charpentier. Les villageois répandraient la nouvelle que la fille du chef a donné une pierre au charpentier.

Ensuite, si le charpentier veut donner cette pierre à quelqu'un d'autre, les villageois le laisseront faire, puisque les registres mentaux de tout

le monde disent que cette pierre lui appartient maintenant [16]. (En gros, quelqu'un peut dépenser une pierre si la plupart des villageois s'accordent à dire qu'elle est en sa possession.)

Intangible

L'aspect impressionnant du système des pierres de rai est que toutes sortes d'activités économiques peuvent avoir lieu sans que les pierres ne changent physiquement de place ; en effet, vous pouvez posséder une pierre même si elle est de l'autre côté de la ville par rapport à votre maison. En fait, vous pouvez même utiliser des pierres de rai même si elles ne sont plus visibles. Il y a des centaines d'années, un navire transportant une pierre de rai a coulé au large de la côte. Les villageois locaux ont estimé que la pierre devait encore exister quelque part sur le fond de l'océan, et donc les gens ont continué à se payer avec cette pierre comme si de rien n'était [17] !

En d'autres termes, dans le système des pierres de rai, l'emplacement physique et le mouvement des pierres n'ont aucune importance. Cela contraste fortement avec les systèmes d'argent tangible traditionnels, où l'emplacement physique et le mouvement de l'argent importent : le seul argent que vous possédez est celui qui se trouve chez vous ou sur votre personne, et la seule façon de payer quelqu'un est de lui remettre des objets physiques.

Cela signifie que le système des pierres de rai est une forme de monnaie intangible. C'est un peu comme de l'argent dans une banque, que nous savons intangible : peu importe où se trouvent les billets d'un dollar – ou même s'ils existent ! – et lorsque vous envoyez de l'argent à quelqu'un, aucun objet physique ne bouge.

Sans intermédiaire

De plus, le système des pierres de rai est démocratique : vous possédez une pierre si une majorité de vos compatriotes en est d'accord. Au lieu de faire confiance à une seule personne ou institution pour savoir combien d'argent vous avez, comme vous le feriez dans M3, vous accordez votre confiance à tout le village.

Ce système démocratique pour décider à qui appartiennent les pierres – en d'autres termes, le *consensus* – présente de nombreux avantages par rapport à un système modéré par des intermédiaires. Imaginez un univers alternatif où le chef du village garderait le journal officiel des paiements et de la propriété de la pierre, au lieu que ce soient les villageois qui conservent collectivement un journal consensuel. (Dans cet univers, le système monétaire yapais se comporterait beaucoup comme le M3 ; le chef jouerait le rôle d'une banque.) Le chef pourrait facilement forcer tout le monde à lui payer des frais pour effectuer un paiement, voler des pierres en effaçant délibérément des paiements de son journal de bord, perdre ce journal de bord (et ainsi freiner l'économie locale), etc.

Le système des pierres de rai est donc à la fois intangible *et* sans intermédiaire. Vous bénéficiez de la commodité du M3 – pas besoin de trimbaler des pierres à travers la ville – sans avoir à vous fier à un intermédiaire. Cela donne un exemple de système monétaire présentant « le meilleur des deux mondes » dont nous avons parlé dans la section précédente.

La leçon à tirer ici est que les systèmes d'argent immatériel exigent toujours la confiance : vous ne renoncerez au contrôle physique de votre argent que si vous pouvez être sûr que quelque chose ou quelqu'un conservera une trace précise de votre argent. L'innovation de Yap a consisté à réaliser que vous pouvez faire confiance aux *systèmes* et non aux intermédiaires ; dans ce cas, le système digne de confiance était le journal mental des transactions que tous les villageois yapais partageaient. En accordant votre confiance à un système partagé et basé sur le consensus – un groupe de personnes qui suivent des règles partagées – plutôt qu'à une seule personne ou entité, vous obtenez de l'argent immatériel et sans intermédiaire.

La blockchain de Bitcoin

Nous ne savons pas si Satoshi avait étudié le système de Yap lors du développement de Bitcoin, mais son point de vue était très similaire.

Le Bitcoin est une monnaie numérique, donc intangible, et il est (en théorie) sans intermédiaire, car il ne dépend pas d'une banque ou d'une autre institution pour suivre les soldes monétaires des gens. Au lieu de cela, Bitcoin s'appuie sur un réseau d'ordinateurs dans le monde entier pour conserver un journal, ou *registre*, partagé de chaque paiement passé. Ce « grand livre public partagé », comme on dit, est appelé une blockchain, et c'est essentiellement une version high-tech de la mémoire partagée des villageois yapais concernant les paiements passés.

En bref, Bitcoin est une version moderne et conviviale des pierres de rai. Il est à la fois intangible et (en théorie) sans intermédiaire, ce qui en fait une alternative convaincante à nos systèmes monétaires traditionnels, qui vous obligent à avoir de la tangibilité ou des intermédiaires.

La feuille Google partagée

Une autre façon, plus technique, de penser à la blockchain est une feuille de calcul Google géante qui serait partagée avec chacun dans le monde entier et comporterait une ligne par transaction :

	A	B	C	D
1	**Transaction ID**	**De**	**À**	**Montant**
2	1	origine	A	50
3	2	origine	B	50
4	3	A	C	20
5	4	B	D	25
6	5	D	C	15
7	6	B	A	5

Une façon simplifiée de penser à la blockchain Bitcoin : c'est une feuille de calcul Google partagée avec le monde entier.

(Naturellement, vous voudrez que cette feuille soit en lecture seule : vous ne voudriez pas que des utilisateurs mal intentionnés modifient les transactions passées.)

Quoi qu'il en soit, imaginez que chaque utilisateur de Bitcoin dans le monde ait une copie de cette feuille de calcul stockée sur leurs ordinateurs. Chaque fois que quelqu'un effectue une nouvelle transaction, la transaction est diffusée à tout le monde et les ordinateurs de chacun téléchargent de nouvelles versions de la feuille de calcul.

Minage

Le seul défaut évident en créant une telle feuille de calcul Google pour suivre les paiements est que quelqu'un pourrait essayer de dépenser de l'argent qu'il n'a pas. Il est clair qu'il faut que les transactions soient vérifiées avant d'être soumises afin que les transactions problématiques soient refusées.

Dans le monde M3, vous feriez confiance à une banque ou à une institution financière pour effectuer cette vérification. Votre banque ne vous permettra pas de transférer de l'argent à un ami si vous ne disposez pas de suffisamment d'argent sur votre compte. Mais dans le monde du Bitcoin, vous ne pouvez pas compter sur une personne de confiance pour effectuer la vérification ; cela irait à l'encontre de l'objectif de ne pas avoir d'intermédiaires.

Au lieu de cela, Bitcoin confie ce travail de vérification aux membres de la communauté. Tout utilisateur de Bitcoin peut utiliser son ordinateur pour vérifier les transactions en attente et n'ajouter que les transactions valides à la blockchain. Par souci d'efficacité, les transactions sont regroupées en *blocs* de quelques milliers de transactions [(18)].

Incitations

Mais, bien sûr, les gens ne feront pas le travail calculatoire de vérification des transactions gratuitement, le logiciel Bitcoin doit donc injecter un peu d'argent pour les inciter. Si vous vérifiez un bloc de transactions, vous percevrez des rétributions pour chaque transaction du bloc, et le logiciel Bitcoin vous paiera également un montant

fixe de bitcoins[2], connu sous le nom de *récompense de bloc*. Les bitcoins de la récompense de bloc n'existent pas avant la vérification – le logiciel Bitcoin les crée à partir de rien (19).

Étant donné que Bitcoin se considère comme une version numérique de l'or (20) et que les vérificateurs se mettent au travail pour extraire de l'argent neuf, ce processus de vérification s'appelle le *minage*, et les vérificateurs sont appelés des *mineurs*. (Vous exploitez avec un ordinateur au lieu d'une pelle, mais le modèle commercial est à peu près le même.)

Donc, si nous voulions revenir à notre feuille Google et la faire ressembler davantage à une véritable blockchain, nous ajouterions des colonnes pour les blocs, les rétributions et les récompenses, comme ceci :

	A	B	C	D	E	F	G	H
1	**Block ID**	**Transaction ID**	**De**	**À**	**Montant**	**Mineur**	**Frais de minage**	**Récompense en blocks**
2	B1	T1	A	B	10	C	1	25
3		T2	A	D	15		1	
4		T3	A	E	5		1	
5	B2	T4	B	C	2	E	1	25
6		T5	D	E	5		1	
7		T6	C	A	10		1	

Un modèle plus avancé de la blockchain de Bitcoin, intégrant le minage, les frais et les récompenses.

Ainsi, l'individu C a extrait le bloc B1, qui contenait trois transactions, et a gagné 28 bitcoins pour sa peine : 25 provenant de la récompense de bloc et 1 pour chaque transaction.

2. La devise est appelée « Bitcoin » avec un « B » majuscule, tandis que les unités de devise sont appelées « bitcoins », avec un « b » minuscule. C'est comme la différence entre « le dollar américain » (le nom de la devise) et « dollars » (les unités de la devise).

Quiz express : en supposant que chaque personne (A, B, C, D et E) a démarré avec 100 bitcoins, combien en ont-ils après avoir effectué ces transactions ?

Les réponses :

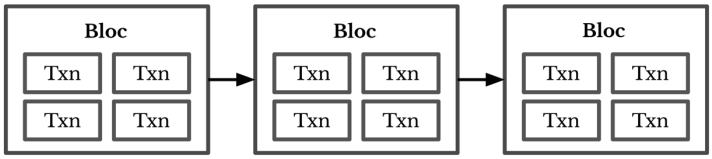
- La personne A a envoyé 10 bitcoins à B et payé des frais de 1 bitcoin, puis a envoyé 15 bitcoins à D et payé des frais de 1 bitcoin, puis envoyé 5 bitcoins à E et payé des frais de 1 bitcoin, puis a reçu 10 bitcoins. Cela signifie que A se retrouve avec 100 - 10 - 1 - 15 - 1 - 5 - 1 + 10 = 77 bitcoins.
- La personne B a reçu 10 bitcoins de A et a envoyé 2 bitcoins (plus des frais de 1 bitcoin) à C. Donc B a maintenant 100 + 10 - 2 - 1 = 107 bitcoins.
- La personne C a gagné 25 + 1 + 1 + 1 = 28 bitcoins du bloc B1, donc elle a 100 + 28 + 2 - 10 - 1 = 119 bitcoins.
- La personne D a maintenant 100 + 15 - 5 - 1 = 109 bitcoins.
- La personne E a également gagné 28 bitcoins grâce au bloc minier B2, donc elle a 100 + 5 + 28 + 5 = 138 bitcoins[3].

Blocs et chaînes

Il s'avère que notre modèle de feuille de calcul n'est que cela : un modèle. C'est une simplification. La véritable blockchain Bitcoin ne stocke pas les blocs dans un format de feuille de calcul.

Au lieu de cela, la blockchain de Bitcoin stocke les blocs dans une « chaîne » linéaire, où chaque bloc pointe mathématiquement vers le précédent (21) :

3. Une journée bien rentable. Nous aimerions tous être la personne E.



La blockchain stocke les blocs dans une chaîne linéaire ; « Txn » est un raccourci Bitcoin pour « transaction ». Chaque bloc fait référence au précédent, mais les informaticiens dessinent généralement des chaînes comme celle-ci avec les flèches pointant d'un bloc au suivant, ce qui est plus intuitif.

De cette façon, l'ordre des blocs est clair même si les blocs ne sont pas explicitement numérotés. Imaginez que vous preniez un roman de poche et que vous déchiriez toutes les pages, supprimant également tous les numéros de page et de chapitre. Imaginez ensuite que vous dispersiez toutes les pages sur le sol.

Vous pourrez néanmoins toujours remettre les pages dans l'ordre, car chaque page fait implicitement référence à ce qui s'est passé sur la dernière page. (Par exemple, si la page X se termine par un personnage qui se rend au palais de justice et que la page Y commence avec le personnage qui entre dans le palais de justice, vous pouvez être à peu près sûr que la page Y vient juste après la page X.)

Hachage

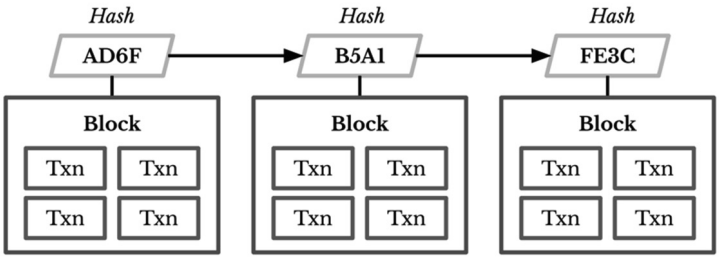
Bitcoin n'a pas de notion de graphique, bien sûr, donc les blocs se référencent mutuellement grâce aux mathématiques. Plus précisément, ils utilisent une technique mathématique appelée le *hachage*, dans laquelle vous insérez un tas d'informations (mots, nombres, blocs Bitcoin, etc.) dans un algorithme qui produit une courte « empreinte » de ces informations [(22)].

Nous autres humains utilisons le hachage tout le temps, par exemple avec les initiales. Un nom long peut facilement être condensé en quelques lettres : un nom long comme « John Fitzgerald Kennedy » devient quelque chose de court comme « JFK ».

Vous avez une entrée (le nom complet) ; la fonction de hachage (le processus de prise des initiales de quelqu'un) ; et une sortie, ou hachage (les initiales).

Les ordinateurs utilisent des fonctions de hachage plus sophistiquées – les plus populaires sont les algorithmes MD5 [23] ou SHA-256 [24] – mais l'idée principale est la même : des données de grande taille en entrée deviennent des sorties courtes.

Dans Bitcoin, chaque bloc a un hachage qui lui est associé. Le hachage de chaque bloc est basé en partie sur le hachage du bloc précédent[4]. De cette façon, chaque bloc fait référence au bloc qui le précède. Donc, si vous avez une liste non ordonnée de blocs et de leurs hachages associés, vous pouvez facilement remettre les blocs dans l'ordre, tout comme la personne qui pourrait réorganiser les pages en examinant les liaisons de l'intrigue.



Les blocs sont enchaînés à l'aide de leurs hachages ; chaque hachage est calculé à partir (entre autres) du hachage du bloc précédent.

(Que se passe-t-il avec les chiffres et les lettres dans les hachages ? Les hachages sont écrits dans le format hexadécimal, en base 16[5]. Ils sont également beaucoup plus longs que 4 caractères [25], mais nos versions abrégées sont suffisantes pour le moment.)

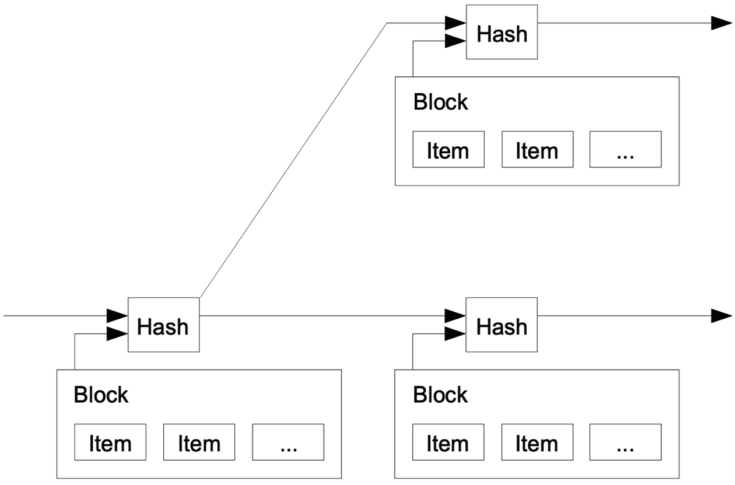
---

4. Nous expliquerons exactement dans quelques pages comment fonctionne le hachage.
5. Voir l'annexe A pour en savoir plus sur les systèmes de nombres hexadécimaux et autres.

Ainsi, Bitcoin regroupe les transactions en blocs et les lie les unes aux autres dans une chaîne. Les blocs rejoignent la chaîne.

Branches et fraude

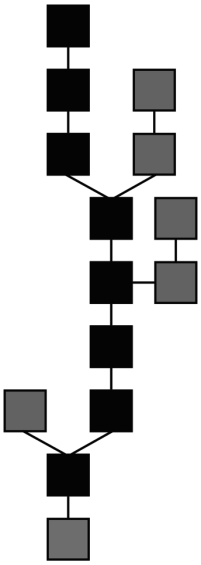
Si vous regardez à nouveau notre système de chaînage basé sur le hachage, vous remarquerez qu'il n'est pas réellement nécessaire que les blocs soient placés dans une chaîne linéaire. Rien ne vous empêche d'avoir deux blocs ou plus juste après un bloc donné :



Plusieurs blocs peuvent mentionner n'importe quel bloc donné comme leur prédécesseur, de sorte que la blockchain peut faire (et fait) des branches. Image adaptée de : Satoshi Nakamoto [26]

L'arbre des blocs

En conséquence, la blockchain n'a pas besoin d'être une chaîne linéaire. En fait, ce n'est généralement pas le cas. La blockchain a tendance à ressembler davantage à un « arbre de blocs », avec un « tronc » et des « branches » :



La blockchain peut avoir de nombreuses branches, tout comme un arbre (imaginez que le bloc du bas est au niveau du sol et que ce diagramme ressemble bien à un arbre.) La plus longue branche est considérée comme la branche « officielle ». Source : Wikipédia [27]

L'arbre des blocs développe parfois une nouvelle branche lorsque deux mineurs génèrent (ou « minent ») un bloc en même temps. C'est rare, mais cela arrive. Quand c'est le cas, deux transactions séparent la transaction la plus récente et une nouvelle branche de l'arbre des blocs est née [28].

Mais, comme avec le système des pierres de rai, Bitcoin se doit d'avoir un historique unique et linéaire des transactions. Vous ne pouvez pas autoriser la coexistence de plusieurs branches. (Pouvez-vous imaginer de dire à quelqu'un : « dans une version de l'historique, j'ai 500 $, mais dans l'autre version, j'ai 600 $ » ?)

BLOCKCHAIN

BULLE OU RÉVOLUTION ?

« Un brillant aperçu de ce qui pourrait être la prochaine grande nouveauté dans le domaine de la technologie, rédigé par des experts des plus grandes entreprises technologiques d'aujourd'hui »
(Nir Eyal, auteur du bestseller* Hooked*)

Certains experts disent que les cryptomonnaies et la blockchain ne sont qu'une arnaque ; pour d'autres il s'agit de « l'invention la plus importante depuis Internet ». Il est difficile de dire qui a raison. Rédigé par des chefs de produit de Google, Microsoft et Facebook, ce livre va au-delà du battage médiatique pour vous offrir une analyse équilibrée, complète et accessible de la blockchain et des cryptomonnaies.

Vous apprenez rapidement les bases de ces technologies ; vous comprenez leurs forces et leurs faiblesses à partir d'études de cas ; vous plongez profondément dans leurs complexités techniques, économiques, politiques et juridiques ; et obtenez un aperçu de leur avenir grâce à des entretiens exclusifs avec des dizaines de leaders de l'industrie technologique.

Cryptomonnaies et blockchain, bulle ou révolution ?

NEEL MEHTA
Product Manager
chez Google

ADI AGASHE
Product Manager
chez Microsoft

PARTH DETROJA
Product Manager
chez Facebook

deboeck SUPÉRIEUR

www.deboecksuperieur.com

ISBN 978-2-8073-3166-2

9 782807 331662