BIBLE

DE L'INVESTISSEMENT DANS LA CRYPTO-MONNAIE

GUIDE SUR LA BLOCKCHAIN, LE MINAGE, LE TRADING,
L'ICO, LA PLATE-FORME ETHEREUM, LES ÉCHANGES

ALAN T. NORMAN

Alan T. Norman

Bible De L'Investissement Dans La Crypto-Monnaie

«Tektime S.r.l.s.»

Norman A.

Bible De L'Investissement Dans La Crypto-Monnaie / A. Norman — «Tektime S.r.l.s.»,

Crypto-monnaie, Bitcoin, ICO, Blockchain, minage... En entendant ces mots il y a quelques années à peine, les gens disaient : c'est une arnaque, une bulle financière. Il ne faut pas investir, le prix est trop bas. Aucun pays ne reconnaîtra la crypto-monnaie. C'est un schéma pyramidal évident, une sorte d'amusement pour les nerds. Jusqu'à récemment, la crypto-monnaie était considérée comme une sorte d'amusement pour une poignée d'élus qui achetaient et vendaient quelque chose et croyaient qu'une nouvelle monnaie ferait un frappée un jour ! Ce n'est pas sérieux, elle s'effondrera dans quelques années. Vous faisiez sûrement partie de ces personnes qui ne prenaient pas au sérieux le Bitcoin et la crypto-monnaie, mais les événements actuels vont à l'encontre même des plus grands sceptiques. Le prix actuel du Bitcoin est de 6644 $. Le prix de la crypto-monnaie la plus populaire bat à plusieurs reprises tous les records impensables. La capitalisation est d'environ 120 milliards de dollars. Une reconnaissance mondiale. Les plus grandes économies du monde - l'Inde et le Japon - ont reconnu le Bitcoin comme monnaie officielle. Les autorités américaines ont reconnu la crypto-monnaie comme un actif. Et ce n'est que le début. Le minage à l'échelle industrielle. Le marché de la crypto-monnaie évolue extrêmement rapidement et il est presque impossible de surveiller la situation et de prendre les bonnes décisions par vous-même. La plupart des gens n'ont pas d'expérience, de temps et d'argent pour cela. Mon livre donne des informations basiques mais assez complètes pour les personnes qui souhaitent créer une entreprise rentable à long terme dans l'un des domaines de la crypto-monnaie : du minage à l'investissement. Donc, ce livre ne concerne pas des moyens illégaux de gagner de l'argent. Ce n'est pas une apologievde la crypto-monnaie vous exhortant à y investir jusqu'au dernier sou. Ce livre vous aidera. Apprenez ce qui suit : quelle façon de gagner de l'argent sur le marché de la crypto-monnaie vous convient le mieux. Par où devriez-vous commencer si vous n'avez que 500 $. Quelles informations sur la crypto-monnaie les experts retiennent. Comment élaborer une stratégie personnelle, créer votre propre entreprise de crypto-monnaie et gagner 3000 à 10 000 $ dès 2018. Je peux également vous garantir que vous:

élucidez la principale tendance actuelle des devises même si vous n'avez aucune idée de l'économie, de la finance et la technologie. Comprenez si vous voulez vraiment investir dans la crypto-monnaie (peut-être, ce type d'entreprise ne vous convient pas du tout et vous perdrez votre temps). Apprenez à vérifier les risques et à ne pas investir dans la première devise disponible. Protégez-vous d'éventuels échecs. Ainsi, mon objectif est assez simple : vous aider à créer et développer des affaires dans l'un des domaines de la crypto-monnaie. Découvrez 7 stratégies d'investissement en crypto-monnaie + 2 stratégies parfaites aujourd'hui !

Содержание

Alan T. Norman
Bible de l'investissement dans la crypto-monnaie

Bible de l’investissement dans la crypto-monnaie

Guide sur la blockchain, le minage, le trading, l’ICO, la plate-forme Ethereum, les Échanges…

Alan T. Norman

Traducteur : Sylvie Cubizolles

Obtenez votre livre gratuit “Bitcoin Whales”

(Se trouve à la fin d’un livre)

Pourquoi Lire Ce Livre

La plupart des personnes accueillent les nouvelles idées avec beaucoup de peur, de scepticisme et même de déni. Bien sûr, il est beaucoup plus sûr de rester dans sa zone de confort et de continuer à marcher sur les sentiers battus. Cependant, à un moment donné, cela vaut peut-être la peine de se demander : jusqu'où cette piste me mènera-t-elle ? Très probablement, cela ne vous mènera pas plus loin que la prochaine étape de votre vie.

Le mouvement est un progrès. Par conséquent, vous devez garder l'esprit ouvert et apprendre de nouvelles choses afin de ne pas vous déliter alors que le monde continue d'avancer. Cela est vrai dans de nombreux domaines de notre vie et encore plus dans les finances personnelles.

D'une part, le papier-monnaie n'est plus répandu. Vous conviendrez probablement qu'il est plus pratique de payer nos frais et notre confort avec la petite carte en plastique émise par votre banque. Ce type de règlement sans espèces est également bien meilleur pour des raisons de sécurité.

Il n'y a pas si longtemps, l'humanité a découvert un autre type d'argent complètement nouveau : l'argent numérique ou la crypto-monnaie. Il s'agit d'une nouvelle génération de monnaie créée grâce à l'utilisation d'un logiciel de cryptage. Ces unités de crypto-monnaie sont formées et préservées grâce à un cryptage algorithmique.

Je voudrais me concentrer un peu sur les types de problèmes que la crypto-monnaie peut résoudre. C'est une question que je soulèverai tout au long de ce livre, mais pour l'instant je veux attirer votre attention sur un concept appelé *confiance*. C'est ce problème important que la crypto-monnaie résout. Laissez-moi vous expliquer en utilisant un exemple de ma vie.

J'ai décidé que je voulais créer une entreprise et gagner de l'argent quand j'étais à l'école. Trois camarades de classe et moi avons décidé de vendre des fleurs. Chacun de nous a noté les informations sur ses gains dans un vieux cahier que nous nous sommes transmis. Quand ce cahier s'est retrouvé entre mes mains et que je voulais vraiment une glace , je me suis demandé si je pouvais modifier les chiffres écrits pour mon propre bénéfice. Mais je me suis sermonné et j'ai pensé : et si mon ami faisait de même ? Ainsi, il est évident que la méfiance peut surgir même entre les amis les plus proches. La crypto-monnaie résout ce problème car elle ne nous permet pas d'ajouter ou de modifier une chose une fois qu'elle est dans le système.

Cependant, l'émergence de la crypto-monnaie, qui résout l'énorme problème de confiance, ne doit pas être associée à l'explosion d'une comète, à un cadeau d'en haut ou à toute autre sorte de début de conte de fées. En réalité, la création de crypto-monnaie est beaucoup plus simple.

Tout d'abord, les technologies correspondantes sont apparues, puis la crypto-monnaie est née sur leur base, suivie du minage (la production de crypto-monnaie). Ce n'est qu'après coup que les jetons, les ICO et divers modèles commerciaux de crypto-monnaie ont vu le jour sur la base de tout cet écosystème. Le registre, qui protège contre la manipulation (c'est-à-dire le référentiel de base de données), est devenu la toute première technologie dans l'économie de la crypto-monnaie. Il y a une petite (ou plutôt grande) particularité chez ces registres : vous pouvez entrer n'importe quelle donnée dans cette base de données mais ne pouvez rien falsifier ou entrer des informations antidatées. Ces contrats auto-exécutoires sont la deuxième technologie importante dans le monde de la crypto-monnaie. Ils sont relies troitement à la base de données.

Je ne vais pas approfondir les détails de toutes ces technologies dans ce livre, car j'ai expliqué les bases dans mon livre précédent, *Mastering Bitcoin for Starters*. Dans le présent manuel, je vais plutôt vous dire comment fonctionne la crypto-monnaie, les dix principales crypto-monnaies et ce que sont les échanges de crypto-monnaie et les échanges de devises numériques. J'expliquerai également la mise en œuvre technique de la Blockchain, la plate-forme Ethereum et de nombreux autres problèmes du monde de la crypto-monnaie. Le point le plus intéressant est que je vais décrire de nombreuses stratégies d'investissement intelligentes.

Dès le début, je tiens à vous avertir que le marché de la crypto-monnaie est vivant et en évolution. Il fonctionne 24 heures sur 24, 7 jours sur 7. Par conséquent, les informations qui étaient à jour le jour où j'ai écrit le livre peuvent ne pas être aussi fraîches le jour où vous l'avez lu. Je recommanderai des ressources dans ce livre auxquelles vous pouvez vous reporter afin de suivre le rythme.

La dernière chose à mentionner ici : je suppose qu'il y a des sceptiques parmi les lecteurs de ce livre. Je conviens que nous devons aborder les nouvelles idées en gardant un certain scepticisme, mais nous devons également être raisonnables. Par conséquent, avant de tirer des conclusions hâtives sur la crypto-monnaie, je suggère de lire attentivement le livre, puis d'analyser les informations que je partage ici. Cela étant dit, mettez de côté vos idées sur la crypto-monnaie pour le moment.

Si vous êtes prêt à plonger dans le monde de la crypto-monnaie, c'est parti !

Chapitre 1. Les mythes sur la crypto-monnaie et les principales règles du marché de la crypto-monnaie

Avant de définir des objectifs dans le secteur de la crypto-monnaie, examinons d'abord certaines idées fausses courantes sur la crypto-monnaie.

Mythes De La Crypto-Monnaie

J'admets franchement que j'ai aussi failli être infecté par le scepticisme à l'égard de la crypto-monnaie au début de mon aventure, car de nombreuses personnes m'ont fait peur en me disant que la crypto-monnaie est une entreprise sauvage, une pyramide financière, etc. De telles fausses croyances empêchent souvent de nombreuses personnes de réussir. Seul un petit nombre de personnes entreprenantes vérifient ces déclarations sur la crypto-monnaie au lieu de les croire aveuglément.

Je suis sûr que vous avez également entendu des allégations selon lesquelles aucun pays ne reconnaîtra jamais la crypto-monnaie, donc la crypto-monnaie n'a pas d'avenir. Pour réfuter cette hypothèse, il suffit de rappeler la récente augmentation de la valeur de la crypto-monnaie. Certains pays ont déjà reconnu la crypto-monnaie comme moyen de paiement. Ainsi, ce soi-disant « divertissement pour geeks » a évolué en une véritable activité pour les banquiers d'investissement et diverses entreprises.

Par conséquent, si, personnellement, vous ne gagnez toujours pas d'argent avec la crypto-monnaie, c'est probablement à cause du grand nombre de déclarations susmentionnées, que vous avez peut-être entendues de pseudo-experts.

Énumérons les déclarations qui arrêtent de nombreuses personnes à mi-chemin :

1. C'est trop risqué. Et si j'investis de l'argent et que la crypto-monnaie est interdite dans le monde entier le lendemain ?
2. Je n'ai aucune connaissance financière et je ne saurai donc pas ce que je fais ;
3. Mon ami/frère/voisin a investi de l'argent dans la crypto-monnaie et a tout perdu ;
4. Le sujet de la crypto-monnaie est trop nouveau et difficile à comprendre tel quel, donc je ferais mieux d'attendre quelques années lorsque tout deviendra clair.

Toutes ces déclarations ne sont que des excuses pour votre inaction. Pendant que vous trouvez des excuses supplémentaires, des personnes du monde entier ont déjà créé une entreprise sur le marché de la crypto-monnaie et réalisent des bénéfices. Demandez-vous : qu'est-ce qui me rend pire que ces personnes ? Si vous réalisez que vous n'êtes pas pire que votre ami/frère/voisin, qui gagne déjà de l'argent sur le marché de la crypto-monnaie, alors posez-vous la question suivante : pourquoi devrais-je entrer dans le monde de la crypto-monnaie en ce moment ?

Pourquoi Vous Devez Entrer Dans Le Monde Des Entreprises De Crypto-Monnaie Maintenant

Je vais donc répondre à cette question point par point. Chacun des arguments comportera le mot “actuellement” afin que vous compreniez mieux pourquoi vous devriez le faire maintenant.

Premièrement, il existe très peu de concurrence sur le marché **actuellement**. Vous êtes surpris ? C’est vrai. Oui, l’intérêt pour ce sujet ne cesse de croître, mais en général, la concurrence est encore très faible. Ce marché est encore assez « sauvage » et non maîtrisé. La raison en est que la plupart des personnes ont tendance à ne pas faire confiance aux nouvelles tendances et aux nouvelles entreprises, comme nous l’avons déjà mentionné ci-dessus.

Deuxièmement, vous pouvez **actuellement** obtenir des rendements élevés sur ce marché. Les prix des crypto-monnaies sont au stade de la croissance et du développement, mais même ainsi, vous pouvez gagner une somme d’argent décente. Tant que vous gérez judicieusement vos risques, vous pouvez réaliser des bénéfices à temps.

Troisièmement, il y a beaucoup de freeloaders sur le marché **actuellement**. Ils arrivent sur le marché de la crypto-monnaie pour gagner rapidement de l’argent sans se plonger dans le sujet. Habituellement, ces personnes viennent des systèmes pyramidaux dirigés par des soi-disant « experts » qui enseignent à autrui sans avoir eux-mêmes une réelle expérience du sujet. Je dois admettre que le marché a encouragé ces personnes au début, alors qu’elles avaient la chance de gagner beaucoup d’argent à l’époque. Cependant, de nos jours, si vous voulez réaliser une telle chose sur le marché de la crypto-monnaie, vous devrez faire de réels efforts.

Quatrièmement, les risques sont faibles sur le marché **actuellement**. Il y a cinq ans, la plupart des personnes attendaient le jour où la crypto-monnaie serait officiellement interdite. Désormais, de nombreux pays du monde entier ont déjà reconnu la pertinence de la crypto-monnaie. La crypto-monnaie a pris un tel élan que personne ne peut simplement appuyer sur le bouton d’arrêt maintenant. Pensez-vous vraiment que ce fait ne prouve pas que vous pouvez investir votre argent sans craindre diverses interdictions et restrictions ?

Enfin, avant de passer aux règles du jeu sur le marché de la crypto-monnaie, je propose d’envisager l’avenir de la crypto-monnaie à travers l’exemple de la société Tesla. Actuellement, le coût d’une Tesla est estimé à un montant qui, selon les prévisions des experts, ne pourra pas rembourser ses dépenses dans 300 ans. Pourquoi les experts intelligents évaluent-ils si bien Tesla alors ? Voyons cela.

De nos jours, une voiture électrique est belle et élégante mais chère et pas très pratique. Cependant, les experts ne sont pas préoccupés par aujourd’hui. Ils visualisent un futur qui peut devenir réalité dans 20 ou 30 ans. Il est difficile d’imaginer dans les années à venir les voitures ordinaires que l’on voit quotidiennement dans les rues aujourd’hui. Vous pouvez imaginer votre vieille voiture bien-aimée à l’avenir, mais personnellement, j’imagine une sorte de véhicule avec un demi-volant avec des panneaux solaires ou quelque chose d’encore plus sophistiqué. Par conséquent, c’est le véhicule électrique qui aura un avenir radieux et prospère, et Tesla est susceptible d’occuper une position de leader sur le marché.

Il s’avère que, dans l’ensemble, personne ne sait avec certitude si Tesla conservera sa position sur le marché au cours des 20 à 30 prochaines années. Cependant, de nombreuses personnes croient fermement que ce sera le cas, et cette conviction les pousse à investir dans l’entreprise. Par conséquent, personnellement, je peux facilement croire que Tesla détiendra un monopole dans tout le secteur de la fabrication automobile dans 20 ans.

Comment cet exemple est-il lié à l’avenir de la crypto-monnaie ? De nos jours, certaines personnes considèrent la crypto-monnaie (comme un véhicule électrique) comme dénuée de sens – une tendance à la mode, intéressante et techniquement curieuse. Mais une tendance, néanmoins.

Cependant, cette petite goutte maintenant est susceptible de devenir une grande mer dominante à l’avenir.

Fixer Des Objectifs Et Identifier Les Principales Règles Du Marché

Avant d'innover, les vrais professionnels apprennent les règles du jeu et se fixent des objectifs, déterminant le type de résultat qu'ils souhaitent atteindre. Puisque nous sommes des professionnels, nous nous occuperons d'abord de cette tâche.

Les points suivants doivent sûrement faire partie des objectifs de trading de crypto-monnaie que vous vous fixerez :

- définir la somme d'argent spécifique ou le pourcentage de vos revenus que vous investirez mensuellement dans le domaine de la crypto-monnaie ;
- définir votre degré de préparation aux risques ;
- définir vos objectifs spécifiques à court et à long terme.

Après avoir défini les objectifs, il est important de comprendre ce qui est nécessaire pour un démarrage réussi et rapide sur le marché de la crypto-monnaie. Vous serez surpris, mais la théorie est ce qui importe le moins dans ce domaine. De nombreuses personnes disent ne pas avoir les informations et les connaissances nécessaires pour se lancer dans ce type d'entreprise. Cependant, la plupart des stratégies dont je vais vous parler ne nécessitent pas une connaissance approfondie du monde de la crypto-monnaie. Il vous suffira de maîtriser les principes de base de l'économie de la crypto-monnaie.

Alors quel est le problème ? Vous avez besoin de pratique. Seule la pratique, pas un livre (pas même le mien), vous aidera à comprendre où acheter, où vendre, comment stocker et comment transférer de la crypto-monnaie.

Vous aurez également besoin de :

- Plusieurs stratégies toutes à faible risque pour entrer sur le marché
- Une possibilité de filtrer le contenu et les informations autour de vous
- La communication avec des traders plus expérimentés du marché de la crypto-monnaie et un « espionnage » de leurs actions
- La gestion des risques
- Un audit par une personne expérimentée.

Et maintenant, nous passons à l'affirmation dont vous devez vous souvenir une fois pour toutes : tout investissement sur le marché de la crypto-monnaie EST UN RISQUE. Si vous n'êtes pas prêt à l'accepter, n'essayez pas. Toute opinion ou prévision concernant le développement d'une devise particulière, la fiabilité de l'ICO (cela sera discuté plus tard) n'est qu'une position biaisée. Il n'y a pas une seule personne dans le monde qui puisse vous donner une garantie absolue pour de futurs développements. Il n'y a absolument pas de bonnes décisions et des garanties à 100 %. Moi ou quelqu'un d'autre ne pouvons que vous donner un conseil, pas des garanties.

Vous êtes la seule personne responsable de chaque décision. Vous ne devez pas par la suite reprocher vos éventuelles pertes financières à une ressource en ligne, où vous lisez des informations sur les perspectives de certaines devises, ou un ami qui vous a recommandé une ICO fiable ou même moi ! En tant qu'auteur de ce livre, je partagerai avec vous mes réflexions sur les crypto-monnaies fiables. Cependant, ce ne sera que mon opinion subjective, encore une fois, seulement en ce moment même. Par conséquent, si vous êtes du genre à reprocher vos éventuels échecs aux autres, et non vous-même, vous feriez mieux de fermer ce livre immédiatement et de ne pas perdre de temps.

Le marché de la crypto-monnaie est vivant et en constante évolution. Par conséquent, lorsqu'il s'agit de trading de crypto-monnaie, il faut apprendre à assumer personnellement la responsabilité de prendre des décisions et toujours se rappeler qu'aucun gain ne peut être réalisé sans prendre de risques.

Oui, il existe des stratégies moins risquées, mais des risques existent dans tous les cas. N'investissez que la somme que vous êtes prêt à perdre sans trop de regret.

Et maintenant, mettez le livre de côté et notez les deux règles à ne jamais enfreindre :

1. N'investissez pas jusqu'au dernier centime.
2. Ayez une réserve d'argent pour profiter des opportunités.

Et enfin, les débutants doivent retenir plusieurs points concernant la sécurité :

- Lorsque vous négociez en bourse, protégez votre compte avec une authentification à deux facteurs et gardez votre mot de passe privé.
- Votre mot de passe doit comporter au moins 26 caractères ; un générateur de mot de passe spécial peut vous aider à en trouver un.
- Ne gardez jamais tout votre argent sur une seule bourse ou dans un seul portefeuille.
- Ne négociez que sur des bourses éprouvées.
- N'utilisez pas de points d'accès publics pour trader sur le marché de la crypto-monnaie.

Chapitre 2. Les principes fondamentaux de la crypto-monnaie et son héros

Adoptons une approche détournée de ce sujet, en partant du secteur bancaire.

L'ensemble du système bancaire de nos jours, quel que soit le pays, est organisé de telle manière que nous ne possédons pas notre argent. Les banques centrales de tous les états détiennent le monopole des émissions, qui est prévu par la législation, créant une pierre d'achoppement sûre pour la légalisation de la crypto-monnaie.

La *monnaie fiduciaire* est un terme utilisé par la communauté des crypto-monnaies pour désigner une monnaie sans valeur intrinsèque comme monnaie par la réglementation gouvernementale ou la loi (dollar, euro, etc.).

En théorie, cette monnaie devrait être garantie au moins par les biens, produits ou services produits sur le territoire d'un pays particulier (PIB) afin que chaque citoyen de ce pays puisse changer son argent personnel contre des produits. Toutes les banques du pays s'engagent également dans la même monnaie, et la banque centrale promet de maintenir sa stabilité et sa fiabilité. C'est ainsi que cela fonctionne en théorie, mais personne ne peut réellement garantir la stabilité de la monnaie.

Le gouvernement d'un pays est le principal client de tous les biens et services pour la population, c'est-à-dire l'un des plus grands employeurs. C'est également le plus gros client pour la construction de routes, de maisons, d'hôpitaux, d'écoles, etc. Cela représente la part du lion du PIB de chaque pays. En conséquence, le gouvernement assure la vie de la population, verse des pensions et des prestations sociales. Tous ces fonds proviennent de la banque centrale, qui peut émettre des devises et financer le gouvernement.

Une politique baptisée *quantitative easing* (assouplissement quantitatif) a été une fois mise en œuvre aux États-Unis et s'est même répandue plus tard en Europe et au Japon. En raison de ce phénomène, la quantité de monnaie dans le monde a considérablement augmenté, tandis que le pouvoir d'achat du dollar a diminué de 95 % au cours des 100 dernières années. Cette tendance se poursuit. Plus il y a d'argent, moins il coûte cher.

Il est important de garder à l'esprit que chaque type de monnaie subit une inflation, ce qui indique la dépréciation de la monnaie sur un certain temps. En d'autres termes, l'inflation est la vitesse de circulation de l'argent. L'économie du pays a ses propres cycles, car les individus contractent des prêts et les remboursent.

Je ne peux m'empêcher de mentionner ces prêts. Aux États-Unis, les taux d'intérêt des prêts sont en moyenne de 1 %. Ils sont restés à zéro pendant longtemps dans le passé. Les banques centrales ont émis de l'argent et acheté des actifs financiers, et par conséquent, les pauvres sont restés pauvres, et ceux qui avaient des actifs financiers, des actions ou des biens immobiliers ont réalisé un profit constant. C'est pourquoi chaque crise rend les pauvres encore plus pauvres et les riches encore plus riches. Ces processus aboutissent à une stratification très puissante de la population. Cependant, hélas, l'économie fonctionne de cette manière, et nous nous approchons d'une sorte d'impasse, comme le disent de nombreux analystes financiers. Tout cela pour démontrer que les banques centrales ne s'acquittent pas très bien de leur fonction.

Les individus ont donc commencé à chercher une autre façon de préserver la valeur de l'argent. Sinon la multiplier, du moins ne pas la perdre. C'est la raison pour laquelle de nombreuses personnes investissent dans l'or, les instruments à revenu fixe, les actions, etc. Dans le même temps, l'économie a commencé à se développer rapidement après l'apparition d'Internet. Ainsi, le concept de monnaie électronique a émergé.

L’idée de créer une monnaie numérique comme le Bitcoin n’est pas entièrement nouvelle. Pourtant, il existe une différence entre le Bitcoin et d’autres types de monnaie numérique. Si vous utilisez des systèmes de monnaie électronique tels que PayPal, Western Union ou Skrill, vos fonds sont stockés dans les mêmes sociétés. Dans ce cas, ces systèmes s’occupent de la gestion centralisée de l’argent, c’est-à-dire que le sort de votre argent dépend des décisions de personnes spécifiques de ces entreprises. Vous n’avez aucun pouvoir pour influencer ces décisions.

Les Avantages De La Crypto-Monnaie

La crypto-monnaie est assez différente. Cette monnaie décentralisée se caractérise par l'indépendance d'un centre de traitement des transactions unique. Il est très difficile de suivre les transactions de crypto-monnaie et impossible de les annuler. En utilisant ce type de monnaie, deux personnes peuvent effectuer une transaction d'achat et de vente directement sur Internet, sans recourir au centre des transactions financières.

Mais discutons plus en détail des avantages de la crypto-monnaie par rapport à la monnaie fiduciaire. Ces avantages sont évidents !

- **Emission et normes de circulation** : la crypto-monnaie est établie une fois et elle est inviolable, tandis que les normes de la monnaie fiduciaire sont modifiées arbitrairement par les banques centrales.
- **Le problème** est résolu : la crypto-monnaie circule du réseau vers le participant tandis que la monnaie fiduciaire circule de la banque centrale vers les banques, des banques vers les entreprises et uniquement des entreprises vers les participants.
- **Le flux de fonds** : direct pour la crypto-monnaie ; par le biais des banques, des systèmes de paiement et des espèces contre de la monnaie fiduciaire.
- **Le nombre de participants** : 5 millions pour la crypto-monnaie ; 7 milliards pour la monnaie fiduciaire.
- **La vitesse de transaction** : élevée pour la crypto-monnaie ; faible pour la monnaie fiduciaire.
- **L'anonymat** : toujours possible pour la crypto-monnaie ; parfois possible lorsqu'il s'agit d'espèces contre de la monnaie fiduciaire.
- **L'inflation** : impossible uniquement pour la crypto-monnaie ; une réalité constante pour la monnaie fiduciaire.
- **La volatilité du taux** : certainement élevé pour la crypto-monnaie ; faible pour la monnaie fiduciaire.

L’inventeur Du Bitcoin Et Pourquoi Il Est Le Héros De Notre Temps

Au milieu de la crise financière mondiale de 2008, une personne du nom de Satoshi Nakamoto a conçu le Bitcoin et créé son implémentation de référence d’origine. Il a publié le premier logiciel de Bitcoin qui a lancé le réseau et les premières unités de la crypto-monnaie Bitcoin. Le Bitcoin est devenu un nouveau type de monnaie numérique, très différent de tous les autres. Sa principale différence réside dans le fait qu’il est décentralisé. Par conséquent, chaque participant ne peut pas influencer son sort.

La question suivante se pose. Il y a de nombreuses personnes sur le réseau, elles ne se connaissent pas et il est logique qu’elles ne se fassent pas confiance. Alors, comment peuvent-elles être sûres que les paiements sont effectués et que leur argent ne sera pas volé ? Cependant, tout a été pensé à l’avance par Satoshi Nakamoto et je l’ai soigneusement décrit dans le livre *Mastering Bitcoin for Starters*. Il a suffit d’affirmer que la vision de Nakamoto pour une monnaie décentralisée était vraie, résolvant ainsi de nombreux problèmes.

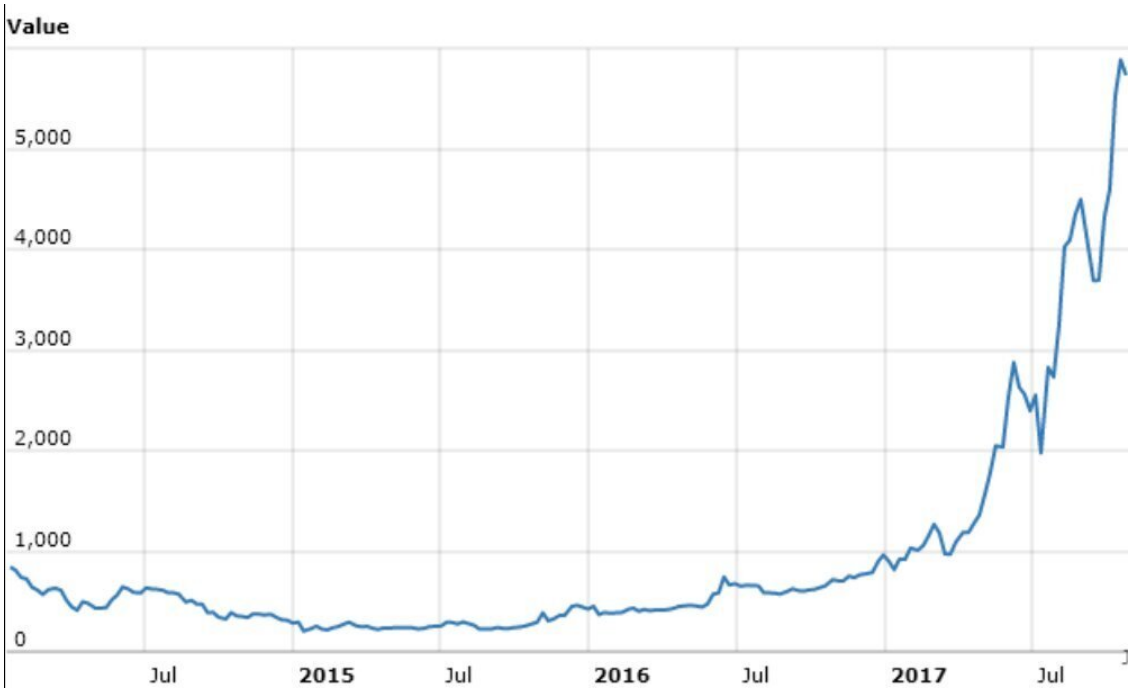
À propos, l’identité de Satoshi Nakamoto est toujours entourée de mystère. Plusieurs tentatives ont été faites pour la divulguer car certaines personnes pensent que Satoshi Nakamoto est un groupe de personnes plutôt qu’une seule personne. Cependant, aucune de ces tentatives ne s’est avérée fructueuse.

Chapitre 3. Le bitcoin et le minage

Pour comprendre l'essence du Bitcoin, nous devons nous plonger dans le minage. Je vous parlerai plus tard du minage en tant que stratégie d'investissement, mais pour l'instant, considérons le minage uniquement en termes de l'émergence du Bitcoin.

Il y a quelques années, de nombreuses personnes considéraient le minage, la production de crypto-monnaie ou de Bitcoins, comme une sorte de passe-temps. Beaucoup ont joué à ce jeu jusqu'à ce que la fameuse situation de la pizza se produise. Ce jour est connu sous le nom de Pizza Day dans la communauté des crypto-monnaies. Le 22 mai 2010, un développeur a payé 10000 BTC à un autre utilisateur du forum Bitcoin pour deux pizzas. À l'époque, le Bitcoin ne valait presque rien. Ces deux pizzas coûtent à l'utilisateur environ 25 $. Actuellement (octobre 2017), un Bitcoin coûte plus de 5000 $. Vous pouvez facilement calculer que ces deux pizzas coûtent des millions de dollars à cette personne.

C'était la première fois que le Bitcoin pénétrait dans le monde réel.



Ce graphique montre que le Bitcoin a connu des hauts et des bas. Cependant, il a été multiplié plusieurs fois depuis 2016.

Le Bitcoin a été miné pour la première fois à l'échelle industrielle lorsque sa valeur a commencé à augmenter. Premièrement, la puissance de calcul a été utilisée pour miner le Bitcoin. Plus tard, les mineurs ont commencé à utiliser des cartes graphiques pour former les blocs. Désormais, ils utilisent un équipement spécialisé appelé ASIC. Les plus grandes fermes de ce type sont maintenant situées en Chine.

Fonctionnement Du Processus De Minage

Le minage est le processus de production de nouvelles crypto-monnaies ou Bitcoins. Voyons comment fonctionne le minage. Lorsque, par exemple, vous envoyez de l'argent de votre portefeuille au portefeuille d'une autre personne, vos transactions tombent dans ce que l'on appelle le « mempool ». Le Bitcoin mempool est une collection de toutes les transactions en attente de recevoir une confirmation du réseau. Les mineurs, guidés par leurs propres principes, collectent les transactions dans des blocs spécifiques puis tentent de les insérer dans la Blockchain. Chaque bloc de la Blockchain génère toutes les dix minutes.

C'est ainsi que nous voyons la transaction en Bitcoin.

C'est la façon dont un ordinateur la voit.

Input Scripts

OP_FALSE
304402201280bf056-
ca0554b4f5a95a2cda31a20f133115c708aab54855ac386fd23b10c02207c5bb3365be40b9de1ebe8759202964d931dab939b23553e3aa7882fd63f6ab201
30450221008c4df3615360c2b26f7655de5bdc995eb2cc24e7759a60c0ee6dbbcab0b1899a022065102895b6868f945517aef647183e4e06e7d03d725f06b
d3c9d71374d33cff501
522103a623c04847602e74a38ec99977741d6b475c6fe2abfe13fc55dbcde3aead46312103aa7e108ae96ab9f13478fa152a1c48ff734e14f5064169755b465
09a9519fc52ae

OP_FALSE
304502210083475cd31a99906966bf069e9100408ba2d2912932be48e3637932972689276330220 6edccad7406618c1748917dcf02a78b4ff50413721c867
dcb22de7450f1c1c5701
3044022065e58aedb77768193757c72a10ed89ccd6ff35346513e9406c39d02a89a38a6002207805b1fa66887e8cae51a4b14ff00bdc2021686d8980a38292
eecf6960be66601
522103a623c04847602e74a38ec99977741d6b475c6fe2abfe13fc55dbcde3aead46312103aa7e108ae96ab9f13478fa152a1c48ff734e14f5064169755b6d46
509a9519fc52ae

Output Scripts
OP_DUP OP_HASH160 d420a78d07141a3a8d0a53c58dc9da5822e21877 OP_EQUALVERIFY OP_CHECKSIG
OP_HASH160 f0071b1141b8728a45d5d5d4ff9d147a3f091e50be OP_EQUAL

Un mineur obtient une récompense pour le minage d'un bloc. Actuellement, la récompense est de 12 bitcoins. Autrement dit, si vous introduisez un bloc bien formé dans le système, vous obtiendrez une telle récompense. À propos, le tout premier bloc (Genesis) a été créé par Satoshi Nakamoto. N'importe qui pourrait le trouver et obtenir 50 bitcoins pour ce denier. Aujourd'hui, la récompense d'un bloc correctement formé commence à chuter. On dit qu'elle chutera à une valeur infinitésimale en 2140.

Un jour, des mineurs ont réalisé qu'il n'était pas rentable de miner de manière autonome. La probabilité que vous trouviez un tel bloc dépend du « taux de hachag e» ou de la puissance de la machine de votre mineur en Bitcoin. Sous certaines valeurs acceptables, si, par exemple, votre taux de hachage représente 10 % du taux de hachage total, vous pourrez trouver de tels blocs avec une probabilité de 10 % et obtenir votre récompense. Donc, si vous exploitez simplement votre ordinateur portable à la maison, vous ne trouverez jamais de nouveau bloc. Par conséquent, afin d'obtenir une récompense plus stable, les mineurs s'unissent dans les soi-disant pools de minage. Ils utilisent leur taux de hachage uni pour récolter des bénéfices plus réguliers.

Maintenant, de nombreux mineurs ont commencé à penser : pourquoi devrais-je miner si je peux acheter du Bitcoin ? C'est également une bonne idée car la valeur du Bitcoin n'est déterminée que par la croyance des personnes qui l'utilisent, tandis que son coût est déterminé par la demande. Si personne ne vous achète votre Bitcoin, cela ne vous coûtera rien. Par conséquent, tant que les individus verront cette technologie comme une opportunité de l'utiliser de manière anonyme, d'effectuer des paiements importants, etc., la valeur du Bitcoin prendra de l'ampleur.

Je ne me concentrerai pas sur le Bitcoin lui-même plus en détail car j'ai dédié mon livre précédent, *Mastering Bitcoin for Starters*, à ce sujet. Pour l'instant, je vais considérer les avantages du Bitcoin, qui soulèvent encore quelques questions.

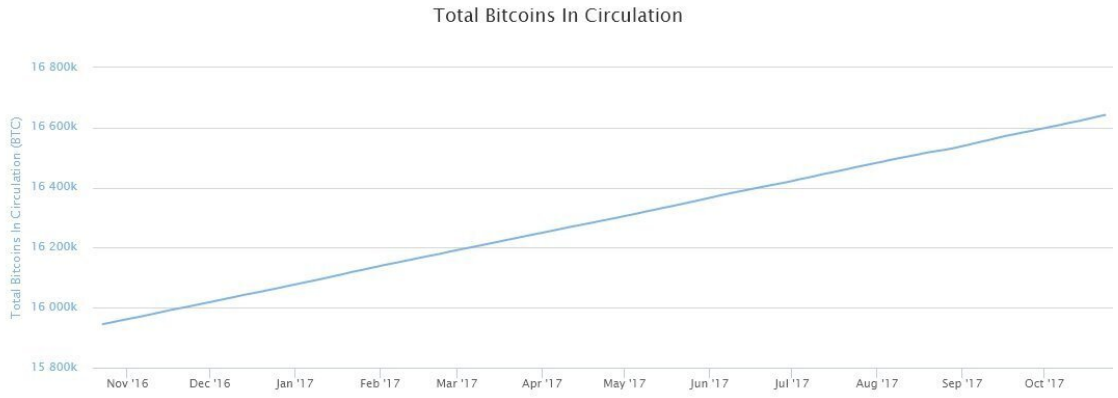
Le premier avantage réside dans les **faibles coûts de transaction**. Cependant, nous devons garder à l'esprit que le Bitcoin n'est pas assez adapté pour les micropaiements. Si vous transférez 1 million de dollars à quelqu'un, cela vous coûtera pas grand chose. Cependant, si vous décidez de payer une tasse de café, les frais seront élevés par rapport au coût de votre café.

Le deuxième avantage est le **traitement des transactions à grande vitesse**. Voici également quelques problèmes. En réalité, chaque bloc de la Blockchain génère toutes les dix minutes, c'est-à-dire que la transaction la plus rapide possible prend dix minutes. Il semble que ce soit plutôt rapide comparé au transfert SWIFT dans une banque, qui peut prendre 2 à 4 jours. Cependant, Visa et MasterCard sont beaucoup plus rapides. Ils peuvent traiter des dizaines de milliers de transactions en plus par unité de temps que le Bitcoin. Il est à noter qu'il existe maintenant d'autres types de crypto-monnaie qui ont été développés pour être plus rapides que le Bitcoin.

Le troisième avantage est le **pseudo-anonymat des participants**. Nous avons déjà étudié que n'importe qui peut suivre toutes les transactions sur le réseau. Si vous connaissez le propriétaire exact d'un portefeuille, vous pouvez suivre absolument toutes les transactions effectuées à partir de celui-ci. On ne peut donc pas dire que le Bitcoin est absolument anonyme. Dès que l'on parvient à faire correspondre votre adresse avec votre personnalité, l'anonymat disparaît. Mais si vous observez la soi-disant « hygiène Internet », c'est-à-dire que vous ne montrez votre portefeuille à personne, alors, fondamentalement, vos transactions ne peuvent pas être suivies. Je dois mentionner, cependant, qu'il existe d'autres crypto-monnaies qui sont plus anonymes que le Bitcoin.

En passant, si vous souhaitez rester anonyme lors de transactions sur le réseau Bitcoin, c'est déjà possible. Il existe de nombreux services qui s'occupent de vos Bitcoins. Ils sont appelés « services de mixage » et sont utilisés pour mélanger ses fonds avec les Bitcoins d'autres personnes, dans l'intention de brouiller l'accès vers la source d'origine des fonds. Comme vous le voyez, les nouvelles technologies semblent renforcer l'anonymat des crypto-monnaies.

Et, enfin, maintenant plus de 16 millions de bitcoins circulent dans le monde, alors qu'un total de 21 millions sera exploité. Ces chiffres sont programmés par l'algorithme du réseau lui-même. La quantité limitée de Bitcoins rend l'inflation de cette monnaie impossible. Cette devise ne se déprécie pas avec le temps car seul un certain montant sera émis. Le Bitcoin a même un modèle déflationniste : de nombreuses personnes perdent leurs devises en oubliant le mot de passe du portefeuille ou en envoyant de l'argent à la mauvaise adresse. Par conséquent, le nombre de Bitcoins diminuera progressivement.



Preuve De Fonctionnement Et Pourquoi C'est Important

Les plus gros problèmes du réseau Bitcoin étaient les suivants : comment s'assurer que les transactions sont vraiment véridiques ; comment s'assurer qu'un mineur ne trompe personne ; que faut-il faire pour choisir le bon bloc et construire réellement la Blockchain. Toutes ces questions sont réglées via l'*algorithme de consensus*.

Le protocole **Proof of Work** (preuve de fonctionnement) confirme qu'un mineur effectue un travail énorme pour trouver un nonce correct et obtenir un hachage réussi. Vous devriez passer beaucoup de temps à trouver celui dont vous avez besoin. Je vais vous expliquer plus en détail.

La difficulté de bloc est ajustée tous les blocs de 2016 et dépend du nombre de zéros au début d'un hachage particulier. Il n'est pas difficile de trouver le hachage lui-même, mais il faut se donner beaucoup de mal pour trouver un hachage réussi avec un certain nombre de zéros. Si vous avez le hachage d'un bloc précédent ainsi que des données d'horodatage et de transaction, il semble qu'il soit très facile de créer un nouveau hachage à partir de celui-ci et de traiter ce bloc. Cependant, vous devez trouver un nonce, dont la valeur est définie de sorte que le hachage du bloc contienne une série de zéros non significatifs. Il faut beaucoup de temps pour cela. Une fois que les mineurs trouvent ce hachage réussi, ils envoient un bloc à la Blockchain. Autrement dit, ils ont déjà confirmé toutes les transactions, après avoir effectué un certain travail. Donc, il ne sert à rien de tromper quelqu'un car un tel travail est très difficile à faire.

Ensuite, toutes les informations sont distribuées dans les nœuds. Tout d'abord, un mineur envoie un nœud. Il peut vérifier si, par exemple, les personnes qui ont envoyé de l'argent d'un point A à un point B avaient vraiment cet argent, c'est-à-dire si toutes les transactions sont valides. Ensuite, les nœuds commencent à échanger ces informations entre eux, et ainsi, le bloc est formé.

En théorie, il peut arriver que deux mineurs créent un seul et même bloc. Comment la Blockchain choisira-t-elle le meilleur bloc ? Le premier principe est la vitesse. Le deuxième principe est le « succès » d'un hachage. Par conséquent, le « succès » d'un hachage est exactement les efforts que les mineurs doivent faire dans le cadre du protocole de preuve de fonctionnement.

Une autre raison pour laquelle vous devez choisir un hachage « réussi » est un ajustement de la difficulté du réseau. Plus les mineurs apparaissent, plus la difficulté du réseau augmente, ce qui signifie que les transactions peuvent être traitées plus rapidement. Si les mineurs ralentissent pour trouver les blocs, la difficulté diminue.

Permettez-moi d'ajouter quelques mots sur la façon de régler la situation lorsque plusieurs mineurs créent des blocs identiques sur le réseau. L'essence du consensus de la Blockchain est que la plus longue chaîne de blocs est considérée comme équitable. Si les blocs commencent à être construits dans une direction différente de la vôtre, votre premier bloc tombera à nouveau dans le pool de transactions non confirmées. Cela se produit souvent lorsque le réseau est surchargé. Donc, pour vous assurer que les blocs suivants sont construits exactement sous votre bloc et que vous obtiendrez la récompense, attendez que plusieurs autres blocs se forment après le vôtre. Si plus de cinq blocs sont formés, l'argent vous appartient définitivement.

À la fin de la sous-section précédente, nous avons discuté des avantages du Bitcoin, il est donc temps de parler des inconvénients de la Blockchain, à savoir l'attaque à 51 % ou la double dépense. Je vais vous expliquer.

Tout pool de minage peut unir ses efforts à un point tel que la probabilité de générer le bloc suivant dans ce pool peut être de 51 %. La communauté des crypto-monnaies a déjà été témoin de la situation lorsque les membres du pool de minage chinois ont artificiellement restreint de nouveaux membres dans leur système et ont réussi à générer environ six blocs d'affilée. C'est après cet incident qu'il est devenu clair qu'il fallait attendre la confirmation de la transaction pendant une heure, pas dix minutes. Autrement dit, si vous créez cinq blocs et que chacun d'eux est formé pendant dix minutes, nous multiplions par cinq et obtenons 50 minutes.

Chapitre 4. La blockchain

Avant d'entrer dans les détails techniques de la technologie Blockchain, il est important de comprendre les problèmes que la Blockchain résout. Pourquoi avons-nous besoin de la Blockchain et que fait-elle que notre technologie actuelle ne peut pas faire ?

Les premiers utilisateurs de la technologie Bitcoin et Blockchain ont repéré ce qu'ils percevaient comme une faille fondamentale dans notre façon de penser les transactions, la confiance et les institutions sociales. Les premières versions de la Blockchain sont arrivées à peu près au même moment que la crise financière de 2007 aux États-Unis, lorsque de nombreuses personnes ont perdu confiance dans les institutions de la société censées protéger les intérêts de l'individu ordinaire. Bien sûr, les gens ont été désillusionnés par le système bancaire à la suite de la crise, mais ils ont également perdu confiance dans le gouvernement pour réglementer les marchés financiers et dans la presse pour enquêter sur les crises potentielles.

La plupart des gens conviendraient que nos institutions ont des défauts et ne sont pas des solutions parfaites. Mais ellesrésolvent les problèmes de confiance, et elles le font depuis des centaines d'années. En réalité, nous vivons probablement à l'époque la plus paisible et la plus confortable de l'histoire de l'humanité. Toute alternative à nos institutions actuelles doit avoir des avantages et des atouts évidents.

L'idée derrière la Blockchain est de remplacer les institutions dirigées par des êtres humains imparfaits par une technologie capable de mieux faire le travail et de responsabiliser les individus. Si vous pouviez créer un moyen pour des étrangers de se faire confiance sans avoir besoin d'une banque ou d'un gouvernement comme intermédiaire, vous vous attaqueriez à l'un des plus grands goulots d'étranglement de la société. Mais pour ce faire, vous avez besoin d'un système puissant pour créer un consensus entre étrangers, et les créateurs de la Blockchain estiment que le pouvoir réside dans la décentralisation.

Fondamentalement, toutes les applications de la Blockchain (et d'autres technologies cryptographiques) sont basées sur le concept de décentralisation. Au lieu d'une autorité centrale rigide et lente qui prend des décisions et régit les relations, la Blockchain cherche à rendre le pouvoir réglementaire aux individus. Au lieu de faire confiance à une grande institution, la Blockchain renforce la confiance grâce au consensus.

Comment fonctionne la blockchain ?

En termes plus simples, la Blockchain utilise une combinaison de cryptographie et d'un registre public pour créer la confiance entre les parties tout en préservant la confidentialité.

Comprendre les mécanismes de fonctionnement est un peu plus difficile, mais afin d'apprécier pleinement le génie derrière la technologie Blockchain, nous devrons nous plonger dans les détails techniques.

Alors que la Blockchain peut inclure de nombreuses autres fonctionnalités, les principes fondamentaux d'une Blockchain sont dans le nom de la technologie :

Le bloc : un bloc est une liste de transactions sur une certaine période. Il contient toutes les informations traitées sur le réseau au cours des dernières minutes. Le réseau ne crée qu'un seul bloc à la fois.

La chaîne : chaque bloc est lié au bloc qui le précède à l'aide d'algorithmes cryptographiques. Ces algorithmes sont difficiles à calculer pour les ordinateurs et prennent souvent plusieurs minutes à résoudre par les ordinateurs les plus rapides du monde. Une fois résolue, la chaîne cryptographique verrouille le bloc en place, ce qui le rend difficile à changer. Nous examinerons cela plus en profondeur dans une minute.

La chaîne s'allonge avec le temps. Une fois qu'un nouveau bloc est créé, les ordinateurs du réseau opèrent ensemble pour vérifier les transactions dans le bloc et sécuriser la place de ce bloc dans la chaîne.

La partie la plus fondamentale de la Blockchain est le registre. C'est là que sont stockées les informations sur les comptes du réseau. Le grand livre à l'intérieur de la Blockchain est ce qui remplace le grand livre d'une banque ou d'une autre institution. Pour une crypto-monnaie, ce grand livre se compose généralement de numéros de compte, de transactions et de soldes. Lorsque vous soumettez une transaction à la Blockchain, vous ajoutez des informations au grand livre sur la provenance et la destination de la devise.

Un registre de Blockchain est distribué sur le réseau. Chaque nœud du réseau conserve sa propre copie du registre et le met à jour lorsque une personne soumet une nouvelle transaction. Ce « grand livre partagé » est la façon dont la Blockchain entend remplacer les banques et autres institutions. Au lieu de demander à la banque de conserver une copie officielle du grand livre, chacun en conservera sa propre copie, puis nous vérifierons les transactions par consensus.

Chaque technologie Blockchain a son propre registre et les différents registres fonctionnent très différemment (comme nous le verrons). Cependant, le grand livre du Bitcoin, le premier registre de Blockchain, nécessite trois informations pour répertorier une transaction :

1. Une entrée : si John veut envoyer un Bitcoin à David, il doit dire au réseau où il a obtenu ce Bitcoin en premier lieu. Peut-être que John a reçu le Bitcoin de Sarah hier, donc la première partie de l'entrée du grand livre le dit.
2. Un montant : c'est le montant que Jean veut envoyer à David.
3. Une sortie : c'est l'adresse de Bitcoin de David et où le Bitcoin doit être déposé

Vient maintenant le concept difficile à saisir : il n'existe pas de Bitcoin. Bien sûr, il n'y a pas de Bitcoins physiques. Vous le saviez probablement déjà. Cependant, il n'y a pas non plus de Bitcoins sur un disque dur quelque part. Vous ne pouvez pas pointer vers un objet physique, un fichier numérique ou un morceau de code et dire : « Ceci est un Bitcoin ». Au lieu de cela, l'ensemble du réseau Bitcoin n'est qu'une série d'enregistrements de transactions. Chaque transaction de l'histoire du Bitcoin vit dans le grand livre distribué du Bitcoin de la Blockchain. Si vous voulez prouver que vous avez 20 Bitcoins, la seule façon de le faire est de pointer vers les transactions où vous avez reçu ces 20 Bitcoins.

Presque toutes les Blockchain ont cette caractéristique en commun. L'historique des transactions est la devise. Il n'y a aucune différence entre les deux. Certaines nouvelles crypto-monnaies modifient la façon dont le grand livre est écrit afin de fournir un plus grand anonymat et une plus grande confidentialité dans les transactions. Elles utilisent certaines techniques de masquage d'identité pour masquer l'expéditeur et le destinataire de la transaction tout en conservant un registre distribué fonctionnel.

Création D'un Bloc

Le registre est au cœur du bloc, mais ce n'est pas la seule chose qui entre dans un bloc nouvellement créé. Il y a un en-tête et un pied de page requis pour chaque bloc. De plus, les transactions incluses dans le bloc sont soumises à un processus qui les compresse, les code et les standardise. Lorsqu'un vérificateur crée un nouveau bloc, il est complètement différent du grand livre sur lequel il était basé. Cependant, le grand livre sous-jacent est toujours là et peut être consulté à l'avenir lorsque de nouvelles transactions nécessitent des informations sur les blocs précédents.

Ajout De Transactions

La première étape de la création d'un bloc consiste à rassembler et à ajouter toutes les transactions en cours au grand livre du bloc. Lorsqu'un utilisateur crée une nouvelle transaction, il diffuse cette transaction sur l'ensemble du réseau. L'ordinateur d'un vérificateur examinera ensuite la transaction pour s'assurer qu'elle est valide.

Étant donné que les devises de la Blockchain ne sont rien de plus qu'une série de transactions, la première étape pour vérifier une transaction consiste à regarder où l'expéditeur dit avoir initialement obtenu son argent. Le vérificateur examinera ensuite l'historique de la Blockchain pour trouver le bloc et la transaction où l'expéditeur a reçu l'argent. Si cette transaction d'entrée est confirmée sur la Blockchain, la transaction est valide et ils devront confirmer l'adresse de la partie destinataire. Si la transaction d'entrée n'a pas été confirmée, la transaction actuelle n'est pas valide et elle ne sera pas incluse dans le grand livre.

Une fois que toutes les transactions de ce bloc ont été vérifiées, il est temps de créer le grand livre. Voici un exemple simple, où les transactions sont répertoriées les unes après les autres :

[Entrée][Montant][Adresse de sortie], [Entrée][Montant][Adresse de sortie], [Entrée][Montant][Adresse de sortie], [Entrée][Montant][Adresse de sortie], [Entrée][Montant][Adresse de sortie]…

Ensuite, le vérificateur appliquera une technique cryptographique appelée hachage à chacune des transactions. Dans sa définition la plus basique, le hachage prend une chaîne de caractères et génère une autre chaîne de caractères. Ainsi, lorsque vous fournissez l'adresse d'entrée, le montant et l'adresse de sortie à un algorithme de hachage, il transformera la transaction en une chaîne de caractères unique à cette transaction, comme ceci :

aba128d3931e54ce63a69d8c2c1c705ea9f39ca950df13655d92db662515eacf

(Il s'agit d'un hachage de transaction réel de la Blockchain du Bitcoin.)

Le hachage est donc utilisé pour normaliser les données tout en s'assurant qu'elles n'ont pas été falsifiées. Si une personne essayait de modifier une transaction dans la Blockchain, elle devrait refaire cette transaction, et cela aurait l'air complètement différente. Il serait évident qu'elle avait été falsifiée.

Pour rendre encore plus difficile la falsification de la Blockchain et réduire la mémoire requise pour stocker le registre des transactions, la plupart des Blockchains hachent plus d'une fois. Cela signifie qu'elles prennent le hachage d'une transaction, le combinent avec un hachage d'une autre transaction et le re-hachent dans un nouveau hachage plus petit. La combinaison de transactions de cette manière est connue sous le nom d'arborescence Merkle, et le hachage racine de toutes les transactions est inclus au début du bloc. Comprendre pourquoi nous avons besoin d'un arbre Merkle est un sujet pour un livre plus approfondi, mais à un niveau de base, l'arbre Merkle montre que toutes les transactions du bloc sont valides tout en utilisant moins de mémoire à long terme.

Horodatage Et Id De Bloc

Le dernier élément d'un bloc est l'horodatage et les informations d'ID de bloc. Cela facilite la recherche ultérieure des blocs précédents. Les transactions futures pourront également pointer vers cet ID de bloc comme le bloc contenant la transaction d'entrée (également appelée « coinbase ») pour la transaction en cours.

Association Des Blocs Ensemble

La dernière étape de la création d'un bloc consiste à le relier aux blocs précédents de la chaîne. Il y existe plusieurs façons de le faire, mais pratiquement toutes impliquent un hachage d'une manière ou d'une autre pour faire du contenu du bloc précédent une partie du nouveau bloc.

N'oubliez pas que le hachage prend une entrée, quelle que soit sa taille, et la transforme en une chaîne de caractères. Si vous modifiez l'entrée même légèrement, la sortie entière est modifiée. Afin d'inclure le contenu du bloc précédent dans le nouveau bloc, nous pouvons prendre le hachage de tout le bloc précédent et l'ajouter au début du bloc suivant. Cela signifie que nous avons effectivement lié l'ancien bloc au nouveau bloc, car si quelque chose change dans l'ancien bloc, même le plus petit changement, le hachage du bloc entier changera.

Désormais, une fois qu'un bloc est terminé, il devient BEAUCOUP plus difficile de le changer. Si vous modifiez un bloc plus ancien, vous devrez hacher à nouveau tout ce bloc. Une fois que vous avez re-haché tout le bloc 1, vous devez casser le bloc 2 ouvert, supprimer l'ancien hachage du bloc 1, insérer le nouveau hachage du bloc 1, et maintenant re-hacher tout le bloc 2. Mais de nouveaux blocs sont créés tous les heure, donc pour modifier une transaction plus ancienne, vous devez modifier chaque bloc après que cette transaction a eu lieu. Plus le temps passe, plus il devient difficile de pirater le réseau et de réussir à modifier une transaction. C'est pourquoi le hachage est au cœur de la sécurité de la Blockchain. La cryptographie rend le registre des transactions difficile à modifier, ce qui signifie que le registre peut être public et sécurisé en même temps.

Cependant, le hachage lui-même n'est pas si difficile. La plupart des ordinateurs pourraient facilement hacher à nouveau une Blockchain en quelques secondes. Donc, afin de garantir que la sécurité de hachage fait son travail, nous devons introduire un niveau de difficulté dans la création d'un nouveau bloc. Idéalement, ce serait quelque chose qui ralentirait un attaquant et rendrait plus probable que les membres honnêtes du réseau gagneront. Dans la Blockchain du Bitcoin (et la plupart des autres Blockchains modernes), cette difficulté supplémentaire est appelée « preuve de fonctionnement ».

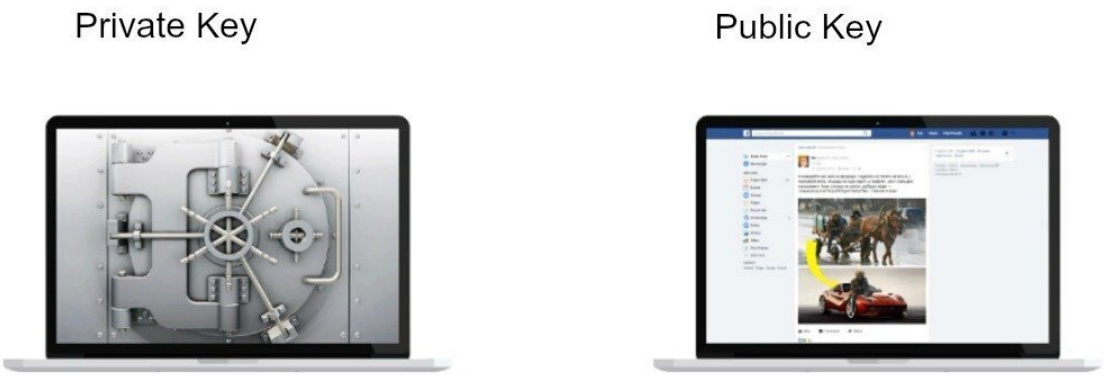
Je n'expliquerai pas la preuve de fonctionnement ici, une explication de base de la preuve de fonctionnement que j'ai abordée dans le chapitre 3 de ce livre, ni les détails approfondis de cette technologie dans mon livre. « Blockchain Technology Explained ».

Chapitre 5. Les portefeuilles ou comment stocker le bitcoin de manière sécurisée

Les personnes traitant de crypto-monnaie utilisent un portefeuille comme dépôt sécurisé et comme instrument pour les paiements entrants et sortants. Analysons les types de portefeuilles disponibles et choisissons le plus approprié en fonction des ressources et des tâches de votre ordinateur.

Il existe des portefeuilles chauds et froids. Il existe également des portefeuilles chauds, mais ils sont beaucoup moins utilisés. Les portefeuilles froids sont utilisés pour stocker de l'argent, tandis que les portefeuilles chauds sont utilisés pour envoyer et recevoir la monnaie rapidement.

En règle générale, un portefeuille a une clé privée et une clé publique. La clé privée n'appartient qu'à vous et vous ne devez jamais la montrer à personne. Vous devez garder cela à l'esprit lorsque vous signez toutes les transactions avec cette clé. Dans le même temps, quelqu'un peut utiliser des clés publiques pour transférer de l'argent sur votre compte, par exemple pour l'achat d'une nouvelle Ferrari . Dans ce cas, vous devez donner à cette personne votre clé publique. Cette clé peut même être publiée sur les réseaux sociaux. Il n'y a rien à craindre.



Je vous suggère de parcourir les types de portefeuilles sur bitcoin.org.

Bitcoin Core sera le tout premier portefeuille à considérer. Il s'agit du portefeuille Bitcoin original du légendaire créateur de Bitcoin, Satoshi Nakamoto. C'est le seul portefeuille officiellement pris en charge qui est constamment mis à jour par la communauté professionnelle du Bitcoin et stocke toute la base de données de Bitcoin sur votre ordinateur, prenant automatiquement en charge le réseau. Bitcoin Core est hautement sécurisé et convivial. Cependant, je ne recommande pas d'installer ce

portefeuille sur votre ordinateur. La première synchronisation dure très longtemps et la taille d'un portefeuille entièrement synchronisé atteint 100 Go, ce qui est un inconvénient majeur.

Je considère la Blockchain comme le portefeuille idéal pour les utilisateurs, en particulier les paresseux. Il ne nécessite pas l'installation d'applications tierces sur l'ordinateur. Il vous permet de créer un portefeuille Bitcoin en quelques secondes et de l'utiliser immédiatement. Ce portefeuille garantit un haut niveau de sécurité pour votre Bitcoin, jouit d'une réputation irréprochable et offre un support 24h/24, 7j/7. L'interface est simple et intuitive, même pour les débutants. L'inconvénient théorique réside uniquement dans le fait que votre portefeuille Bitcoin est situé sur une ressource tierce et non sur votre ordinateur.

Конец ознакомительного фрагмента.