CRYPTO-MONNAIES

BITCOIN

COMMENT INVESTIR

LE SECRET

MICHAEL VERMINNEN

Faut il investir?

vDepuis un certain temps, on entend de plus en plus parler des crypto-monnaies, mais le sujet reste assez flou pour de nombreuses personnes. Pour beaucoup, il s'agit d'un moyen de s'enrichir — mais aussi d'une pratique potentiellement risquée. Qu'en est-il vraiment ? Peut-on se lancer dans ce projet ? Et comment se protéger de certains pièges ? Nous faisons le point sur ce système en plein essor.

TABLE DES MATIÈRES

Une crypto, qu'est ce que c'est?

Les spécificités de la crypto-monnaie
Le terme « crypto-monnaie » est une abréviation de la notion « monnaie cryptographique ». Concrètement, il s'agit d'une monnaie totalement électronique, magnétique — et entièrement virtuelle. S'il existe plusieurs crypto-monnaies, aucune ne dispose de billets, de pièces ou de tout autre objet susceptible de la matérialiser.

En parallèle, la monnaie est cryptée : elle ne peut être utilisée que par les possesseurs du code de décryptage. Des systèmes très sophistiqués existent pour éviter les failles de sécurité, à l'image de la reconnaissance par empreinte digitale.

La monnaie et les informations qui permettent de la crypter sont enregistrées dans un réseau appelé blockchain. Véritables successeurs du relevé de compte, les blockchains délivrent publiquement les informations sur les transactions en crypto-monnaies.

Ces monnaies n'ont pas de cours légal et ne sont pas contrôlées par une quelconque instance particulière.

La crypto-monnaie reste une monnaie !
Même si elle fonctionne différemment de l'euro ou du dollar, la crypto-monnaie reste — comme son nom l'indique — une vraie monnaie. Elle peut donc être mobilisée pour toutes sortes de transactions, qu'il s'agisse d'achats, de ventes ou de crédits. Le fait que la blockchain — consultable par tous — regroupe toutes les opérations effectuées peut décourager les utilisateurs potentiels. Mais il faut savoir que certaines crypto-monnaies (comme le Black Coin, le Zerocoin ou encore le Darkcoin) préservent aussi l'anonymat.

Pourquoi investir en crypto?

Pour beaucoup de personnes, l'investissement dans une crypto-monnaie est comparable à celui que l'on pourrait faire sur des valeurs « refuge » comme l'or, par exemple. Acheter de l'or permet de le revendre à quelqu'un qui en aura l'utilité.Le principe est le même pour la crypto-monnaie : elle peut être utilisée pour des contrats, des achats et toutes sortes de transactions. Ainsi, un premier investissement sur une monnaie cryptée peut rapporter sur le moyen ou le long terme. De plus en plus de personnes sont intéressées par ce dispositif, notamment parce qu'il est plus sécurisé que nos comptes bancaires, et non soumis aux fluctuations des monnaies traditionnelles.Cependant, il existe plusieurs milliers de crypto-monnaies actuellement en circulation. Certaines ont un fort potentiel, et d'autres sont inintéressantes – voire parfois dangereuses, parce qu'elles peuvent faire perdre de l'argent. Pour faire du trading en ligne, tournez-vous toujours vers des offres fiables comme le site internet IronFX, une référence sur le secteur.D'une façon générale, il faut bien se renseigner avant de se lancer, car ce genre d'investissement ne peut pas être réalisé sans connaissances précises. Il ne faut pas, non plus, se lancer dans des paris trop risqués : investissez des sommes qui sont raisonnables pour vous, en fonction de vos propres moyens. Et pour avoir des chances de vous enrichir plus tard, il faut bien sûr prendre quelques précautions.

Quelques conseils pour débuter

Ne choisissez pas n'importe quelle monnaiePuisqu'il existe de très nombreuses crypto-monnaies, il va de soi que toutes n'ont pas le même potentiel. Le Bitcoin se présente comme une valeur sûre, parce qu'il est connu de tous. Mais il est conseillé de s'intéresser aux autres alternatives, à leur mode de fonctionnement, à leur actualité et leur principe. Pour mieux évaluer une crypto-monnaie, il faut parcourir les discussions sur son « subreddit » et les « metrics » reddits. En effet, le site communautaire Reddit regorge d'informations liées aux crypto-monnaies. Sur redditmetrics.com, on peut connaître les statistiques d'une crypto-monnaie, mais aussi la communauté qui existe tout autour.Vérifiez l'absence d'accusation de scamEn anglais, « scam » signifie « escroquerie ». Avant d'investir dans une crypto-monnaie, vous pouvez taper son nom puis le mot « scam » dans votre moteur de recherche, afin de vérifier qu'il s'agit bien d'un système fiable. Attention, certaines accusations peuvent aussi être infondées : il faut vraiment prendre le temps de lire plusieurs données, de les confronter entre elles et de se forger un jugement objectif.Identifiez les initiateurs du projetPour qu'une crypto-monnaie soit sûre, il faut qu'elle soit gérée par des personnes compétentes. Il est donc primordial de connaître les développeurs de la monnaie avant d'investir. L'équipe doit être expérimentée et formée. De plus, il est utile de se familiariser avec son actualité, les éventuels conflits, les effets de la compétition sur la santé de la monnaie, etc.L'investissement dans une crypto-monnaie peut être particulièrement rémunérateur à terme. Mais il ne faut pas oublier que cette pratique est très complexe : il s'avère risqué de se lancer sans risque si l'on ne prend pas le temps de se renseigner sur la santé, l'actualité, le potentiel, le mode de fonctionnement et les statistiques d'une crypto-monnaie.Alors si vous êtes intéressé par la finance et si vous avez envie de mieux comprendre cette monnaie en plein essor, prenez le temps de vous informer et lancez-vous !

Qu'est ce qu'un brocker?

Un broker FOREX est un opérateur faisant le lien entre vous – le trader – et le marché réel du FOREX. C'est l'équivalent de ce que l'on appelait avant couramment « courtier » ou « cambiste ».Aujourd'hui les brokers se présentent sous forme d'un logiciel (accessible en ligne ou téléchargeable) qui vous permet d'effectuer vos opérations de trading sur internet.Tous les brokers offrent la possibilité de trader en mode virtuel ou mode « démo ». Ce qui vous laisse tout le loisir de vous entrainer à spéculer sur le marché du FOREX sans prendre le risque de pouvoir perdre de l'argent réel !Lorsque vous négociez en argent réel, le broker prend note de vos ordres et les applique instantanément (ou quasiment) en investissant votre argent à l'aide de grandes banques internationales. Votre capital se retrouve donc sur le marché du Forex, jusqu'à ce que vous clôturiez votre transaction afin de récupérer votre capital gonflé par vos bénéfices ou réduit par vos pertes.Il existe des dizaines de brokers différents. Certains sont privilégiées pour les débutants, d'autres pour les traders intermédiaires, et certains sont réservés aux traders experts munis d'une bourse substantielle. C'est pourquoi bien choisir son broker est essentiel pour se lancer correctement dans le monde du trading Forex.Différence entre broker market maker et no dealing deskUne autre importance existe également, il y a 2 types de brokers :les NO dealing desk qui sont des intermédiaires entre le trader (vous) et le marché interbancaire. Toutes vos transactions sont automatiquement passées sur le marché. Il existe deux types de broker no dealing desk, les STP (Straight Through Process, comme FXCM) et les ECN (Electronic Communication Network) (+ d'infos sur les broker forex no dealing desk)les dealing desk (ou market maker) qui servent de bureau de change. Cela signifie qu'ils se comportent eux même comme le marché. Certaines positions sont couvertes, d'autres non. (+ d'infos sur les broker forex market maker)Nous avons sur Forexagone édité une sélection des meilleurs brokers en ligne, et surtout des notes pour vous aider à choisir le logiciel qui vous conviendra le mieux ainsi que les détails des bonus forex qu'ils proposent. Pour les grands débutants nous conseillons d'utiliser Etoro qui est la plateforme la plus simple et intuitive.Pour des traders intermédiaires ou confirmés nous conseillons d'autres logiciels plus poussés (comme 4XP) sur lesquels vous pourrez trouver des outils plus sophistiqués et une plateforme répondant aux plus grandes exigences qu'un trader expérimenté pourrait avoir.

Qu'est ce qu'un wallet?

Un wallet ou portefeuille numérique est un logiciel qui permet de stocker, d'envoyer et de recevoir des crypto monnaies.Parce que les devises numériques n'existent pas physiquement, ce blockchain wallet ne contient pas réellement de pièce. Toutes les transactions d'une même monnaie numérique sont enregistrées et stockées sur une blockchain et le portefeuille permet de consulter ces informations et d'effectuer des actions dessus.

Les monnaies numériques ont des types d'adresses différents, et il est généralement possible d'en envoyer seulement entre adresses de portefeuille similaires : par exemple, il est obligatoire d'envoyer des bitcoins à une adresse de portefeuille bitcoin et des ethers à une adresse de portefeuille Ethereum.Comment fonctionnent les portefeuilles de crypto monnaies ?Un wallet crypto monnaie contient une clé publique et une clé privée. La clé publique est une longue suite de chiffres et de lettres correspondant à l'adresse du portefeuille. C'est l'adresse du destinataire à saisir lors que l'on souhaite effectuer un transfert d'argent. C'est similaire à un relevé d'identité bancaire (RIB) d'un compte bancaire classique. La clé privée quant à elle permet d'accéder aux fonds du wallet stockés dans la blockchain. C'est un peu comme votre identifiant et mot de passe pour accéder à vos comptes bancaires en ligne. Il est impératif de le garder secret, en lieu sûr.En plus de stocker vos clés publiques et privées, les portefeuilles cryptographiques interagissent avec les différentes blockchains de différentes crypto monnaies afin de vérifier son solde, envoyer et recevoir des fonds.Comment les wallets et les blockchains interagissent ?La blockchain de n'importe quelle crypto monnaie contient un enregistrement public de toutes les transactions qui ont été effectuées dans cette devise depuis sa création. L'adresse de votre portefeuille enregistre toutes vos transactions, c'est ce qui lui permet de tenir à jour votre solde. Les montants envoyés et reçus ainsi que les adresses des wallets sont des informations publiques.

Le trading et la bourse

Pour réaliser des investissements ou faire du trading, il faut passer des ordres sur les marchés financiers. Ce sont deux styles différents mais qui ont le même objectif, acheter bas et revendre au plus haut.Il existe différent styles de trading comme le scalping, day trading ou encore le swing trading. La différence? C'est uniquement la durée de ta position. Le scalping, tu restes sur une action quelques secondes à quelques minutes. Le day trading, ton investissement doit être clôturé avant la fin de journée. Le swing trading, tu gardes une position plusieurs jours, semaines, mais il faut faire attention à la volatilité et aux gaps qui peuvent partir à la hausse, comme à la baisse ! Les traders vont sur les marchés financiers comme le Nasdaq, le CAC ou encore sur le Forex.En revanche, les investissements sont davantage axés sur le revenu au fil du temps. Cela fait de la production de revenus, tels que les dividendes et les paiements d'intérêts obligataires. Les investisseurs bénéficient d'une appréciation du capital. Acheter une maison pour y vivre, ce n'est pas investissement. Par contre, acheter une maison pour le louer, c'est un investissement qui rentre dans tes actifs. Tu gagnes de l'argent au moment de l'achat si tu as bien appris à investir.D'accord, mais en bourse? Depuis des dizaines d'années, la bourse évolue environ de 10% par an. Investir en bourse, ce n'est pas comme le trading. Ton portefeuille doit être conservé pour une très longue durée (plus de 20 ans) pour bénéficier des intérêts composés....L'investissement en bourse et le placement le plus sous-estimé mais aussi le plus craint.Il recèle pourtant des opportunités hors du commun.Un seul bon placement peut rapporter plusieurs fois sa mise en quelques années. Des rendements inimaginables avec un compte bancaire, une assurance vie ou de l'immobilier.

Le minage

Avant d'aller plus loin, vous devez savoir que la plupart des utilisateurs du bitcoin ne font pas de minage ! Le minage de bitcoin est une forme de commerce très compétitif. À moins que vous fassiez du minage uniquement pour le plaisir, vous devez trouver le moyen de le faire de façon très efficace afin de vous permettre de générer des profits..Si vous voulez obtenir des bitcoins sur la base d'une puissance de calcul précise mais que vous ne voulez pas vous occuper d'acquérir le matériel vous-même, vous pouvez acheter un contrat de minage.Détails techniquesDurant le minage, votre ordinateur effectue des hashs cryptographiques (deux SHA256 successifs) sur ce qu'on appelle une entête de bloc. Pour chaque nouveau hash, le logiciel de minage utilise un nombre aléatoire différent qu'on appelle le nonce. Selon le contenu du bloc et la valeur du nonce, le hash produit aura une forme similaire à l'exemple suivant:93ef6f358fbb998c60802496863052290d4c63735b7fe5bdaac821de96a53a9aCe hash peut être converti dans un très long nombre. (Il s'agit d'un nombre hexadécimal, ce qui signifie que les lettres A-F sont les nombres 10-15). Afin de rendre le minage difficile, il y a ce qu'on appelle la difficulté cible. Afin de créer un bloc valide, un mineur doit trouver un hash qui est inférieur à la difficulté cible. Par exemple, si la difficulté est de100000000000000000000000000000000000000000000000000000000000000000000000000n'importe quel nombre qui débute par un zéro serait accepté et considéré comme inférieur à la cible. Exemple :0787a6fd6e0782f7f8058fbef45f5c17fe89086ad4e78a1520d06505acb4522fSi nous diminuons la cible à010000000000000000000000000000000000000000000000000000000000000000000000000nous avons maintenant besoin d'un nombre débutant par deux zéros :00db27957bd0ba06a5af9e6c81226d74312a7028cf9a08fa125e49f15cae4979Parce que la cible est un nombre encombrant avec beaucoup de chiffres, un nombre plus simple est généralement utilisé pour exprimer la cible actuelle. Ce nombre est appelé la difficulté de minage. La difficulté de minage se calcule en comparant à quel point il est difficile de générer un bloc comparativement au premier bloc créé. Ce qui signifie qu'une difficulté de 70000 équivaut à 70000 fois plus d'efforts qu'il en fallait pour Satoshi Nakamoto pour générer le premier bloc. A l'époque où le minage était beaucoup plus lent et mal optimisé.La difficulté change à chaque 2016 blocs. Le réseau essaie d'assigner la difficulté de telle sorte à ce que la puissance de calcul mondiale prenne exactement 14 jours pour générer 2016 blocs. C'est pourquoi la difficulté augmente de pair avec la puissance du réseau..

Le minage

MatérielAu commencement, faire du minage avec un processeur (CPU) était la seule façon de miner des bitcoins. Les cartes graphiques (GPU) ont éventuellement remplacés les CPU en raison de leurs nature qui permettait une augmentation entre 50x à 100x dans la puissance de calcul en utilisant moins d'électricité par megahash comparativement à un CPU.Bien que n'importe quel GPU moderne puisse être utilisé pour faire du minage, l'architecture des GPU de marque AMD s'est avérée bien supérieure à nVidia pour miner des bitcoins et la carte ATI Radeon HD 5870 a été la plus économique pendant un temps.Pour une liste plus complète des cartes graphiques et de leurs performances, consultez le Wiki Bitcoin: Comparaison du matériel de minageDe la même manière que la transition CPU vers GPU, le monde du minage a évolué vers l'usage des Field Programmable Gate Arrays (FPGA) comme plateforme de minage. Bien que les FPGAs n'offraient pas une augmentation de 50x à 100x de vitesse de calcul comme la transition de CPU à GPU, ils offraient une meilleure efficacité énergétique.Une carte graphique typique de 600 MH/s consomme environ 400w d'électricité, tandis qu'un appareil FPGA habituel peut offrir un taux de hash de 826 MH/s à 80w de consommation électrique, un gain de 5x plus de calculs pour la même puissance énergétique. Puisque l'efficacité énergétique est un facteur déterminant dans la profitabilité du minage, il s'agissait d'une étape importante pour la migration de GPU à FPGA pour plusieurs personnes.Le monde du minage de bitcoin est maintenant en migration vers les Application Specific Integrated Circuit (ASIC). Un ASIC est une puce conçue spécifiquement afin d'accomplir une seule et unique tâche. Contrairement aux FPGAs, un ASIC ne peut pas être reprogrammé pour effectuer d'autres tâches. Un ASIC conçu pour miner des bitcoins ne peut et ne pourra rien faire d'autre que de miner des bitcoins.La rigidité d'un ASIC lui permet d'offrir une augmentation de la puissance de calcul de 100x tout en réduisant la consommation électrique comparativement à toutes les autres technologies. Par exemple, un appareil classique de offre 60 GH/s (1 Gigahash équivaut à 1000 Megahash. 1GH/s = 1000 Mh/s) tout en consommant 60w d'électricité. Comparativement au GPU, il s'agit d'une augmentation de la puissance de calcul de 100x et d'une réduction de la consommation électrique d'un facteur de 7.Contrairement aux générations de technologies qui ont précédées l'ASIC, l'ASIC est la "fin de la ligne" lorsqu'on parle de changement de technologie important. Les CPUs ont été remplacés par les GPUs, eux-même remplacés ensuite par les FPGAs qui ont été remplacés par les ASICs.Il n'y a rien qui puisse remplacer les ASICs aujourd'hui ou dans un futur immédiat. Il y aura des raffinements technologiques dans les produits ASIC et des améliorations dans l'efficacité énergétique mais rien qui ne corresponde à une augmentation de 50x à 100x de la puissance de calcul ni une réduction de 7x dans la consommation électrique comparativement à la technologie précédente.

Le minage

Ce qui signifie que l'efficacité énergétique d'un appareil ASIC est le seul facteur important de tout produit ASIC, puisque la durée de vie estimée d'un appareil ASIC est supérieure à l'histoire entière du minage de bitcoin. Il est concevable qu'un appareil ASIC acheté aujourd'hui soit toujours en opération dans deux ans si l'appareil offre encore une consommation électrique suffisamment économique pour demeurer profitable. La profitabilité du minage est aussi déterminée par la valeur du bitcoin mais dans tous les cas, plus un appareil a une bonne efficacité énergétique, plus il est profitable.LogicielIl y a deux manières de faire du minage : par vous-même ou en faisant partie d'une équipe (un pool). Si vous faites du minage par vous-même, vous devez installer le logiciel Bitcoin et le configurer pour JSON-RPC (voir: Faire fonctionner Bitcoin). L'autre option est de rejoindre un pool. Il y a plusieurs pools disponibles. Avec un pool, le profit généré par n'importe quel bloc généré par un membre de l'équipe est divisé entre tous les membres de l'équipe. L'avantage de rejoindre une équipe est d'augmenter la fréquence et la stabilité des gains (c'est ce qu'on appelle réduire la variance) mais les gains seront inférieurs. Au final, vous gagnerez la même somme avec les deux approches. Miner en solo vous permet de toucher des gains énorme mais très peu fréquents, tandis que miner avec un pool peut vous offrir de petits gains stables et réguliers.Une fois que vous avez votre logiciel configuré ou que vous avez rejoint un pool, la prochaine étape est de configurer le logiciel de minage. Le logiciel le plus populare pour GPU/FPGA/ASIC est présentement CGminer ou un dérivé conçu spécifiquement pour les FPGA et les ASICs, BFGMiner.Si vous voulez un aperçu rapide du minage sans installer de logiciel, essayez Bitcoin Plus, un mineur de Bitcoin fonctionnant dans votre navigateur avec votre CPU. Ce n'est aucunement profitable pour faire du minage sèrieux, mais il s'agit d'une bonne démonstration du principe du minage en équipe.

Le smart contrat

Les smart contracts, sont des programmes informatiques qui s'exécutent sans l'intervention d'un tiers de confiance, généralement sur une blockchain comme celle d'Ethereum. Ils sont constitués de clauses, qui sont les conditions qui doivent être remplies pour qu'une partie du contrat soit appliquée. Ces conditions sont définies préalablement par le créateur du contrat et sont écrites de manière immuable sur la blockchain. Le contrat peut alors être automatiquement déclenché lorsque certaines conditions sont remplies sur la chaîne. Contrairement à un contrat traditionnel, aucune tierce partie ne va procéder à la réalisation du contrat, tout est automatisé.Sur la blockchain Ethereum, créée par Vitalik Buterin, un smart contract est identifié par une adresse publique par exemple 0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f. En plus de gérer des transactions en éthers, cette adresse contient du code et des données, nécessaires au bon fonctionnement du programme. Contrairement à un compte classique qui demande à une personne de signer les transactions, un contrat va réagir tout seul aux différentes interactions, de manière autonome.Notez au passage que les smart contracts forment la base de ce qu'on appelle les applications décentralisées ou DApps.

Origine des smart contractsLe concept de smart contract a été formalisé par l'informaticien, juriste et cryptographe américain Nick Szabo. Dans son premier écrit public sur le sujet en 1994, ce dernier décrivait cela comme « un protocole de transaction informatisé qui exécute les termes d'un contrat ». Il a par la suite affiné son idée dans des écrits divers comme Smart Contracts: Building Blocks for Digital Markets en 1996 ou Formalizing and Securing Relationships on Public Networks en 1997.Le terme « smart contract », inventé par Szabo lui-même, est un peu déroutant, car un smart contract n'est pas vraiment intelligent, ni vraiment un contrat au sens juridique, mais est un programme qui s'exécute selon des conditions simples. Szabo a façonné cette expression pour la communication : le mot smart en anglais est en effet régulièrement utilisé pour appuyer sur le côté astucieux et évolutif d'une nouvelle technologie. Un téléphone multifonction est ainsi appelé un smartphone en anglais comme en français. Une carte à puces est une smart card, on parle de smart city pour une ville connectée, de smart bombs pour des bombes guidées, etc.Bien qu'il ait attiré l'attention de nombreux cypherpunks dans les années 1990, le concept de smart contract n'a pas été implémenté car aucune technologie ne permettait alors de le mettre en application de manière suffisamment robuste. Il a fallu attendre l'émergence de la technologie blockchain avec l'apparition de Bitcoin en 2009 pour que l'idée soit réellement mise en œuvre : bien que sa capacité à gérer des contrats soit limitée, ce dernier constitue en effet un système de monnaie programmable.La véritable révolution arrive en 2015 avec le lancement d'Ethereum, qui permet de construire des contrats autonomes plus complexes, notamment en utilisant un langage de programmation spécifique appelé Solidity. Ce dernier permet aux développeurs d'écrire des processus évolués dans un court laps de temps.Cette émergence a permis à beaucoup d'autres plateformes basées sur le même modèle d'apparaître, comme Tezos, Cardano, EOS, NEO ou TRON. La montée en puissance de ces protocoles a permis à l'idée du contrat intelligent de renaître pour automatiser et améliorer de nombreux processus. Un contrat intelligent permet de se passer d'intermédiaire, et donc de tiers de confiance pour réaliser certaines clauses prévues dans le contrat.

La blockchain

.Vous (un « nœud ») avez un fichier de transactions sur votre ordinateur (un « registre »). Deux comptables publics (que nous appellerons des « mineurs ») possèdent le même registre sur leur ordinateur respectif (il est donc « distribué »). Lorsque vous effectuez une transaction, votre ordinateur envoie un e-mail à chaque comptable pour les en informer.Chaque comptable se précipite pour être le premier à vérifier que vous pouvez vous permettre cette transaction (et gagner son salaire en « Bitcoins »). Le premier à effectuer la vérification et la validation appuie sur « RÉPONDRE À TOUS », et joint sa technique de vérification de la transaction (le « proof-of-work »). Si l'autre comptable est d'accord, tout le monde actualise son fichier…Cette opération est rendue possible par la technologie « blockchain ».C'est sûrement plus compliqué que cela, non ?Oui, mais pas tant que ça au niveau du concept. Les choses se compliquent quand on le met en œuvre et qu'on tente d'en retirer de la valeur. L'exemple ci-dessus sera bien évidemment jugé trop simpliste pour certains, mais il peut constituer un point de départ pour d'autres.Dans un environnement traditionnel, des tiers de confiance servent d'intermédiaires aux transactions financières. Si vous envoyez un jour de l'argent à l'étranger, vous passerez par un intermédiaire, en général une banque. La transaction ne sera normalement pas instantanée (et pourra prendre jusqu'à 3 jours), et l'intermédiaire prélèvera une commission pour ses services, sous forme de frais de conversion au taux de change ou autres.La technologie de chaîne de blocs originale est libre de droits et offre une alternative aux intermédiaires traditionnels pour les transferts en monnaie numérique Bitcoin. L'intermédiaire est remplacé par la vérification collective de l'écosystème, ce qui offre un degré élevé de traçabilité, de sécurité et de rapidité.Dans l'exemple ci-dessus (une « chaîne de blocs publique »), il existe plusieurs « nœuds » comme vous sur le réseau qui agissent simultanément en tant qu'exécuteurs des transactions et mineurs. Les transactions sont regroupées par blocs avant d'être ajoutées à une chaîne de blocs. Les mineurs reçoivent une prime en Bitcoins en fonction du temps de calcul nécessaire pour déterminer a) si la transaction est valide et b) la clé mathématique qu'il convient de lier au bloc de transactions dans le registre ouvert, à l'emplacement adéquat. Plus le nombre de transactions exécutées est important, plus les Bitcoins viennent grossir l'offre de monnaie virtuelle. La « prime » que les mineurs reçoivent se réduira tous les quatre ans, jusqu'à ce que la production de Bitcoins finisse par cesser (même si, selon les estimations, cela ne sera pas avant 2140 !). Bien entendu, si la chaîne de blocs avait initialement pour but de fonctionner avec des Bitcoins, d'autres monnaies virtuelles peuvent être utilisées, à l'instar d'Ether.

La blockchain

La Blockchain, c'est quoi ? La Blockchain est une infrastructure partagée d'échange et de stockage de l'information. Sa particularité est de permettre d'authentifier et de tracer l'ensemble des échanges entre les acteurs économiques ou les personnes physiques.

La première blockchain est apparue en 2008 avec la monnaie numérique bitcoin, développée par un inconnu se présentant sous le pseudonyme Satoshi Nakamoto. Elle en est l'architecture sous-jacente. Si blockchain et bitcoin ont été construits ensemble, aujourd'hui de nombreux acteurs (entreprises, gouvernements, etc) envisagent l'utilisation de la technologie blockchain pour d'autres cas que la monnaie numérique.

https/www.volontedereussir.com