BITCOIN EN 10 MINUTES

Tout ce que vous avez toujours voulu savoir sur le bitcoin

Brought to you by Relai

QU'EST-CE QUE LE BITCOIN?

Le bitcoin, la crypto-monnaie qui connaît le plus grand succès au monde, fait la une des journaux dans le monde entier. Beaucoup veulent profiter de son succès, d'autres sont indifférents ou même sceptiques. La monnaie numérique a suscité d'innombrables discussions sur l'argent, les investissements et la technologie. Certains voient dans le bitcoin un pur véhicule de spéculation ou le dénoncent comme une bulle, tandis que d'autres parlent d'innovation, de révolution monétaire, voire de rédemption du système monétaire actuel.

Divers pays, dont la Chine, considèrent le bitcoin comme une menace et ont déclaré la guerre à la crypto-monnaie. D'autres gouvernements, comme celui du Salvador, ont introduit le bitcoin comme moyen de paiement officiel dans l'espoir d'une croissance économique.

Mais qu'est-ce que le bitcoin ? Est-ce de l'argent ? De l'or numérique ? Un engouement pour les informaticiens et les spéculateurs ? Ou quelque chose d'entièrement différent ? Dans les paragraphes suivants, nous allons répondre à ces questions et examiner de plus près la monnaie numérique afin de mieux comprendre la philosophie et les fonctionnalités du bitcoin. Pour ce faire, il est important de commencer par le tout début : l'histoire des origines du bitcoin.

L'HISTOIRE DU BITCOIN

Les débuts du Bitcoin remontent au début des années 90. En 1992, un groupe d'informaticiens californiens a créé une liste d'adresses électroniques pour échanger des idées avec des personnes partageant les mêmes idées sur la cryptographie, les mathématiques, la politique et la philosophie. Ils se sont baptisés „Cypherpunks", un jeu de mots entre cyberpunk (personne de la littérature de science-fiction qui est sceptique à l'égard de la société, à juste titre) et cipher (chiffrer).

Les Cypherpunks

Les Cypherpunks sont rapidement devenus une équipe hétéroclite. Malgré leurs origines différentes, ils étaient unis par la conviction qu'Internet allait bientôt devenir l'une des arènes les plus disputées de la liberté humaine.

Pour se protéger contre la menace de contrôle, de surveillance et de censure de l'internet et préserver un internet libre et ouvert, les Cypherpunks ont utilisé une arme puissante : la cryptographie, le cryptage des informations.

Dans leur manifeste de 1993, ils ont déclaré : "Les cypherpunks écrivent du code [informatique]. Nous savons que quelqu'un doit écrire un logiciel pour défendre la vie privée, et [...] nous allons l'écrire."

Mais la cryptographie seule ne serait pas suffisante pour un Internet libre. Car, et les Cypherpunks en étaient convaincus, Internet ne peut être

véritablement libre s'il ne dispose pas de sa propre monnaie. Une monnaie indépendante des États, des banques centrales et des entreprises ; une crypto-monnaie aussi juste et décentralisée que l'Internet lui-même.

Expérimentations Monétaires

Mais la création d'une monnaie numérique indépendante a posé des défis techniques aux Cypherpunks. Dès 1990, le cryptologue David Chaum avait créé eCash, la première crypto-monnaie, qui n'était pas décentralisée mais garantissait l'anonymat grâce à la cryptographie. Cependant, eCash n'a pas pu s'imposer à long terme face aux autres systèmes de paiement en ligne. La société à l'origine du projet a dû déposer le bilan après 8 ans de service et eCash a disparu.

D'autres tentatives ont suivi, parmi lesquelles E-Gold s'est distinguée. E-Gold était une crypto-monnaie adossée à l'or et ouverte à tous. Fondée en 1996, pendant l'ère des dot-com, la société a touché la corde sensible de ses pairs, traitant plus de deux milliards de dollars de transactions par an à son apogée.

Mais E-gold était contrôlé par une institution centrale et donc vulnérable aux attaques. Des problèmes juridiques ont rapidement suivi, et le gouvernement américain a intenté une action en justice contre E-Gold. En 2008, E-Gold a été reconnu coupable par un tribunal américain de blanchiment d'argent et de violations du Patriot Act. Tous les actifs ont été gelés et E-Gold a dû cesser ses activités.

Ces tentatives ratées ont démontré deux faits aux Cypherpunks. Premièrement, l'eCash et l'E-gold étaient tous deux garantis par une garantie. Cette garantie s'est avérée être un point faible, car elle pouvait être saisie par les États. Par conséquent, une crypto-monnaie libre ne devrait pas avoir de points centraux d'attaque tels qu'une société enregistrée, un compte bancaire ou un emplacement de serveur centralisé. Et deuxièmement, les gouvernements et les régulateurs n'ont aucun intérêt dans une monnaie numérique indépendante de l'État.

Pour les Cypherpunks, la question fondamentale, pour laquelle aucune solution n'avait encore été trouvée, demeurait : Comment une monnaie numérique indépendante peut-elle fonctionner sans une partie centrale pour tenir les comptes et s'assurer que l'argent n'est pas dépensé deux fois ? Après tout, s'il était possible de résoudre le problème de la double dépense sans dépendre d'une partie centrale, il serait peut-être possible de créer une monnaie numérique libre, propre à Internet.

Un Acte de Création Mystique

Pour ces raisons, les Cypherpunks ont commencé à discuter des con-

ceptions d'une crypto-monnaie sans partie centrale et sans garantie. Deux des concepts les plus importants étaient b-money (1998) et BitGold (2005). Ces idées théoriques, qui n'ont jamais été mises en pratique, étaient déjà très similaires au Bitcoin dans leur conception. Une paire de clés publiques/privées était envisagée pour le cryptage et une preuve de travail devait être fournie pour la création de pièces numériques supplémentaires, comme c'est également le cas pour Bitcoin. Dans son livre blanc, l'inventeur du bitcoin a également confirmé qu'il avait connaissance de l'existence de b-money et de BitGold.

Cependant, étant donné que b-money et BitGold reposaient sur un système de vote pour le consensus (l'accord sur qui possède quelles unités monétaires à l'heure actuelle), ils étaient vulnérables aux attaques malveillantes qui pouvaient manipuler ces élections et ainsi fausser la propriété.

Pour ce dernier problème, qui faisait encore obstacle à la création d'une nouvelle monnaie Internet, une solution a été présentée le vendredi 31 octobre 2008. Ce jour-là, le Bitcoin Whitepaper, dans lequel Satoshi Nakamoto explique son concept de réseau de paiement décentralisé, est envoyé par e-mail aux Cypherpunks. Deux mois plus tard, le 3 janvier 2009, le réseau Bitcoin est mis en service.

Les premières réactions au nouveau réseau ont été discrètes. Quelques enthousiastes ont commencé à tester le réseau et à signaler des erreurs. Au début, cependant, c'est surtout Satoshi Nakamoto lui-même qui a assuré le fonctionnement du réseau. Mais peu à peu, la nouvelle de la nouvelle monnaie Internet s'est répandue sur les forums informatiques et technologiques et l'intérêt pour le réseau s'est accru. Après un an, le réseau Bitcoin comptait déjà quelques utilisateurs. Le bitcoin lui-même, cependant, n'avait pas encore de valeur.

Qui est Satoshi Nakamoto ?

Le livre blanc sur le bitcoin, ainsi que la communication par e-mail de l'inventeur du bitcoin, étaient tous deux signés du nom de Satoshi Nakamoto. Cependant, la véritable identité de l'inventeur de Bitcoin reste inconnue à ce jour, car son nom semble être un pseudonyme. Pour s'adresser aux personnes partageant ses idées et, plus tard, à la communauté des développeurs de Bitcoin, Nakamoto a utilisé au moins trois adresses électroniques différentes, qu'il a soigneusement cryptées pour dissimuler la véritable identité de l'expéditeur.

Plusieurs personnes ont déjà prétendu être Satoshi Nakamoto. Mais jusqu'à aujourd'hui, aucune d'entre elles n'a réussi à le prouver. Car la preuve ultime, à savoir l'envoi de bitcoins depuis l'une des adresses de portefeuilles appartenant très probablement à Satoshi, n'a encore été four-

nie par personne.

De plus, le groupe de ceux qui ont communiqué „personnellement“ avec Satoshi Nakamoto via Internet est très restreint. Satoshi Nakamoto a écrit son dernier message à la communauté Bitcoin le 12 décembre 2010, mais il ne s‘agissait en aucun cas d‘un message d‘adieu - Satoshi a simplement cessé de communiquer après cela.

Son retrait, cependant, ne s‘adressait qu‘à la communauté au sens large. Nakamoto a continué à rassembler autour de lui un petit groupe de programmeurs de base et les a informés de la poursuite du développement du réseau Bitcoin. Mais en avril 2011, il a envoyé un dernier message à ce groupe également. Aussi mystérieusement que Nakamoto était apparu en 2008, il a de nouveau disparu trois ans plus tard.

La „Journée de la Pizza“ de Bitcoin

Mais comment le bitcoin a-t-il pris de la valeur ? Au début, les bitcoins pouvaient être extraits et envoyés entre les membres du réseau, mais les unités numériques n‘avaient aucune valeur. De plus, le groupe de personnes qui connaissaient le bitcoin, et encore moins qui pouvaient l‘envoyer et le recevoir, était encore très restreint.

Cela a changé le 22 mai 2010, lorsqu‘une demande inhabituelle est apparue sur le forum Internet bitcointalk.org. Un homme de 28 ans, Laszlo Hanyecz, originaire de Floride, proposait 10 000 bitcoins à la personne qui commanderait deux pizzas à son domicile. Un étudiant californien a accepté l‘offre et s‘est fait livrer deux grandes pizzas d‘une valeur de 41 dollars à son domicile. En retour, Hanyecz lui a envoyé les 10 000 bitcoins.

Depuis ce jour, le 22 mai est célébré chaque année par les Bitcoiners comme le „jour de la pizza“. Cette journée est devenue populaire parce qu‘elle illustre trois choses :

- Les bitcoins ont de la valeur
- Les bitcoins conviennent comme moyen d‘échange et de paiement.
- Le bitcoin en tant que monnaie est désinflationniste. Le nombre de bitcoins supplémentaires mis en circulation diminue régulièrement, ce qui peut entraîner une augmentation de leur valeur.

Les deux pizzas sont entrées dans les livres d'histoire comme les plus chères du monde. En calculant leur coût avec le prix du bitcoin de décembre 2021, un montant incroyable de 460 millions de dollars américains a été payé pour ces pizzas. C'est beaucoup d'argent. Mais le bénéficiaire des 10 000 bitcoins les a déjà dépensés, lui aussi. Dans une interview, il a déclaré qu'il avait vendu les bitcoins peu de temps après pour payer un voyage en voiture - au prix actuel des bitcoins, probablement le voyage le plus cher de l'histoire de l'humanité également.

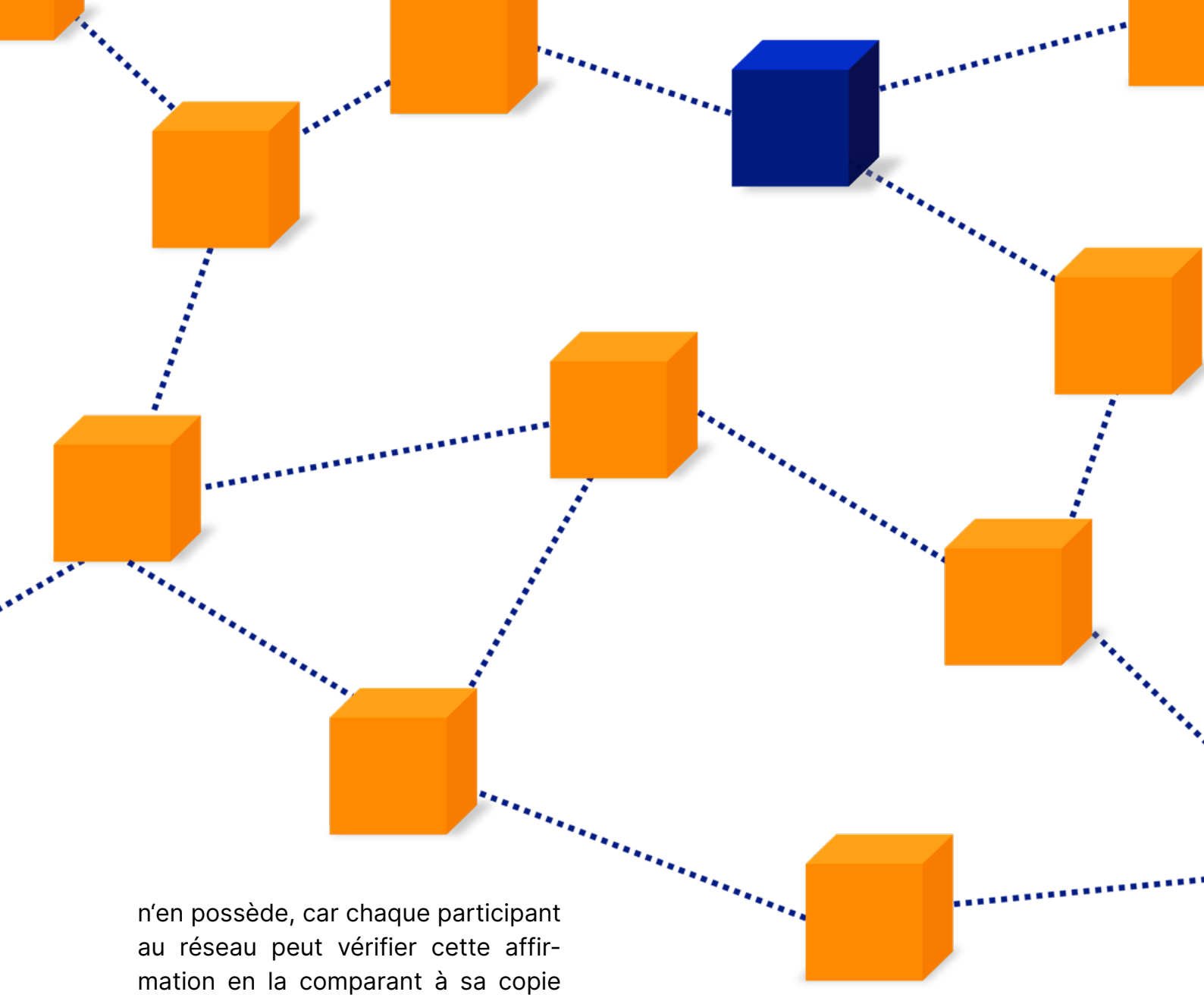
Le Bitcoin „Pizza Day" illustre également de manière impressionnante pourquoi le „hodling" - dérivé de „to hold" - est si populaire parmi les Bitcoiners. Le „hodling" consiste à conserver ses bitcoins pendant de longues périodes dans l'intention de ne jamais les vendre (éventuellement). Après tout, qui voudrait dépenser ses bitcoins aujourd'hui alors qu'ils pourraient valoir le double, le triple, voire le décuple dans les années à venir ?

COMMENT FONCTIONNE LE BITCOIN ?

Après avoir appris l'histoire du bitcoin, nous allons maintenant nous plonger dans son mode de fonctionnement. L'objectif est de comprendre comment le réseau Bitcoin fonctionne, quels problèmes il résout et quels sont ses avantages pratiques.

L'intention derrière Bitcoin est d'être un réseau décentralisé. Aucun participant au réseau ne doit pouvoir le diriger seul - le pouvoir de décision et la supervision sont répartis entre tous les participants. C'est important car aucun individu, aucun gouvernement et aucune entreprise ne peut modifier le réseau de manière indépendante, les changements ne sont possibles que collectivement.

Bitcoin fonctionne de telle sorte que chaque participant au réseau dispose à tout moment d'une copie identique du registre de propriété le plus à jour - par conséquent, chacun sait toujours qui possède actuellement quels bitcoins. Ainsi, personne ne peut prétendre posséder plus de bitcoins qu'il

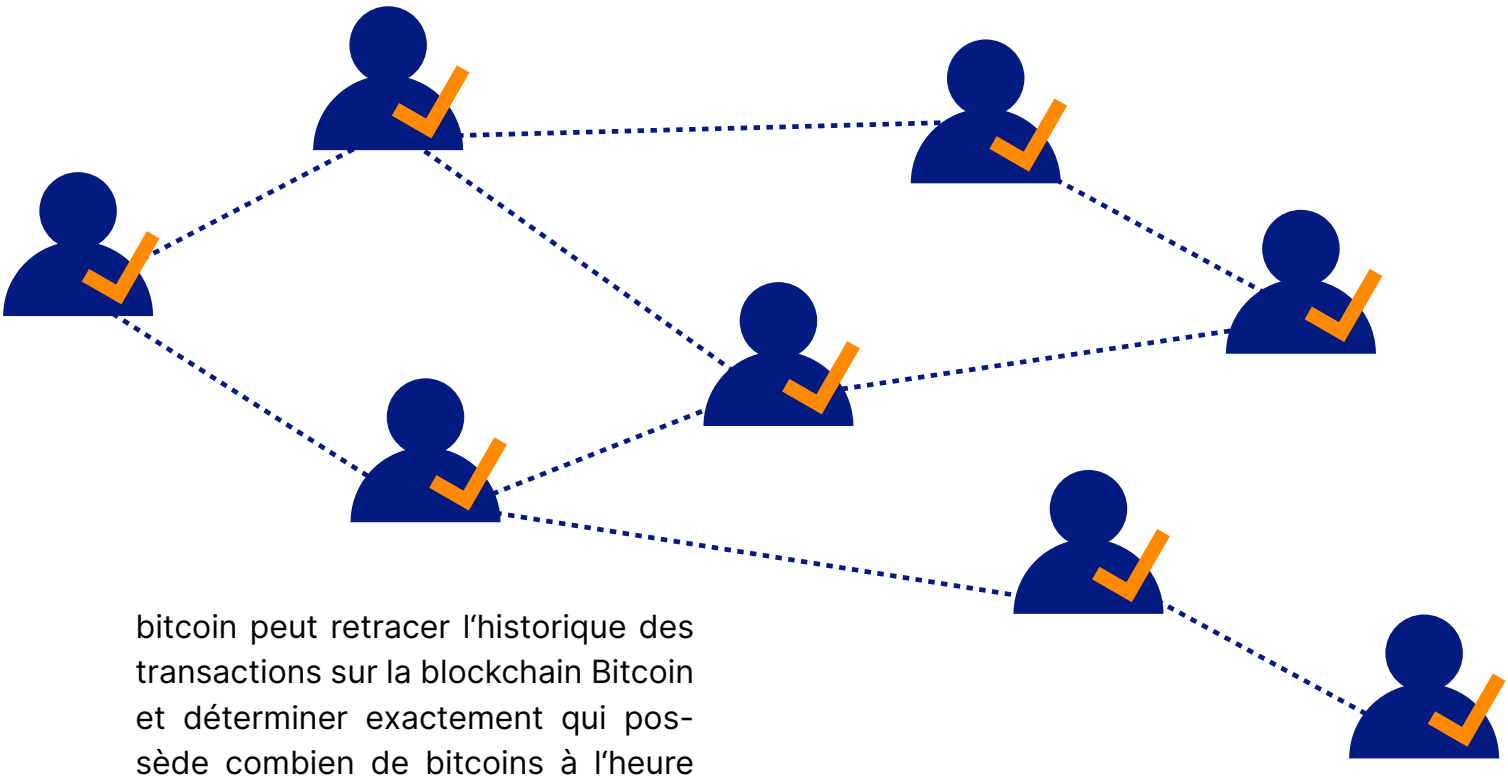


n'en possède, car chaque participant au réseau peut vérifier cette affirmation en la comparant à sa copie du grand livre et prouver qu'elle est fausse.

Avant le lancement de Bitcoin, les réseaux décentralisés étaient confrontés à deux défis majeurs. Premièrement, comment s'assurer que tous les participants reçoivent les dernières mises à jour sur les changements de propriété, c'est-à-dire les informations sur les bitcoins qui ont été transférés et à qui. Et deuxièmement, comment les participants peuvent-ils vérifier avec une certitude absolue que les informations qu'ils reçoivent sont correctes.

La blockchain

Ces difficultés ont été surmontées grâce à l'invention de la blockchain. Une blockchain stocke des informations et des données dans un ordre chronologique. Dans le cas du bitcoin, toutes les transactions effectuées depuis la création du bitcoin sont stockées par ordre chronologique dans des dizaines de milliers de blocs, qui forment ensemble la blockchain du bitcoin. Tout participant au réseau souhaitant savoir qui possède quel

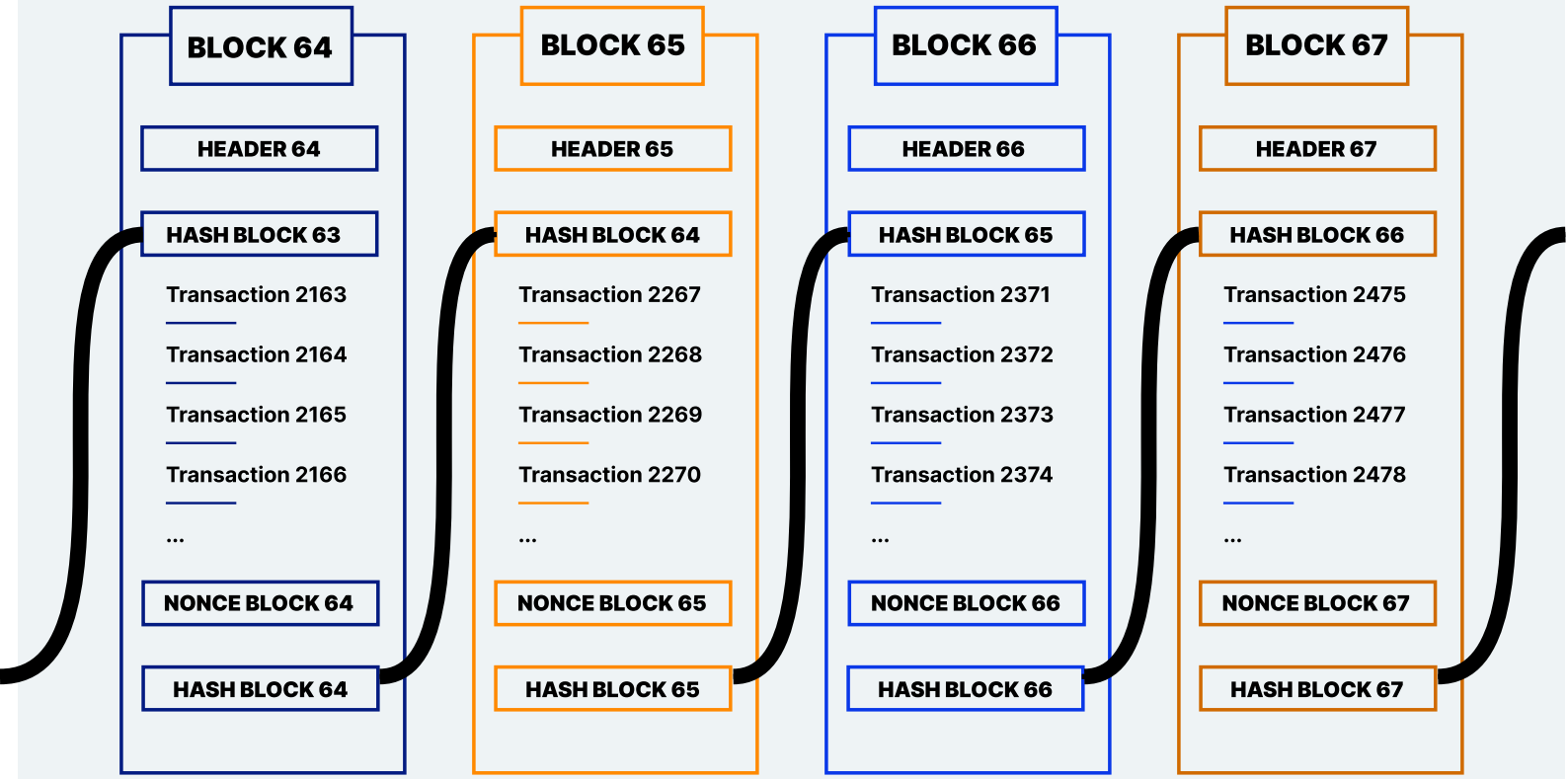


bitcoin peut retracer l'historique des transactions sur la blockchain Bitcoin et déterminer exactement qui possède combien de bitcoins à l'heure actuelle. Ainsi, si quelqu'un veut envoyer un bitcoin, n'importe qui peut vérifier si ce bitcoin appartient bien à la personne en question.

Jusqu'à présent, ce mécanisme n'a rien de nouveau puisque les banques utilisent un processus similaire. Si un client veut dépenser un franc suisse, la banque consulte l'historique des transactions pour voir si le franc appartient toujours au client ou s'il a déjà été dépensé (envoyé à quelqu'un d'autre). Toutefois, la caractéristique unique d'une blockchain est que ces informations ne sont pas stockées sur le serveur d'une banque centrale, mais sur les ordinateurs de tous les participants au réseau (appelés „nœuds complets") et existent donc en plusieurs dizaines de milliers d'exemplaires dans le monde entier. C'est également la raison pour laquelle le bitcoin ne peut pas être simplement supprimé - pour ce faire, il faudrait supprimer la copie de la blockchain de tous les ordinateurs participants du monde entier en même temps.

Cependant, le défi auquel les blockchains sont confrontées est que chaque participant au réseau doit être en mesure de déterminer avec une certitude absolue que sa copie de la blockchain est correcte et qu'aucune transaction erronée ou frauduleuse n'entre dans sa copie du grand livre. Étant donné que de nouveaux blocs contenant de nouvelles transactions sont ajoutés à la blockchain toutes les 10 minutes, la blockchain est en croissance constante et doit être mise à jour en permanence sur tous les ordinateurs participants dans le monde.

Ces blocs nouvellement joints doivent être vérifiables par tous. La vérification est effectuée à l'aide de règles immuables définies dans le code informatique du réseau Bitcoin. Ces règles définissent exactement quelles transactions sont autorisées et



L'en-tête, le résultat de la fonction de hachage du bloc précédent, toutes les transactions du bloc actuel et un Nonce (numéro aléatoire) sont placés dans une fonction mathématique. Le Nonce est modifié jusqu'à ce que le résultat de la fonction de hachage contienne suffisamment de zéros précédents. Ce processus s'appelle le minage.

lesquelles ne le sont pas. Chaque utilisateur qui télécharge la copie de la blockchain peut donc vérifier si toutes les transactions sont conformes aux règles données. Si une transaction viole les règles, c'est-à-dire si elle est incorrecte ou frauduleuse, elle est rejetée par les participants au réseau (nœuds complets) et n'est pas incluse dans la blockchain.

L'extraction minière - Proof-of-Work (PoW)

En outre, le réseau Bitcoin dispose d'un mécanisme permettant de limiter l'ajout de nouveaux blocs. Si de nouvelles transactions et de nouveaux blocs pouvaient être ajoutés à la blockchain par n'importe qui, le réseau se retrouverait dans le chaos, car la blockchain ne serait pas en mesure de se mettre à jour dans le monde entier au même état assez rapidement.

Pour éviter cela, le bitcoin fonctionne avec un mécanisme de preuve de travail. Pour qu'une personne puisse gagner le droit d'ajouter un nouveau bloc à la blockchain, elle doit fournir une preuve de travail. Une illustration simple de ce processus est un groupe de personnes cherchant des aiguilles dans une botte de foin. La première personne qui trouve une aiguille est autorisée à ajouter un nouveau bloc à la blockchain. En outre, le trouveur est récompensé par de nouvelles unités de bitcoin ainsi que

par les frais de transaction contenus dans ce bloc. Dès que le bloc a été joint, ce processus recommence.

En réalité, les mineurs exécutent une fonction de hachage mathématique (algorithme de hachage SHA-256) à la recherche de nombres spécifiques. Le numéro de hachage du bloc précédent, les transactions du bloc actuel et un numéro aléatoire (nonce) sont hachés ensemble. Le numéro aléatoire est modifié jusqu'à ce que la fonction de hachage produise un résultat comportant un nombre minimal de zéros de tête. Par exemple, le bloc #700000, créé le 11 septembre 2021, avait le numéro de hachage valide suivant: 0000000000000590fc0f3eba193a278534220b2b37e 9849e1a770ca959.

La recherche de ce nombre, également appelée „minage", a deux fonctions principales : premièrement, elle relie les blocs entre eux d'une manière mathématique-cryptographique afin que chacun puisse facilement vérifier l'ordre correct. En même temps, le mécanisme de preuve de travail rend presque impossible la modification de cet ordre. Ensuite, ce mécanisme retarde l'ajout de nouveaux blocs de sorte que, en moyenne, un nouveau bloc n'est ajouté à la blockchain que toutes les 10 minutes. Ainsi, tous les participants au réseau dans le monde ont suffisamment de temps pour mettre à jour le même et dernier état de la blockchain.

En résumé, les mineurs font fonctionner le réseau Bitcoin. Grâce à eux, de nouvelles transactions sont traitées et ajoutées à la blockchain. Les nœuds complets conservent des copies du grand livre, s'assurent que les règles sont respectées et veillent à ce qu'aucune transaction frauduleuse n'entre dans la blockchain.

21 million Bitcoin

Bien que de nouveaux blocs soient constamment ajoutés à la blockchain du bitcoin et que les mineurs soient récompensés pour ce travail par de nouveaux bitcoins, le nombre total de bitcoins est limité à 21 millions de bitcoins. Il n'y aura jamais plus de 21 millions de bitcoins. Mais ces 21 millions de pièces ne sont pas en circulation depuis le début. Au contraire, elles sont libérées par le code Bitcoin selon un calendrier d'émission strict.

Lorsque Bitcoin a été lancé, le code a libéré 50 nouveaux bitcoins aux mineurs toutes les 10 minutes environ. Quatre ans après le lancement, le nombre de bitcoins libérés toutes les dix minutes a diminué de moitié. Ce processus est appelé „réduction de moitié" et décrit le fait que la récompense par bloc pour les mineurs diminue de moitié tous les quatre ans. Actuellement, il y a déjà 19 millions de bitcoins en circulation. Les bitcoins restants seront exploités jusqu'en 2140. Après cela, les mineurs ne seront rémunérés que par des frais de transaction.

La quantité strictement limitée d'unités de bitcoin est l'une des propriétés fondamentales des crypto-monnaies et fait du bitcoin une marchandise extrêmement rare. Cette rareté numérique absolue est également une condition préalable importante à la fonction de réserve de valeur du bitcoin sur de longues périodes. C'est la raison pour laquelle le bitcoin est souvent appelé or numérique ou or 2.0.

Le résultat : La Propriété Numérique

En examinant l'ensemble des caractéristiques du réseau Bitcoin, on comprend l'importance de cette invention. Pour la première fois dans l'histoire, il existe un bien numérique qui n'est disponible qu'en nombre strictement limité. Les bitcoins ne peuvent être ni copiés ni dupliqués.

Grâce à cette réalisation, le bitcoin est souvent qualifié de bien numérique. En effet, tout comme chaque parcelle de terre sur cette terre est unique et n'existe qu'une seule fois, chaque unité Bitcoin est également unique et n'existe qu'une seule fois dans l'espace numérique.

De plus, ces unités Bitcoin peuvent être véritablement possédées. Seule la personne en possession de la clé privée correspondante, qui est une combinaison de chiffres et de lettres composée de 64 caractères, peut déplacer le bitcoin associé. En d'autres termes, sans cette clé privée, les bitcoins ne peuvent pas être volés, confisqués ou bloqués. Cela permet au propriétaire d'avoir un contrôle absolu sur ses ressources financières, qu'il soit millionnaire, réfugié politique ou créancier persécuté. Pour la première fois depuis l'invention de l'ordinateur, il est possible de posséder véritablement des actifs numériques.

POURQUOI LE BITCOIN?

Mais pourquoi tout ce battage autour du bitcoin ? La possibilité de posséder véritablement un actif numérique peut être révolutionnaire. Mais pourquoi quelqu'un voudrait-il posséder des bitcoins en premier lieu ?

Le Meilleur Des Deux Mondes

Au cours des siècles passés, les métaux précieux, puis l'argent liquide sous forme de pièces et de billets, étaient utilisés comme moyens de paiement. Ils présentaient l'avantage de pouvoir être stockés et dépensés indépendamment de tiers. L'expression „l'argent liquide, c'est la liberté imprimée" résume très bien cette situation. Toutefois, l'inconvénient des métaux précieux et de l'argent liquide est qu'ils sont difficiles à utiliser dans l'espace numérique de l'Internet. Au plus tard depuis l'avènement des achats en ligne, les cartes de débit et de crédit se sont donc imposées auprès de la population.

Mais maintenant que la plupart des gens utilisent de l'argent numérique sur des comptes bancaires au lieu d'espèces, les risques de contrepartie auxquels ils sont confrontés augmentent. Si, par exemple, un établissement financier se déclare insolvable, l'épargne des clients peut être perdue. Ou, comme cela s'est produit à Chypre en 2013, si les retraits d'espèces sont sévèrement limités, que des contrôles de capitaux sont mis en place et qu'une expropriation forcée sur les comptes d'épargne a lieu, alors les gens n'ont plus le contrôle de leur argent. Ou, comme c'est actuellement le cas dans de nombreux pays occidentaux, si les clients bancaires ne sont pas autorisés à envoyer de l'argent à leurs proches parce qu'ils vivent à Cuba ou en Iran, ils dépendent d'un tiers pour approuver toutes leurs transactions.

Avec le passage de l'argent papier à l'argent numérique, stocké sur des comptes bancaires, nous ne sommes finalement plus maîtres de notre propre argent. Jusqu'à présent, cependant, cet inconvénient était le prix à payer pour participer à une vie numérisée.

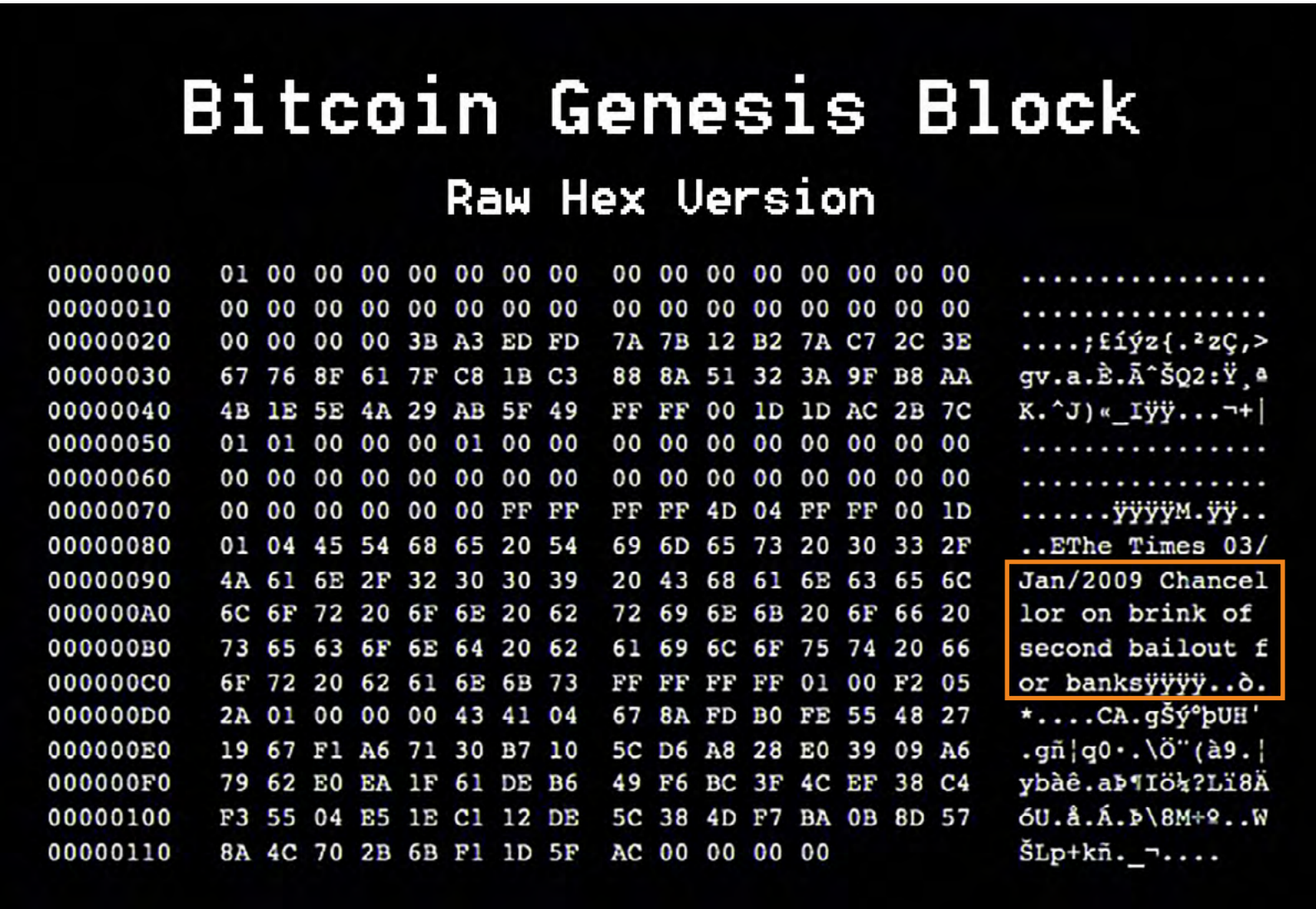
Le bitcoin offre une solution à ce dilemme. En tant que monnaie numéri-

que, il est parfaitement adapté à une utilisation dans l'espace numérique. En même temps, les bitcoins peuvent être stockés en tant que propriété numérique sans avoir à compter sur des tiers (banques) pour leur garde. Ainsi, les propriétaires de bitcoins peuvent stocker leurs pièces - sous forme de clés privées - sous leur matelas ou dans tout autre endroit qu'ils jugent le plus sûr.

Un Timing Parfait

Le bitcoin a été créé dans le contexte de la crise financière mondiale de 2008/09. Sur le premier bloc de la blockchain Bitcoin - également appelé bloc Genesis - Satoshi Nakamoto a laissé un message fort. Il a cité un titre publié dans le journal The Times qui disait : „Le chancelier est au bord d'un second sauvetage des banques."

Par cet acte, Satoshi a exprimé la philosophie de critique de l'État des Cypherpunks. Lors de la crise financière de 2008, les banques centrales ont mis en circulation de grandes quantités d'argent frais pour sauver les banques. Mais au final, ce sont les épargnants qui en ont fait les frais, car leurs économies ont perdu de la valeur en raison de la dilution de l'argent. Ce fait a une fois de plus confirmé les Cypherpunks dans leur méfiance à l'égard de l'État et des banques centrales et a renforcé leur conviction qu'une monnaie indépen-



dante de l'État était nécessaire de toute urgence.

Le même procédé, mais à plus grande échelle, s'est répété depuis le déclenchement de la pandémie de Covid-19. Rien qu'en 2020, la masse monétaire américaine a été augmentée de 50 %, et dans d'autres pays - dont la Suisse - la presse à imprimer numérique fonctionne en permanence. Conséquence directe : des taux d'intérêt bas records - voire négatifs en Suisse - et une forte inflation des actifs.

Couverture Contre la Dévaluation des Devises

Le bitcoin a donc été lancé au meilleur moment possible. La question de l'argent a rarement été aussi pertinente et les points d'interrogation aussi importants qu'aujourd'hui. Avec son offre limitée à 21 millions, le bitcoin offre un contraste agréable avec les bilans sans cesse croissants des banques centrales. Son offre limitée offre une protection contre la dilution de son capital, comme cela a été observé avec toutes les monnaies du monde au cours des dernières décennies.

En raison de sa configuration spécifique, le bitcoin est conçu pour garantir la préservation du pouvoir d'achat sur de longues périodes. Étant donné que le bitcoin est rare, il devrait être encore plus performant dans cette tâche que l'or, dont l'afflux net est de 1 à 2 % chaque année. En outre, les coûts de stockage et de transport du bitcoin sont également nettement inférieurs à ceux de l'or, ce qui permet également une meilleure préservation de la valeur dans le temps.

Protection de la Propriété

Un autre problème que Bitcoin atténue est la protection des biens. Alors que l'or ou l'argent liquide doivent généralement être stockés de manière sécurisée à grands frais pour les protéger du vol, les bitcoins peuvent être stockés et transportés à un coût pratiquement nul. Même des montants importants peuvent être emportés partout dans le monde grâce à un code composé de douze ou vingt-quatre mots. Une fois mémorisé et détruit physiquement, ce code ne peut être volé par personne, ce qui sécurise les bitcoins derrière le code et permet à son propriétaire de les emporter avec lui dans la tombe s'il le souhaite.

ACHETER DU BITCOIN

Il y a deux façons de se procurer des bitcoins. Soit vous gagnez des bitcoins en tant que mineur, soit vous achetez des bitcoins à une autre personne. Étant donné que le minage avec des appareils domestiques est devenu pratiquement impossible de nos jours, le seul moyen qui reste aux nouveaux arrivants est d'acheter des bitcoins.

Bourses et Courtiers de Crypto-Monnaies

Le moyen le plus simple d'acheter des bitcoins est de passer par une bourse de crypto-monnaies ou un courtier. Ces derniers fonctionnent de manière similaire aux plateformes de négociation d'actions. Après avoir ouvert un compte personnel, on peut transférer des francs suisses, des euros ou des dollars américains par virement bancaire ou par carte de crédit. Une fois l'argent arrivé sur le compte personnel à la bourse d'échange, il est possible d'acheter des bitcoins 24 heures sur 24 et 7 jours sur 7 en quelques clics au prix actuel du marché. En Europe, il est possible d'acheter des bitcoins sans inscription, vérification ou dépôt préalable d'argent avec la populaire application d'investissement en bitcoins Relai.

Pair-à-pair

Comme alternative aux échanges de crypto-monnaies, le bitcoin peut également être acheté directement auprès d'autres acteurs du marché via des plateformes pair-à-pair, sans

passer par une bourse. Cela permet un plus grand anonymat, car aucune donnée personnelle ne doit être révélée dans ce processus.

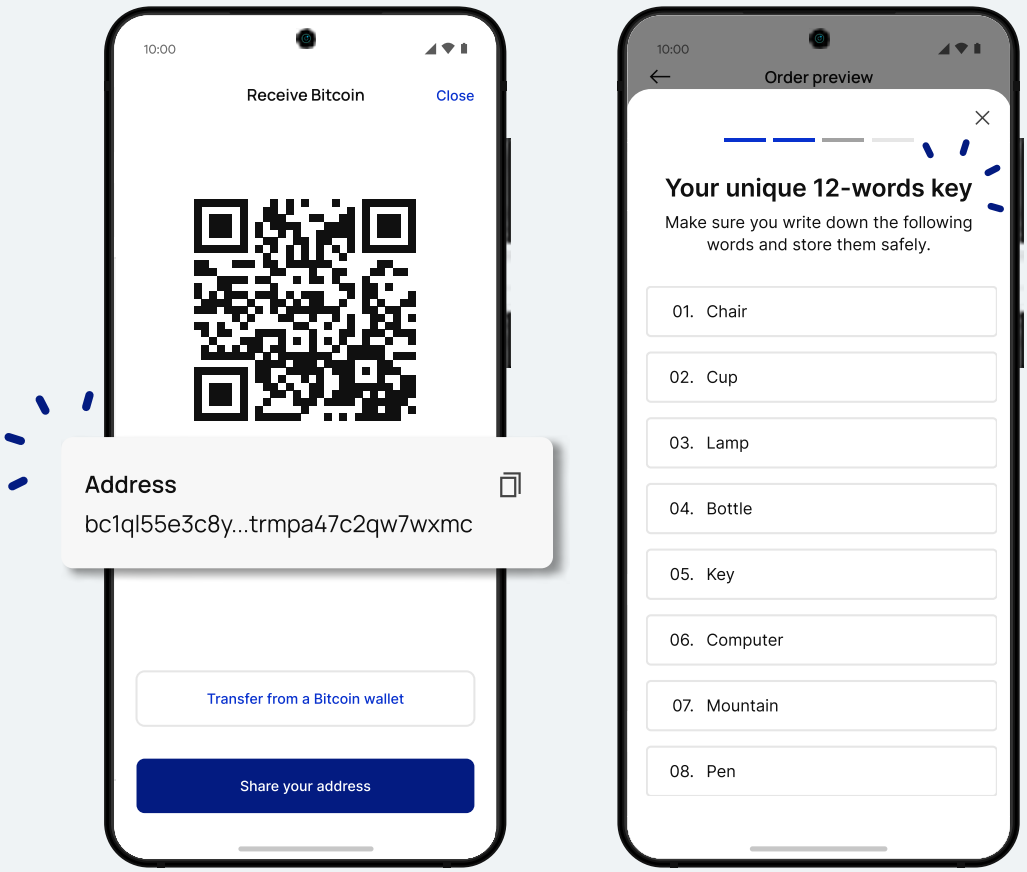
GAB Bitcoin

Il est également possible de retirer des bitcoins via des distributeurs automatiques. Ceux-ci sont déjà disponibles dans de nombreux pays, notamment en Suisse, en Allemagne et en Autriche. Aux distributeurs automatiques de bitcoins, les bitcoins peuvent être retirés de manière anonyme avec de l'argent liquide ou une carte de crédit. Il n'est pas nécessaire d'avoir un compte ou un portefeuille de crypto-monnaies.

Stocker les Bitcoins en Toute Sécurité

Une fois les bitcoins acquis, la question de leur manipulation et de leur stockage en toute sécurité se pose. Les bitcoins et les crypto-monnaies sont régis par le principe suivant : „pas vos clés, pas vos pièces". Pour être véritablement propriétaire de votre bitcoin, vous devez être en possession des clés privées correspondantes. Cette expression quelque peu technique signifie que vous n'avez réellement le contrôle de vos bitcoins que si vous les stockez dans un portefeuille numérique personnel dont vous possédez les clés privées.

Tant que les bitcoins sont déposés sur une bourse de crypto-monnaies, ils sont sous le contrôle de la bourse. Si la bourse est piratée, fait faillite ou est frauduleuse, les bitcoins peuvent être perdus à jamais.



Autoconservation

Contrairement à un compte bancaire, Bitcoin vous donne la possibilité de stocker vos unités monétaires dans un portefeuille personnel. Cela vous permet d'être votre propre banque et présente l'avantage de vous donner un contrôle absolu sur vos bitcoins. En contrepartie, cela s'accompagne également de responsabilités. La clé privée, qui se présente souvent sous la forme de douze ou vingt-quatre mots, doit être stockée et gardée en sécurité par le propriétaire du bitcoin concerné lui-même. Une manipulation incorrecte ou négligente peut entraîner la perte irrévocable des bitcoins.

Wallets: Portefeuilles Numériques

Les portefeuilles numériques permettent de stocker en toute sécurité les bitcoins, ou plus précisément les clés privées. Les bitcoins eux-mêmes sont toujours stockés sur la blockchain et ne peuvent pas être transférés dans un portefeuille. Seules les clés d'accès aux bitcoins peuvent être stockées dans un portefeuille.

Les portefeuilles ont donc été créés pour stocker les clés privées en toute sécurité et de manière simple. En outre, ils permettent d'envoyer et de recevoir des bitcoins en quelques clics seulement. Les portefeuilles sont donc un outil utile pour manipuler les bitcoins.

Portefeuille logiciel (Software Wallet)

Les portefeuilles les plus courants sont les portefeuilles logiciels. Les portefeuilles logiciels peuvent être configurés comme des applications de bureau ou des applications pour smartphone. Lors de la configuration, les clés privées du portefeuille sont listées sous la forme de douze ou vingt-quatre mots (phrase mnémonique). Ces mots sont synonymes de bitcoin dans ce portefeuille. Quiconque connaît ces mots a le contrôle des pièces. Par conséquent, les mots doivent être notés de manière analogue, de préférence sur papier, en secret et conservés en lieu sûr. Si l'ordinateur ou le smartphone est perdu ou volé, le portefeuille peut être restauré à tout moment grâce à ces mots.

Les portefeuilles logiciels présentent l'avantage de pouvoir être configurés rapidement et d'être faciles à utiliser. Cependant, comme les portefeuilles logiciels sont des programmes informatiques installés sur un appareil et connectés directement à l'internet, il existe toujours un risque d'attaques de pirates informatiques.

Portefeuille matériel (Hardware Wallet)

Si vous attachez de l'importance à la sécurité, vous devriez plutôt utiliser un portefeuille matériel. Ces petits appareils stockent les codes d'accès aux bitcoins sur un dispositif de type clé USB qui n'est connecté à l'ordinateur qu'en cas de besoin. Le dispo-

sitif est conçu de manière à ce que même un ordinateur infecté par un logiciel malveillant ne puisse pas accéder aux codes.

Lors de la création d'un portefeuille matériel, douze ou vingt-quatre mots (phrase mnémonique) sont générés, qui doivent être notés de manière analogue et conservés en lieu sûr. Si le porte-monnaie matériel est perdu, il peut être restauré à l'aide de ces mots. Des exemples de porte-monnaie matériels sont BitBox et Trezor.

Made in Switzerland

LE PLUS SIMPLE D'EUROPE BITCOIN APPLICATION

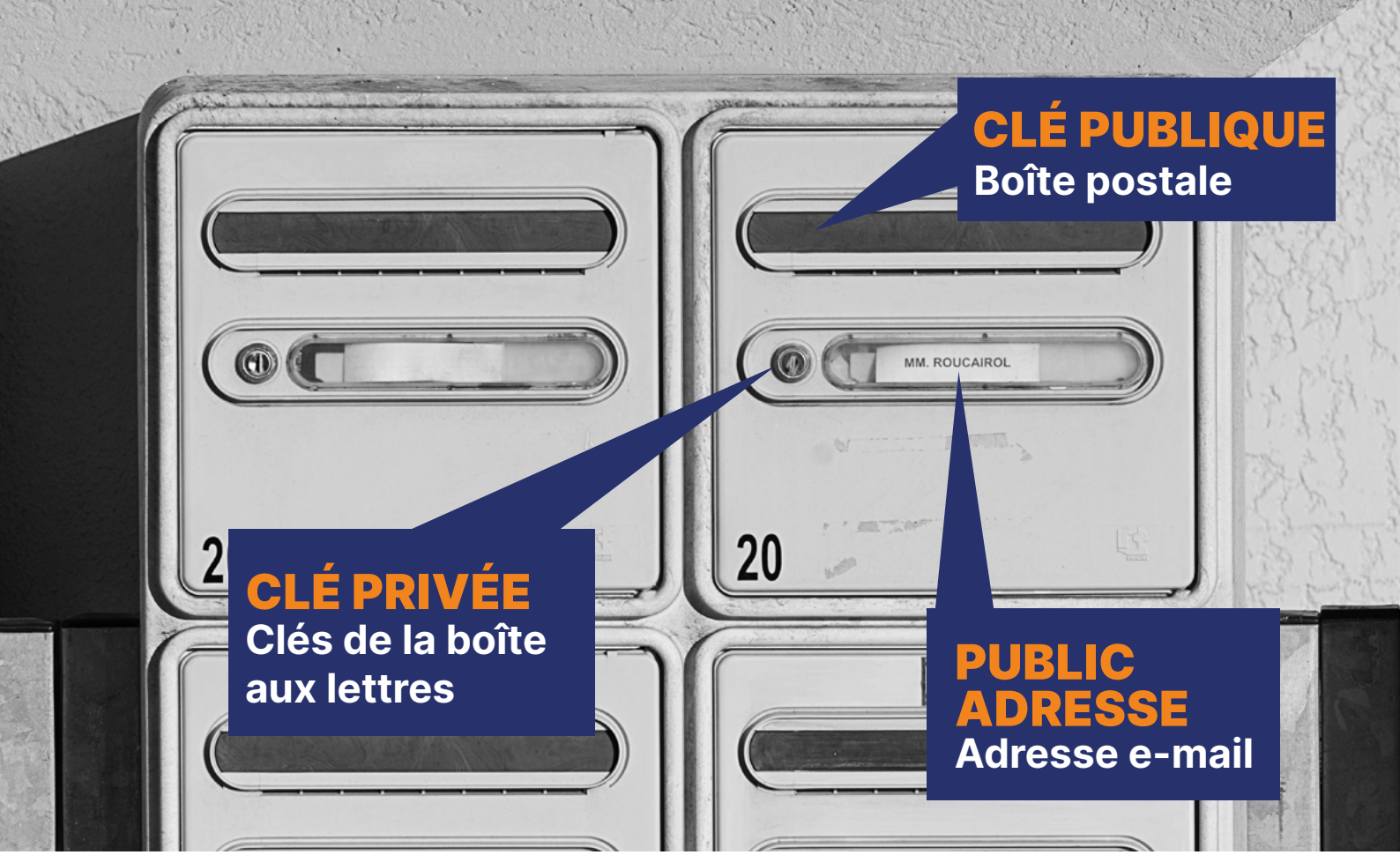
Bitcoins reçus	BTC 0.00254340
24.09.2021	CHF 50.65

Relai

Download on the App Store

GET IT ON Google Play

Achetez des bitcoins en une minute à partir de 10 EUR/CHF seulement, sans vérification.



Envoyer et recevoir du bitcoin

Envoyer et recevoir des bitcoins est très facile. Chaque porte-monnaie Bitcoin a son adresse publique générée à partir de ce que l'on appelle la clé publique. Cette adresse sert d'adresse de réception, à l'instar d'un IBAN. Quiconque possède cette adresse peut envoyer des bitcoins au porte-monnaie correspondant. L'adresse est souvent affichée sous la forme d'un QR code, ce qui simplifie encore la manipulation.

Si vous souhaitez envoyer des bitcoins à quelqu'un, vous pouvez soit saisir l'adresse bitcoin du destinataire dans votre portefeuille sous „envoyer", soit scanner le QR code correspondant. Les frais de transaction encourus sont automatiquement déduits du portefeuille de l'expéditeur. Le montant des frais de transaction varie en fonction de la charge du réseau et peut être consulté ici. Il faut en moyenne 10 minutes pour que le transfert parvienne au destinataire. Toutefois, il peut également prendre plus de temps, en fonction du nombre de frais de transaction que vous êtes prêt à payer.

Payer avec Bitcoin

Lorsque le bitcoin a été créé, on espérait qu'il pourrait un jour être utilisé pour payer des biens de consommation courante. Et en théorie, cela est possible aujourd'hui. Certains services fiscaux gouvernementaux, des organisations à but non lucratif et un nombre croissant d'entreprises acceptent le bitcoin comme moyen de paiement. Mais comme les transactions via le réseau Bitcoin peuvent

coûter plusieurs francs et prendre au moins 10 minutes, cela n'a de sens que pour les gros montants. Pour envoyer des bitcoins à bon marché et rapidement, il faut une solution alternative.

Le Réseau Lightning (Lightning Network) - plus rapide et moins cher

Par conséquent, une couche supplémentaire a été construite au-dessus du réseau Bitcoin. Ce réseau, appelé Lightning, permet de payer avec des bitcoins en quelques secondes à un coût minimal. Dans des pays comme le Salvador, le réseau Lightning est déjà utilisé activement et avec succès.
À l'avenir, le paiement des biens de consommation courante avec des bitcoins se fera donc en grande partie via le réseau Lightning. Les développements dans ce domaine vont bon train. Twitter, par exemple, a récemment introduit une fonction „pourboire" qui utilise le réseau Lightning. De plus, l'application Strike propose des paiements dans le monde entier, dans différentes monnaies, sans frais, via le réseau Lightning. Il faut donc s'attendre à ce qu'à l'avenir, seuls les gros montants soient réglés directement via le réseau Bitcoin, tandis que toutes les autres transactions passeront par le réseau Lightning.

Étant donné que ce sont principalement les petits montants qui sont envoyés via le réseau Lightning, les satoshis, ou Sats en abrégé, sont utilisés comme unité de compte à la place du bitcoin. Un bitcoin est égal à 100 000 000 de satoshis. Pour utiliser le réseau Lightning, un porte-monnaie Lightning doit être configuré.

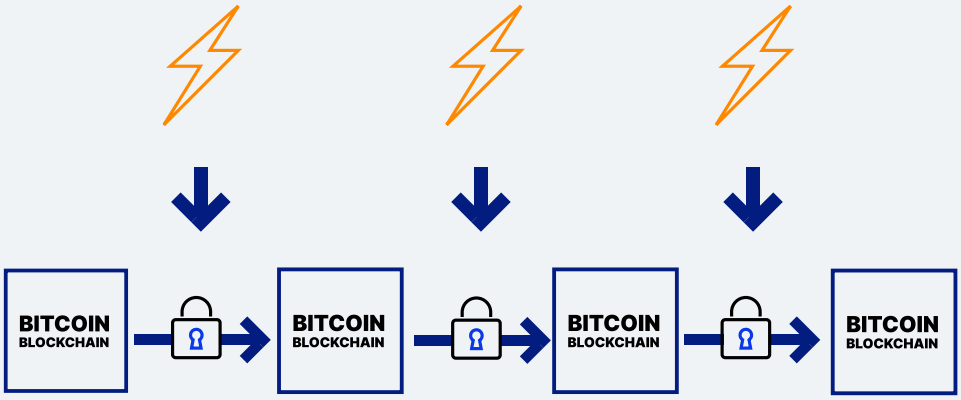
UN REGARD VERS L'AVENIR

Au cours de ses plus de dix années d'existence, le bitcoin a connu de nombreux hauts et bas. La cryptomonnaie a été déclarée morte ou est tombée dans l'oubli auprès du grand public à plusieurs reprises après de lourdes pertes de prix. Cependant, le bitcoin s'est répandu inexorablement dans le monde entier au cours de la dernière décennie.

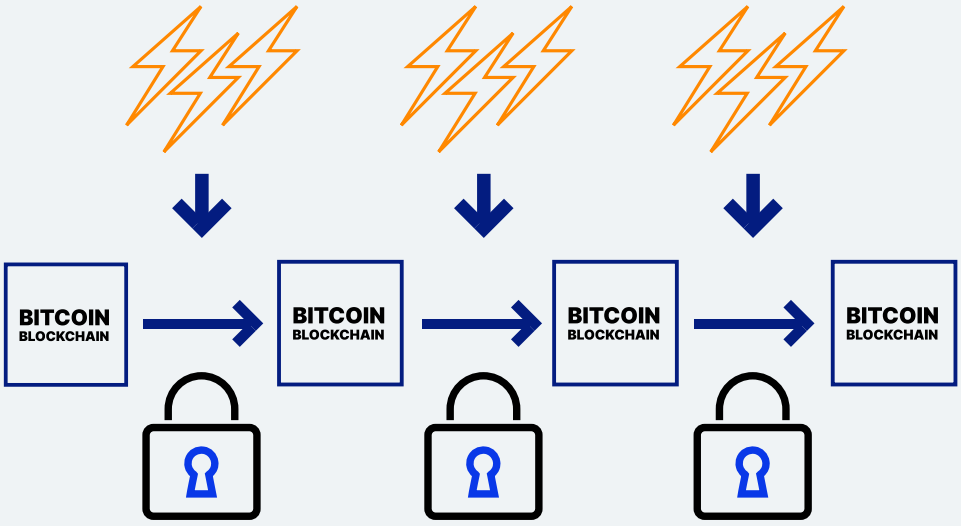
Bitcoin et Énergie

L'une des premières préoccupations souvent soulevées concernant le développement de Bitcoin est la consommation d'énergie du réseau Bitcoin. Le minage de Bitcoin consomme déjà une quantité importante d'électricité dans le monde. Et

Moins l'énergie sous forme de puissance de calcul est utilisée pour construire la blockchain Bitcoin, plus il est facile de la modifier par la suite.



Plus l'énergie sous forme de puissance de calcul est utilisée pour créer la blockchain Bitcoin, plus il est difficile de la modifier par la suite.



cette consommation est susceptible d'augmenter à l'avenir, à mesure que de plus en plus de personnes se lancent dans le minage de Bitcoin.

Lorsqu'on parle de Bitcoin et d'énergie, il est important de comprendre que la quantité d'énergie qui alimente le réseau Bitcoin est essentielle à la sécurité du réseau. Plus le réseau est alimenté en énergie, plus il est sécurisé. En effet, pour modifier la blockchain Bitcoin, il faut dépenser à nouveau la même quantité de puissance de calcul - et donc d'énergie - qui a été investie pour créer la blockchain en premier lieu. Cependant, avec des millions d'ordinateurs dans le monde fournissant de la puissance de calcul au réseau Bitcoin, il est pratiquement impossible pour un individu, une organisation ou un État de rassembler suffisamment de puissance de calcul pour apporter les plus petites modifications à la blockchain. Par conséquent, la puissance de calcul et la consommation d'énergie associée constituent un élément de sécurité important du réseau Bitcoin.

De plus, les ordinateurs de minage Bitcoin ont l'avantage de pouvoir être situés n'importe où dans le monde. Comme les mineurs ont besoin de

l'électricité la moins chère possible pour être rentables, ils s'installent souvent dans des endroits où il y a beaucoup d'excédents, et donc de l'énergie bon marché. À long terme, il est probable que ce soit dans des endroits où il y a beaucoup d'énergie renouvelable, car celle-ci produit l'électricité la moins chère.

Selon le Bitcoin Mining Council, les mineurs de Bitcoin utilisent actuellement environ 56 % d'énergie renouvelable et la tendance est à la hausse. De nombreux experts en bitcoins pensent que le minage de bitcoins sera alimenté par des énergies renouvelables à hauteur de 100 % à l'avenir.

En attendant, la consommation d'énergie de Bitcoin se résume à la question de savoir si une monnaie et une réserve de valeur sûres et infalsifiables valent ou non cette dépense d'énergie.

El Salvador - Le Bitcoin Comme Monnaie Nationale

Il y a quelques années, des visionnaires pensaient déjà qu'il était possible que le bitcoin soit un jour reconnu comme monnaie légale par les États-nations. À l'été 2021, le moment était venu : Le Salvador était le premier pays au monde à introduire le bitcoin comme monnaie légale. Dans les magasins, les restaurants et chez les prestataires de services de toutes sortes, le paiement peut être effectué non seulement en dollars américains mais aussi en bitcoins. À cette fin, les citoyens ont reçu un portefeuille Bitcoin personnalisé, qui permet d'effectuer des paiements via le réseau Lightning en quelques secondes et à un coût minime.

D'autres pays comme l'Ukraine, le Brésil et le Panama discutent actuellement de projets de loi similaires. Si d'autres pays devaient suivre l'exemple du Salvador, cela augmenterait d'une part la demande de bitcoins et, d'autre part, renforcerait la crédibilité du bitcoin en tant que „monnaie". L'acceptation du bitcoin comme monnaie légale dans un nombre croissant de pays représente donc une phase décisive dans le processus d'adaptation du bitcoin à l'échelle mondiale.

Les Lois et Règlements

Ces évolutions ont conduit les États-nations, les banques centrales et les entreprises à s'intéresser de près aux crypto-monnaies. Divers États, dont la Suisse, ont publié des règlements et des directives concernant les crypto-monnaies. Cette étape est saluée par de nombreux acteurs du marché, car elle crée une sécurité juridique tant pour les projets de crypto-monnaies que pour les investisseurs concernés.

Des réglementations se profilent également à l'horizon aux États-Unis, qui ont jusqu'ici adopté une approche de laissez-faire. La forme exacte que

prendront ces nouvelles lois de régulation aux États-Unis est suivie de près par la communauté crypto mondiale, car elles auront un impact majeur sur l'ensemble du secteur crypto.

Autres Crypto-Monnaies

Le bitcoin n'est de loin pas la seule crypto-monnaie actuelle. Il existe désormais plus de 16 000 crypto-monnaies et actifs différents. Ces pièces et jetons ont des caractéristiques et des fonctionnalités différentes et n'ont pas tous été conçus comme des „monnaies" ou de l'argent. Certaines s'apparentent davantage à des actions, dans la mesure où leur valeur reflète le succès d'un projet cryptographique. D'autres sont nécessaires à l'utilisation d'un service particulier. Et d'autres encore - les jetons dits „mèmes" - sont avant tout des monnaies ludiques.

Pour éviter les pertes, il est donc conseillé d'examiner de plus près la monnaie concernée et le projet qui la sous-tend avant d'investir.

Monnaies Numériques des Banques Centrales - Central Bank Digital Currencies (CBDC)

Les crypto-monnaies sont en train de passer d'une phase Wild-West non réglementée à un monde de crypto-finance réglementé. Cette évolution n'a pas laissé les banques centrales indemnes, et des idées ont été émises selon lesquelles les banques centrales devraient émettre leurs propres crypto-monnaies. Ces „monnaies numériques de banque centrale", ou CBDC, combineraient, selon leurs partisans, la stabilité d'une monnaie d'État avec les avantages d'une monnaie basée sur la blockchain. En bref, elles créeraient de l'argent numérique, pour ainsi dire.

Toutefois, en fonction de sa conception, une CBDC peut prendre des formes fondamentalement différentes.
Divers pays ont lancé des essais pilotes avec différents types de CBDC, et des CBDC ont déjà été lancées dans quelques pays. Cependant, on attend avec impatience de savoir si et sous quelle forme les zones monétaires économiquement fortes telles que les États-Unis, l'UE ou la Chine lanceront leurs CBDC.

Concours D'argent

Notre société s'est tellement habituée aux monnaies d'État au cours des dernières décennies que d'autres types de monnaie étaient à peine imaginables pour beaucoup jusqu'à récemment. Pourtant, il n'y a pas si longtemps, la circulation parallèle de différents types d'argent faisait partie de la vie quotidienne. Il y avait des billets de banque de diverses banques, des pièces de monnaie faites de différents métaux et d'autres valeurs monétaires qui pouvaient être utilisées comme moyens de paiement.

Avec le bitcoin, les monnaies non étatiques sont à nouveau disponibles comme alternative aux monnaies étatiques. Jusqu'à présent, la majorité des gouvernements ont toléré le bitcoin. Dans une certaine mesure, cela pourrait être dû à sa nature décentralisée, qui rend le bitcoin difficile à attaquer. Pour les citoyens, cela signifie qu'une alternative numérique à la monnaie d'État est désormais disponible aux côtés de l'or et de l'argent. Les effets de cette concurrence monétaire supplémentaire seront passionnants à observer à l'avenir.
.

BITCOIN, ET MAINTENANT?

Si vous vous demandez ce que vous devez faire de toutes ces informations, laissez-moi vous faire une suggestion. Entrer dans le monde du bitcoin ne coûte rien, ni temps ni argent. Mais vous apprendrez à connaître une technologie qui est sur le point de changer notre monde et l'avenir.

Par conséquent : Créez un compte sur une bourse de crypto-monnaies ou téléchargez un portefeuille sur votre smartphone et achetez des bitcoins pour 50 CHF. Ou demandez à un collègue de vous envoyer des bitcoins sur votre portefeuille. Mais mettez la main sur des bitcoins au moins une fois.

Car si le bitcoin devait percer et devenir aussi omniprésent qu'Internet, vous n'en aurez pas seulement une connaissance théorique, mais vous l'aurez aussi utilisé vous-même. Parfois, cela fait toute la différence, car cela vous permet de voir et de sentir la technologie, ce qui vous donne une longueur d'avance sur la majorité des gens.

ABOUT

A PROPOS DE L'AUTEUR

Daniel Jungen est un économiste et journaliste financier spécialisé dans les crypto-actifs. Daniel est cofondateur d'InsightDeFi, une boutique de recherche spécialisée dans tout ce qui touche à la crypto. Avec ses partenaires d'InsightDeFi, ils publient une lettre d'information bihebdomadaire (en allemand) sur le bitcoin, le DeFi et les crypto-monnaies.

À PROPOS DE RELAI

Fondée en Suisse par Julian Liniger et Adem Bilican après avoir eu du mal à trouver un espace sûr et sans tracas pour acheter des bitcoins, Relai rend l'épargne et l'investissement en bitcoins accessibles à tous. L'application réservée aux bitcoins est conçue pour être simple et intuitive, permettant à toute personne en Europe d'acheter et de vendre des bitcoins en quelques minutes, sans avoir besoin de s'inscrire, de vérifier ou de faire des dépôts. Audité de manière indépendante, et avec plus de 35 millions de CHF de bitcoins investis sur sa plateforme, Relai donne aux consommateurs la possibilité de débloquer de nouveaux moyens d'épargne et d'investissement.

Pour en savoir plus, consultez Relai.app.

Merci à Sovereign Monk (@svmonk21) qui a traduit cet e-book de l'anglais au français