BITCOINS

- TATA Fella
- Soukeur Meryem

1CS Groupe1

ESI 15/05/2016

TABLE DES MATIÈRES

Contenu

Inroduction

Bitcoin est un réseau de consensus distribué permettant l'existence d'un nouveau système de paiement et d'une monnaie entièrement numérique. Il s'agit du premier réseau de paiement pair à pair décentralisé fonctionnant grâce à ses utilisateurs, sans autorité centrale ou intermédiaire. Pour ses utilisateurs, Bitcoin est comparable à de l'argent liquide pour Internet. Bitcoin peut aussi être vu comme le plus grand système de comptabilité à 3 entrées.

Bitcoin est la première implémentation d'un concept appelé crypto-monnaie, qui a été décrit pour la première fois par Wei Dai en 1998 dans la liste de diffusion « cypherpunks », suggérant l'idée d'une nouvelle forme d'argent qui utiliserait la cryptographie pour contrôler sa création et ses transactions plutôt qu'une autorité centrale. La première spécification et preuve du concept a été publiée en 2009 dans une liste de diffusion sur la cryptographie par Satoshi Nakamoto. Satoshi a quitté le projet fin 2010 sans révéler grand chose à son sujet. Depuis, la communauté a grandi de manière exponentielle avec plusieurs développeurs travaillant sur Bitcoin.

L'anonymat de Satoshi a souvent suscité des inquiétudes injustifiées, en grande part liées à l'incompréhension de la nature libre et ouverte de Bitcoin. Le protocole et le logiciel Bitcoin sont publiés de manière ouverte et n'importe quel développeur autour du globe peut relire le code et développer sa propre version du logiciel Bitcoin. Tout comme les développeurs actuels, l'influence de Satoshi était limitée à l'adoption de ses changements par d'autres et par conséquent il ne contrôlait donc pas Bitcoin. Ainsi, l'identité du créateur de Bitcoin est aujourd'hui sans doute aussi pertinente que celle de l'inventeur du papier.

Fonctionnement du bitcoin

Du point de vue de l'utilisateur, Bitcoin n'est rien de plus qu'une appli mobile ou un logiciel pour ordinateur qui fournit à un portefeuille personnel permettant à un utilisateur d'envoyer et recevoir des bitcoins. C'est ainsi que fonctionne Bitcoin pour la majorité de ses utilisateurs.

En coulisse, le réseau Bitcoin partage un grand livre comptable nommé « chaine de blocs ». Celui-ci contient chaque transaction jamais traitée permettant à l'ordinateur d'un utilisateur de vérifier la validité de chaque transaction. L'authenticité de chaque transaction est protégée par des signatures numériques correspondant aux adresses émettrices, permettant à tous les utilisateurs d'être pleinement en contrôle de l'envoi de bitcoins à partir de leurs propres adresses Bitcoin. De plus, toute personne peut également traiter des transactions en utilisant la puissance de calcul de matériel spécialisé et gagner une récompense en bitcoins en retour de ce service. C'est ce qu'on appelle souvent le « minage ».

Utilisation du bitcoin

Il y a un nombre croissant d'entreprises et d'individus qui se servent de Bitcoin. Cela inclut des entreprises sur rue et des points de vente tels que des restaurants, des appartements, des cabinets d'avocats et des services en ligne populaires tels que Namecheap, WordPress, Reddit et Flattr. Bien que Bitcoin reste un phénomène relativement nouveau, il témoigne d'une croissance rapide. À la fin du mois d'août 2013, la valeur de tous les bitcoins en circulation a dépassé 1,5 milliard $ US avec des millions de dollars échangés quotidiennement en bitcoins.

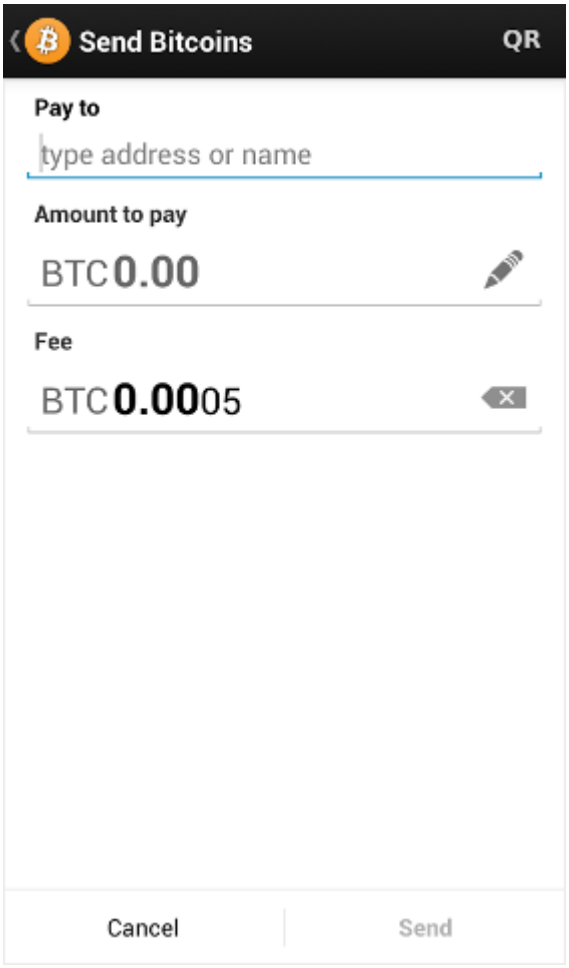
Acquésition des bitcoins

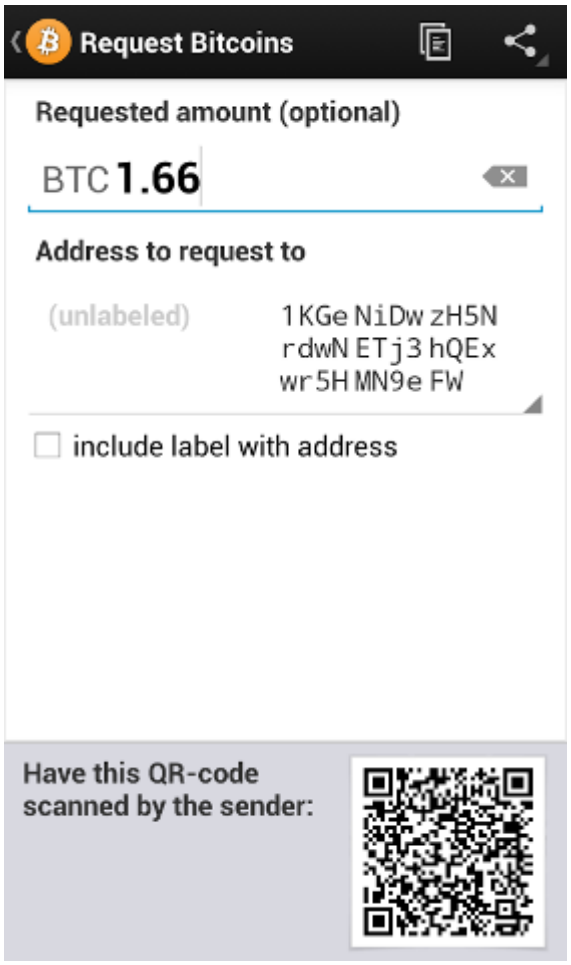
- En tant que paiement pour des biens ou des services.
- Par l'achat de bitcoins sur une bourse de change.
- En échangeant des bitcoins avec quelqu'un près de chez vous.
- En gagnant des bitcoins par le biais de minage compétitif.

Bien qu'il soit possible de trouver des individus qui acceptent de vendre des bitcoins en échange de paiements par PayPal ou par cartes de crédit, la plupart des bourses de change n'acceptent pas ces méthodes de paiement en raison de cas où des clients paient pour des bitcoins avec PayPal et renversent leur propre transaction par la suite, ce qu'on appelle communément un rejet de débit.

Effectuer un paiement avec bitcoin

Effectuer des paiements avec Bitcoin est plus facile que de faire des achats à l'aide d'une carte de débit ou de crédit, et les paiements peuvent être reçus sans avoir de compte commercial. Les paiements s'effectuent à l'aide d'un logiciel portefeuille, soit sur votre ordinateur ou sur votre téléphone portable, en entrant l'adresse du destinataire, le montant à payer et en appuyant sur envoyer. Pour faciliter la saisie de l'adresse du destinataire, plusieurs portefeuilles peuvent obtenir l'adresse en scannant un code QR ou en approchant deux téléphones dotés de la technologie NFC.





Prix du Bitcoin

Le prix du bitcoin est déterminé par l'offre et la demande. Lorsque la demande pour les bitcoins augmente, le prix augmente et lorsque la demande diminue, le prix diminue. Il n'y a qu'un nombre limité de bitcoins en circulation et de nouveaux bitcoins sont créés à un rythme prévisible et décroissant, ce qui signifie que la demande doit suivre ce niveau d'inflation afin de maintenir la stabilité du prix. Étant donné que Bitcoin demeure

un marché relativement petit comparativement à ce qu'il pourrait être, la quantité d'argent requise pour affecter le prix à la hausse ou à la baisse n'est pas élevé et, pour cette raison, le prix du bitcoin demeure très volatile.

Transaction des bitcoins

Recevoir un paiement avec Bitcoin est presque instantané. Toutefois, il y a un délai de 10 minutes en moyenne avant que le réseau ne commence à confirmer votre transaction en l'incluant dans un bloc et avant que vous ne puissiez dépenser les bitcoins que vous recevez. Une confirmation signifie qu'il existe un consensus dans le réseau à l'effet que les bitcoins que vous avez reçus n'ont été envoyés à personne d'autre et sont considérés comme étant votre propriété. Une fois que votre transaction est incluse dans un bloc, elle continuera d'être enfouie sous chaque bloc après celui-ci, ce qui consolidera exponentiellement ce consensus et diminuera le risque d'une transaction renversée. Chaque utilisateur est libre de déterminer à quel moment il considère une transaction confirmée, et 6 confirmations est souvent considéré comme étant aussi sécurisé qu'une attente de 6 mois pour une transaction par carte de crédit.

de vos bitcoins rapidement peut également nécessiter des frais. Si votre activité s'apparente à des transactions conventionnelles, les frais devraient demeurer très bas.

L’anonymat du bitcoin

Bitcoin est conçu de manière à permettre à ses utilisateurs d'effectuer des paiements avec un niveau acceptable de confidentialité, de même que toute autre forme de monnaie. Bitcoin n'est toutefois pas anonyme et ne peut pas offrir le même niveau de confidentialité que l'argent liquide. L'utilisation de Bitcoin laisse beaucoup de traces publiques. Divers mécanismes existent ou sont développés pour protéger la confidentialité des utilisateurs. Cependant, il reste du travail à faire avant que ces fonctions soient utilisées correctement par la majorité des utilisateurs de Bitcoin.

Certaines préoccupations ont été soulevées à l'idée que des transactions privées puissent être utilisées à des fins illégales avec Bitcoin. Toutefois, il convient de souligner que Bitcoin sera sans aucun doute sujet à des réglementations similaires à celles déjà en place dans les systèmes financiers actuels. Bitcoin ne peut pas être plus anonyme que l'argent liquide et il ne risque pas d'empêcher la tenue d'enquêtes criminelles. En outre, Bitcoin est également conçu pour empêcher un large éventail de crimes financiers.

Protection des consommateurs des bitcoins

Bitcoin offre la liberté à chacun d'effectuer des transactions selon ses propres termes. Chaque utilisateur peut envoyer et recevoir des paiements d'une manière similaire à l'argent liquide mais peut également prendre part à des contrats plus complexes. Les signatures multiples permettent à une transaction d'être acceptée par le réseau uniquement si un certain nombre d'un groupe de personnes défini accepte de signer la transaction. Ceci pourrait permettre la création de services de médiation innovants dans le futur. De tels services pourraient permettre à un tiers d'approuver ou refuser une transaction dans le cas d'un désaccord entre les autres partis sans pour autant avoir de contrôle sur leur argent. Contrairement à d'autres méthodes de paiement, Bitcoin laisse toujours une preuve publique qu'une transaction a eu lieu, qui peut potentiellement être utilisée dans un recours contre des entreprises aux pratiques frauduleuses.

Génération des bitcoins

Les bitcoins sont générés par un processus compétitif et décentralisé que l'ont nomme « minage ». Ce processus implique que des individus sont récompensés par le réseau pour leurs services. Les mineurs traitent les transactions et sécurisent le réseau en utilisant du matériel spécialisé et, en échange, collectent des nouveaux bitcoins.

Le protocole Bitcoin est conçu de façon à ce que les nouveaux bitcoins soient créés à un rythme fixe. Cela fait du minage de bitcoins une affaire très concurrentielle. Lorsque davantage de mineurs se joignent au réseau, faire des bénéfices devient de plus en plus difficile et les mineurs doivent améliorer leur rendement pour diminuer leurs coûts d'opération. Aucune autorité centrale ni développeur ne détient le pouvoir de contrôler ou manipuler le système de manière à augmenter ses profits. Tous les nœuds Bitcoin à travers le monde rejetteront tout ce qui n'est pas conforme aux règles qui doivent être suivies par le système.

Les bitcoins sont créés à un rythme décroissant et prévisible. Le nombre de nouveaux bitcoins créés chaque année est automatiquement réduit de moitié au fil du temps jusqu'à ce que l'émission de bitcoins s'arrête complètement avec un total de 21 millions de bitcoins en circulation. À ce state, les mineurs de bitcoins seront probablement soutenus exclusivement par un nombre élevé de petits frais de transaction.

Contrôl du réseau bitcoin

Le réseau Bitcoin n'appartient à personne, tout comme la technologie derrière le courriel n'appartient à personne. Bitcoin est contrôlé par l'ensemble de ses utilisateurs autour du monde. Alors que les développeurs améliorent les logiciels, ils ne peuvent pas imposer de modification dans le protocole Bitcoin parce que chaque utilisateur est libre de choisir quel logiciel et quelle version il utilise. Afin de rester compatibles avec les autres, tous les utilisateurs doivent utiliser des logiciels se conformant aux mêmes règles. Bitcoin ne peut fonctionner correctement qu'avec un consensus total entre ses utilisateurs. Par conséquent, les utilisateurs et développeurs ont grand intérêt à protéger ce consensus

Minage des bitcoins

Le minage est le processus d'utiliser de la puissance de calcul informatique afin de traiter des transactions, sécuriser le réseau et permettre à tous les utilisateurs du système de rester synchronisés. Ceci peut être perçu comme le centre de données de Bitcoin, à l'exception qu'il a été conçu pour être entièrement décentralisé avec des mineurs opérant dans tous les pays et sans aucun individu contrôlant le réseau. Le nom « minage » est utilisé en analogie au minage de l'or parce qu'il s'agit également d'un mécanisme temporaire pour émettre de nouveaux bitcoins. Toutefois, à l'inverse de l'or, le minage de bitcoins offre une récompense en échange d'un service utile et nécessaire pour faire fonctionner un réseau de paiement sécurisé. Le minage sera toujours nécessaire même après l'émission du dernier bitcoin.

Fonctionnement du minage de bitcoins

Toute personne peut devenir un mineur de bitcoins en utilisant un logiciel et du matériel spécialisé. Les logiciels de minage reçoivent les transactions diffusées à travers le réseau de pair à pair et effectuent les tâches appropriées pour traiter et confirmer ces transactions. Les mineurs de bitcoins effectuent ce travail parce qu'ils peuvent être rémunérés par les frais de transactions payés par les utilisateurs pour obtenir un traitement plus rapide de leurs transactions ainsi que les nouveaux bitcoins émis selon une formule déterminée.

Pour que de nouvelles transactions soient confirmées, elles doivent être incluses dans un bloc ainsi qu'une preuve mathématique de travail. De telles preuves sont très difficiles à générer car il n'existe aucun moyen de les créer autrement que par l'essai de milliards de calculs par secondes. Cela force les mineurs à effectuer ces calculs avant que leurs blocs ne soient acceptés par le réseau et avant d'être récompensés. Plus il y a de mineurs sur le réseau, plus la difficulté de trouver des blocs valides est automatiquement augmentée par le réseau pour assurer que le temps requis pour trouver un bloc valide demeure égal à 10 minutes en moyenne. Il en résulte que le

minage est une forme d'entreprise très compétitive où aucun mineur individuel ne peut contrôler ce qui est inclus dans la chaine de blocs.

La preuve de travail est également conçue pour dépendre du bloc précédent afin de forcer un ordre chronologique dans la chaine de blocs. Ce système rend exponentiellement difficile de renverser une transaction précédente étant donné que cette action exige de recalculer les preuves de travail de tous les blocs subséquents. Lorsque deux blocs sont découverts au même moment, les mineurs travaillent sur le premier bloc qu'ils reçoivent et basculent sur la plus longue chaine de blocs dès que le bloc suivant est trouvé. Ceci permet au minage de sécuriser et maintenir un consensus global basé sur la puissance de traitement.

Les mineurs de bitcoins ne peuvent pas tricher en augmentant leurs propres récompenses ni traiter de transactions frauduleuses qui pourraient corrompre le réseau Bitcoin puisque tous les nœuds Bitcoin rejetteraient tout bloc contenant des données invalides selon les règles du protocole Bitcoin. En conséquence, le réseau demeure sécurisé même si tous les mineurs de bitcoins ne sont pas nécessairement de confiance.

Comment le minage aide-il à sécuriser bitcoins ?

Le minage crée l'équivalent d'une loterie compétitive rendant très difficile l'ajout consécutif de nouveaux blocs de transactions dans la chaine de blocs par quiconque. Ceci protège la neutralité du réseau en empêchant tout individu de gagner le pouvoir de bloquer certaines transactions. Ceci empêche également tout individu de remplacer des parties de la chaine de blocs pour renverser ses propres transactions, ce qui pourrait être utilisé pour frauder les autres utilisateurs. Le minage rend le renversement d'une transaction précédente exponentiellement plus difficile en nécessitant la réécriture de tous les blocs à la suite de cette transaction.

La sécurité des bitcoins

La technologie Bitcoin - le protocole et la cryptographie - a de solides antécédents de sécurité et le réseau Bitcoin est probablement le plus grand projet d'informatique distribuée dans le monde. La vulnérabilité la plus commune avec Bitcoin réside dans l'erreur de l'utilisateur. Les fichiers portefeuille qui contiennent les clés privées peuvent être accidentellement supprimés, perdus ou volés. Bitcoin s'apparente à de l'argent liquide sous une forme numérique. Heureusement, les utilisateurs peuvent employer des pratiques de sécurité solides pour protéger leur argent et utiliser des fournisseurs de services qui offrent un bon niveau de sécurité et d'assurance contre le vol et les pertes.

Piratage des Bitcoins

Les règles du protocole et la cryptographie utilisée pour Bitcoin fonctionnent toujours des années après son lancement, ce qui s'avère une bonne indication de la qualité du concept. Toutefois, des failles de sécurité ont été trouvées et corrigées avec le temps dans plusieurs implémentations logicielles. Comme toute autre forme de logiciel, la sécurité des logiciels Bitcoin dépend de la vitesse avec laquelle les problèmes sont trouvés et corrigés. Chaque fois qu'un nouveau problème est découvert, Bitcoin gagne un peu plus en maturité.

Des idées fausses circulent à propos des vols et des brèches de sécurité survenues chez diverses bourses de change et entreprises. Bien que ces événements soient malheureux, aucun d'entre eux n'implique un piratage du protocole Bitcoin ni n'implique un défaut inhérent à Bitcoin, de la même manière que le vol d'une banque ne remet pas en question le dollar. Toutefois, il est juste d'affirmer qu'un ensemble de solutions et de bonnes pratiques de sécurité sont requises afin d'offrir une meilleure protection de l'argent des utilisateurs et réduire le risque général de vol et de perte. Au fil des dernières années, de telles fonctions de sécurité se sont développées rapidement, telles que le

chiffrement des portefeuilles, les portefeuilles hors-ligne, les portefeuilles matériels et les transactions multi-signatures.

La possibilité de comploter contre Bitcoin

Il n'est pas possible de changer le protocole Bitcoin aussi facilement. Tout client Bitcoin qui ne se conforme pas aux mêmes règles ne peut pas imposer ses propres règles sur les autres utilisateurs. Selon la spécification actuelle, la double dépense est impossible sur la même chaine de blocs et il n'est pas possible non plus de dépenser des bitcoins sans signature valide. Par conséquent, il n'est pas possible de générer des sommes incontrôlées de bitcoins à partir de rien, de dépenser les fonds d'autres utilisateurs, de corrompre le réseau, ni rien de semblable.

Toutefois, une majorité de mineurs peut choisir de bloquer ou renverser des transactions récentes de façon arbitraire. Une majorité d'utilisateurs peut également faire pression afin que certains changements soient adoptés. Puisque le protocole Bitcoin ne fonctionne correctement qu'avec un consensus complet entre tous ses utilisateurs, changer le protocole peut être très difficile et exige une majorité écrasante d'utilisateurs de façon à ce que les utilisateurs restants n'aient presque aucun autre choix que de suivre. En général, il est difficile d'imaginer les raisons qui pousseraient un utilisateur à adopter des changements qui pourraient compromettre son propre argent.

Bitcoin est-il vulnérable face aux ordinateurs quantiques ?

Oui, la plupart des systèmes dépendant de la cryptographie le sont en général, incluant les systèmes bancaires traditionnels. Toutefois, les ordinateurs quantiques n'existent pas encore et n'existeront probablement pas dans un futur rapproché. Dans l'éventualité où les ordinateurs quantiques pourraient représenter une menace imminente pour

Bitcoin, le protocole pourrait être mis à niveau afin d'utiliser des algorithmes post-quantiques. Étant donné l'importance qu'aurait une telle mise à jour, il est raisonnable de s'attendre à ce que celle-ci soit activement révisée par les développeurs et adoptée par tous les utilisateurs.

Conséquences de la perte des bitcoins

Un utilisateur perdant son portefeuille a pour effet de retirer de l'argent de la circulation. Les bitcoins perdus demeurent dans la chaine de blocs comme tout autre bitcoin. Toutefois, les bitcoins perdus restent dormants à jamais puisqu'il n'existe aucun moyen pour qui que ce soit de retrouver les clés privées qui permettraient de les dépenser à nouveau. Selon les règles de l'offre et de la demande, si moins de bitcoins sont disponibles, ceux restant seront davantage en demande et leur valeur augmentera pour compenser.

Lagalité des bitcoins

Bitcoin n'a pas été déclaré illégal par force de loi dans la plupart des juridictions. Toutefois, certaines juridictions (telle que l'Argentine et la Russie) restreignent ou bannissent sévèrement les devises étrangères. D'autres juridictions (telle que la Thaïlande) peuvent limiter l’octroi de licences pour certaines entités telles que les bourses de change de bitcoins.

Les organismes de réglementation de diverses juridictions prennent des mesures afin de fournir des règles aux particuliers et aux entreprises sur la manière d'intégrer cette nouvelle technologie avec le système financier réglementé. Par exemple, le « Financial Crimes Enforcement Network » (FinCEN) du département du trésor des États-Unis a émis des directives non contraignantes sur la façon dont il caractérise certaines activités impliquant les monnaies virtuelle

Réglementation des bitcoins

Le protocole Bitcoin lui-même ne peut être modifié sans la coopération de presque tous ses utilisateurs, qui choisissent quel logiciel utiliser. Tenter d'assigner des droits spéciaux à une autorité locale dans les règles du réseau Bitcoin mondial n'est pas une possibilité réalisable dans la pratique. N’importe quelle riche organisation pourrait choisir d'investir dans de l'équipement de minage pour contrôler la moitié de la puissance de calcul du réseau et devenir capable de bloquer ou renverser les transactions récentes. Toutefois, rien ne garantit qu'elle pourrait conserver cette puissance étant donné que cela exige d'investir autant que tous les autres mineurs dans le monde.

Il est toutefois possible de réguler l'usage de Bitcoin d'une manière similaire à celle de tout autre instrument. Tout comme le dollar, Bitcoin peut être utilisé à des fins très variées dont certaines peuvent être considérées légitimes ou illégitimes en regard des lois applicables à chaque juridiction. À ce titre, Bitcoin n'est pas différent de tout autre outil ou ressource et peut être sujet à différentes réglementations dans chaque pays. L'utilisation de Bitcoin pourrait être rendue difficile par des réglementations contraignantes, dans quel cas il est difficile de déterminer quel pourcentage des utilisateurs continueraient à utiliser la technologie. Un gouvernement qui choisirait de bannir Bitcoin empêcherait le développement d'entreprises et de marchés sur son propre territoire, cédant l'innovation à d'autres pays. Le défi pour les autorités de réglementation, comme toujours, est de développer des solutions efficaces tout en ne portant pas atteinte à la croissance de nouveaux marchés et entreprises émergents.

Avantages du bitcoin

LIBERTÉ DE PAIEMENT - Il est possible d'envoyer et recevoir n'importe quel montant d'argent instantanément, partout dans le monde et à tout moment. Pas de frontières, ni de limites imposées. Bitcoin permet à ses utilisateurs de pleinement contrôler leur argent.

- **TRÈS PEU DE FRAIS -** Les paiements avec Bitcoin sont actuellement traités gratuitement ou avec des frais extrêmement bas. Les utilisateurs peuvent volontairement inclure des frais de transaction pour recevoir un traitement prioritaire, ce qui se traduit par une confirmation plus rapide des transactions par le réseau. De plus, des services commerciaux existent pour assister les commerçants avec le traitement des transactions, convertissant les bitcoins en monnaie fiduciaire et en déposant les fonds directement dans leurs comptes bancaires sur une base journalière. Puisque ces services sont basés sur Bitcoin, ils peuvent être offerts à moindres frais que PayPal et les les cartes de crédit.
- **MOINS DE RISQUE POUR LES COMMERÇANTS -** Les transactions avec Bitcoin sont sécurisées, irréversibles et ne contiennent pas d'informations sensibles ou personnelles de clients. Ceci permet aux commerçants d'être protégés contre des pertes dues aux fraudes et aux oppositions de paiement sans conformité PCI nécessaire. Les commerçants peuvent s'étendre vers de nouveaux marchés où les cartes de crédit sont inexistantes ou dans lesquels le taux de fraude est inacceptable. Le résultat net : des marchés élargis et moins de coûts administratifs.
- **SÉCURITÉ ET CONTRÔLE -** Les utilisateurs de Bitcoin ont un contrôle total de leurs transactions. Il est impossible pour un commerçant d'imposer des frais non désirés ou cachés comme cela peut se produire avec d'autres méthodes de paiement. Les paiements avec Bitcoin peuvent être effectués sans aucune information personnelle liée à la transaction. Ceci offre une protection forte contre le vol d'identité. Les utilisateurs de Bitcoin peuvent également protéger leur argent à l'aide de sauvegardes et du chiffrement.

- **TRANSPARENCE ET NEUTRALITÉ -** Toutes les informations relatives à la masse monétaire de Bitcoin sont facilement accessibles dans la chaine de blocs de telle sorte que chacun puisse vérifier ou utiliser ces informations en temps réel. Personne ne peut contrôler ou manipuler le protocole Bitcoin car il est cryptographiquement sûr. Cela permet d'avoir la certitude que la base du réseau Bitcoin est entièrement neutre, transparente et prévisible.

Désavantages du bitcoin

- **NIVEAU D'ADOPTION -** Plusieurs personnes ignorent toujours l'existence de Bitcoin. Chaque jour, plus d'entreprises acceptent les bitcoins parce qu'elles en sont attirées par les avantages, mais la liste demeure petite et doit croître davantage pour pouvoir bénéficier de l'effet de réseau.
- **VOLATILITÉ -** La valeur totale des bitcoins en circulation et le nombre de commerces utilisant Bitcoin demeurent très inférieurs à ce qu'ils pourraient être. Pour cette raison, le prix des bitcoins peut être significativement affecté par des événements relativement petits et des activités boursières ou commerciales. En théorie, cette volatilité diminuera au fur et à mesure que le marché et que la technologie gagneront en maturité. Jamais une telle jeune monnaie ne s'est développée dans le passé, et il est donc difficile (et excitant) d'imaginer comment les choses se passeront.
- **DÉVELOPPEMENT EN COURS -** Les logiciels Bitcoin sont encore en version bêta et plusieurs de leurs fonctions sont activement développées. De nouveaux outils, fonctions et services sont développés afin de rendre Bitcoin plus sécurisé et accessible. Certains ne sont toutefois pas prêts pour tous. La plupart des entreprises autour de Bitcoin sont nouvelles et n'offrent pas d'assurance. En général, Bitcoin est encore dans un processus de maturation.

Conclusion

Du point de vue technologique, le Bitcoin est sans conteste une véritable innovation. En effet, la création d'unités monétaires par un algorithme mathématique limitées à un nombre défini dès sa création est un concept inédit. La décentralisation de la gestion de cette monnaie virtuelle est innovante. A l'évidence, l'utilisation du bitcoin ou d'autres monnaies virtuelles comparables, apporte de nombreux avantages à ses utilisateurs, notamment en termes de simplicité et de coût de gestion.

Pour autant, le développement du Bitcoin n'est pas exempt de risques. Intrinsèquement, le bitcoin apparaît comme une "monnaie" spéculative et donc volatile. A l'évidence, beaucoup des utilisateurs du Bitcoin aujourd'hui le considèrent davantage comme un possible bon placement que comme un moyen de paiement, ce qui a généré une "bulle spéculative".

De même, du fait de son caractère décentralisé et dérégulé, le bitcoin est considéré par certains comme facilitant certaines pratiques illégales, telles la fraude fiscale, le blanchiment d'argent ou le commerce de biens et services illicites.

Enfin, l'actualité récente, avec la faillite annoncée de des plus importantes plateformes d'échange, laisse craindre des critiques encore plus virulentes à l'encontre du Bitcoin, notamment sur la sécurité des investisseurs.

Si le Bitcoin ne devait pas poursuivre son développement du fait de ces défauts intrinsèques, il demeurerait en tout état de cause le précurseur d'une véritable révolution monétaire basée sur les monnaies virtuelles.