



BANQUE DE LA RÉPUBLIQUE D'HAÏTI



BITCOIN, LES CRYPTO-MONNAIES ET LA TECHNOLOGIE DU BLOCKCHAIN

QUELQUES RISQUES LIÉS AU DÉVELOPPEMENT DES CRYPTO-MONNAIES

1) La possibilité d'une bulle financière : les valeurs des bitcoins et des autres crypto-monnaies pourraient subitement et durablement chuter, entraînant ainsi des pertes financières importantes pour les détenteurs de ces actifs. Ceci pourrait être dû à une baisse soudaine de la demande pour les crypto-monnaies en raison d'une perte de confiance dans la poursuite de leur adoption comme moyen de paiement ou comme réserve de valeur.

2) Le développement d'activités illicites utilisant les crypto-monnaies, fraudes, ... : vu le relatif anonymat que procure les transactions en crypto-monnaies, ces dernières sont devenues des moyens de choix pour des acteurs impliqués dans des activités illicites et des fraudes.

3) Les limites techniques et la dépendance à Internet : La taille future de la base de données et des blocs pourraient empêcher la propagation des informations à travers les nœuds du réseau. De plus, Bitcoin, étant dépendant du protocole Internet (IP), pourrait être ralenti ou bloqué par les fournisseurs de services Internet.

4) Les problèmes environnementaux : La consommation énergétique due au minage des bitcoins n'est pas négligeable. Les sources de production de cette énergie sont pour la plupart polluantes.



LA BRH FACE AUX CRYPTO-MONNAIES ET À LA TECHNOLOGIE DU BLOCKCHAIN

Les crypto-monnaies n'ont pas cours légal en Haïti. Toutefois, la BRH, tout en reconnaissant les vertus des innovations technologiques pour la croissance économique, invite les acteurs à la prudence en prenant en compte les risques y relatifs.



BANQUE DE LA RÉPUBLIQUE D'HAÏTI



Angle des Rues Pavée et du Quai, Port-au-Prince, Haïti



+509 22 99 12 00 / +509 22 99 12 02



www.brh.ht



@BRHHaiti

OÙ LES BITCOINS SONT-ILS STOCKÉS ?

Les bitcoins sont stockés sur tous les nœuds du réseau à la fois, dans le blockchain. Vous pouvez recevoir des bitcoins que vous ayez un portefeuille logiciel ou pas, que ce portefeuille soit éteint ou non, ou que vous ayez les clés cryptographiques notées sur du papier. Un logiciel est nécessaire seulement quand il faut dépenser ses bitcoins. Celui qui connaît la clé cryptographique privée possède les bitcoins qui lui sont associés.

QUELQUES AVANTAGES

1) Souplesse, versatilité, large diffusion : Il est possible d'envoyer ou de recevoir de l'argent partout dans le monde, à n'importe quel moment, sans limitation et indépendamment d'une autorité quelconque.

2) Sécurité, transparence, robustesse : La transaction, consultable par tous les utilisateurs, est irréversible et l'acheteur ne peut pas répudier. Bitcoin s'est montré résilient à plusieurs occasions.

3) Valeur refuge : Le bitcoin peut conserver au moins sa valeur face à d'autres monnaies subissant une forte inflation.



Bitcoin, les autres crypto-monnaies et la technologie du blockchain font beaucoup parler d'eux. De quoi s'agit-il ? À quoi peuvent-ils servir ? Comment se positionne la BRH face au développement de ces nouvelles technologies ?

CRYPTO-MONNAIES

Monnaies virtuelles utilisant la cryptographie et la technologie du blockchain. On peut citer en exemple : Bitcoin, Ethereum, Litecoin.

BITCOIN

De l'anglais « bit »: unité d'information en informatique et « coin » : pièce de monnaie, Bitcoin est à la fois une monnaie virtuelle et un système de paiement créés par un individu ou un groupe d'individus se présentant sous le nom de Satoshi Nakamoto en 2009. Les bitcoins, unités de compte, ne sont pas émis ou créés par une banque centrale ou une banque commerciale, comme c'est le cas pour la plupart des autres monnaies (gourde, dollar, euro, ...). Ils n'existent que sous forme numérique. À ce titre, il n'y a donc pas de pièces ou de billets de bitcoins.

COMMENT LES BITCOINS SONT-ILS CRÉÉS ?

Les bitcoins sont créés et gérés à partir d'un logiciel partagé entre des ordinateurs en réseau (réseau utilisateur à utilisateur ou peer to peer). Dans ce logiciel, les bitcoins sont créés conformément à un protocole, Bitcoin, qui rétribue les Agents ayant traité des transactions. Ces Agents peuvent par la suite échanger leurs bitcoins contre d'autres monnaies, commodités, biens ou services suivant un taux de change déterminé par l'offre et la demande. Un individu choisissant de participer à ce réseau met à contribution la puissance de calcul de son ordinateur afin de vérifier, sécuriser et inscrire les

transactions dans un registre électronique appelé « blockchain ». Cet immense registre est accessible et partagé à toutes les personnes connectées au réseau Bitcoin. Les transactions en bitcoins se basent principalement sur deux technologies :

• LA CRYPTOGRAPHIE ASYMÉTRIQUE

Technologie selon laquelle les participants à un réseau informatique sont authentifiés par des codes secrets pour assurer leur signature en vue d'interdire, entre autres, la falsification des identifiants des parties prenantes. Grâce à cette technique, toute tentative de falsification sur le réseau Bitcoin est détectée et automatiquement diffusée sur l'ensemble du réseau. Les transactions de bitcoins sont traçables. Cependant, la cryptographie ne garantit pas la confidentialité ou le chiffrement des données transmises sur le réseau.

• LA TECHNOLOGIE DU BLOCKCHAIN

C'est une technologie de stockage et de transmission d'informations, transparente, sécurisée, sans organe central de contrôle, sans tiers de confiance et sans hiérarchie qui veut « démocratiser » la transaction comme Internet l'a réalisé avec l'information. Il s'agit, techniquement, d'une base de données distribuée et sécurisée de toutes les transactions effectuées depuis le démarrage du système, groupées à intervalles réguliers en blocs formant ainsi une chaîne.

Cette base est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. Chaque bloc contient des données, une empreinte (hash) du bloc et une empreinte (hash) du bloc précédent. Une fois ajouté à la chaîne, un bloc ne peut être ni modifié ni supprimé, ce qui garantit l'authenticité et la sécurité du réseau. Soulignons que Bitcoin est la première application de la technologie blockchain.

AUTRES APPLICATIONS DE LA TECHNOLOGIE BLOCKCHAIN

La technologie « blockchain » offre, toutefois, de nombreuses possibilités d'application en dehors des crypto-monnaies. Vu qu'elle permet d'authentifier et de retracer des transactions et de contrecarrer des tentatives de falsification, sans tiers de confiance, plusieurs expériences sont menées actuellement où elle est utilisée pour le transfert des actifs (monétaires, titres, votes, actions, obligations, ...), les applications en tant que registre (cadastres, ...), les « smart contract » et pour certifier la provenance de produits agricoles. Il ne s'agit là que de quelques utilisations potentielles, la recherche sur les applications du blockchain est en plein développement et de nouvelles applications sont envisagées continuellement.

D'OÙ PROVIENT LA VALEUR DU BITCOIN ET DES CRYPTO-MONNAIES ?

Comme toute monnaie, la valeur du bitcoin et celle des crypto-monnaies est fortement liée à leur rareté. C'est ainsi que leurs concepteurs ont mis sur pied des mécanismes pour éviter toute création monétaire excessive qui entraînerait une baisse de leur valeur par rapport aux autres monnaies. Par exemple, le logiciel à la base du réseau Bitcoin est calibré pour que le nombre de bitcoins ne dépasse jamais 21 millions . De même, obtenir un nouveau bitcoin à partir du réseau n'est pas de tout repos. Actuellement, ceci nécessite des ordinateurs puissants et une consommation d'électricité très élevée.