



Le Bitcoin et la Blockchain.

Posted on 14 novembre 2024 by Patrick Rouillier

Une blockchain est un outil informatique permettant de stocker des données de façon décentralisée. Elle constitue le support d'une application Bitcoin (avec B majuscule) dont l'unité de valeur monétaire est le bitcoin (avec b minuscule)

La Blockchain

Contrairement à une base de données classique, hébergée sur un seul serveur et dépendant d'un administrateur la blockchain stocke les données sur un ensemble d'ordinateurs et ne nécessite aucun administrateur.

Elle est constituée d'un certain nombre de blocs, liés entre eux par des liens (chain). Chaque bloc de données fournit un « Hash » : image calculée des données contenues dans le bloc. Le « Hash » est crypté de façon à ce qu'il ne puisse être décrypté. La conversion « Données - Hash » ne fonctionne que dans le sens du cryptage.

Chaque bloc de données fournit au bloc qui le suit dans la chaîne le « Hash » de ses données. De sorte que si, par malveillance, un bloc est modifié, son nouveau « Hash » ne correspond plus au « Hash » qu'il avait fourni au bloc suivant et la chaîne se met en erreur en attendant correction. C'est une sécurité contre le piratage.

Le Bitcoin

C'est un système d'échange de valeurs ou de documents entre particuliers dont la trace est conservée dans le système sur la base de la Blockchain.

Étudions un échange entre Jean et Camille.

1. Pour participer au système Bitcoin il leur faut d'abord chacun créer un portefeuille. Pour cela ils s'identifient avec un pseudo, sans jamais révéler leur véritable identité. Ils reçoivent alors chacun une adresse publique Bitcoin, une clé privée qui leur permet de recevoir des fonds ou des documents et une clé privée qui leur permet d'envoyer des fonds ou des documents.
2. Camille crée une transaction dans laquelle elle indique l'adresse publique de Jean et le montant en bitcoins qu'elle souhaite lui envoyer. Elle ajoute le montant de frais impliqué par la transaction (c'est l'acheteur qui paye les frais de transaction)

3. Camille signe sa transaction avec sa clé privée (pour identifier l'origine des fonds)
4. La transaction est alors envoyée sur le réseau Bitcoin. Elle est dirigée vers des nœuds, qui sont des ordinateurs chargés de valider les transactions.
5. Ces nœuds sont gérés par des « mineurs » (rien à voir avec les contraintes d'âge, les mineurs sont des simples vérificateurs rétribués sur les frais de transaction)
6. Les « mineurs » vérifient la validité de la transaction et la signature de Camille. Ils créent un nouveau bloc dans la Blockchain
7. Après plusieurs validations (2 à 6) la transaction est confirmée et Jean, dans son portefeuille, reçoit les bitcoins que Camille lui a envoyés.
8. Chaque vérification dure environ 10 minutes et la confirmation revient au bout d'environ une heure.

Avantages du Bitcoin

1. Anonymat. A aucun moment l'utilisateur ne dévoile sa véritable identité. Seul son pseudo l'identifie dans le réseau.
2. Alors que les transactions bancaires utilisent comme intermédiaires des banques, dans Bitcoin la transaction se passe directement entre des utilisateurs anonymes. La transaction ne laisse aucune trace dans le système bancaire. La trace n'existe que dans Bitcoin. Elle est disponible, en public, pour tous les inscrits ... sous réserve d'avoir la capacité de télécharger toute la Blockchain, ce qui suppose une puissance de calcul énorme.
3. Dans le système monétaire les banques centrales des pays peuvent émettre de la monnaie. Elle le font souvent en cas de crise ce qui génère de l'inflation et une perte de valeur de la monnaie. Dans Bitcoin le montant en bitcoin disponible est fixé une fois pour toute (21 millions de bitcoins). Une nouvelle émission supposerait l'accord de 95% des inscrits ce qui est peu probable.
4. Cette garantie de stabilité peut faire du bitcoin une valeur refuge, au même titre que l'or. Il est souvent utilisé comme tel plus que comme moyen de paiement. Il sert aussi à la spéculation.
5. Actuellement le bitcoin est convertible, c'est à dire que l'on peut l'échanger contre des dollars, des euros Le taux de change dépend de l'offre et de la demande dans Bitcoin, donc des achats et ventes de bitcoins. Il n'est pas directement soumis, comme le sont les monnaies classiques, au contexte socio-économique ou politique.
6. Pour un investisseur le rendement du bitcoin a été fantastique. De presque rien, le bitcoin vaut aujourd'hui environ 80.000 dollars
7. Des contrats intelligents peuvent être signés entre deux parties, sans intermédiaires (avocat, notaire), donc à moindre coût et dans l'anonymat . Ils sont directement gérés, mis en œuvre et exécutés par le système Bitcoin. Ils

ne peuvent être annulés.

Inconvénients du Bitcoin

1. La faible disponibilité en bitcoin en fait une valeur très volatile, sensible au moindre mouvement spéculatif. Il peut varier de 10 à 15 % en moins de 24 heures. Les pertes et les gains y sont très rapides.
2. Le bitcoin peut s'écrouler si les investisseurs s'en détournent et vendent leurs actifs. Un crash peut très vite arriver.
3. Aujourd'hui le bitcoin est convertible. Cependant il évolue en dehors de toute régulation bancaire et hors du contrôle des états. Nul ne connaît son avenir à moyen ou long terme.
4. Les contrats intelligents passés sur Bitcoin ont une reconnaissance juridique des plus floue. En cas de dysfonctionnement la responsabilité (machine, programmeur, signataires) est des plus difficile à apprécier. La validité peut être contestée si des clauses s'éloignent trop de celles des contrats standards.

Conclusion

Bitcoin est un système qui détourne le système bancaire et le contrôle des états. Il s'autogère et s'auto contrôle sans l'intervention d'une autorité. Hautement spéculatif il fonctionne sur l'engouement des investisseurs sur des gains faciles hors du contrôle des états.

Si pour une raison ou une autre les investisseurs sans détournent il est susceptible de crash violent. Son avenir peut être tout rose ou tout noir.