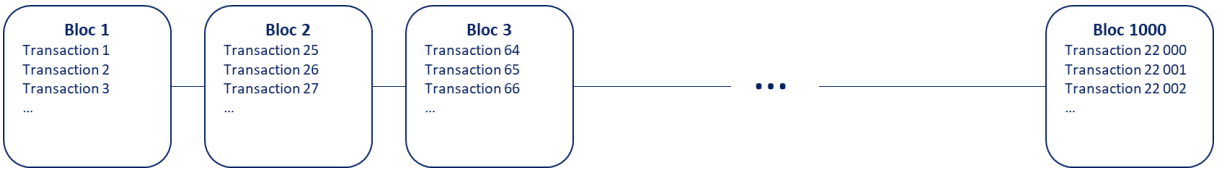
LES 10 COMMANDEMENTS DE LA BLOCKCHAIN

Lundi 15 janvier 2018 – par Guillaume GUERDOUX

Tu ne confondras plus Blockchain et Bitcoin

La Blockchain est une technologie permettant de stocker des données de manière décentralisée (« tout le monde possède les données »), transparente (« tout le monde peut voir les données »), sécurisée (« personne ne peut altérer les données ») et autonome (« personne ne contrôle les données »).

Le Bitcoin est une application particulière de la technologie Blockchain dans le domaine de la crypto-monnaie. La Blockchain s'utilise comme un livre de compte répertoriant toutes les transactions réalisées avec la crypto-monnaie Bitcoin.



Miner préservera l'intégrité de la Blockchain

Le minage consiste à faire valider un bloc par un membre du réseau au moment de sa création.

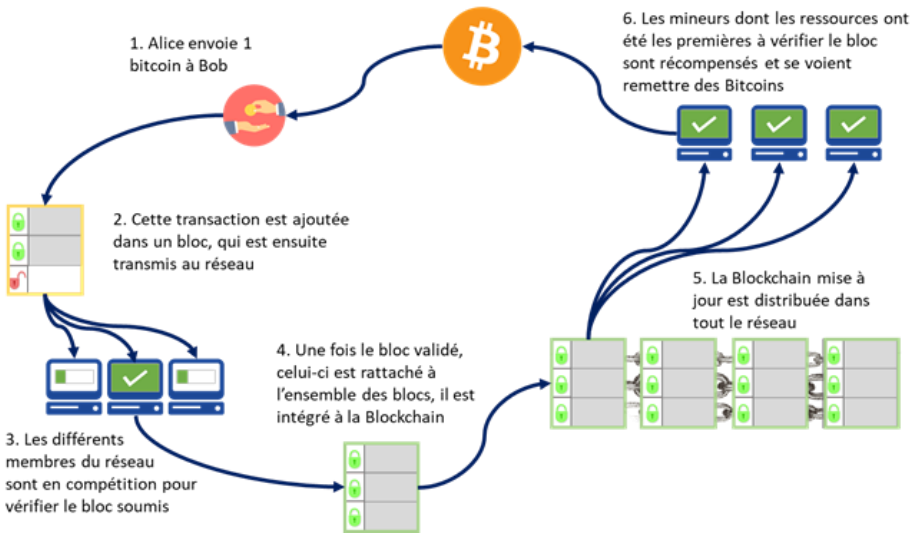


Illustration : Processus d'ajout de transaction à la Blockchain Bitcoin

Celui-ci met à disposition sa puissance de calcul et décrète que le bloc est valide, ou invalide. Comme tout travail mérite salaire, ce membre reçoit des Bitcoins en échange de sa contribution.

Tous les membres du réseau sont ainsi en compétition pour valider ce bloc et récupérer les précieux Bitcoins.

Le minage rapportera, mais sera long et coûteux

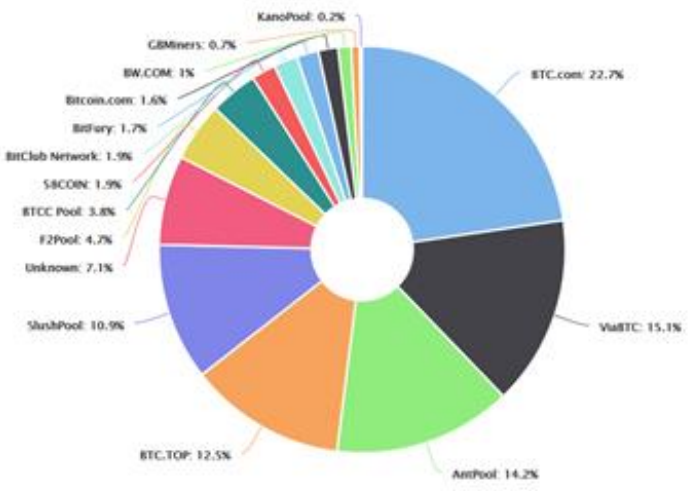
En moyenne, créer un bloc valide dans une blockchain de type Bitcoin nécessite 10 minutes. Ce temps provient du fait qu'il faut résoudre un problème mathématique très complexe pour valider un bloc, appelé « preuve par le travail ».

Le minage d'un nouveau bloc dépend donc de deux principes :

- La chance : le mineur peut trouver la solution du problème imposé en quelques secondes, comme il peut la trouver en plusieurs heures.
- La puissance de calcul : plus le mineur dispose de ressources, plus il peut paralléliser ses recherches et trouver la solution rapidement.

En pratique, les mineurs se regroupent dans des pools et mettent en commun leur puissance de calcul pour résoudre le plus de problèmes mathématiques possibles.

Le regroupement des mineurs menacera l'intégrité de la Blockchain



Aujourd'hui, seulement 4 pools contrôlent plus de 50% de la puissance informatique minière du Bitcoin !

Ces acteurs, s'imposant comme majeurs dans l'économie, suscitent des craintes et créent des risques politiques sur certaines crypto-devises.

En effet, une prise de contrôle de plus de 51% des ressources informatiques minières pourrait remettre en cause l'intégrité de toutes les transactions et permettre d'écrire une nouvelle réalité de la Blockchain.

Tu ne penseras plus que la Blockchain est énergivore

La technologie Blockchain en elle-même n'est pas énergivore. La consommation d'énergie dépend du type de Blockchain utilisée et du type d'algorithmes utilisés (preuve par le travail, preuve d'enjeu, etc.)

Le Bitcoin utilise une preuve par le travail dont la résolution est très compliquée, nécessitant une puissance de calcul et un temps de calcul importants et donc une grande quantité d'énergie.

D'autres cryptomonnaies comme le Groestlcoin (GRS) se basent sur une minimisation des ressources de calcul nécessaires pour valider les différents blocs.

Les cryptomonnaies n'utiliseront pas toutes la même technologie Blockchain

La Blockchain est un concept mis en application de multiples façons. Ainsi, les cryptomonnaies majeures utilisent pratiquement toutes une technologie Blockchain différente.

Le Bitcoin utilise un système de preuve par le travail quand l'Ethereum utilise maintenant un système de preuve de participation. Le Bitcoin dévoile l'identité des auteurs de chaque transaction quand le Z-cash préserve l'anonymat de tous ses utilisateurs.

Finalement, de nouvelles cryptomonnaies n'utilisent plus la technologie Blockchain mais de nouvelles technologies, comme le Iota basé sur le Tangle

La Blockchain posera la question de la responsabilité

Le principe de la Blockchain suppose son inaltérabilité, ne définit ainsi pas de gouvernance et adopte la devise : « Code is Law ». Or, le code informatique, rédigé par un être humain, peut, lui, contenir des failles.

Le scandale de la plate-forme d'échange DAO (Decentralized Autonomous Organisation) fournit un exemple concret de faille de sécurisation. Un pirate informatique a exploité une faille informatique de cette plateforme pour récupérer une somme d'Ethereum correspondant à 50 millions de dollars.

Aucune gouvernance ni organe de contrôle n'étant défini, les actions à mettre en œuvre furent difficiles à identifier et la décision fut soumise au vote de la communauté. Ce vote résulta en une scission de la Blockchain : une partie de la communauté décida de ne pas modifier la Blockchain Ethereum, donnant naissance à l'Ethereum Classic tandis que l'autre partie de la communauté décida de modifier la Blockchain Ethereum passée en annulant cette transaction (hard fork).

Le principe « Code is law » de la Blockchain pose donc question vis-à-vis des actions à mener lors d'une fraude et plus globalement vis-à-vis de la responsabilité : comment définir une justice de la Blockchain ?

Les smart contracts ne représenteront pas la solution miracle au système contractuel

Les smart contracts sont des programmes autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable et inscrites dans la blockchain.

Un exemple illustratif consiste à étudier le fonctionnement d'une assurance annulation pour un vol sous la forme de smart contracts.

Avec leur utilisation, les passagers sont automatiquement indemnisés en cas de retard du vol, sans avoir besoin d'effectuer une quelconque demande. Les smart contracts sont reliés à une base de données et se déclenchent automatiquement, réalisant le processus de remboursement de bout en bout sans intervention humaine.

Toutefois, ce processus suppose une entière confiance en la base de données source. Il pourrait s'agir d'une simple déclaration sur l'honneur (accident automobile, dégâts des eaux, etc.) nécessitant la mise en place d'un organe de contrôle, annulant toute autonomie de la Blockchain.

Les smart contracts prouvent ainsi leur efficacité dans un processus de gestion au même titre que l'automatisation, assurant une transparence et une inaltérabilité des termes du contrat entre deux parties mais ne permettant pas de sécuriser entièrement sa réalisation, notamment du fait d'une potentielle malveillance de la part de la source d'informations.

La Blockchain ressuscitera le mythe du Peer 2 peer

Les citoyens ont perdu confiance dans les institutions, ils se méfient des grandes entreprises, des banques, des assurances et des gouvernements. La Blockchain fait revivre l'espoir de partage, de transparence et de confiance entre utilisateurs. Ceux-ci ne seraient plus assujettis ni à des frais bancaires ni à des frais assurantiels.

La Blockchain attise aujourd'hui les passions, comme le peer 2 peer, un des anciens mythes fondateurs du Web, a pu le faire il y a 15 ans : saura-t-elle transformer l'essai ?

La finalité de la Blockchain tu questionneras

La Blockchain se pose comme une technologie très prometteuse et disruptive. Couplée aux applications de l'intelligence artificielle, de nombreux produits et services seront dès lors inutiles : les transactions bancaires se feront en Bitcoin, les contrats assurantiels seront conclus sous la forme de smart-contracts, les transactions entre objets connectés se feront en Iota, etc.

La Blockchain s'est construite par essence contre toute contrainte de régulation. Ainsi, comment protéger les utilisateurs face à un risque qu'ils ne peuvent maîtriser ?