



QU'EST CE QUE LA BLOCKCHAIN ?

Sommaire

La blockchain

- Historique
- Fonctionnement
- Caractéristiques de la blockchain

Que contiennent les blocs ?

- De nombreux usages
- Les « smart contracts »

Avantages et inconvénients

- Avantages
- Inconvénients

Pour comprendre la blockchain, il faut remonter à un besoin fondamental : la confiance. Celle-ci repose le plus souvent sur un intermédiaire appelé « tiers de confiance ». Il peut s'agir d'une marque, d'un notaire, d'une banque...

La question de la confiance est sensible sur les réseaux et en particulier sur Internet, en raison du piratage, des spams, du rançonnage et de toute autre forme de menace.

La blockchain est l'innovation dont tout le monde parle, et pour cause : elle propose de révolutionner la gestion de la confiance en remplaçant les tiers de confiance traditionnels.

Son développement intéresse les géants d'Internet, mais aussi les banques, les assurances et les industries.

En 2015, plus de 480 millions de dollars ont été investis pour développer ses applications, dans des secteurs aussi variés que la logistique, le divertissement, la finance ou le tourisme.

Cette « chaîne de blocs » est une technologie de stockage ou de transmission d'informations transparente, sécurisée, et fonctionnant sans organe central de contrôle¹.

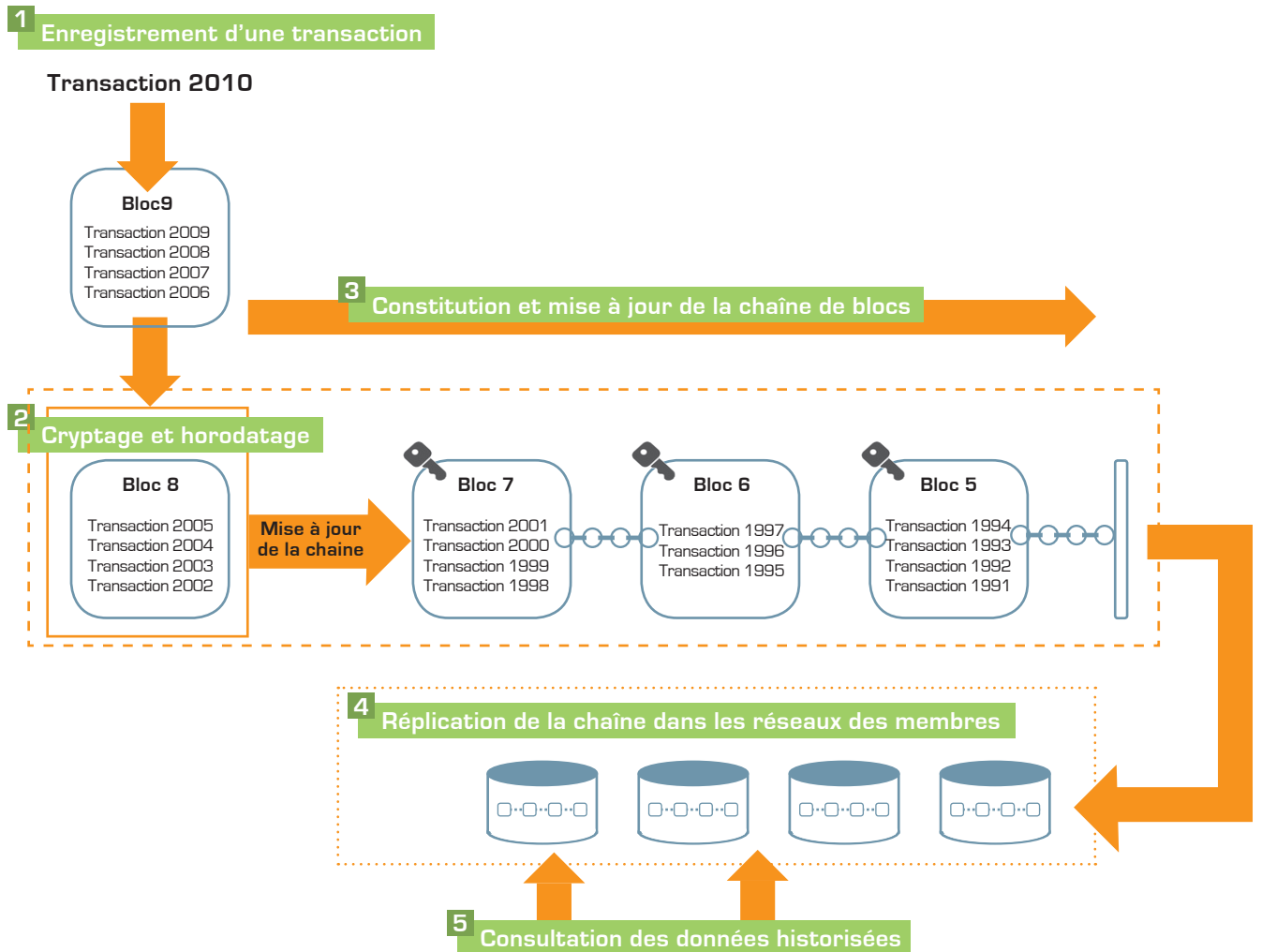
Elle peut trouver des applications dans la traçabilité de la viande, la certification de diplôme ou encore la sécurisation des échanges entre les machines d'un atelier de production.

Le terme Blockchain, est utilisé pour désigner tant la technologie au sens large (« la blockchain ») que les bases de données reposant sur son utilisation (« une blockchain »).

Cette notice s'intéresse au fonctionnement de la blockchain, à ses atouts, et aux applications qui peuvent en découler.

¹ Définition par Blockchain France <http://bit.ly/1Tapshu>

Processus d'enregistrement de données sécurisées dans la blockchain



LA BLOCKCHAIN

HISTORIQUE

À l'origine, la technologie blockchain a été développée pour assurer la confiance nécessaire au développement de la première monnaie numérique pérenne apparue en 2009, le Bitcoin.

Il était alors impératif de créer un système sécurisé capable de conserver l'historique des transactions.

Cette traçabilité permet de vérifier qu'une personne qui vend un bien en est le propriétaire, et que la personne qui l'achète possède les fonds nécessaires, le tout, sans vérification par une autorité centrale (une banque, dans un modèle traditionnel).

En 2016, le réseau Bitcoin constitue la blockchain la plus étendue avec une capitalisation monétaire à plus de 10 milliards d'euros.

FONCTIONNEMENT

La blockchain est une technologie qui rassemble des blocs composés d'informations numériques qui sont réunis pour former une chaîne d'enregistrements. Il s'agit, en quelque sorte, d'un « registre » qui mémorise au fil du temps des informations de référence.

Chaque bloc contient des informations qui proviennent d'utilisateurs membres de ce système de blockchain. Ces informations peuvent être, par exemple, des éléments d'une transaction financière entre deux personnes.

La blockchain est une technologie de base de données distribuée qui utilise des ressources de calcul disponibles via les machines (ordinateurs) des utilisateurs. Ces ressources ont pour fonctions de crypter et d'horodater les blocs et de les mettre à disposition en ligne. Dans le jargon du blockchain, ces ressources informatiques sont appelées des « mineurs ».

Il est impossible de modifier ou de supprimer les traces des transactions, les données historiques peuvent seulement être consultées.

REMARQUE

Le mathématicien Jean-Paul Delahaye décrit la blockchain comme un « très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible ».

LES CARACTÉRISTIQUES DE LA BLOCKCHAIN

■ Un réseau décentralisé ou « distribué »

Contrairement à une base de données traditionnelle, la blockchain n'est pas stockée sur un serveur central, les utilisateurs détiennent tous une partie de cette base de données sur leur propre machine (serveur, ordinateur). Concrètement, chaque bloc est répliqué chez un grand nombre d'utilisateurs.



■ Un réseau autonome

Il n'y a pas d'autorité centrale de validation, la blockchain s'autorégule. Lorsque s'effectue un échange entre des utilisateurs d'une blockchain, un processus de validation par consensus garantit l'authenticité et l'intégrité des données échangées qui seront inscrites dans un bloc.

Tout le monde peut « écrire » du moment que la majorité des autres membres du réseau valident l'écriture. En d'autres termes, pour parvenir à corrompre le système il faudrait mobiliser 51% de la puissance informatique du réseau, ce qui s'avère compliqué compte tenu du nombre d'utilisateurs.

■ Un réseau sécurisé

Les informations que contiennent les blocs sont protégées par des procédés cryptographiques, si bien qu'elles deviennent impossibles à modifier une fois que le bloc a intégré la chaîne.

Par ailleurs, la réplication des blocs en temps réel chez un grand nombre d'utilisateurs rend très difficile, voire impossible, la manipulation frauduleuse car une modification d'une chaîne de blocs dans le système est automatiquement repérée par les autres ressources qui invalident toute différence.

■ Un réseau transparent

La transparence d'un réseau blockchain ne signifie pas que tout transfert d'information est public, mais seulement qu'il est possible d'accéder à l'historique des échanges.

Pour chaque échange, l'identifiant des utilisateurs n'est pas nécessairement leur nom réel ; c'est pour cette raison que la blockchain n'est pas anonyme mais « pseudonyme ».



QUE PEUVENT CONTENIR LES BLOCS ?

■ DE NOMBREUX USAGES

Toute forme d'information peut être inscrite au sein des blocs, le réseau blockchain n'est pas uniquement un support d'informations transactionnelles et peut s'ouvrir à de nombreux usages :

- La certification et l'authentification de documents ou de biens (titres de propriété, normes...)
- La traçabilité de produits dans des secteurs sensibles (pharmaceutique, luxe, agro-alimentaire...)
- L'automatisation d'échange de données ou de transactions « machine-to-machine », dans le secteur de l'internet des objets et de manière plus globale pour les équipements connectés (supply chain, production...)
- L'exploitation de données personnelles en assurant sécurité et anonymisation (recherche dans la santé, big data...)

■ LES « SMART CONTRACTS »



Étendre les usages de la blockchain, c'est ce qu'ambitionnent les « smart contracts ». Ces petits scripts (programmes) informatiques exécutent automatiquement les termes d'un accord si les conditions sont remplies.

Leur intégration dans une blockchain permet de les rendre infalsifiables.

Nick Szabo² donnait l'exemple d'un contrat de leasing pour un véhicule dans un article datant de 1997³ : « Si le propriétaire cesse d'effectuer les versements, le smart contract peut invoquer un protocole qui rend automatiquement le contrôle de la clé du véhicule au vendeur ».

De la logistique au tourisme en passant par l'internet des objets, des sociétés développent déjà des cas d'usages :

- ChainOrchestra développe des blockchains privées pour faire communiquer les objets connectés de l'industrie
- TransActive Grid crée des réseaux locaux de revente d'énergie solaire entre particuliers. Grâce aux smart contracts, l'énergie peut être provisionnée sur le réseau, achetée et vendue en temps réel en toute sécurité

- Everledger propose d'utiliser la blockchain pour la certification et le suivi d'objets de valeur, permettant ainsi de lutter contre la fraude



AVANTAGES ET INCONVÉNIENTS

AVANTAGES

- Sécurité et inviolabilité des données
- Réduction des coûts d'infrastructure informatique
- Optimisation des processus grâce à l'automatisation des transactions

INCONVÉNIENTS

- Encadrement juridique encore flou
- Coût d'implémentation actuel
- Usages toujours au stade d'expérimentations

² Nick Szabo est un informaticien, juriste et cryptographe connu pour ses travaux de recherche dans les contrats numériques et la monnaie numérique.

³ <http://ojphi.org/ojs/index.php/fm/article/view/548/469>