La blockchain, une technologie de registre distribué

Cet article est complémentaire à la recherche « **La chaîne de blocs et l'industrie canadienne des médias** », un projet mis en œuvre par Téléfilm Canada, le Fonds des médias du Canada et Badel Media, avec la collaboration du Pôle Médias HEC Montréal.

Parution le 2 mai 2019
10 minutes de lecture

Définir la blockchain

Définir de façon simple la blockchain n'est jamais chose facile et chaque spécialiste du sujet l'abordera d'une façon et dans un contexte différents. Mais pour la résumer, certains fondamentaux doivent être présentés. Ce sont souvent eux qui permettent au lecteur de visualiser les applications et la portée de cette technologie.

Disons tout de suite que la blockchain consiste en des protocoles informatiques, essentiellement en code source ouvert, et fait partie de la famille des technologies de registre distribué (TRD). Les registres sont depuis toujours des enregistrements chronologiques d'information sur des transactions, généralement le transfert d'un bien, de son usage ou de sa propriété notamment, d'une personne ou organisation à une autre. Leur version informatique, une TRD, n'est pas un concept nouveau et plusieurs approches et technologies en émergent, complémentaires ou concurrentes les unes envers les autres.

Ce qui distingue particulièrement la blockchain des autres TRD, c'est la notion de **consensus**. Autrement dit, la mise en place d'un mécanisme issu d'un ensemble de règles acceptées par les participants au réseau, et nécessaire pour son bon fonctionnement. **Car soulignons de nouveau que la distribution est au cœur de la blockchain** : distribution de l'information, des processus, des rôles et des responsabilités, dans une vision commune, un but commun. Le consensus est l'élément essentiel à la base de la gouvernance d'un système décentralisé se voulant ne plus reposer sur une autorité centrale de contrôle.

Caractéristiques clés

Si nous décidons de limiter la description à son plus simple, nous pouvons définir la blockchain comme étant une base de données. Une base de données qui a donc la particularité d'être distribuée, c'est à dire, en quelque sorte, répliquée et synchronisée sur les différents nœuds informatiques d'un réseau.

Cette distribution a pour bénéfices :

- Une plus grande **transparence** des données, par la multiplication des points d'accès ; ce qui facilite leur authentification mais surtout leur suivi, c'est à dire leur **traçabilité** ;
- **L'immutabilité** de ces données : déjà sécurisées par les techniques de cryptographie en usage sur une blockchain, les données entrées dans un registre distribué seront d'autant plus immuables que chaque « copie » de ce registre devra être cohérente avec les autres.

Usages fondamentaux de la blockchain

Toutes les applications de la blockchain sont liées à au moins un de ces quatre usages :

- **Le cadastre**, ou le registre chronologique de transactions entre entités authentifiées ;
- **Le transfert de valeur** qui induit la désintermédiation comme impact potentiel ;
- **L'automatisation**, via des contrats intelligents, ou contrats codés, qui ont pour bénéfice une plus grande efficience de processus administratifs et d'affaires ;
- **La numérisation d'actifs** avec pour promesse la création de nouvelles formes de valeurs et de modèles d'affaires.

Dans le cadre de cette introduction au fonctionnement de base de la technologie, nous nous concentrons sur les deux premiers points : **cadastre** et **transfert de valeur**.

Éléments de base du fonctionnement

Notons aussi que le fonctionnement décrit concerne avant tout les blockchains publiques du type de la blockchain bitcoin. Les blockchains privées et hybrides ou de consortium (par exemple liées à une organisation ou à un secteur d'activités) auront des types de consensus qui ne reposent généralement pas sur les mêmes principes. Elles seront par conséquent beaucoup moins « décentralisées » au sens propre du terme car ces blockchains visent plus à distribuer des rôles et processus, accroître la traçabilité et l'efficacité, instaurer de nouveaux types de relations entre parties prenantes, dans un but commun de répondre à un enjeu sectoriel.

Résumons ici en premier lieu les éléments à la base des blockchains publiques :

- Les données sont encryptées et « scellées » dans des blocs, une fois un processus de validation et d'authentification complété via le mécanisme de consensus accepté par les membres du réseau. Ce mécanisme repose aussi sur des principes de cryptographie. Pour la blockchain bitcoin (débutée en janvier 2009 et première application d'affaires de la technologie blockchain), ce consensus se nomme la Preuve de travail (*Proof-of-Work*).

- Les blocs sont reliés les uns aux autres par un identifiant unique. Au final, ces blocs interconnectés constituent une chaîne . Et plus cette chaîne sera longue, plus elle deviendra immuable et donc sécuritaire. Car tenter de modifier une donnée dans un bloc, équivaut à toucher à l'intégrité de la chaîne. L'éventuelle modification sera en effet traçable, et contestable, en raison de la non correspondance des données du bloc affecté avec celles des autres blocs.

- La blockchain est aussi théoriquement inaltérable puisque sa prise de contrôle nécessite celle d'au moins 51% des nœuds du réseau. Avec l'exemple du bitcoin, une telle éventualité peut représenter une quantité de ressources informatiques extrêmement grande, laissant ainsi peu de place à des comportements malveillants. Malgré les impacts environnementaux (consommation électrique, etc.), c'est aussi cette exigence en ressources informatiques qui garantit la fiabilité du système.

Consensus, gouvernance et confiance

La technologie des registres distribués introduit une forme de comptabilité collective, donc théoriquement de vérification par quiconque et en presque temps réel. En l'absence d'autorité centrale de contrôle, le système en lui-même, décentralisé et avec son mécanisme de consensus, est l'instrument de **confiance** entre les parties prenantes. Ce qui en fait certainement sa plus grande innovation, que ce soit au niveau technologique comme de la **gouvernance**.

Le **minage** est une pièce maîtresse de la confiance dans le système. Cette activité de minage, caractérisée par des ressources informatiques mises à disposition du réseau moyennant incitatifs et compensations, permet de valider les nouvelles transactions et de les ajouter au registre, après approbation par consensus. Dans une blockchain comme la blockchain bitcoin notamment, ce consensus est un mécanisme compétitif de résolution de calculs mathématiques qui est donc la preuve de travail.

Le minage basé sur la preuve de travail

Chaque ordinateur connecté à la blockchain peut en principe devenir un "mineur". En principe, car le minage (dans sa forme actuelle de preuve de travail) nécessite de plus en plus grandes ressources informatiques. Généralement, ces ressources sont de type ASIC (*Application-Specific Integrated Circuit*). Donc des systèmes conçus pour une application particulière.

Dans cette fonction, les mineurs choisissent un ensemble de transactions à partir d'un "*pool*" de toutes les transactions en attente de validation sur le réseau. Pour cela les bénéfices espérés des mineurs pour le traitement jouent énormément sur le choix et donc sur l'ordre de priorité des transactions à traiter. Car l'économie du minage repose logiquement sur la recherche d'un profit (rétribution pour le traitement de la transaction versus coût de la ressource informatique).

Pour le Bitcoin, les mineurs du système sont rémunérés via une combinaison de devises virtuelles nouvellement émises et de frais de transaction ou commissions. Comme ordre d'idée, à l'heure actuelle, le premier qui résout le défi mathématique lié à la validation d'un bloc de transactions prêt à être approuvé se voit octroyé 12,5 nouveaux bitcoins.

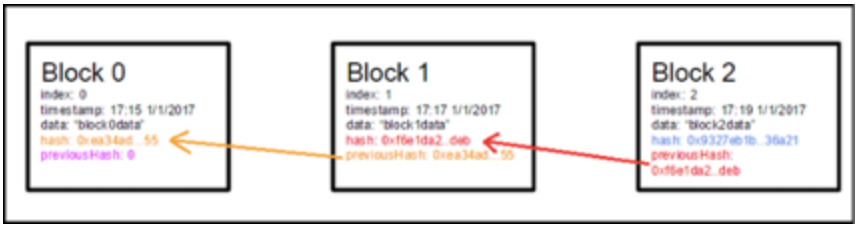
Autant de bitcoins qui sont et seront injectés dans le réseau jusqu'à un maximum de 21 millions (fin août 2018 un peu plus de 17 millions étaient en circulation, le dernier bitcoin devant être émis autour de 2141, soit 132 ans après sa création). En d'autre termes, et à un rythme décroissant pour atteindre ces 21 millions dans un horizon de temps suffisamment long, le minage, ou "processus d'extraction", est aussi l'activité essentielle d'émission de nouveaux bitcoins.

À l'intérieur du bloc...

Le processus compétitif de la blockchain Bitcoin est configuré de manière à ce que toutes les 10 minutes un nouveau bloc soit ajouté. Afin de respecter ce rythme, le défi à solutionner est sujet à une difficulté adaptable en fonction de la puissance de calcul totale du réseau. Aussi, ce rythme sera donc complètement variable selon le protocole utilisé pour une blockchain autre que Bitcoin.

Mais avant que cet ajout d'un nouveau bloc ne soit possible, il y a deux étapes :

1/ Les mineurs doivent donc d'abord **résoudre un calcul mathématique** spécifique : il s'agit de la fonction cryptographique de hachage qui vise à identifier, de façon aléatoire, une valeur (nonce) dont la juxtaposition aux données du bloc précédent produira un hache (*Hash*) qui devra être inférieur à un certain seuil (le défi mathématique à résoudre). Pour simplifier, ce hache est également l'empreinte unique du bloc et est une suite unique de caractères (256 sur la blockchain Bitcoin). Avec le changement d'une donnée d'un bloc, un nouveau hache sera généré. D'où un problème de correspondance qui pourra facilement être repéré sur un réseau décentralisé dont les noeuds détiennent autant de copies du registre. Le hache est une sorte d'image standardisée de taille fixe rendant quasi impossible de trouver la valeur de sortie à partir de la valeur d'entrée. Le bloc original d'une chaîne ne peut donc être modifier. Immuable, ce premier bloc est le bloc "genèse" (*Genesis*).



2/ Une fois le problème résolu par un mineur, celui-ci doit **publier le bloc auprès de tous les autres ordinateurs du réseau qui ensuite le valident**. Seuls les blocs contenant des transactions approuvées à l'unanimité sont ajoutés à la chaîne. Les blocs (d'une taille maximale variable, mais par exemple limitée à 1 Mo pour la blockchain bitcoin) sont intégrés à une chaîne dans une séquence chronologique. Chaque bloc approuvé et publié se caractérise essentiellement par son empreinte (*Hash*), son horodatage (*Timestamp*), ainsi qu'un champs de données caractérisant les transactions. L'immuabilité d'une blockchain est appuyée par le fait qu'elle est entièrement copiée sur les noeuds du réseau (poids total de la blockchain Bitcoin fin août 2018 : environ 180 Go).