# CE QUE FAIT ET CE QUE NE FAIT PAS LA BLOCKCHAIN

Ce qu'autorise et interdit la mécanique de la blockchain

Jacques BAUDRON - jacques.baudron@ixtel.fr

Mai 2021

*Tentative de démystification de la blockchain*

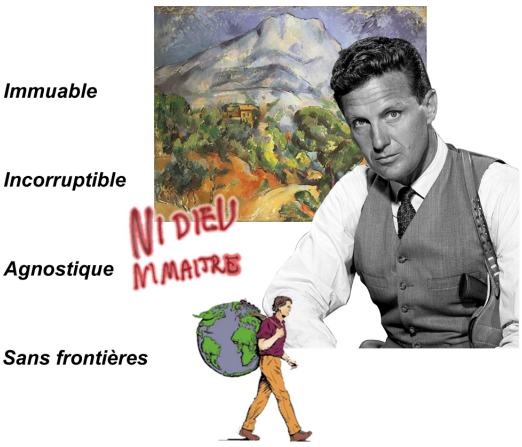
## QUATRE PIEDS POUR LA BLOCKCHAIN

La blockchain est une chambre d'enregistrement électronique qui certifie date, auteur et intégrité de chaque écriture. Le fonctionnement est à rapprocher de celui des actes notariés ou des enveloppes Soleau. Son architecture informatique la dote de quatre propriétés :

Propriété 1 : la blockchain est **immuable**.
Cette propriété est obtenue en multipliant les copies. Elle est (quasi) indestructible.

Propriété 2 : la blockchain est **incorruptible**.
En chaînant les enregistrements, toute modification d'une écriture s'accompagnerait de modifications sur toutes les suivantes et ce, sur toutes les copies. Elle est (quasi) infalsifiable.

Propriété 3 : la blockchain n'a **ni dieu ni maitre**.
À chaque enregistrement, une des copies est désignée aléatoirement (y compris avec le minage) comme référence recopiée par les autres. Aucune organisation centrale n'est nécessaire, on parle de système distribué.




Propriété 4 : la blockchain n'a **pas de frontières.**
S'appuyant sur Internet qui n'a ni frontières ni régulations, la blockchain hérite de ses (et ces) caractéristiques.

*Ces quatre propriétés dessinent les domaines d'application privilégiés. Immuable et incorruptible, la blockchain jouit d'une réputation de sécurité. N'ayant nul besoin de chef, elle est très prisée dans les configurations où différents acteurs partagent un même recueil de données sans que l'un d'entre eux ne puisse prétendre à la gouvernance du système. Les transactions monétaires enregistrées dans le registre utilisé comme un livre de comptes s'épanouissent dans un monde sans frontières.*

## QUATRE CHOSES QUE NE FAIT PAS LA BLOCKCHAIN NATIVEMENT

Gardons-nous d'attribuer à la blockchain des vertus qui ne sont pas innées.

- Simple chambre d'enregistrement, la blockchain n'apporte aucune garantie sur le contenu des enregistrements.
*Illustration : une blockchain ne garantit pas qu'un produit est bio mais que la totalité des acteurs de la chaîne d'approvisionnement a déclaré que le produit est bio. Comme le ferait une base de données classique.*

- La blockchain n'apporte aucune garantie face à une fuite des données.

*Le chiffrement le permet, comme dans tout type de bases de données. Mais il n'est pas natif dans une blockchain.*

- Quoique constitué d'un nombre important de machines, la blockchain ne décuple pas sa puissance : toutes les copies sont identiques.
*À l'inverse, la nécessité d'un consensus rend la blockchain « pataude ». À l'inverse de tout type de bases de données.*

*Une Ferrari est promise, un jouet est fourni. Le contrat est garanti sur sa forme, mais pas sur son fond.*

- La transparence des mouvements dans la blockchain peut être ou pas ouverte à tous.
*Le droit en lecture est proposé à tous dans la blockchain de la plupart des crypto-actifs ou des chaines d'approvisionnement. Comme dans tout type de base de données.*

## DEUX TYPES DE BLOCKCHAIN

Le choix des opérateurs effectuant les écritures dans le registre est primordial pour s'assurer que les multiples copies sont identiques. Accessible à tout internaute ou réservé à des individus identifiés, le mode d'écriture dans la blockchain caractérise deux familles.

- Dans une blockchain **ouverte** tout le monde peut écrire dans le registre. Pour contourner certaines attaques internet, les participants doivent prouver qu'ils sont de bonne foi. Dans le cas de beaucoup de blockchains dont celle du bitcoin et ses près de dix mille nœuds, l'énergivore recherche par force brute d'une signature joue ainsi un rôle analogue aux « captchas » qui vous demandent de reconnaître un texte ou un lampadaire pour signifier que vous n'êtes pas un robot. C'est la preuve de travail. Pour inciter à faire ces recherches, le premier à tomber par hasard sur la bonne signature est rémunéré en monnaie nouvellement créée, bitcoin ou ether par exemple. Par analogie avec la recherche de l'or, l'opération s'appelle minage.
- Dans les blockchains **privées** seules quelques entités membres d'une association ou d'un consortium par ailleurs dûment accréditées sont autorisées à écrire dans la blockchain, ce qui permet d'échapper aux différentes formes de preuves de travail.

## TROIS DES USAGES DE LA BLOCKCHAIN

La monnaie et les registres partagés sont des domaines où les blockchains sont à l'aise.

### *MONNAIE*

Immuable et incorruptible, l'indélébile registre de la blockchain est taillé pour recevoir les livres de compte bancaires. L'application première est d'ordre monétaire, le bitcoin. Ajoutons que le registre ne connait pas de frontières ce qui autorise des transferts entre devises. Cette nouvelle mécanique monétaire rebat les cartes de la finance. Bitcoin ou ether les plus connues des « cryptos » ont aujourd'hui plusieurs milliers de petits cousins.

#### *REGISTRE PARTAGÉ*

Sans dieu ni maître, la blockchain séduit ces consortium où aucun membre n'accepterait d'en voir un autre bénéficier d'une quelconque préséance grâce à la détention de l'outil : chambre entre banques, acteurs d'une chaîne d'approvisionnement.

#### *NON-FONGIBLE TOKEN*

Les « NFT » sont un bon exemple d'application de la blockchain très en vogue en ce moment.

Les « tokens » désignent les enregistrements dans la blockchain.

« Non-fongibles » signifie qu'à l'opposé d'un bitcoin les différents enregistrements ne sont pas échangeables mais qu'à l'image de l'humain ils ont chacun leur personnalité. *Associés à un « smart contract », ils peuvent par exemple comptabiliser les passages à l'antenne d'un morceau musical et calculer les droits d'auteur et les taxes dues à la SACEM.*

## TROIS MENACES SUR LA BLOCKCHAIN

Réputée immuable et incorruptible, la blockchain doit pourtant composer avec de réelles menaces issues de son mécanisme ou d'Internet.

### LA LOI DES 51%.

L'enregistrement de la version désignée comme référence est effectué par chaque détenteur d'une copie. Un désaccord porté par un groupe de détenteurs peut dès lors entériner un choix différent voire modifier des écritures déjà enregistrées. Les dissensions issues de ce comportement débouchent classiquement sur un dédoublement de la blockchain. D'une manière générale, la détention de plus de la majorité des copies permet de prendre la gouvernance d'une blockchain. Le risque n'est pas que théorique comme en témoignent les nombreuses bifurcations déjà observées.

Le problème est que les concentrations existent déjà au niveau du minage.


*Le consensus choisit une référence parmi les copies. Le pouvoir peut être pris sur une blockchain en ayant la main sur plus de la moitié des copies.*

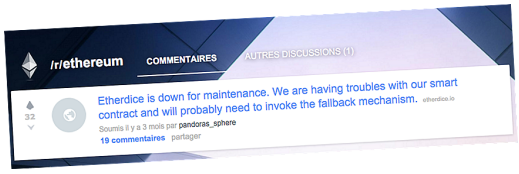
### LES FRAGILITÉS D'INTERNET

Reposant sur Internet, la blockchain est censée bénéficier de sa résilience. Il y a cela dit deux ombres au tableau.

- La première est que les infrastructures supportant la blockchain ne représentent qu'une petite partie d'Internet. Peu de fournisseurs d'accès à Internet participent à la plateforme et sont connectés par un nombre restreint de routes, ce qui rend le réseau vulnérable tant aux attaques qu'au pouvoir ainsi donné aux fournisseurs d'accès.

- La deuxième est une faiblesse déjà connue au niveau du protocole de routage des paquets sur Internet. Chacun des sous réseaux (plus de soixante mille !) qui constitue Internet envoie un message listant les sous réseaux voisins. Le message est propagé à tous les autres sous réseaux pour qu'ils puissent construire les routes pour atteindre tout point. Or les procédures permettant de s'assurer que l'annonceur est légitime et que le contenu de l'annonce est plausible sont loin d'être mises en œuvre. Le détournement de trafic, la rétention de paquets ou la coupure du réseau sont autant de menace pour la blockchain.

### LES ERREURS DANS LES CONTRATS




Les contrats (« smart contracts ») sont une intéressante possibilité des blockchains. Ce sont des programmes permettant de conditionner une action à des évènements. Ils sont enregistrés dans la blockchain.

Problème : ces programmes ne peuvent pas par définition être modifiés et sont exécutés simultanément sur toutes les machines de la blockchain. L'informelle coutume des logiciels mis au point grâce aux retours des utilisateurs devient impossible et a déjà donné lieu à des détournements.

De nouveau, la blockchain garantit l'horodatage et l'intégrité de ce qui est enregistré mais pas le contenu lui-même.

## EN BREF ...

- Le principe évoqué succinctement ici s'appuie sur la blockchain du bitcoin, mais bien des cousins existent et existerons qui s'appuient sur les bases d'un système résistant aux attaques, sans nécessiter une gouvernance et construits sur Internet : le hashgraph par exemple.

- Les vertus de la blockchain sont celles d'une chambre d'enregistrement mais il faut se garder d'en imaginer d'autres au premier rang des quels la confiance dans une information passée par la blockchain : ce n'est pas parce qu'une information est infalsifiable qu'elle est vraie.

- La confiance que l'on peut avoir dans la solidité de la blockchain reste bornée par celle d'Internet et par le risque de domination si une entité exerce un pouvoir sur la majorité des copies.

- La consommation démesurée du minage ne concerne que certaines blockchains publiques qui utilisent la dépense énergétique pour se protéger des intrus. Les blockchains privées ne sont pas affectées car les écritures ne peuvent être réalisées que par -des individus habilités peuvent intervenir.

Ces avertissements ne doivent pas occulter la puissance et la souplesse de l'outil. Deux domaines à mon sens en tirent profit : les chaînes d'approvisionnement et la monnaie.

*Jacques Baudron - mai 2021 - jacques.baudron@ixtel.fr*

## A PROPOS DE L'AUTEUR

*Créateur de la société iXTEL société spécialisée en architecture de réseau et qualité de service auprès des opérateurs et de l'IUT-T, membre fondateur de Forum ATENA, intervenant dans diverses écoles d'ingénieurs dont le groupe Télécom, l'Université de Lille et l'Institut Léonard de Vinci, Jacques Baudron se penche sur l'impact des nouvelles plateformes reposant sur internet : blockchain, big data, Intelligence Artificiel, « bulles » des réseaux sociaux …*