



HAL
open science

La blockchain, un nouveau fondement pour la confiance numérique ?

Thibault Langlois-Berthelot

► **To cite this version:**

Thibault Langlois-Berthelot. La blockchain, un nouveau fondement pour la confiance numérique ?. Observatoire d'IN Groupe, 2021, pp.5. hal-03314567v1

HAL Id: hal-03314567

<https://hal.science/hal-03314567v1>

Submitted on 5 Aug 2021 (v1), last revised 21 Oct 2021 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Copyright

Article rédigé pour le compte de la société IN Groupe :

www.ingroupe.com/blockchain-nouveau-fondement-confiance-numerique

English version :

www.ingroupe.com/en/blockchain-new-foundation-digital-trust

La blockchain, un nouveau fondement pour la confiance numérique ?

Dans un contexte de digitalisation croissante des échanges, la confiance numérique est devenue un enjeu majeur pour les États, les citoyens et les entreprises : la blockchain caractérise-t-elle une illusion technologique ou bien la fondation d'une nouvelle confiance numérique ?

La technologie blockchain s'institutionnalise

Depuis le 28 avril 2016¹, le droit français reconnaît une existence juridique – principalement financière – aux « Dispositifs d'Enregistrement Électronique Partagé (DEEP) », davantage connue par le grand public sous son appellation anglophone de « blockchain technology ». Plus récemment², la Commission d'enrichissement de la langue française a publié une liste de termes et de définitions similaires (« actifs numériques », « automate exécuter de clauses », « cyberjeton ») à adopter concernant cette nouvelle technologie et ses applications, tout en réaffirmant l'importance de l'utilisation de termes français, face à une adoption internationale des DEEPs.

Cette timide reconnaissance normative et linguistique française témoigne de l'intérêt ainsi que de l'adoption progressive de cette nouvelle technologie, qui révolutionne techniquement le partage d'informations numériques, et théoriquement, son approche par le marché.

¹ [Ordonnance n°2016-520 du 28 avril 2016](#) (art. L.223-12 & L.223-13 du Code Monétaire et Financier), en application de la [loi Macron du 6 août 2015](#), confère à la technologie blockchain une première reconnaissance légale en droit français

² Commission d'enrichissement de la langue française. (2021, janvier). [Vocabulaire des actifs numériques](#) (Texte 108 sur 142). Journal officiel de la République française.

Une technologie, de multiples définitions

D'un point de vue strictement matériel et physique, une blockchain ne représente qu'un réseau d'ordinateurs - plus ou moins nombreux et puissants - qui s'échangent des informations et des données. Ce n'est donc pas tant l'infrastructure matérielle de cette technologie qui est révolutionnaire, mais plutôt son protocole et ses algorithmes. En effet, ces derniers dictent aux ordinateurs, qui s'y connectent, une nouvelle façon inédite de s'échanger des informations réciproques.

Le plus souvent, ces ordinateurs connectés dédient une partie de leur puissance de calcul pour valider, enregistrer et maintenir en toute autonomie et simultanément, un journal et un historique commun des échanges effectués par les utilisateurs d'un DEEP. La nature de ces transactions d'informations peut varier selon la finalité propre à chaque DEEP : transactions financières (e.g. sous la forme d'actifs digitaux), transactions contractuelles (contrats numériques), transactions sociales (droits de votes électroniques et signature électronique) voire même transactions *phygitaes* (traçabilité numérique de biens et produits physiques).

Dès lors, la particularité d'une blockchain réside dans le fait que chaque ordinateur du réseau puisse respectivement valider des demandes de transaction, tout en copiant puis en stockant simultanément sur chaque ordinateur, chacune des transactions émises par l'ensemble des utilisateurs du réseau. Ainsi, l'ensemble des transactions validées par chaque machine est regroupé au sein de blocs de transactions successifs et cryptographiquement liés de façon consensuelle les uns aux autres : une chaîne de blocs se forme.

Généralement, la répartition des ordinateurs d'un réseau blockchain est parcellée et distribuée dans diverses régions du monde : il s'opère ainsi une décentralisation du journal et de l'historique des transactions de données. Dans ce dernier cas, le réseau blockchain ne nécessite plus l'intervention d'un tiers de confiance centralisé afin d'assurer la validité, la continuité et le maintien des transactions numériques de ses utilisateurs. De cette façon, le réseau est maintenu par des machines qui contribuent ensemble à résoudre des défis mathématiques et cryptographiques, afin de valider des blocs de transactions, et sans pour autant se connaître ou se faire confiance.

Une nouvelle économie numérique de la confiance, impliquant un rôle réduit des intermédiaires centralisés, émerge.

Une nouvelle révolution technique, pour une nouvelle confiance numérique

Les DEEPs offrent une tolérance optimale face à d'éventuelles pertes ou corruptions des données : toutes les informations échangées sont dupliquées et disponibles sur chaque ordinateur du réseau. Elles ne peuvent pas être modifiées ou encore supprimées sans l'accord unanime des autres ordinateurs. Dès lors, une machine corrompue pourrait être mise en « quarantaine » sans que le réseau principal - c'est-à-dire la majorité des autres machines – n'ait besoin d'être mis hors ligne ou en maintenance pour ses utilisateurs.

Cette résilience des registres distribués en fait, par nature, un outil de choix pour les entreprises souhaitant favoriser des collaborations internes et externes à leur organisation, tout en partageant de façon accessible, rapide, sécurisée et immuable, leurs informations et données.

Dans les faits, la technologie blockchain abrite et regroupe de nombreuses variantes technologiques, de la même façon qu'internet fait aujourd'hui fonctionner et héberge de multiples technologies (intelligence artificielle, objets connectés) et applications (e-mails, réseaux sociaux, intranets d'entreprises).

Concrètement, les différents modèles ainsi que nombres d'ordinateurs branchés au réseau, leurs consensus, leurs méthodes de validation des transactions ou encore l'accès plus ou moins restreint – soit public, privé ou hybride - au journal et à l'historique des transactions, peuvent sensiblement varier selon les finalités souhaitées pour chaque technologie de registre distribué. C'est pourquoi il existe aujourd'hui autant de technologies de registres distribués, que d'écosystèmes et d'acteurs qui lui sont rattachés.

De ce fait, la technologie blockchain permet de répondre à divers enjeux d'innovation sectoriels et métiers : services financiers (tokenisation d'actifs numériques³), transports et logistiques (traçabilité numérique de biens physiques), secteurs publics (e-gouvernement et institutions augmentés), assurance (assurance fiable, transparente et instantanée) ou encore identité décentralisée (identité numérique souveraine de citoyens, d'entreprises ou même d'objets connectés, basés sur un DEEP).

Pour résumer et dans de nombreux cas d'usage, la technologie blockchain permet de réduire le nombre ainsi que le degré d'intervention des intermédiaires de confiance traditionnels : elle permet en théorie l'émergence d'une nouvelle révolution de la confiance numérique, tout en garantissant une confiance technique et cryptographique optimale à tous ses utilisateurs.

En définitive, les DEEPs devraient continuer à se développer puis à prospérer, face à un environnement qui se digitalise progressivement et dans lequel les notions de « dépendance numérique » et de « confiance numérique », riment toujours plus pour les entreprises, les institutions et les citoyens, avec besoin de « souveraineté numérique ».

³ La tokenisation des actifs consiste à transposer des caractéristiques intrinsèques de la technologie blockchain – sécurité, immuabilité, rapidité, transparence, unicité – à des actifs tangibles (biens immeubles, biens meubles) ou intangibles (parts sociales, caractéristiques d'un personnage dans un jeu vidéo). Concrètement, il est possible de transférer, immobiliser ou encore diviser des représentations virtuelles uniques, de ses actifs.