La *blockchain* : concept, technologies, acteurs et usages

Par Côme BERBAIN
Sous-directeur adjoint Expertise à l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

La *blockchain* est à la mode : difficile, en effet, d'ignorer ce terme utilisé en abondance, dans des acceptions variées ! Afin d'appréhender ce nouveau phénomène, il est nécessaire de tenter de le définir, d'identifier ses éléments structurants et de s'interroger sur la pertinence de ses propriétés et de ses promesses.
La multitude des expérimentations dans un grand nombre de secteurs économiques nous invite à nous interroger sur la pertinence de l'utilisation de la *blockchain* en fonction des cas d'usage, et sur les motivations réelles des différents acteurs.
Bien loin d'être uniquement techniques, les enjeux fondamentaux de la *blockchain* ont trait à l'organisation, à la gouvernance et à la définition même des solutions permettant de répondre à la question de la confiance dans les interactions humaines. En ce sens, la *blockchain* est un nouvel outil technique qui induit et participe à la transformation numérique de nombreux secteurs, en particulier de celui des métiers du droit.

Un seul concept recouvrant plusieurs technologies

La confiance entre des acteurs réalisant des transactions repose généralement sur un système centralisé : les acteurs, ne pouvant se faire confiance mutuellement, choisissent de faire confiance à une entité qu'ils reconnaissent tous (État, banque, notaire…). Ce tiers de confiance tient un registre de leurs transactions, garantissant ainsi la régularité de leurs échanges. En fonction du type de transactions, l'accès au registre peut être libre pour tous, ou restreint à certains acteurs. Dans tous les cas, le tiers de confiance détient le monopole de la mise à jour du registre des transactions afin d'écarter tout risque de fraude.

Le concept de la *blockchain* est de proposer des extensions de ce modèle centralisé permettant une gestion collaborative d'un registre distribué et de s'abstraire ainsi de la nécessité d'une autorité centrale de confiance. Ce concept repose sur deux caractéristiques :

- le registre est implanté à l'aide d'une « chaîne » de blocs de données décrivant les transactions, liés entre eux par un procédé cryptographique (d'accès public, ce registre est généralement décentralisé) ;
- tout utilisateur peut ajouter des éléments au registre. Ces éléments sont assemblés sous la forme de blocs, et il existe un processus permettant de valider de manière définitive les nouveaux blocs au fur et à mesure que ceux-ci sont ajoutés à la « chaîne » : ce processus vise à empêcher la falsification du registre et est en général également public et réalisé de manière décentralisée.

Plusieurs technologies (Bitcoin, Ethereum, Ripple…) se sont construites autour de ce paradigme. Elles s'appuient sur des briques techniques préexistantes (registre distribué, signature électronique, cryptographie asymétrique, preuve de travail, machines virtuelles…), l'innovation résidant dans leur assemblage.

Plus précisément, les éléments structurant les différentes technologies de *blockchain* existantes sont au nombre de quatre :

- le registre et son contenu : le registre étant une forme de stockage distribué, il est possible d'y inclure des éléments de diverses natures. L'utilisation du registre pour répertorier des transactions demeure le cas majoritaire. Néanmoins, il est possible d'y stocker aussi bien des fichiers que des communications. Les *smart contracts* [(1)] permettent d'étendre la notion de stockage distribué à celle de capacité de calcul distribué ;
- l'accès au registre pour les différents acteurs : la publicité (chaîne publique, chaîne privée ou chaîne en consortium), le type des acteurs (personnes morales ou personnes physiques) et l'identité affichée (réelle ou pseudonymique) des acteurs en sont les principaux paramètres. Deux types d'acteur se distinguent : les utilisateurs et les valideurs ;

(1) Un smart contract *est un contrat formalisé sous la forme de codes informatiques stockés dans une technologie de* blockchain *et dont l'exécution est automatique, dès lors que les conditions en sont réunies.*

- la validation du registre par consensus (le terme de « consensus » doit être pris ici dans son acception anglo-saxonne) : en fonction des mécanismes de validation choisis, la possibilité pour l'ensemble des acteurs de contribuer à l'émergence du consensus (ou celle d'exprimer un désaccord) ne peut être garantie. L'ensemble des acteurs partage cependant un accord sur l'état du registre. Plusieurs méthodes de validation distribuée aux propriétés distinctes coexistent : preuves de travail, preuve de participation (*proof of stake*), consensus fédéré… ;
- la régulation des acteurs : afin d'inciter les acteurs à contribuer à la communauté (notamment en mettant à disposition des moyens informatiques), mais également afin d'obtenir un équilibre du système, il est nécessaire de mettre en place un mécanisme de régulation ; le plus souvent, celui-ci repose sur une monnaie (associée à la technologie retenue).

Chaque technologie correspond à des choix en matière de solutions retenues pour ces différentes problématiques. L'effectivité des promesses de la *blockchain* dépendant de ces choix, elle ne peut être évaluée que pour une technologie donnée. Le Tableau ci-dessous illustre ces choix, pour trois technologies.

	Bitcoin	Ethereum	Ripple
Contenu	Transactions monétaires	Transactions, *Smart Contracts*	Transactions financières
Accès	Public	Public	Restreint au monde financier. Publicité des informations de transaction, mais pas des informations de paiement
	Pseudonyme	Pseudonyme	Identité réelle
Validation	Preuve de travail	Preuve de travail – en transition vers un modèle de preuve de participation	Vote sur la correction des transactions entre les valideurs (avec un seuil de 80 %)
Régulation	Génération de nouveaux bitcoins et ajustement de la difficulté de la preuve de travail	Rémunération en éther. Consommation de gaz en fonction de la quantité de calcul distribué dans les *smart contracts*	Monnaie associée XRP (*Ripples*)

Les propriétés et leurs limites structurelles

La principale promesse de la *blockchain* est la décentralisation de la confiance, qui permet la disparition du tiers de confiance teneur du registre. Cette promesse repose sur l'infalsifiabilité du registre : tout élément inséré dans le registre est immuable, il ne peut être ni supprimé ni même modifié. Le système préserve également l'ordre de validation des différents éléments. Cette infalsifiabilité structurelle porte en elle sa propre limite en matière de gestion des contentieux : même des transactions qui correspondraient à des actions illégales ou contestées ne peuvent être supprimées, seule une correction de leurs effets peut être apportée au moyen de nouvelles transactions.

Le processus de validation, qui vise à garantir l'infalsifiabilité, est donc la pierre angulaire des différentes technologies. Fonctionnellement, il correspond à l'émergence d'un consensus entre l'ensemble des valideurs, et ce, sur chaque nouveau bloc (malgré la présence potentielle d'acteurs non coopératifs ou malveillants) : cela renvoie à un problème mathématique connu, celui dit des généraux byzantins, qui doivent correspondre entre eux par messages conçus sur la base d'un algorithme et gagner ainsi la bataille même s'il y a parmi eux des traîtres. Néanmoins, il n'existe pas de lien démontrable entre ce problème théorique et les solutions utilisées par les différentes technologies existantes.

Le caractère distribué du registre induit une transparence et une auditabilité des éléments pour les acteurs. Dans le cas de technologies publiques, cela confère un avantage majeur quant à la confiance des acteurs, mais peut limiter les types de données manipulables, telles que des données à caractère personnel [2]. À l'inverse, dans le cas de technologies ou de déploiements privés, seuls les acteurs impliqués bénéficient de cette propriété.

L'infalsifiabilité et la transparence engendrent une caractéristique supplémentaire de résilience des systèmes utilisant ces technologies : en cas d'incident ou d'atteinte majeure, tout acteur est en mesure de créer un nouveau système à partir d'un état sur lequel le consensus est assuré. Ce processus nécessite néanmoins qu'une part significative des acteurs (utilisateurs et valideurs) accepte de basculer dans le nouveau système (les quelques cas existants ont montré que les acteurs ont tendance à se diviser, entre ceux de la chaîne historique et ceux de la nouvelle chaîne, en fonction de leurs intérêts propres).

Au-delà de ces propriétés intrinsèques, la question des performances est centrale dans la comparaison entre un système reposant sur une technologie de *blockchain* et les systèmes classiques. Très variables en fonction des technologies, ces performances sont en augmentation, notamment dans le cas des transactions financières : le temps de validation d'un bloc est de 10 à 20 minutes pour Bitcoin, de quelques minutes pour Ethereum, et de quelques secondes seulement pour les nouvelles crypto-monnaies. Par ailleurs, les technologies reposant sur les preuves de travail impliquent d'effectuer des quantités très importantes de calculs qui les rendent particulièrement peu efficaces en termes énergétiques.

Une multitude de services construits à partir des technologies disponibles

Les technologies construites autour de la *blockchain* se présentent comme des protocoles ou des plateformes à partir desquels il est possible de construire des services répondant à des cas d'usage. Certains services pourtant non financiers s'appuient même sur le Bitcoin, qui a été conçu au départ exclusivement pour réaliser des transactions monétaires. Il existe aujourd'hui des milliers de

(2) Il est néanmoins possible de trouver des solutions à cette limite grâce à des techniques permettant de manipuler les éléments sans en révéler le contenu, telles que le zero-knowledge protocol *(preuve à divulgation nulle de connaissance).*

services reposant sur des technologies construites autour du concept de *blockchain*, et de nouvelles variantes apparaissent régulièrement.

Les domaines d'application et les cas d'usage sont extrêmement variés : au-delà d'un secteur financier fortement mobilisé par le phénomène Bitcoin (210 milliards de dollars d'investissements estimés en 2016), des services existent dans l'énergie, le commerce (diamant ou œuvres d'art), les transports et la logistique, la gestion des droits numériques (musique, films ou jeux vidéo), la santé, l'administration et l'État (cadastre)… Le suivi de transactions, leur traçabilité ou la lutte antifraude sont les cas les plus répandus.

Le développement de ces services fait apparaître quatre enjeux principaux qui doivent être pris en compte afin d'évaluer l'adéquation entre un cas d'usage, un service et une technologie :

- la gouvernance : les règles d'organisation des communautés d'acteurs (utilisateurs ou valideurs) ainsi que leur mécanisme de régulation sont déterminants pour la pérennité du service ;
- l'efficacité technique : la comparaison avec les techniques classiques de bases de données réparties accessibles *via* des API est rarement en faveur des nouveaux services. Les performances des technologies de *blockchains* ne sauraient en être trop éloignées, sous peine d'échec ;
- la reprise de l'existant et la gestion des contentieux à venir (nombre de services ignorent cet enjeu) ;
- la numérisation des sous-jacents : certains services nécessitent que l'on associe de manière certaine des objets physiques (tels qu'un diamant, une toile ou l'énergie produite par une éolienne) à leur contrepartie numérique utilisée dans la chaîne correspondante. Cette question dépasse les seuls usages dans le cadre de la *blockchain*, mais cet écosystème a permis de développer plusieurs solutions d'efficacité apportant des degrés de garantie variables. Une réponse est l'utilisation d'« oracles » (également utilisables notamment pour les *smart contracts*), c'est-à-dire de tiers de confiance spécialisés choisis par les utilisateurs du service.

Un écosystème aux motivations variées

L'enthousiasme suscité par la *blockchain* et son potentiel d'applications ont entraîné la constitution rapide d'un écosystème riche. La *blockchain* figure en très bonne place dans le pic des espérances exagérées du « *Hype Cycle* » de Gartner [3] : c'est un signe d'effet de mode et de démultiplication des initiatives, mais également d'immaturité du domaine et d'apprentissage par l'expérimentation.

Plusieurs types d'acteur participent à l'écosystème de la *blockchain* :

- de nombreuses *start-ups* se sont lancées, y compris dans un rôle de conseil ;
- des tiers de confiance historiques (tels que les notaires, qui anticipent la mutation de leur métier) montent des expérimentations pour leurs propres usages ;
- de grands groupes, notamment dans le domaine financier (banques, assureurs…), l'expérimentent en partenariat avec des *start-ups* ou avec les acteurs du monde de la recherche et de l'innovation ;
- les pouvoirs publics, tant en France qu'à l'international (Caisse des Dépôts, France Stratégie, *UK Government Office for Science*) accompagnent ou observent le phénomène.

Les motivations des différents acteurs sont variées. La première d'entre elles est l'apprentissage : nombre d'initiatives visent principalement à tester des modèles techniques et organisationnels et à obtenir des retours d'expérience afin de mieux comprendre le concept de *blockchain* et les technologies associées, et de tenter de les maîtriser.

Par ailleurs, étant structurellement décentralisée, la *blockchain* entraîne l'apparition d'un effet de réseau : l'on assiste, de ce fait, à une course entre de nombreux acteurs désireux de devenir le service ou la plateforme de référence dans leur secteur et de s'assurer ainsi une position dominante (« *Winner takes all* »). Dans cette course prennent place aussi bien les tiers de confiance traditionnels que des entreprises clientes souhaitant se passer de ces intermédiaires ou de nouveaux entrants cherchant à modifier de fond en comble l'organisation d'un secteur. Enfin, un certain nombre de *start-ups* visent autant leur rachat par un grand groupe que le développement d'une activité propre.

Un élément de la transformation numérique

L'apparition de la *blockchain* correspond à une nouvelle approche, décentralisée, de l'informatique, dont les impacts réels n'apparaîtront qu'à long terme. Il est difficile de déterminer dans quelle mesure les comparaisons avec l'apparition des protocoles TCP/IP (*Transmission Control Protocol/Internet Protocol*), dans les années 1980, sont pertinentes. Néanmoins, en permettant d'aller au-delà de la simple dématérialisation des transactions et des contrats, la *blockchain* nous offre la possibilité de modifier la manière dont nous concevons la gestion de la confiance dans les relations humaines et au sein des organisations associées. Initiant la transformation numérique de secteurs complets, elle va bien au-delà d'une simple question technique.

L'apparition des *smart contracts* (contrats intelligents), en particulier, va modifier en profondeur les métiers du droit : le bitcoin, la première application de la *blockchain*, concerne les paiements, qui sont la forme la plus simple de contrat. Les métiers du droit ont notamment pour fonction de traduire en clauses juridiques et en contrats les intentions des parties. Au-delà de la simple dématérialisation des contrats, les *smart contracts* correspondent à la transformation numérique de cette activité : ils permettent de traduire en code informatique les intentions des par-

(3) www.gartner.com/technology/research/methodologies/hype-cycle.jsp

ties et d'obtenir l'exécution automatique du contrat ainsi constitué, illustrant le principe « *Code is law* ». Cela justifie l'intérêt que les professions juridiques manifestent à l'égard des *smart contracts*.

Même si la rédaction des *smart contracts* est un exercice complexe encore mal maîtrisé, et même si la gestion des contentieux reste une question ouverte, on peut s'attendre à voir se développer de nouvelles professions autour de la rédaction de *smart contracts* en lien avec plusieurs technologies de *blockchain*, ainsi que des échanges de bibliothèques de *smart contracts*. Là encore, les conséquences de la *blockchain* ne se cantonnent pas aux aspects techniques, elle a aussi des impacts juridiques et organisationnels. L'expérimentation est plus que jamais nécessaire pour comprendre ces nouveaux outils techniques et imaginer les nouvelles applications et les nouvelles formes d'organisation associées.