ENTRETIEN

THIBAULT DOUVILLE et THIBAULT VERBIEST

> *Blockchain* et tiers de confiance : incompatibilité ou complémentarité ?

Thibault Douville *est agrégé de droit privé, professeur à l'Université du Mans et codirecteur du Master droit du numérique de l'Université de Caen*
Thibault Verbiest *est avocat aux barreaux de Paris et de Bruxelles, associé du Cabinet DS Avocats*

La technologie blockchain n'a-t-elle pas pour essence d'exclure les tiers de confiance ?

La *blockchain* est une technique de désintermédiation, permettant de se passer des « tiers de confiance ». Cette notion assez vague regroupe les personnes qui, en raison de leurs compétences, de leur mission et de leur statut, créent les conditions de la confiance pour les transactions (États, banques, professions réglementées…). Par comparaison, la *blockchain* assure par elle-même cette confiance. Elle est à même de garantir l'intégrité des transactions qui sont inscrites dans le registre distribué entre les différents nœuds du réseau. Elles font, en effet, avant leur intégration aux blocs constitutifs de la *blockchain*, l'objet d'une vérification et d'une validation par un procédé technique déterminé (preuve de travail, preuve de possession…). Des transactions peuvent alors intervenir entre des personnes qui ne se connaissent pas, rendant inutile les tiers de confiance, marginalisant les intermédiaires, notamment les plateformes numériques, et réduisant notablement les coûts de transactions. Les crypto-monnaies (Bitcoin, Ethereum…) et dans leur prolongement les ICO (*initial coin offering*) illustrent ce schéma.

La mise en œuvre de la technologie* blockchain *peut-elle réellement se passer des tiers de confiance ?

La question se pose à plusieurs titres. Le premier tient à l'identification des parties. Les principales *blockchain* publiques fonctionnent sur le principe de l'anonymat, les transactions interviennent entre des adresses sur le réseau. Pour autant, ces adresses correspondent à des utilisateurs, elles sont d'ailleurs déduites à partir des clés publiques de ces derniers. Du reste, le lien entre les clés utilisées et un utilisateur n'est pas garanti. Par comparaison, en matière de signature électronique, c'est le certificat électronique délivré préalablement par un prestataire de services de confiance (PSC) qui permet d'établir ce lien. Pour répondre à cette problématique de vérification de l'identité du client (processus *Know your customer*), certains projets basés sur la *blockchain* prévoient d'intégrer des données d'identification dans les transactions tandis que d'autres cherchent à développer des solutions d'authentification au moyen d'une *blockchain*, une vérification de l'identité de l'utilisateur intervenant de manière automatique, par exemple par comparaison entre la photographie du demandeur et celle figurant sur un document d'identité. De plus, les transactions opérées par une *blockchain* peuvent porter sur des éléments générés ou intégrés à celle-ci ou qui y sont extérieurs. Dans le premier cas, la technologie *blockchain* repose sur une vérification des transactions précédentes dans le registre. Dans le second cas, aucune vérification n'est possible dès lors que les données n'ont pas été antérieurement intégrées dans la *blockchain*. Pour garantir la confiance dans les transactions, une authentification des informations doit être réalisée à ce stade. Concrètement, imaginons le transfert de la propriété d'un bien au moyen d'une *blockchain* : il convient de s'assurer - comme les notaires le font actuellement en matière immobilière - que le vendeur est bien le propriétaire du bien. À défaut, une cession potentiellement irrégulière figurerait définitivement dans le registre. Ensuite, la *blockchain* repose sur des outils techniques, comme la signature électronique ou l'horodatage des blocs, qui obéissent à un cadre réglementaire et technique pour produire des effets juridiques. Enfin, si la technologie *blockchain* est par elle-même sûre, ce n'est pas le cas des plateformes techniques ou des applications qui permettent son fonctionnement. C'est d'ailleurs la faiblesse d'un *smart contract* qui a entraîné le vol d'Ether à l'occasion d'une levée de fonds en mai 2016.

En définitive, l'authentification des utilisateurs et des données nécessaires aux transactions et la sécurisation des outils techniques montrent que le recours à des tiers de confiance demeure nécessaire en matière de *blockchain*.

Quels tiers de confiance pourraient être amenés à intervenir en matière de* blockchain *?

Ils sont assurément très divers. Tout dépend de l'usage qui est fait de la *blockchain* : fonction d'archivage et probatoire ; fonction d'échange. Certains sont d'ores et déjà identifiables. C'est le cas des PSC pour les services de confiance (signature électronique, horodatage) associés à une *blockchain*. Ce pourrait être aussi le cas, dans le cadre du futur schéma national d'identification électronique, des fournisseurs d'identité. S'agissant de l'authentification de l'objet des transactions, les notaires ou les huissiers ont, en raison de leur qualité d'officier ministériel, un rôle évident à jouer. Une certification de sécurité des intermédiaires techniques et des applications serait également utile pour laquelle des prestataires agréés ont vocation à intervenir.

En définitive, tiers de confiance et *blockchains* sont complémentaires pour garantir la confiance dans les transactions. Pour les *blockchains* publiques, marquées par leur caractère international, on peut imaginer que des organisations autonomes décentralisées (DAO) fixent les conditions du recours aux tiers de confiance. Mais pour quelle reconnaissance juridique ? Les *blockchains* privées ou semi-privées ne présentent pas les mêmes difficultés et, de ce point de vue, offrent peut-être le plus de potentialités, quitte à trahir l'état d'esprit initial de la technologie blockchain.