

MAI 2017

Newsletter

Auteurs:
Roland Mathys
Samuel Klaus



ICT / NEW TECHNOLOGIES

Blockchain – mythes, faits et questions juridiques

La **Blockchain** fait le buzz. Toutefois, les mythes qui entourent la *blockchain* ne correspondent pas toujours à la réalité. Cette Newsletter clarifie les notions et éléments centraux de cette technologie, tout en mettant en exergue certains problèmes juridiques. Dans une moindre mesure, l'accent sera également mis sur les aspects techniques de cette technologie.

1 LA TECHNOLOGIE *BLOCKCHAIN*

1.1 *BLOCKCHAIN* = TECHNOLOGIE GÉNÉRIQUE

"*La blockchain*" en tant que telle n'existe pas, à la différence par exemple de "l'électricité". Le terme *blockchain* désigne une technologie générique pouvant être utilisée de manière variée, pour des produits très divers. Tout comme une voiture peut se décliner en fourgons de livraison, voitures de sport, voitures familiales ou SUV, la *blockchain* trouve de nombreuses applications.

1.2 FONCTIONNEMENT ET NATURE

La *blockchain* en tant que technologie constitue une base de données numérique, ou **registre (ledger)**, dans lequel les titulaires de certains droits sont enregistrés et qui peut, mais ne doit pas, être géré de manière **décentralisée (distributed)**. Dans la branche, on parle donc plutôt de **distributed ledger technology** ("DLT"). Les applications fondées sur la *blockchain* sont donc en fait simplement des **registres d'ayant droits**, comme l'est p.ex. le registre foncier dans le monde non dématérialisé. Dans un tel registre,

les ayants-droits ne sont (en général) pas enregistrés par leur nom, mais de manière anonyme (cryptographique). L'authentification de l'ayant-droit s'effectue grâce à l'utilisation par ce dernier d'une clef cryptographique, qui est unique à chaque ayant-droit (la *private key*). Toute modification portée au registre (p.ex. lors d'une transaction) ne peut donc être opérée que par le détenteur de la *private key* (comparable au propriétaire d'un bien immobilier qui doit présenter sa pièce d'identité au registre foncier). L'historique complet de la transaction est enregistré dans le registre (c'est-à-dire la *blockchain*) et est visible en permanence (comme il est également possible de retracer les changements de propriétaires dans le registre foncier).

C'est la **rapidité et le faible coût du système** qui constituent les avantages d'un registre basé sur une *blockchain*. Alors qu'une transaction dans le registre foncier ne sera enregistrée qu'après plusieurs jours, une modification dans un registre *blockchain* peut intervenir en quelques secondes seulement. La question de savoir quels types de

droits sont gérés par une *blockchain* est secondaire (voir ch. 1.3); c'est l'avantage d'une réalisation facilitée qui est pertinent (de la même manière que le contenu de toute lettre peut être envoyé par e-mail – plus rapidement et à moindre coût).

"Les applications *blockchain* / DLT sont des systèmes de règlement très efficaces et peu coûteux."

Étant donné que la totalité du règlement doit être faite informatiquement, les registres *blockchain* ne doivent pas obligatoirement être gérés par un fournisseur d'infrastructure centralisée (avec intermédiaire, respectivement tiers de confiance), mais peuvent être gérés de manière **distribuée** (*distributed ledger*). Dans ce cas, des copies identiques des registres (c'est-à-dire de la *blockchain*) sont enregistrés simultanément sur une multitude d'ordinateurs (appelés *nodes*), sur lesquels est installé un logiciel permettant de lire les informations. Une comparaison des informations figurant auprès de chaque *node* est effectuée régulièrement, à un rythme prévu par les concepteurs du système, afin que toute modification du registre puisse immédiatement être répercutée dans tous les *nodes* (qui constituent chacun une forme de backup virtuel).

1.3 DOMAINES D'APPLICATION

Des applications DLT sont imaginables **dans tous les domaines pour lesquels des transactions impliquant la modification d'un droit doivent être enregistrées rapidement, être traçables, et également bon marché**. Il peut s'agir de versions digitales de registres papier existants (comme par exemple une version *blockchain* du registre foncier ou d'un registre des actions) ou également de nouveaux registres, dont la mise en œuvre avait jusqu'à présent échoué en raison du coût et de la complexité de la mise en œuvre (comme p.ex. un registre de pièces de rechange, d'œuvres d'art, de diamants, pour permettre de prouver leurs origines et ainsi enrayer les contrefaçons, l'art spolié et les "blood diamonds"). La majorité des applications *blockchain* se retrouvent aujourd'hui dans le domaine des monnaies cryptographiques (comme p.ex. le bitcoin).

2 MYTHES ET FAITS

Les applications basées sur la *blockchain* et la DLT sont souvent présentées comme particulièrement **sûres**. Les enregistrements dans une *blockchain* ne seraient par ailleurs **pas modifiables**, et il ne serait **plus nécessaire d'utiliser un tiers de confiance (fournisseur d'infrastructure centralisée)**, étant donné que le registre est distribué.

2.1 SÛRE?

De manière générale, les **techniques cryptographiques** basées sur la DLT sont **sûres** (si elles sont implémentées correctement). **Ce n'est toutefois pas parce qu'une application est basée sur la technologie *blockchain* qu'elle est automatiquement sûre dans son ensemble**. Reprenons l'exemple de la voiture pour illustrer ce propos: ce n'est pas parce que la technologie utilisée dans les moteurs à combustion est à présent considérée comme "sûre", que toute voiture équipée d'un moteur à combustion est une "voiture sûre".

2.2 PAS MODIFIABLES?

Dire que de manière générale, la technologie *blockchain* rend les données qu'elle contient non modifiables, ne correspond pas à la réalité. Dans les faits, l'intégrité d'une *blockchain* dépend de différents facteurs qui, en fonction de la mise en œuvre de la DLT, **rendent en réalité possible des modifications (ultérieures)**.

L'application installée sur les machines servant comme nodes permet une intervention potentiellement intrusive dans des DLT gérées de manière décentralisée. D'une manière qui marqua les esprits, ce cas de figure se présenta en été 2016, lorsque le logiciel utilisé pour le véhicule d'investissement "The DAO", basé sur de la DLT, fut modifié, pour annuler une transaction indésirable de USD 50 mio, contre le gré de la personne concernée (mot-clef: *Ethereum Hard Fork*).

Il est également possible dans d'autres cas de manipuler une *blockchain*, en fonction du **mécanisme de comparaison des différents nodes** utilisé. Si c'est en première ligne la capacité de calcul des nodes qui est déterminante (comme pour certaines monnaies cryptographiques), cela ouvre également des possibilités de manipulation, comme p.ex. en été 2014 dans le cadre de la *blockchain Bitcoin* (mot-clef: *GHash.io 51% attack*).

2.3 PAS BESOIN D'UN TIERS DE CONFIANCE?

La DLT fut conçue, entre autres, pour permettre la mise en place d'un système qui ne serait pas contrôlé par un fournisseur de registre centralisé (comme p.ex. une banque), **la confiance en une telle autorité centrale n'étant donc plus une condition préalable**. Toutefois, **un certain degré de confiance est également nécessaire pour les applications DLT, mais la confiance est accordée à une autre personne**: Alors que traditionnellement, dans un système centralisé, l'on faisait confiance à l'organisme de règlement, pour les applications DLT, la confiance est maintenant accordées aux concepteurs et développeurs du programme permettant de faire fonctionner cette application (changements volontaires (voir ch. 2.2 [*Ethereum*]), implémentation erronée, code défectueux, etc.). En outre, un système entièrement décentralisé impose également d'accorder une certaine confiance aux exploitants des nodes, étant donné qu'une majorité de nodes, agissant de manière coordonnée, pourrait influencer la *blockchain* (voir ch. 2.2 [*GHash.io*]).

2.4 DÉCENTRALISÉ?

Théoriquement, il est possible de baser des applications DLT **sur un système décentralisé** (comme p.ex. le Bitcoin). Toutefois, même dans une telle constellation, une tendance vers une certaine centralisation se dessine, dans le sens d'une possibilité de prise de contrôle ou d'influence sur le programme de gestion de l'application ou par des effets de concentration régis par les conditions du marché (p.ex. si des nodes s'unissent pour former des *mining-pools*, pour augmenter leur capacité de calcul et ainsi produire des effets d'échelle; concernant les conséquences, voir ch. 2.2 [*GHash.io*]).

Aux inconditionnels de la décentralisation complète, il est possible d'opposer le fait que le **contrôle par un organisme central** peut à lui seul permettre d'**instaurer une certaine confiance dans le système de règlement** concerné (voir ch. 2.3), si un cadre juridique adéquat est prévu (voir ch. 3.2). Un organisme de contrôle central permet en outre une

utilisation de la DLT dans des domaines où un système de décentralisation complète **n'est pas permis** par la **réglementation en vigueur** (p.ex. dans le domaine bancaire, des papiers valeurs, etc.).

3 CONSÉQUENCES ET QUESTIONS JURIDIQUES

3.1 LA MISE EN ŒUVRE EST DÉCISIVE

La DLT est une technologie de base, et non pas un produit particulier. Les propriétés et qualités d'un produit basé sur la *blockchain* résultent de son implémentation concrète.

La mise en œuvre technique et juridique est décisive.

"La DLT en tant que telle n'est pas à elle seule garante du succès – c'est bien la mise en œuvre technique et juridique qui est décisive."

La définition de la **mise en œuvre technique** peut être illustrée par le succès des voitures électriques: les voitures électriques existent depuis longtemps et sous plusieurs formes, toutefois; ce n'est qu'à travers une application technologiquement très évoluée et attractive pour un large public que la mise en œuvre de cette technologie a réussi sa percée. Il existe une multitude d'applications basées sur la *blockchain*; **la DLT en tant que telle n'est pas à elle seule garante du succès – c'est bien la mise en œuvre technique et juridique qui est décisive.**

Bien que les applications DLT soient purement électroniques et fonctionnent de manière quasi "virtuelle", elles n'agissent jamais de manière déconnectée de l'économie réelle. Des **interfaces avec l'économie réelle** sont nécessaires, et à ce moment-là la **conception juridique d'une application DLT et des relations entre les participants devient particulièrement importante**. En effet, des règles de droit sont indispensables afin de pouvoir accorder sa confiance au système, s'agissant en particulier de la manière de traiter les erreurs (p.ex. dans la mise en œuvre), les problèmes (p.ex. dans la réalisation technique) et les d'ambiguïtés (p.ex. lors de questions litigieuses, en particulier concernant l'admissibilité de certaines actions, voir ch. 2.2 [*Ethereum*]).

3.2 QUESTIONS JURIDIQUES

S'agissant du cadre légal applicable, des questions particulières se posent en relation avec le droit des obligations (pour les aspects réglementaires, voir la [newsletter d'avril 2017](#)):

La question essentielle réside dans le fait de **savoir qui contracte avec qui, dans le cadre d'une application de la DLT** (et qui sont les **titulaires de droits** et d'**obligations**). En fonction de la nature de l'application reposant sur la DLT, les utilisateurs peuvent être directement liés juridiquement avec d'autres usagers ou bien par exemple avec les organismes centraux (voir ch. 2.4).

Se pose également la question de la qualification juridique des **smart contracts**. Cette notion fait référence à des instructions de transfert avec traitement automatisé dans le cadre de l'application de la DLT. L'utilisation du terme "*smart contract*" est trompeuse car elle **ne recoupe pas la notion d'accord au sens juridique du terme** mais celle de mécanismes de traitement automatisés prédéterminés en fonction de la réalisation, ou non, d'une condition. Une fois

programmés, les *smart contracts* n'offrent que peu de possibilités de modifications ultérieures et peuvent conduire à des résultats inattendus. **Les smart contracts ne vont pas avoir pour effet de réduire la nécessité d'un cadre juridique, mais au contraire l'augmenter.**

Pour apporter une solution à ces questions juridiques, en particulier en cas d'application DLT avec un organisme de contrôle central, il peut être envisageable de prévoir les conditions de participation au système DLT concerné, sous forme de conditions générales "**Blockchain-CG**". En fonction du type d'application basée sur la DLT, il sera possible de régler aux moyens de conditions générales des questions comme p.ex. l'objet du droit, le type de droits gérés, l'anonymat, l'éventuel mécanisme de coordination et de synchronisation, etc..

Dans un **système autorégulé**, la coordination est assurée par divers mécanismes de coordination ainsi que de prise de décision (par exemple droits de votes ou droits de veto). Se poseront ici des questions relevant non seulement du droit des contrats, mais aussi du **droit des sociétés**, en particulier si les utilisateurs, les exploitants de *nodes* ou les membres sont soumis à divers ordres juridiques.

Bien que théoriquement la mise en œuvre d'une DLT ne devrait pas poser problème, en réalité, il existe un risque que subsistent des erreurs, des ambiguïtés, et des litiges. Dès lors, il conviendra de porter une attention toute particulière aux mécanismes de résolution des litiges. L'une de nos prochaines newsletters sera spécifiquement dédiée à ce thème.

4 CONCLUSION

Un grand nombre d'affirmations relatives aux "*blockchains*" découlent de mythes et du marketing ou de l'effet de mode. Toutefois, les faits parlent d'eux-mêmes: **le DLT est une technologie fondamentalement prometteuse s'agissant de l'enregistrement et de la visibilité de transactions**. Sa mise en œuvre permettra en outre d'accélérer le phénomène de digitalisation, y compris dans des domaines encore peu touchés.

La terminologie technique utilisée crée une illusion d'infaillibilité qui **éveille des attentes en partie déçues et dissimule de réels problèmes**. La réussite de la mise en application d'une DLT dépendra non seulement d'une programmation techniquement irréprochable, mais également d'**une réglementation juridique appropriée apportant des vraies solutions aux problèmes particuliers** que posent les blockchains.

"La réussite de la mise en application d'une DLT dépendra non seulement d'une programmation techniquement irréprochable, mais également d'une réglementation juridique appropriée apportant des vraies solutions aux problèmes particuliers que posent les *blockchains*."

Contacts

Le contenu de cette Newsletter ne peut pas être assimilé à un avis ou conseil juridique ou fiscal. Si vous souhaitez obtenir un avis sur votre situation particulière, votre personne de contact habituelle auprès de Schellenberg Wittmer SA ou l'un des avocats suivants répondra volontiers à vos questions:

A Genève:



Olivier Hari

Conseil
olivier.hari@swlegal.ch

A Zurich:



Roland Mathys

Associé
roland.mathys@swlegal.ch



Louis Burrus

Associé
louis.burrus@swlegal.ch



Samuel Klaus

Avocat
samuel.klaus@swlegal.ch



SCHELLENBERG WITTMER SA / Avocats

ZURICH / Löwenstrasse 19 / Case postale 2201 / 8021 Zurich / Suisse / T+41 44 215 5252

GENÈVE / 15bis, rue des Alpes / Case postale 2088 / 1211 Genève 1 / Suisse / T+41 22 707 8000

SINGAPOUR / Schellenberg Wittmer Pte Ltd / 6 Battery Road, #37-02 / Singapour 049909 / www.swlegal.sg

www.swlegal.ch

Cette Newsletter est disponible en français, anglais et allemand sur notre site internet www.swlegal.ch.