Livre blanc

L’utilité de la signature électronique sur blockchain publique pour les grands comptes : intérêt, faisabilité et valeur juridique

Mai 2020

Document Co-rédigé par le cabinet d’avocats Solegal & la société Blockchain EZ

Préambule

Nous donnons dans ce présent document un avis sur l'utilité et la valeur juridique de la signature électronique sur blockchain publique pour les besoins des entreprises et des institutions publiques et des associations.

Nous estimons que la signature électronique sur blockchain publique est compatible avec la réglementation en vigueur (code civil français et règlement eIDAS). Elle représente une solution idéale pour les projets de certification documentaire, notamment en cas de volume important de documents à traiter.

Ce document a été rédigé par une équipe mixte d'avocats spécialisés en droit du numérique et de consultants en informatique experts sur les technologies blockchain. A des fins de vulgarisation, nous avons ici volontairement limité notre analyse, en ne présentant notamment ni l'intégralité de la règlementation et de la jurisprudence applicables, ni le fonctionnement technique détaillé et les bénéfices de la technologie.

Le document est structuré en quatre chapitres. Chacun d'entre eux vise à vulgariser un aspect spécifique du sujet :

1. La signature électronique sur Blockchain : pourquoi ?

1.1 La signature électronique : un marché et un besoin en forte croissance

La digitalisation de la production documentaire permet très souvent aujourd'hui de s'affranchir de l'impression papier des documents, de leur envoi postal, des rencontres physiques entre signataires et autres contraintes. Toute organisation garde cependant le besoin de prouver l'authenticité des documents numériques qu'elle émet, ou de vérifier celle des documents qu'elle reçoit.

De même, lorsque ces documents sont attachés à une notion de consentement et de signature par un tiers, cette même organisation devra vérifier l'identité de son interlocuteur (et prouver la sienne par la même occasion, dans un échange réciproque).

Le développement des technologies de l'information, les smartphones et internet a fortement accéléré celui de la signature électronique, dont le marché (vente de services et matériel) a été multiplié par près de quatre sur les cinq dernières années pour dépasser en 2020 les trois milliards de dollars. Cette forte croissance semble vouloir perdurer encore quelques années avec des projections atteignant 6 milliards de dollars en 2026 (https://www.fortunebusinessinsights.com/industry-reports/digital-signature-market-100356). La signature électronique vise à certifier l'authenticité d'un document, et éventuellement apporter une preuve de consentement par un tiers, il s'agit d'un marché différent de celui de la sécurité des échanges, se basant lui sur des technologies de chiffrement et du cryptage de l'information.

Poussé par le marché, la réglementation a dû s'adapter pour fournir un cadre réglementaire relativement clair à partir de 2014 avec l'arrivée des normes européennes eIDAS. Ces normes autorisent différents types de solution techniques. Pour diverses raisons, le marché s'est pour l'instant construit essentiellement autour des solutions reposant sur l'émission de certificats et le recours à des tiers de confiance. Ces dernières, complexes dans leur fonctionnement, sont utilisées car elles répondent aux exigences réglementaires requises pour la signature de documents très engageants (actes notariés, marchés publiques, contrats d'assurance vie, etc.). Cependant, l'utilisation de ces tiers de confiance présente beaucoup de contraintes, et en particulier des coûts élevés, pour des documents ne nécessitant qu'une signature simple qui est de très loin la signature la plus utilisée au regard des besoins du marché.

« Nous estimons que les entreprises ne signent qu'une infime minorité de leurs productions documentaires »

Nous constatons en effet qu'il est rare de rencontrer des entreprises, même parmi les plus grandes, capables de signer des documents de manière unilatérale pour moins de 20 centimes le document, et de manière bilatérale pour moins d'un euro. Dans les faits, les coûts et contraintes associées aux principales solutions actuelles de signature électronique ont pour effet de limiter les signatures par les entreprises de leurs productions documentaires; souvent seuls les contrats clients sont signés.

Pourtant, il subsiste toujours dans la relation client de nombreux contentieux associés aux devis, aux factures émises, aux relevés de compte, aux certificats d'achat, d'assurance ou de propriété, etc. Au sein de l'entreprise, les systèmes de paraphes internes, ou les formulaires RH (tel que les demandes de congés ou les dépôts des notes de frais) ne sont par ailleurs que rarement signés de manière électronique, malgré leur valeur engageante.

Pourquoi ? Principalement à cause du coût des solutions de signature électronique « traditionnelle », qui obligent les entreprises dans leurs analyses coûts / bénéfices à ne privilégier que les documents à forte valeur ou ceux astreints à une obligation réglementaire (tels que les contrats d'assurance vie ou les fiches de paye).

1.2 Une alternative à connaitre : la signature électronique sur blockchain

L'utilisation de la technologie blockchain apporte aujourd'hui une alternative extrêmement intéressante au recours à des prestataires tiers de confiance. Elle permet en effet de se substituer à ces tiers pour bénéficier des services d'horodatage, de stockage de la preuve et de l'historique des actions prises pour vérifier l'identité de l'émetteur original et des éventuels cosignataires d'un document.

Les avantages de la signature électronique sur blockchain, parfois aussi appelée notarisation ou ancrage documentaire sur blockchain, sont nombreux :

- *Réduction de coût drastique* : la signature électronique sur blockchain permet de réduire drastiquement le coût unitaire de la signature d'un document. Dans un contexte de signature massive et unilatérale (ex : signature de milliers de factures sortantes), nous estimons que les coûts unitaires peuvent être divisés par dizaines ;
- *Preuve publique* : la preuve devient publique, un tiers peut aisément aller vérifier par lui-même la véracité d'une signature. De plus, le fonctionnement de cette preuve et de la blockchain sous-jacente est le même dans tous les pays du monde, pour tous ses utilisateurs ;
- *Confidentialité* : il n'est plus nécessaire d'envoyer les documents aux tiers de confiance. La blockchain ne stocke que les éléments de preuves, le document reste donc en toute confidentialité sur votre réseau d'entreprise ;
- *Format universel* : la signature électronique sur la blockchain permet de signer tous types de documents (morceaux de musiques, photos, plans d'architecture…), et ce quel qu'en soit le format (pas uniquement des PDF). De plus, le document ne transitant pas sur les réseaux, il n'y a plus de limite quant à la taille des documents pouvant être traités ;
- *Pérennité* : la signature initiale se suffit à elle-même, elle ne devient pas caduque dans le temps, à la différence des signatures avec certificats qui doivent être renouvelés régulièrement et dont on doit vérifier la possible révocation ;
- *Non dépendance à un tiers* : l'approche blockchain permet d'éviter le recours à un tiers de confiance et aux risques associés : risque de faillite, changements de stratégie produit ou tarifaire, brèche de sécurité.

La signature électronique sur blockchain se démocratise, mais reste cependant encore confrontée à des difficultés de mise en œuvre :

- Peu de DSI ont en interne les compétences requises pour créer leurs propres API d'intégration/ connecteurs de signature électronique sur blockchain ;
- La signature de document en masse au sein d'une unique transaction blockchain pour de très faibles coûts nécessite de maitriser le concept d'arbre de Merkle, une structure de données encore méconnue ;
- L'utilisation d'une blockchain publique nécessite de payer des frais de transactions dans le crypto-actif de référence de la blockchain. Ces montants sont très faibles et ne sont pas un problème en soi. Ils nécessitent cependant l'obtention préalable de crypto-actifs, ce qui demande un certain niveau de compétence de la part des équipes comptables et financières ;
- La gestion du lien entre l'identité numérique et l'identité réelle des signataires est à la charge de l'entreprise qui se doit de mettre en place ses propres méthodes d'authentification (email, SMS, etc.).

Il est probable que dans les années à venir les plus grands groupes de sociétés auront développé en interne leurs propres services de signature électronique sur blockchain, en réutilisant des composants logiciels – sous licence ou en open source – pour signer massivement leurs productions documentaires.

2. La blockchain : son fonctionnement

2.1 Introduction : la blockchain

La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle.

Elle constitue une base de données sécurisée et distribuée qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création.

La blockchain est par définition une solution collaborative, qui n'a d'intérêt que si elle est utilisée par une communauté. Plus une blockchain est utilisée, plus sa communauté est large, plus sa sécurité est importante. Ses différents utilisateurs se partagent à travers elle des données, sans intermédiaire, ce qui permet éventuellement à chacun de vérifier la validité de la chaîne. A l'inverse d'une solution centralisée où les données sont stockées sur les seuls serveurs d'une seule entreprise, ici les données sont dupliquées et stockées sur les serveurs de tous les acteurs participant au réseau blockchain, c'est ce que l'on appelle son aspect distribué.

La technologie blockchain repose sur les principales caractéristiques suivantes :

- La **décentralisation** : un réseau pair à pair où chaque nœud du réseau remplit une ou plusieurs fonctions ;
- La **transparence** : l'historique des transactions est consultable en permanence par n'importe qui via une connexion internet et un explorateur de blockchain, le code source d'une blockchain publique est ouvert et consultable par tous ;
- La **fiabilité :** la blockchain repose sur des mécanismes de cryptographie éprouvés et extrêmement robustes, tels que la gestion de binômes clés publiques/clés privées et des fonctions de hachage. De plus, les transactions sont toutes validées par des algorithmes (que l'on appelle consensus) avant d'être partagées au sein de blocs de données;
- L'**immuabilité** : une fois insérée dans la blockchain, une transaction est infalsifiable, y compris par des acteurs malveillants qui participeraient au réseau ;
- L'**automatisation** : les transactions sont exécutées de manière autonome par des programmes informatiques sans recours à un tiers.

En ce qui concerne la signature électronique, c'est la fonction d'immuabilité de la blockchain qui nous intéressera. En effet, la blockchain garantit l'intégrité des preuves que nous allons y déposer, tout en les horodatant. Elle apporte la fiabilité exigée par les normes eIDAS, et sa grande transparence permet de facilement présenter les preuves à des tiers, voire éventuellement à un tribunal.

D'un point de vue technique, il est intéressant de noter que la technologie blockchain utilise les mêmes mécanismes cryptographiques que les solutions de signature électronique « standards » basées sur une infrastructure technique de type PKI (Public Key Infrastructure), à savoir les algorithmes de cryptographie à clés publiques et les fonctions de hachage.

2.2 Les différentes blockchains

Une blockchain correspond à un réseau communautaire animé par des participants. Ce réseau peut être fermé, limité à quelques personnes ou entités, et a priori spécifique à un usage particulier. C'est ce que l'on appelle une blockchain privée.

En premier lieu, dans le contexte de la signature électronique, nous recommandons d'utiliser une blockchain publique, ouverte à tous, et dont le fonctionnement est clair et documenté et dont le code est open source. Une blockchain publique fonctionne de la même manière pour tous ses utilisateurs, dans tous les pays. Son fonctionnement est donc compris de nombreux experts qui peuvent au besoin venir le présenter devant les tribunaux. De même, nous recommandons le recours à une blockchain reconnue, car plus une blockchain publique est utilisée et son nombre de participants élevé, plus ses mécanismes de sécurité seront forts, facilitant ainsi la démonstration de sa fiabilité, potentiellement au cours d'une procédure judiciaire.

A ce titre, nous recommandons d'utiliser une blockchain publique dont la capitalisation de marché – qui est une manière simple d'estimer la popularité d'une blockchain - est supérieure au milliard d'euros ; il en existe une douzaine à l'heure où ces lignes sont écrites[1].

Un deuxième critère nous parait intéressant à prendre en compte, en particulier pour les institutions et organisations de toutes tailles qui se lancent dans une démarche de Responsabilité Sociale et Environnementale. Il s'agit de l'efficience écologique de la blockchain, et donc du « consensus » qu'elle utilise pour valider les transactions.

Ce que l'on appelle consensus correspond aux algorithmes internes à la blockchain utilisés pour valider et transmettre les informations parmi les membres de la blockchain. Chaque blockchain fonctionne de manière légèrement, voire totalement différente, de ses voisines.

Les blockchains historiques, telles que Bitcoin ou Ethereum, fonctionnent sur un consensus appelé « Proof of Work », mettant en concurrence l'ensemble des membres du réseau pour une grande sécurité mais qui nécessite une forte consommation de ressources informatiques et énergétiques.

Certains pourront préférer des blockchains fonctionnant sur d'autres principes, comme par exemple le « Proof of Stake » et ses variantes ou seul un nombre restreint de membres de la communauté, qui dans certaines blockchains sont par exemple tirés au sort, seront à un instant T en charge de valider les transactions. La consommation électrique est des centaines, voire des milliers, de fois plus réduite. Si certains pourront y voir un risque légèrement plus élevé d'un point de la sécurisation du réseau de la blockchain, d'autres y verront un engagement écoresponsable.

Un troisième critère doit être pris en considération, celui de la gouvernance de la blockchain. Il est important de connaitre les principaux membres de sa communauté, comment elle peut évoluer et qui décidera de ses nouveaux apports. En d'autres termes, quelles sont les probabilités que la blockchain puisse bénéficier d'améliorations, et donc quelles sont les chances que vous ayez besoin dans quelques années de changer de blockchain ou non. Il convient aussi de vérifier s'il existe un risque de défaillance globale de la blockchain suite à la possible défaillance d'un acteur en particulier. Nous recommandons d'analyser aussi le risque d'ingérence

[1] La capitalisation de marché correspond à la valeur totale en €uros de l'ensemble des « *coins* » , la cryptomonnaie native à la blockchain, émis . Capitalisation =nombre de coins x valeur de marché du *coin*. Vous trouverez une liste, a priori mise à jour en temps réel sur le site https://coinmarketcap.com/fr/coins/. Au 03/06/2020, le top 10 incluait notamment les blockchains Bitcoin, Ethereum, Ripple, EOS, Cardano ou encore Tezos.

politique dans la vie future d'une blockchain, ainsi que la localisation des participants et principaux utilisateurs d'un réseau. Pour un niveau de service équivalent, nous recommandons ainsi pour des raisons de souveraineté à une institution publique française de plutôt étuider une blockchain comme Tezos (dont une partie importante de la R&D et des utilisateurs est originaire de France et d'Europe) que d'autres blockchains, par ailleurs prometteuses, dont la plupart des participants et des serveurs sont en majorité situés sur le territoire chinois ou américain.

Finalement, et selon la nature de vos projets, des arguments plus techniques tels que la vitesse de transaction (c'est-à-dire le temps requis pour recevoir la confirmation d'une signature), le coût d'une transaction (important si vous ne souhaitez pas mutualiser vos signatures), la qualité du langage de développement, ou la capacité de développer des fonctions avancées en utilisant des smart contract (ce que la blockchain Bitcoin ne sait par exemple pas proposer) peuvent faire la différence.

2.3 La fonction de hachage, source de la preuve

La signature électronique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.

Les fonctions de hachage cryptographique permettent de garantir l'**intégrité** d'un document de par leurs propriétés d'irréversibilité et d'unicité (dite de « résistance aux collisions »). En effet, une fonction de hachage produit un résultat (ou hash) de taille fixe (quelle que soit la taille du document fourni, la fonction retourne toujours un résultat de même taille). Aussi, pour le même exact document, le hash calculé sera toujours exactement le même :

- L'irréversibilité de cette fonction signifie qu'il est impossible, compte tenu des outils algorithmiques et informatiques actuels, de réussir à trouver le document fourni à partir du résultat de cette fonction ;
- La résistance aux collisions signifie qu'il est impossible de trouver deux documents qui aboutissent au même hash ;
- De facto, si deux documents donnent le même hash, c'est qu'ils sont identiques ;
- Horodater un hash dans une blockchain correspond à horodater le document. Signer le hash correspond à signer le document.

Vous trouverez ci-dessous des exemples de hash générés en utilisant l'algorithme SHA256[2], vous constaterez qu'à la moindre différence dans le contenu d'origine, le résultat est très différent.

Contenu d'origine	Hash généré en SHA256 (64 caractères)
bonjour	2CB4B1431B84EC15D35ED83BB927E27E8967D75F4BCD9CC4B25C8D879AE23E18
Bonjour	9172E8EEC99F144F72ECA9A568759580EDADB2CFD154857F07E657569493BC44
Bonjour!	083DE31AC1FA14F95671A6E39CC6C72D8FED1590B2A51759BC3F54A76B4169C4
Ceci est une phrase plus longue	E909641E7203A7FB25754D14FE2FFE45E043BF9FA63E2597768C7E975B5D1592
Ce livre blanc dans sa version PDF du 30/05/2020	839D56A1BA8CECF8F4B204476AF4F5B0C08DAB322D22D7CEB059F38444B5F871

Les fonctions de hachage sont très utilisées dans les protocoles blockchain. Elles servent ainsi à générer des signatures pour authentifier chaque transaction, à garantir un lien entre l'adresse d'un utilisateur de la blockchain et sa clé publique, à identifier une transaction ou un bloc ou encore à lier les blocs de la blockchain entre eux de manière à garantir l'intégrité de cette blockchain.

[2] Vous pouvez vérifier par vous-même, de nombreux sites sur internet proposent des générateurs de hash en ligne, comme par exemple https://passwordsgenerator.net/sha256-hash-generator/

Dans un contexte de notarisation de documents sur une blockchain, il est très intéressant d'utiliser un arbre de Merkle[3] pour pouvoir stocker au sein de cet arbre le résultat du hachage d'un nombre important de documents et d'enregistrer uniquement sur la blockchain la valeur de la racine de l'arbre. Cela présente l'avantage de réduire considérablement le volume de données à stocker sur la blockchain ainsi que le nombre de transactions à réaliser pour enregistrer ces données sur la blockchain, tout en garantissant l'intégrité de chaque document.

2.4 L'authentification du signataire

La cryptographie à clés publiques permet de garantir l'**authentification** de l'auteur d'un document via sa signature électronique. Ce système fonctionne avec deux clés, une clé publique connue de tous et une clé privée maintenue secrète par son propriétaire. C'est cette clé privée qui permet à une entité de signer une demande de transaction et donc de prouver qu'elle en est à l'origine. La clé publique permet à une autre entité du système de vérifier l'authenticité de la signature.

Il faut cependant indiquer que les clés publiques sont des chaines de caractères générées par algorithme, n'indiquant pas le nom de leur détenteur[4]. Il est donc de la responsabilité du détenteur d'une clé de communiquer sur l'association de celle-ci à son identité propre (s'il le souhaite).

Dans un protocole blockchain ce système permet de garantir l'authenticité de chacune des transactions injectées dans cette blockchain.

D'un point de vue technique la signature électronique d'un document consiste à signer via un système cryptographique à clés publiques le hash d'un document résultant de l'application d'une fonction de hachage sur ce document.

Comme évoqué précédemment la technologie blockchain dispose nativement de ces mécanismes cryptographiques et les utilise pour garantir l'intégrité et l'authenticité des transactions intégrées dans son réseau. Ainsi, cette technologie est parfaitement apte à être utilisée pour signer électroniquement des documents.

3. La valeur probante de la signature électronique sur la blockchain

3.1 La signature électronique et la technologie blockchain

La signature électronique est un ensemble de mesures techniques qui visent à garantir l'intégrité d'un document et d'en authentifier son auteur. Cette dernière est donc obligatoirement liée à un document mais également à la personne qui l'appose. Ainsi, la signature électronique a pour objectif de démontrer à un tiers que le document signé a été approuvé par une personne identifiée.

La blockchain quant à elle fonctionne comme un vaste registre public intégrant l'ensemble des transactions effectuées par ses utilisateurs depuis sa création. Ces **transactions** sont regroupées à l'intérieur de blocs qui

[3] L'arbre de Merkle est une structure historiquement utilisée par les protocoles blockchain pour organiser le stockage des transactions au sein de chaque bloc. Il s'agit d'une méthode permettant de structurer des données en vue d'y accéder et d'en vérifier l'intégrité plus rapidement tout en minimisant l'espace de stockage de ces données. Elle porte la dénomination d'arbre du fait que cette structure organise les données en les regroupant par deux, donnant ainsi la forme d'un arbre inversé.

[4] Ce pseudo-anonymat permet une signature électronique compatible avec les règles du RGPD européen (Règlement Général sur la Protection de Données).

sont ordonnés du plus ancien au plus récent. Chaque bloc contient des informations relatives au bloc précèdent de sorte qu'il est impossible de modifier un bloc sans avoir à modifier toute la blockchain en aval. Les utilisateurs peuvent télécharger l'intégralité de la blockchain et vérifier à tout moment son intégrité. Le contrôle de la Blockchain est donc décentralisé. Prenons l'exemple de blockchain Bitcoin, ainsi lorsqu'un utilisateur souhaite transférer une valeur à un autre utilisateur, il va **signer** une transaction avec une clé privée qu'il est le seul à connaitre et renseigner l'adresse Bitcoin de l'utilisateur bénéficiaire. Des mineurs[5] possédant la copie complète de la blockchain vont alors vérifier la validité de la transaction et sa conformité vis-à-vis de l'historique de la blockchain. Si la blockchain confirme ensuite que l'utilisateur possède le solde de crypto-actif nécessaire à sa transaction (pour rémunérer les mineurs), la transaction sera donc rajoutée au nouveau bloc de la chaine.

En outre, il convient de préciser que les informations objet des transactions sont « ancrées » dans la blockchain au moyen de différentes mesures de sécurité, sachant que techniquement ce ne sont ni les informations, ni les documents qui sont stockés en tant que tels dans la blockchain mais uniquement leur **empreinte numérique (dite « hash »)** inscrite de façon irréversible, immuable, intangible.

Dès lors, la signature électronique sur la blockchain est un ensemble de mesures techniques qui vise à sceller une transaction permettant ainsi d'authentifier la signature.

Eu égard aux garanties précitées fournies par la blockchain, on peut s'interroger sur la force probante de la signature électronique sur la blockchain comme mode de preuve.

3.2 Les réglementations encadrant la signature électronique et sa force probante

A ce jour, il n'existe aucune règlementation française spécifique portant sur la signature électronique sur blockchain. Néanmoins, les législateurs se sont penchés il y a déjà quelques années sur les questions liées au moyen de preuve d'un écrit électronique ou d'une signature électronique. Leurs réponses sont à prendre en considération pour les besoins de la problématique soulevée dans notre livre blanc.

3.2.1 La législation française

Le Code civil français consacre le principe de la **liberté de la preuve** dans son article 1358, ainsi la preuve peut être établie par tout moyen notamment en droit civil et commercial.

Cette liberté de la preuve est en outre expressément prévue par la loi pour les actes juridiques dont le montant est inférieur à 1.500 euros. Ainsi, **sont concernés de très nombreux documents papier édités au quotidien par les entreprises**, tels que les factures aux faibles montants éditées et adressées aux consommateurs (ex. téléphonie), des devis pour des prestations au budget modéré, ou encore des contrats portant sur des produits dont la valeur est inférieure à 1500 euros. L'écrit sur support papier formalisé à travers les documents précités dispose ainsi d'une force probante.

Or, l'article 1366 du Code civil donne la même force probante à l'écrit électronique qu'à l'écrit sur support papier, sous réserve néanmoins qu'il réponde à deux conditions, à savoir que soit **identifiée** la personne dont il émane et que l'écrit soit établi et conservé dans des conditions de nature à assurer son **intégrité**.

[5] Les participants d'une blockchain publique peuvent se donner des rôles différents. Certains participeront plus activement à son bon fonctionnement, et prêteront leur infrastructure technique (temps de calcul, espace de stockage, bande passante et électricité) pour participer au processus de validation et de diffusion des transactions. Ils sont pour cela récompensés par la distribution de crypto-actifs générés par la blockchain. Par analogie avec les mineurs d'or, qui par leur labeur ramènent des pépites à la surface et créent de la valeur, les membres validateurs de Bitcoin sont appelés des mineurs. D'une blockchain à l'autre cette appellation peut varier, mais le principe reste le même.

Par ailleurs, l'article 1367 du même code pose les principes suivants :

- La signature à valeur juridique identifie son auteur ;
- Si la signature est électronique elle doit consister en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ;
- Ce procédé est présumé fiable si la signature est qualifiée au sens du règlement européen eDIAS (voir section 3.2.2. ci-après).

Enfin, si la loi ne définit pas la notion d'intégrité, la doctrine a pu affirmer que l'intégrité de l'écrit électronique suppose que ce dernier ne puisse être modifié ou que les modifications apportées soient visibles.

Dès lors, **la démonstration d'un procédé fiable d'indentification dont l'intégrité est assurée, permet de déterminer la valeur juridique d'une signature électronique**.

Ainsi, il est intéressant de transposer ces textes à la signature électronique sur blockchain. En effet, et comme indiqué à la section 3.1 ci-dessus, lorsqu'un utilisateur réalise une transaction sur la blockchain, il utilise une clé privée, c'est-à-dire qu'il signe électroniquement sa demande de transaction. De l'autre côté, le destinataire de la transaction possède lui aussi la clé publique du signataire (elle est unique et associée à la clé privée)[6] qui garantit l'identité du signataire. En associant ces deux clés, la transaction sera alors émise sur la blockchain. La preuve de cette transaction est immuablement inscrite sur le « registre », dont tous les utilisateurs disposent d'une copie : ce dispositif garantit ainsi la sécurité et l'authenticité des opérations.

Outre la législation en vigueur précitée, il est intéressant de relever que plusieurs initiatives françaises sont favorables à la reconnaissance de la force probante légale de la technologie blockchain au sens large du terme. Il en va par exemple ainsi du rapport de France stratégie (institution autonome placée auprès du Premier ministre) de juin 2018 portant sur les enjeux des blockchains, d'une question parlementaire datant de juillet 2019 à l'attention du Ministère chargé de l'économie, des finances et du numérique (question n°22103), ou encore de l'adoption de la loi PACTE en mai 2019 encadrant les levées de fonds réalisées en crypto-monnaies (dites « ICO »).

3.2.2 La réglementation européenne

En droit européen, les problématiques relatives aux documents et à l'identification électroniques sont abordées par le règlement n° 910/2014 du 23 juillet 2014 dit « eIDAS ».

Ce texte définit trois niveaux de signatures électroniques qui ont toutes un intérêt selon les différents besoins et activités d'une entreprise : la **signature dite simple**, la signature avancée et la signature qualifiée. Le règlement n'encadre pas précisément la signature électronique simple et ne fait que l'évoquer. Cela concerne les hypothèses suivantes : une signature à la main scannée, une case cochée sur un site internet, une signature réalisée sur la tablette d'un livreur, etc.

[6] Le concept du binôme clé publique / clé privée, que l'on appelle cryptographie asymétrique, est beaucoup plus ancien que la blockchain, et est utilisée depuis des décennies pour gérer des mots de passe, des certificats, ou des connexions internet sécurisée. Pour en faire une analogie très simplifiée, la clé publique correspondrait à l'IBAN d'un compte bancaire - que tout le monde peut voir, et la clé privée correspondrait à un code PIN - élaboré et confidentiel. Sans le code PIN, il est impossible d'émettre une transaction.

A contrario, le règlement pose des conditions précises concernant la validité des signatures avancées et qualifiées. Ainsi, l'article 26 du règlement exige que la signature avancée réponde aux conditions suivantes : (a) être liée au signataire de manière univoque ; (b) permettre d'identifier le signataire ; (c) être créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et (d) être liée aux donnés associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

En outre, l'article 25 du règlement définit la signature qualifiée. La doctrine affirme ainsi que la signature qualifiée doit répondre (a) aux critères de la signature électronique avancée ; (b) être crée à l'aide d'un dispositif de création de signature électronique qualifiée et (c) reposer sur un certificat qualifié de signature électronique délivré par un prestataire de confiance qualifié. Ce type de signature très sécurisée bénéficie d'une présomption de fiabilité.

En conséquence, la signature électronique sur blockchain s'apparente selon nous à la signature simple au sens du règlement eIDAS. Or, ce niveau de signature bénéficie d'une valeur probatoire.

En effet, le règlement eIDAS ne préconise pas de niveau de signature électronique spécifique selon la nature des transactions. En outre, ce texte affirme en son considérant 27 le principe de neutralité technologique : "*Le présent règlement devrait être neutre du point de vue de la technologie. Les effets juridiques qu'il confère devraient pouvoir être obtenus par tout moyen technique, pour autant que les exigences posées par le présent règlement soient satisfaites. ".*

De même, l'article 25 du règlement dispose « *l'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée* ».

Dès lors, les signatures électroniques sont légales dans l'Union Européenne, et ce quelle que soit la technologie sous-jacente, y compris la technologie blockchain dont les garanties en termes de sécurité ont été rappelées à la section 2 ci-dessus.

Outre, les réglementations précitées, il est intéressant de souligner que plusieurs pays ont exprimé leur volonté de légiférer afin d'encadrer la technologie blockchain. C'est par exemple le cas de l'Italie qui, avec l'adoption d'une loi en janvier 2019, a reconnu la force probante de l'horodatage électronique via la blockchain. L'horodatage consistant à apposer sur un fichier ou un document une date fiable et certaine. C'est également le cas de plusieurs États américains tels que l'Illinois et l'Arizona, qui ont adopté des législations en 2018 et janvier 2020 reconnaissant la valeur légale des transactions sur la blockchain.

3.3 La recevabilité de la signature électronique en justice

3.3.1 La jurisprudence française

L'article 1368 du Code civil dispose : « *A défaut de dispositions ou de conventions contraires, le juge règle les conflits de preuve par écrit en déterminant par tout moyen le titre le plus vraisemblable*. »

Cet article, qui confirme l'équivalence probatoire entre un écrit papier et un écrit électronique, confère au juge le pouvoir souverain d'apprécier quelle est la preuve littérale la plus vraisemblable, en fonction du cas d'espèce qui lui est soumis, notamment selon le mode de conservation mis en œuvre.

En conséquence, et en l'absence de précisions sur les conditions d'application des critères de force probante d'un écrit électronique, l'admission de celle-ci est appréciée au cas par cas par les juges. La jurisprudence

apprécie ainsi de façon casuistique les conditions donnant une valeur probante à la signature électronique. La signature électronique simple a par exemple été considérée comme une preuve valable dans le cadre de mandats signés électroniquement (Cour d'Appel Aix-en-Provence juin 2014, Cour d'Appel Caen mai 2015 et Cour d'Appel Nîmes octobre 2015). Néanmoins, les juges s'accordent sur le fait qu'une signature électronique a valeur probante dès lors qu'elle est intègre et fiable. Les juges sont donc particulièrement attentifs à la qualité des pièces produites (Cour d'Appel Aix-en-Provence – septembre 2019).

Or, dans le cadre de contentieux de plus en plus nombreux impliquant l'usage d'une technologie avancée, il est d'usage pour les parties concernées de prendre soin de faire une démonstration simple et cohérente, vulgarisant les termes techniques inutiles à la compréhension du magistrat. Le recours à l'expertise technique n'est bien évidemment pas systématique. Ainsi, il pourra être justifiée devant les tribunaux que la blockchain est un procédé fiable et sécurisé, ce qu'a confirmé une décision de justice récente rendue en Chine.

3.3.2 Exemple étranger

En juin 2018, le tribunal de Hangzhou, spécialisé dans les affaires liées à internet, a accepté pour la première fois, dans le cadre d'un procès, une preuve ancrée dans la blockchain. En l'espèce, un litige opposait une entreprise de médias à un tiers à qui elle reprochait d'avoir contrefait ses droits de propriété intellectuelle sur son site internet. Elle en demandait réparation en justice.

Comme moyen de preuve, la plaignante avait capturé le code source du site en cause puis enregistré les données ainsi collectées sur une plateforme de dépôt de preuves basée sur la technologie blockchain, permettant d'encoder des éléments numériques (images, codes sources, pages web etc.) et de les horodater afin de se préconstituer la preuve électronique que : (a) celui qui a encodé ces éléments numériques en est bien le propriétaire ; et (b) l'encodage s'est fait à telle date et à telle heure, permettant ainsi de justifier d'une antériorité en cas de contestation.

La juridiction chinoise a considéré que ce type de moyen de preuve était recevable, si le procédé est fiable, authentique et confère une date certaine, en précisant ceci : « *Le tribunal estime qu'il devrait rester ouvert et neutre sur l'utilisation de blockchain des analyses au cas par cas. Nous ne pouvons pas exclure la blockchain simplement parce que c'est une technologie complexe mais nous ne pouvons pas non plus en généraliser l'utilisation comme mode de preuve juste parce qu'elle est inviolable et traçable. Dans le cas d'espèce précis, l'utilisation d'une plateforme de blockchain tierce, fiable et sans conflit d'intérêts, permettait de constituer le fondement juridique de la preuve d'une violation de droits de propriété intellectuelle* ».

Suite à la décision du tribunal chinois d'Hangzhou, la Cour Suprême chinoise a confirmé le jugement dans un arrêt de septembre 2019 en reconnaissant la valeur de la preuve ancrée sur la blockchain si « *les données numériques soumises comme preuve par les parties concernées ont été collectées et stockées via une blockchain avec signatures numériques, horodatages fiables, vérification de la valeur de hachage ou via une plateforme de dépôt numérique et qu'elles peuvent prouver l'authenticité de cette technologie ainsi utilisée* ».

En conséquence, et au regard de la réglementation et de l'appréciation qui en est faites par les tribunaux, la signature électronique sur blockchain remplit selon nous les conditions nécessaires pour bénéficier d'une force probatoire au sens d'une signature électronique simple.

3.4 Cas d'usage

3.4.1 La preuve de l'antériorité en matière de propriété intellectuelle

Les grands comptes travaillent au quotidien sur des projets de R&D ou des projets innovants impliquant des questionnements réguliers liés à la protection des concepts émergents et leur formalisation. Les équipes en charge de l'innovation ne disposent pas toujours des réflexes juridiques ou ne peuvent bénéficier du soutien des juristes internes.

Ne sachant pas à quel stade du processus de création il convient de protéger ces créations ou souhaitant éviter d'engager des frais d'enregistrement pour des projets susceptibles de rester au point mort ou encore souhaitant gagner du temps en ne faisant pas intervenir un organisme tiers, ces équipes prennent souvent le risque de ne pas conserver la preuve de l'antériorité des créations. Or, certaines de ces créations peuvent a posteriori se révéler pertinentes.

A défaut de conserver les preuves de leurs travaux ou créations, les entreprises se retrouvent parfois dans l'impasse face à des concurrents mieux organisés. Rappelons à ce titre que le Code de la propriété intellectuelle prévoit que la qualité d'auteur d'une création appartient (sauf preuves contraires) à celui ou ceux sous le nom de qui l'œuvre est divulguée.

Pour pallier ce risque, le stockage sur la blockchain d'une création se concrétisant par l'ancrage d'une « empreinte numérique » unique, conservée de façon immuable peut s'avérer être une option satisfaisante. Seule cette empreinte numérique sera conservée dans la blockchain. Le changement d'une donnée pourrait générer une empreinte complètement différente. La vérification d'une empreinte correspondante à une œuvre permet donc de s'assurer que les informations conservées dans la blockchain sur ladite création ne sont pas modifiées.

Lors d'un contentieux, apporter la preuve de l'inscription d'une œuvre sur la blockchain pourrait jouer un rôle probatoire substantiel. Bien que la blockchain ne dispose ni d'une reconnaissance légale stricto sensu en tant que preuve, ni d'une reconnaissance « officielle » par les tribunaux, elle emprunte tout de même des procédés cryptographiques de la signature et de l'horodatage électronique.

En outre, la liberté de la preuve inhérente aux actions en contrefaçon de droits d'auteur ou devant le tribunal de commerce en matière de concurrence déloyale devrait permettre d'utiliser la blockchain comme mode de preuve lors d'un procès, s'il est démontré que le procédé est fiable, authentique et confère une date certaine.

3.4.2 La preuve de la date d'émission des factures

En tant que grand compte, vous établissez une grande quantité de factures pour vos clients. Vous pouvez souhaiter apporter une preuve d'authenticité de ce document pour vous pré-constituer une preuve (édition à telle date) en cas de litige face à des mauvais payeurs.

De plus, votre facture peut-être elle-même parfois utilisée comme un élément de preuve par son destinataire. Elle peut être un justificatif de domicile pour un particulier. Un justificatif d'une preuve d'achat pour un remboursement devant un assureur. Un justificatif comptable associé à des frais par une entreprise lors d'un contrôle fiscal.

Or, en matière de facture ou de tout autre pièce comptable, le code de commerce précise que la preuve est admissible en justice, libre et fiable sous réserve que cette pièce comptable présente les mentions obligatoires (articles 110-3, 123-33 et 441-9). Ceci vaut aussi bien pour la facture papier que la facture électronique, étant rappelé que la version électronique va selon la Loi de finances 2020 progressivement devenir obligatoire.

L'émetteur de la facture électronique n'est par ailleurs souvent pas le seul à s'intéresser à sa certification. Les réceptionnaires de cette facture ont eux aussi souvent intérêt à pouvoir en vérifier l'origine et l'authenticité, pour lutter contre tous types de fraude (arnaque au fournisseur, faux justificatif de domicile, etc.). La plupart des organisations ont mis en place des processus de contrôle, parfois extrêmement industrialisés. Les banques, pour ne citer que cet exemple, dépensent ainsi des dizaines de millions d'euros en France chaque année pour contrôler l'authenticité des factures utilisées comme justificatifs de domicile à l'ouverture d'un compte.

Plusieurs solutions sont utilisées, mais aucune n'a connu de succès. Le dernier essai du marché correspondait à une norme, le code 2D-DOC, consistant à ajouter un QR code unique sur chaque facture. Avec des coûts élevés et un taux d'usage limité, cette solution ajoute également d'autres contraintes, et notamment la nécessité de modifier le contenu des factures pour y trouver la place de rajouter ce nouvel élément.

Une solution de signature électronique sur blockchain apporte de nombreux avantages à ce cas d'usage :

- Aucun besoin de modifier le système d'information actuel ;
- Aucun besoin de modifier le format des factures ;
- La massification de la signature permet des coûts unitaires presque négligeables ;
- Il est facile de fournir à tout un chacun les moyens de vérifier l'authenticité de la facture.

4. Comment passer à la signature électronique sur Blockchain

Vous trouverez ci-dessous quelques pistes pour démarrer avec la signature électronique sur blockchain.

1) N'hésitez pas à apprendre, comprendre, et poser des questions

N'hésitez pas à nous contacter pour toute question que vous pourriez avoir, qu'elle soit d'ordre juridique, technique ou financière.

2) Définissez un périmètre documentaire cible simple

Nous vous recommandons de démarrer par un premier projet sur un périmètre restreint qui pourra être élargi par la suite. Il vous faut donc identifier les documents que vous souhaitez signer. Voici quelques idées pour définir ce périmètre :

- Limitez-vous à un projet de certification et d'horodatage de documents ne nécessitant pas le consentement d'un contre-signataire : facture, certificat de propriété ou d'achats, notes internes, documents de propriété intellectuelle, etc.
- Identifiez des documents pour lesquels la création d'une preuve d'authenticité est une vraie valeur ajoutée ;
- Dans la mesure du possible, travaillez sur un projet où la certification des documents peut se faire de manière massive et automatisée, le projet sera plus simple, et la valeur ajoutée plus grande.

Si vous utilisez déjà dans votre organisation des solutions de signature électronique, nous vous invitons à vérifier le niveau de signature requis pour chaque catégorie de document signé. S'ils nécessitent réellement une signature dite qualifiée ou avancée, excluez-les du périmètre pour l'instant. Pour les autres, examinez les coûts que représente les outils de signature que vous utilisez actuellement. S'ils sont importants, vous avez peut-être trouvé un excellent périmètre d'étude. Si en plus, ces documents ne sont signés que par votre organisation, sans besoin de recueil de consentement auprès d'un tiers, le cas d'usage est parfait.

3) Rédigez votre cahier des charges fonctionnel et technique

Nous vous conseillons de formaliser le cycle de vie des documents que vous envisagez d'horodater et signer, sans prendre en considération les contraintes de la signature blockchain :

- Quels outils IT génèrent le document ?
- A quel moment seront-ils signés ?
- Comment et où seront stockés les documents. Si vous souhaitez pouvoir présenter les documents devant un tribunal, il vous faut donc archiver une copie exacte du document qui aura été signé.
- Comment ces documents sont-ils transmis à leur destinataire ?
- Faut-il, et si oui sous quelle forme (site web, mobile…), mettre un outil à disposition de tiers pour procéder à la vérification d'un document ?
- Etc.

Sur les aspects techniques, nous vous invitons tout d'abord à prendre connaissance du fonctionnement d'une blockchain, afin de pouvoir choisir celle qui vous conviendrait le mieux.

Vous allez devoir héberger des clés sécurisées (ou externaliser leur stockage), et des questions de sécurité IT se poseront à vous. Cela est particulièrement vrai si vous souhaitez faire signer des particuliers, et donc procéder à une vérification de leur identité personnelle. Contactez nous pour découvrir les solutions envisageables dans votre contexte.

Si vous envisagez de construire votre propre plateforme en totale autonomie, vous allez aussi avoir besoin d'acheter quelques crypto-actifs pour payer les frais de transactions de la blockchain de votre choix. Votre direction financière se posera sûrement des questions quant à leur comptabilisation.

Finalement vous invitons ensuite à fixer vos contraintes en matière d'hébergement applicatif, de sécurité IT et de disponibilité de vos équipes. Préférez-vous ainsi une solution clés en main pour un métier sans avoir à vous préoccuper de la technologie, ou au contraire souhaitez-vous que vos équipes IT montent en compétences sur le sujet et aient l'occasion de mettre en œuvre par elle-même une solution ?

4) Créez ou achetez les composants logiciels qu'il vous faut

C'est ici qu'intervient l'ingénierie logicielle. Vous pouvez utiliser une solution proposée par un éditeur du marché, il y en a plusieurs, ou développer votre propre plateforme.

Si vous avez des compétences IT au sein de votre organisation et/ou si vous souhaitez conserver une indépendance vis-à-vis de fournisseurs de services, nous vous invitons à étudier la solution Tezos DigiSign, qui présente plusieurs avantages :

- Elle contient un grand nombre de composants qui devraient être suffisants pour vous permettre de démarrer rapidement un projet. Si vous connaissez déjà le sujet et avez des objectifs clairement fixés, ou si vous êtes accompagnés, vous pouvez espérer avoir de premiers résultats en moins d'un mois de projet ;
- Elle est gratuite, c'est une solution Open Source sans droit de licence associé ;
- Elle est personnalisable, c'est une solution Open Source. Elle s'intégrera ainsi facilement à un SI déjà en place ;
- Elle fonctionne nativement sur Tezos. Tezos est une blockchain d'origine française, de grande taille, sécurisée, développée dans un langage facilitant son audit par des tiers, écologiquement responsable et

disposant de principes de gouvernance clairs. Elle est donc parfaite pour servir d'outil de gestion et stockage de preuves numériques.

Nous vous invitons à contacter Sword Group[7], à l'initiative de ce projet, la fondation Tezos ou les équipes derrière ce livre blanc pour toute information sur la solution Tezos DigiSign.

5) Préparez-vous au changement

Vous allez offrir une nouvelle fonctionnalité à vos utilisateurs ou clients, il serait dommage de ne pas leur annoncer en la mettant en valeur.

Vous êtes sur le point aussi d'utiliser une technologie innovante, sur laquelle certains de vos collaborateurs vont sans doute vous questionner, soyez prêt à répondre à leurs questions.

6) Prévoyez un retour d'expérience … et éventuellement déployez plus largement votre plateforme

Ce projet était le premier du type que vous faisiez. Maintenant que votre plateforme de signature sur blockchain est en place, l'investissement requis pour signer de nouveaux types de documents complémentaires est très faible.

Est-il cependant justifié dans votre contexte ? La solution que vous avez mise en place est-elle la bonne ? Pour répondre à ces questions, nous vous invitons avant même la première mise en production à prévoir en interne une ou plusieurs réunions d'analyse de votre retour d'expérience.

[7] Pour les contacter, vous pouvez notamment utiliser l'adresse tezosdigisign@sword-group.com.

A propos de nous

Solegal est un cabinet d'avocats indépendant dédié à l'entreprise et à ses acteurs : créateurs, dirigeants, investisseurs et repreneurs. L'expertise technique de Solegal repose sur trois spécialités : le droit des affaires, la fiscalité et le droit de l'immatériel. Les besoins de nos clients ne s'arrêtant pas aux frontières de chacune de ces spécialités, nous proposons l'association de compétences la mieux adaptée à chaque client. Cette approche de la relation client permet à Solegal de proposer un accompagnement à forte valeur ajoutée, en particulier dans les domaines et secteurs suivants : Talents, Patrimoine, Digital & Tech, Entreprises de croissance, Entertainment & Sport et Professions réglementées. La technologie blockchain ayant investi ces secteurs professionnels et ne connaissant pas de frontière, c'est tout naturellement que le Cabinet Solegal s'est intéressé aux enjeux juridiques de la blockchain.
https://www.solegal.fr/positionnement/digital-tech/

Blockchain EZ est une société de conseil et d'intégration spécialisée dans les technologies des Blockchain. Notre nom l'indique : nous sommes un pure player Blockchain (et plus largement des Distributed Ledgers Technologies). Blockchain EZ se veut agnostique aux technologies : non seulement la blockchain n'est pas une solution qui s'adaptera à tous les besoins clients, mais en plus la concurrence au sein des multiples approches blockchain existantes et à venir nécessite une ouverture d'esprit et une veille constante, aucun d'entre elle n'étant parfaite. Blokchain EZ est une société de services capable d'intervenir à 360° sur les projets de ses clients : de la phase de conception à la mise en production et au-delà, de l'assistance technique à la vente de projets au forfait.
www.blockchain-ez.com

Ont participé à la rédaction de ce document :

Betty Sfez (bsfez@solegal.fr)
Avocat associé IT / DATA / IP. DPO externe. Speaker HEC Paris Executive Education

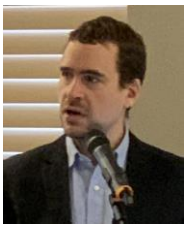
Betty Sfez intervient en droits de l'informatique, du numérique et de la propriété intellectuelle. Elle accompagne les sociétés technologiques ainsi que les entreprises utilisatrices dans le cadre de leurs projets SI et de transformation digitale : rédaction de contrats IT et commerciaux, audit RGPD, recommandations pour le déploiement de projets blockchain, cloud computing et big data, contentieux commercial, gestion de la cyber-fraude, etc. Betty Sfez conseille également ses clients dans leurs stratégies de protection des actifs immatériels et, plus généralement de l'innovation.

Guillaume Angeli
Avocat IT / DATA / IP

Guillaume Angeli intervient en droit du numérique et droit de la propriété intellectuelle. Il accompagne notamment les PME et les startups dans le cadre du développement de leurs projets e-commerce et marketplaces (rédactions de CGV/CGU/mentions légales et mise en conformité à la réglementation). Il assiste également les clients du cabinet en matière de gestion des droits d'auteur et suivi de portefeuilles de marques et de noms de domaine. Enfin, Guillaume Angeli intervient lors de contentieux en matière d'atteintes à l'e-réputation des entreprises et de ses dirigeants.

Vincent Chouteau (vincent.chouteau@blockchain-ez.com)
Expert technique Blockchain & Signature Electronique

19 ans d'expérience dans les métiers du conseil en informatique en tant que développeur, chef de projet, consultant puis directeur de projet. Vincent est historiquement un expert en matière de dématérialisation et de signature électronique. Crypto-investisseur averti, Vincent suit depuis plusieurs années de très près les évolutions du marché et de la technologie Blockchain. Il cofonde en 2019 Blockchain EZ et prend le rôle de directeur technique et d'architecte blockchain.



Alain Broustail (alain.broustail@blockchain-ez.com)
Consultant Senior, expert Blockchain & Dématérialisation

Alain bénéficie de 19 ans d'expérience dans le secteur du conseil et du logiciel. En 2011, il prend la responsabilité du pôle conseil/AMOA de Sword Group à Paris et monte une équipe de 60 consultants aujourd'hui dédiée aux problématiques de dématérialisation / gestion documentaire / partage de l'information. En 2018 Alain participe à ses premiers projets Blockchain, et en janvier 2019 il cofonde Blockchain EZ dont il assure depuis la présidence Consultant senior, il est habitué à accompagner les directions générales dans leurs processus de décisions. Conférencier expérimenté, professeur vacataire au CNAM sur le thème Blockchain & Ingénierie Documentaire, Alain anime aussi des formations Blockchain pour des associations professionnelles et des clients de tout type.