REVUE DE LITTÉRATURE : MISE EN PLACE DES CONTRATS INTELLIGENTS BASÉS SUR UN REGISTRE DISTRIBUÉ DE TYPE CHAÎNE DE BLOCS (*BLOCKCHAINS*)

Introduction

Pour plusieurs, la technologie des chaînes de blocs (ou *blockchains*) est en voie de devenir le cinquième paradigme de l'informatique, après l'ordinateur central (*mainframe*), l'ordinateur personnel (PC), l'Internet et la révolution du mobile et des réseaux sociaux (**Swan, 2015 à la p vii**). La Commission européenne la considère comme une « avancée majeure » et s'attend à « ce qu'elle fasse changer les services numériques et transforme les modèles économiques dans divers secteurs comme les soins de santé, l'assurance, la finance, l'énergie, la logistique, la gestion des droits de propriété intellectuelle ou les services publics » (**Commission européenne, 2018**). L'enthousiasme est partagé par le gouvernement canadien qui applaudit le « potentiel révolutionnaire » des chaînes de blocs pour le développement humain (**CRDI, 2017**).

D'importants acteurs du monde financier, de l'assurance et des entreprises se sont lancés dans des projets pilotes explorant le potentiel transformateur de cette innovation technique. Alors que ses défenseurs ne lésinent pas sur les perspectives prometteuses qu'annonce la mise en place de registres distribués « scellés » par des empreintes/signatures cryptographiques, attardons-nous dans un premier temps sur la mise en place des contrats intelligents basés sur des chaînes de blocs.

1. Les chaînes de blocs (*blockchains*) ou la technologie des registres distribués

Rappelons que la révolution Internet, tout en facilitant l'échange de données à l'échelle mondiale, repose fondamentalement sur l'hébergement de fichiers sur un serveur donné – qu'il soit local ou distant (*cloud computing*) – rendant les administrateurs systèmes et fournisseurs de services *cloud* responsables en ce qui concerne la sécurité, l'intégrité et la confidentialité des données stockées sur leurs dispositifs informatiques (pare-feu). Des protocoles sécurisés (HTTPS, SMTPS, POPS, IMAPS), basés sur des certificats numériques émis par des autorités de certification (AC) reconnues, assurent l'authentification, la confidentialité et l'intégrité des données en transit (p.ex. numéro de carte bancaire, mot de passe) lors des communications Web.

Une chaîne de blocs – concept appliqué pour la première fois par l'énigmatique Satoshi Nakamoto, l'inventeur du Bitcoin, dans l'architecture de son système de paiement électronique pair à pair (**Nakamoto, 2008**) – associe un ensemble de techniques, protocoles et outils préexistants pour constituer un registre distribué et sécurisé de toutes les transactions effectuées dans la chaîne depuis son démarrage. Plutôt que d'héberger les données sur un seul serveur, ou différentes données sur des serveurs différents, ce registre horodaté est formé d'un ensemble de mineurs ou nœuds de stockage, jouant le rôle d'autant de serveurs où sont enregistrées les mêmes informations/opérations en ordre chronologique. Afin de valider les nouvelles transactions, la chaîne de blocs en exige une vérification indépendante effectuée par chacun des nœuds (mineurs) du réseau, en hachant (chiffrant) un nouveau bloc de transactions en attente à partir de l'empreinte/signature unique (résultat de hachage) obtenue du bloc de transactions qui le précède immédiatement dans le temps. Une fois validée par un mineur, la solution est soumise aux autres nœuds du réseau, lesquels doivent l'approuver à une majorité simple (50% + 1) de la puissance de calcul (CPU) totale du réseau afin d'ajouter le nouveau bloc à la chaîne des transactions confirmées. Cette preuve de travail cryptographique (*proof of work* ou PoW) exige une grande puissance de calcul, décourageant les tentatives – coûteuses – de fraude. Et un hachage

irréversible (impossibilité de décrypter à rebours) protège contre la falsification des blocs de données d'ores et déjà incorporés à la chaîne.

Il peut donc exister plusieurs *blockchains* non interreliées, constituant autant de systèmes décentralisés ou registres distribués où sont consignées des transactions à des fins différentes (échange de cryptomonnaies, contrats intelligents). Lorsque l'accès à une chaîne de blocs est restreint à un certain groupe d'utilisateurs ou de membres, on parle d'une chaîne de blocs privée. Si tout le monde peut se constituer utilisateur ou mineur d'une chaîne de blocs donnée en installant une application « portemonnaie » (p.ex. Bitcoin) ou en greffant un matériel de minage (p.ex. Butterfly Labs, Bitcoin Ultra, CoinTerra) à la manière d'une carte graphique ou clé USB sur son poste de travail, il s'agit d'une chaîne de blocs dite publique.

Le concept de chaîne de blocs repose donc sur un mode de gouvernance décentralisé comptant sur le consensus majoritaire des utilisateurs du réseau : « Le bon fonctionnement des échanges est garanti par une organisation générale que tout le monde peut examiner car tout y est public : les protocoles de base, les algorithmes cryptographiques utilisés, les programmes les rendant opérationnels et les données des comptes. » (**Delahaye, 2014 à la p 2**) Nakamoto se posait en effet la question de savoir comment transiger de façon sécuritaire dans un monde numérique sans passer par un tiers de confiance ou organe central de contrôle (**Nakamoto, 2008**), tout en résolvant le classique « problème des généraux byzantins » (**Lamport et al, 1982**). De même que des généraux de l'armée byzantine (ou autre) demeurés loyaux doivent trouver moyen de collaborer à l'offensive malgré un certain nombre de traîtres tentant de les confondre avec des instructions contradictoires, « [un] système [informatique] doit être capable de maintenir sa fiabilité dans le cas où une part minoritaire des composants enverrait des informations erronées ou malveillantes pour contourner la vérification de la double dépense » (**Savoye, 2016**).

L'intégrité de la chaîne repose donc sur le « pari » voulant qu'aucun opérateur hostile ne détienne, à un moment donné, plus de la moitié de la puissance de calcul de toute la chaîne. Le risque d'une « attaque des 51% » dépend de la puissance de calcul totale de la chaîne et de sa répartition au sein des mineurs intégrés à la chaîne : plus le nombre de mineurs participants est élevé, plus la puissance de calcul totale peut être distribuée et plus il est difficile pour un seul acteur d'en obtenir un contrôle majoritaire. Cette possibilité n'est pas seulement hypothétique : en juin 2014, la coopérative des mineurs GHash.IO aurait justement dépassé le seuil des 51% de la chaîne Bitcoin (**Matonis, 2014**). Malgré le retrait volontaire des mineurs de GHash.IO dans l'intérêt de l'idéal communautaire (**Higgins, 2014**) et la cessation définitive des activités de la coopérative depuis le 24 octobre 2016 (**Danova, 2016**), cette percée donne à réfléchir sur l'implantation d'éventuels garde-fous pour éviter une attaque malicieuse des 51% (**Higgins, 2014**).

Une alternative pour valider la création d'un nouveau bloc de transaction sur une chaîne de blocs consiste à privilégier une preuve dite d'enjeu (*proof of stake* ou PoS) plutôt qu'une preuve de travail. Une preuve d'enjeu repose sur un consensus proportionnel non pas à la puissance de calcul (CPU) des mineurs, mais pondéré au degré de participation ou à la quantité de cryptomonnaies détenues dans le portefeuille virtuel des utilisateurs : « Plus un utilisateur dispose d'unités de compte de la blockchain, plus sa participation à la validation d'une transaction est importante » (**Rodriguez, 2017**), au sens où il aura plus de chances d'être

sélectionné comme le validateur pour le dernier bloc de transactions. Dans l'éventualité où cet utilisateur n'est pas intéressé ou disponible (p.ex. hors ligne), un deuxième validateur sera sélectionné, et ainsi de suite. Une sélection aléatoire pondérée opérant à chaque validation assure l'absence de monopole et le caractère distribué de la prise de décision. Peercoin (PPCoin) a été la première chaîne de cryptomonnaie mobilisant à la fois les preuves d'enjeu et de travail, à une empreinte écologique beaucoup plus réduite (**King & Nadal, 2012**).

Le dispositif de type chaîne de blocs innove par rapport aux supports technologiques « traditionnels » en ce qu'il apporte un niveau élevé de traçabilité et de sécurité dans les échanges en ligne, tout en réduisant les coûts de transaction.

Traçabilité – Étant donné que chaque nouveau bloc de transactions doit être confirmé à partir du hash obtenu du bloc précédent, un système horodaté à la chaîne se consolide avec le consensus partagé par tous les participants du réseau. La particularité d'une fonction de hachage (*hash*) – à la différence d'un chiffrement (*encryption*) – est bien l'irréversibilité des résultats que l'on ne pourra plus reconvertir aux chaînes de caractères originales. S'y ajoute une sécurité renforcée par :

1) l'invariabilité de la longueur des résultats de hachage (valeur de sortie) indépendamment de la taille des données originales (valeur d'entrée), et
2) la sensibilité des résultats de hachage aux menues différences (une modification mineure dans les données originales générera un résultat de hachage complètement différent).

Cette impossibilité de retrouver les données originales serait particulièrement adaptée au stockage à long terme des données tout en préservant leur contenu à l'abri des regards indiscrets. En effet, la validité des données stockées pourra être confirmée à partir de leur empreinte/signature unique (*hash*). Plus l'historique des transactions ou la taille des fichiers hachés s'avère volumineuse, plus simple sera-t-il d'en vérifier le *hash* au lieu de les réexaminer *de novo*.

Sécurité / Confidentialité – La nécessité de « consolider » la chaîne par un vote majoritaire des mineurs du réseau rend une chaîne de blocs particulièrement robuste aux altérations – accidentelles ou frauduleuses – des données validées et cryptographiquement hachées. Ces dernières ne sont pas seulement stockées sur un seul « serveur » sous la surveillance d'un organe central de contrôle, mais sont distribuées sur un ensemble de nœuds sous une forme cryptographique particulièrement sensible aux menues variations (*hash*). Une chaîne de blocs permet à des personnes d'échanger en ligne en préservant leur anonymat respectif tout en se passant des services d'authentification assumés jusqu'alors par un tiers (p.ex. Paypal).

Réduction des coûts de transaction – La perspective de se dispenser des services onéreux des tiers de confiance permet aux deux parties contractantes d'économiser les frais de gestion ou de transaction, comme les commissions bancaires ou les honoraires du notaire. Indépendamment du nombre de blocs, le temps de validation des nouvelles transactions étant automatiquement ajusté pour une durée moyenne équivalente (p.ex. 10 minutes dans le cas de la chaîne Bitcoin), s'y ajoute une économie de temps permettant de compléter une transaction en l'espace de 10 minutes.

Toutefois, la preuve de travail requise pour valider les nouvelles transactions ainsi que les ressources informatiques nécessaires à la transmission et au stockage des données requièrent une consommation énergétique substantielle en continu (**O'Dwyer et Malone, 2014**), dont les coûts se répercuteront à plus ou moins longue échéance sur la société au sens large. Cette préoccupation pourra éventuellement être atténuée avec la preuve d'enjeu ou une preuve hybride de travail et d'enjeu (PoW/PoS), dont le réseau Ethereum s'en prévaudra très prochainement avec la mise en œuvre progressive de l'algorithme de Casper (**Buterin, 2017; Buchko, 2017**).

2. Un contrat dit intelligent

Le contrat, dans son acception traditionnelle et juridique, est essentiellement un accord de volontés ou « *meeting of the minds* » entre des parties cocontractantes en vue de produire des effets de droit :

> *Code civil du Québec*, art 1378, al 1 : « Le contrat est un accord de volonté, par lequel une ou plusieurs personnes s'obligent envers une ou plusieurs autres à exécuter une prestation. »
>
> *Code civil belge*, art 1101 : « Le contrat est une convention par laquelle une ou plusieurs personnes s'obligent, envers une ou plusieurs autres, à donner, à faire ou à ne pas faire quelque chose. »
>
> *Household Fire and Carriage Accident Insurance Co Ltd v Grant* (1879) 4 Ex D 216, j Thesiger : "… in order to the effecting of a valid and binding contract, that the minds of the parties should be brought together at one and the same moment, that notion is practically the foundation of English law upon the subject of the formation of contracts."
>
> *Baltimore & Ohio R Co v United States* (1923), 261 US 592 à la p 597 : "an agreement … founded upon a meeting of minds, which, although not embodied in an express contract, is inferred, as a fact, from conduct of the parties showing, in the light of the surrounding circumstances, their tacit understanding."

L'existence d'un accord de volontés mis à part, aucune exigence de forme particulière (verbal ou écrit, à distance ou face-à-face) n'est rattachée *a priori* à la formation ou à la validité d'un contrat, sous réserve de certaines formalités imposées pour la validité de certains contrats (p.ex. donation immobilière), pour rendre l'existence de certains droits opposables aux tiers (p.ex. publicité foncière), ou pour la protection des parties vulnérables (p.ex. contrat de consommation).

L'expression « contrat intelligent » ou (*smart contract*) est venue du juriste-informaticien américain Nick Szabo (**Szabo, 1996**). Dès au milieu des années 1990, ce dernier relevait l'intérêt de réduire les coûts de transaction psychologiques et computationnels des parties contractantes à l'aide d'algorithmes et en leur faisant bénéficier des avancées en cryptographie et en automation (sans faire appel nécessairement aux chaînes de blocs). Pour M. Szabo, le champ d'application des contrats intelligents pourrait couvrir toutes les phases contractuelles depuis la recherche informationnelle jusqu'au règlement des conflits en passant par la négociation, la conclusion du

contrat et son exécution (**Szabo, 1997**). C'est donc pour l'essentiel un ensemble d'engagements, spécifiés sous forme numérique, y compris dans des protocoles à partir desquels les parties exécutent leurs engagements : « *I call these new contracts "smart", because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.* » (**Szabo, 1996**)

Ce qui fait dire à certains qu'un contrat dit intelligent est davantage une modalité d'exécution des contrats qu'un nouveau type de contrat comme tel : « Les *smart contracts* sont une manière de coder un contrat et de rendre son application automatique, donc plus facile, plus rapide et plus sûre. » (**Barbry, 2017**) Son « intelligence » tient à « sa capacité d'auto-exécution des obligations contractuelles enregistrées » (**Barreau, 2017**). Cette auto-exécution est néanmoins convenue entre les cocontractants et fait partie de leur entente contractuelle, sans constituer pour autant tout le contrat. Quel serait l'intérêt de substituer ainsi une relation d'homme à homme à une interface de machine à machine (**Banerjee et al, 2017**) ? L'idée de base consiste à intégrer, dans la mesure du possible, certaines clauses contractuelles – telles que la garantie, le cautionnement, la délimitation des droits de propriété, etc. – dans une architecture logicielle et matérielle qui en rend la violation contractuelle relativement coûteuse, voire prohibitive. À ce titre, M. Szabo nous donne l'exemple du distributeur automatique, un prototype de contrat intelligent :

> « *Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a freshman computer science problem in design with finite automata, dispense change and product according to the displayed price. The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas.* » (**Szabo, 1997**)[1]

Selon M. Szabo **(Szabo, 1996)**, les quatre déterminants d'une relation contractuelle – « intelligente » ou non – sont les suivants :

- L'observabilité (*observability*), soit la capacité des parties contractantes de constater leur performance contractuelle mutuelle, ou de s'en prouver l'exécution. M. Szabo l'attribue au domaine traditionnel de la comptabilité (*accounting*).
- La vérifiabilité (*verifiability*), soit la possibilité pour une partie contractante de prouver à un tiers arbitre le respect ou la violation d'une clause contractuelle, ou la capacité pour un tiers arbitre de le découvrir par d'autres moyens. Il s'agit, nous précise Szabo, de la responsabilité réservée aux disciplines d'audit et vérifications (*auditing and investigation*).

L'observabilité et la vérifiabilité supposent la faculté de faire la distinction entre les violations contractuelles intentionnelles et par inadvertance (de bonne foi).

- L'effet relatif (*privity*) des contrats, au sens où la connaissance et l'examen du contenu et de l'exécution contractuels soient accordés aux parties seulement dans la mesure nécessaire à l'exécution du contrat, à l'abri de l'intervention ou du regard indiscret de

tierces personnes non parties à la relation contractuelle. Cet effet relatif est assuré par les mesures de sécurité, de confidentialité et de protection des renseignements personnels.

- La force exécutoire (*enforceability*) du contrat, tout en en minimisant la nécessité d'une exécution forcée. Les incitatifs agissant dans ce sens peuvent être la mesure de sa réputation et l'intégration de protocoles « auto-exécutoires ».

De ces quatre déterminants combinant les impératifs de confidentialité (secret) et de traçabilité (suivi), M. Szabo en tire la finalité visée par sa conception de contrats intelligents, cherchant à tirer le meilleur parti du pouvoir de surveillance et de contrôle des tiers tout en minimisant leur intervention :

> « *Smart contracts often involve trusted third parties, exemplified by an intermediary, who is involved in the performance, and an arbitrator, who is invoked to resolve disputes arising out of performance (or lack thereof). Privity implies that we want to minimize vulnerability to third parties. Verifiability and observability often require that we invoke them. A mediator must be trusted with some of the contents and/or performance of the contract. An arbitrator must be trusted with some of the contents, and some of the history of performance, and to resolve disputes and invoke penalities fairly. In smart contract design we want to get the most out of intermediaries and arbitrators, while minimizing exposure to them. One common outcome is that confidentiality is violated only in case of dispute.* » (**Szabo, 1996**)

Un contrat intelligent est ainsi plus qu'un (simple) échange de données informatisées (*cf. Electronic data interchange* –EDI). Il participe jusque dans la cristallisation même de « l'accord de volontés » contractuelles, en automatisant l'identification des parties même à leur insu, un peu comme une transaction d'achat complétée via un terminal point de vente (PDV) au supermarché :

> « *For example, grocery store POS machines don't tell customers whether or not their names are being linked to their purchases in a database. The clerks don't even know, and they've processed thousands of such transactions under their noses. Thus, via hidden action of the software, the customer is giving away information they might consider valuable or confidential, but the contract has been drafted, and transaction has been designed, in such a way as to hide those important parts of that transaction from the customer.* » (**Szabo, 1996**)

Cette identification des parties contractantes – non nécessairement présente dans une transaction complétée dans le monnayeur d'un distributeur automatique – fait appel aux techniques développées en cryptographie pour assurer la sécurité des transactions et la confidentialité des clauses contractuelles. Cet impératif de confidentialité s'impose tout au long de la relation contractuelle, *a fortiori* lors du stockage et de la transmission des données pertinentes. C'est ici qu'intervient le potentiel innovateur des chaînes de blocs (*blockchains*), comme nous allons le voir plus loin.

3. La mise en place des contrats intelligents basés sur des chaînes de blocs (*blockchains*)

En raison de ses différents avantages, la chaîne de blocs – outre le Bitcoin et autres cryptomonnaies (Ether, Litecoin, Bitcoin Cash, Ripple …) – laisse présager de multiples applications en matière de contrats intelligents. Dans les mots de la professeure Dominique Guegan :

> « … un contrat intelligent [déployé sur une chaîne de blocs] correspond à des programmes informatiques autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable avec des instructions conditionnelles du type « if… Then… », utilisant les informations disponibles sur le blockchain. Ces contrats doivent être capables de réduire les coûts de vérification, d'exécution, d'arbitrage et de fraude. Ils peuvent être amenés à gérer des fonds ou à authentifier des entités externes. Et donc dans cet environnement, le code doit être digne de confiance. Ainsi les développeurs et les utilisateurs de contrats intelligents doivent être en mesure de vérifier les propriétés de ces contrats et de disposer de correcteurs fiables. » (**Guegan, 2017 à la p 2**)

En effet, de par sa structure décentralisée, l'avènement des chaînes de blocs pourrait révolutionner les échanges en ligne en éclipsant le rôle – jusqu'alors indispensable – des tiers de confiance comme les banques, les chambres de compensation, les courtiers, les notaires, les maisons de disques et les distributeurs ainsi que des plateformes électroniques intermédiaires comme Uber (réservation de voitures) et Airbnb (site de location d'appartements) en mettant directement en relation les prestataires de service et leurs clients.

Les applications intelligentes susceptibles d'être intégrées sur une chaîne de blocks comprennent le transfert des titres de propriété, la vente des actions ou d'obligations, l'approvisionnement des marchandises, le ravitaillement en électricité, les enchères, la gestion de l'identité et de la réputation, l'attestation des titres de compétence, voire l'authentification des pièces de preuve produites aux assises criminelles (**Davidson, 2017**) …

Voici un aperçu de quelques contrats intelligents d'ores et déjà implantés sur des chaînes de blocs.

3.1. L'assurance contre les risques

La toute première possibilité technique de rattacher de « vrais » contrats intelligents sur une chaîne de blocs a été réalisée sur la plateforme Ethereum, développée par la société suisse Ethereum Switzerland GmbH (EthSuisse) à l'initiative du jeune programmeur russo-canadien Vitalik Buterin (**Buterin, 2013**). Les contrats intelligents y utilisent l'unité de compte dénommée Ether (ETH) comme moyen d'échange, alors qu'une autre unité de compte, appelée « gaz », paye les frais de transaction en alimentant les activités de minage.

En septembre 2017, le groupe d'assurance Axa inaugure « un produit d'assurance d'un genre nouveau », offert exclusivement sur sa plateforme d'assurance paramétrique, baptisée Fizzy[2]. Cette dernière promet une indemnisation automatique des assurés ayant souscrit, jusqu'à 15 jours avant leur départ, une assurance contre les retards d'avions.

« Votre vol a 2h de retard ? Recevez votre argent sans réclamer », nous assure le site officiel de l'offre Fizzy. Dans ses Conditions générales, Axa nous présente le fonctionnement d'un « contrat Fizzy » en ces termes :

> « Lors de la souscription à distance d'un *Contrat FIZZY*, ses éléments essentiels (*vol garanti, retard garanti* et *indemnité*) sont traduits par notre *plateforme* sous la forme d'un code informatique pour former un « smart contract », c'est-à-dire un programme qui va solliciter de manière autonome les informations nécessaires à son exécution (au cas d'espèce, l'heure

d'arrivée du *vol garanti* pour déterminer s'il y a eu un *sinistre*) et exécuter automatiquement les actions contractuellement induites par celles-ci.

Pour garantir l'autonomie et l'indépendance de ce smart contract, celui-ci est en outre intégré dans un des registres publics décentralisés les plus populaires et sécurisés : la « Blockchain Ethereum ».

Il en résulte que, dès lors qu'est reçue l'information relative au *retard* de votre *vol* via le fournisseur de données aériennes *Flightstats*, notre *plateforme* initie de manière autonome et indépendante le processus de paiement de votre *indemnité* en cas de *retard garanti*.

De sorte, *FIZZY* est un contrat d'assurance sans surprise. En effet, en cas de *sinistre* :

- *Vous* n'avez rien à déclarer;
- *Vous* n'avez pas de justificatifs à produire pour prouver votre *sinistre* et/ou vos *dommages*;
- Il n'y a pas d'exclusions ou de déchéances contractuelles;
- Votre *indemnité* correspond exactement au montant des *dommages* que *vous* avez souhaité garantir;
- *Vous recevrez* sans délai votre *indemnité.*

(…)

Enfin, *FIZZY*, c'est aussi un contrat qui préserve vos droits en *vous* laissant la possibilité de *nous* déclarer de manière traditionnelle votre *sinistre* si votre *indemnité* ne vous est pas parvenue automatiquement. » (**AXA *FIZZY*, à la clause 2.2**) [italiques dans l'original, comme termes définis dans le Glossaire rattaché aux Conditions générales]

Bref, Axa délègue la décision d'indemnité à un réseau décentralisé et indépendant, « renforçant ainsi la confiance que le client peut avoir en Axa » (**Raynal, 2017**).

En effet, le contrat d'assurance se prête bien à une simplification technique et automation du type « chaîne de blocs », en ce qu'aucune exigence de forme ou formalité additionnelle autre que la conjonction de l'offre et de l'acceptation n'est requise au soutien de la validité ou de l'opposabilité (aux tiers) d'un tel contrat. En plus d'en automatiser l'exécution des engagements contractuels (caractéristique commune à tout contrat intelligent), l'avantage de l'intégrer sur une chaîne de blocs réside dans l'automatisation de la collecte d'informations pertinentes/nécessaires permettant à un système « intelligent » de constater par lui-même la survenue d'un sinistre déclenchant l'obligation d'indemnisation; dispensant l'assuré de son obligation de déclarer son sinistre dans des délais stricts et le prémunissant contre une éventuelle déchéance du droit à l'indemnisation pour déclaration tardive ou frauduleuse. Bien sûr, le paiement d'indemnité est aussi automatisé avec un dépôt direct dans le compte de la carte bancaire ayant servi au paiement de la prime.

Au reste, la chaîne de blocs joue un rôle de facilitateur, sans plus. En cas de défaillances techniques (p.ex. carte bancaire volée ou perdue ou non-réception de l'indemnité), les assurés sont invités, soit à mettre à jour leurs renseignements bancaires dans leur espace personnel (**AXA *FIZZY*, à la clause 6.1.3**), soit à contacter l'assureur en déclarant leur sinistre en ligne, avec les formalités d'usage (**AXA *FIZZY*, à la clause 6.2.1**).

3.2. L'enregistrement et la passation des titres fonciers

Dans les pays où les titres de propriété (surtout immobilière) ne sont généralement pas enregistrés dans un cadastre officiel ou qui seraient très vulnérables à la corruption bureaucratique, permettre aux citoyens d'enregistrer leur propriété sur une chaîne de blocs offre plusieurs avantages.

Si, au Honduras, l'implantation d'une chaîne de blocs au secours de la transparence avait besoin d'un soutien plus large que quelques figures anti-corruption du gouvernement (**Blockchain France, 2015**), la République de Géorgie se dit enthousiaste à l'idée de lancer un projet pilote sur la plateforme Exonum afin de permettre à ses citoyens d'enregistrer leur propriété sur une chaîne de blocs cadastrale :

> « *Why the blockchain ? It will help do three major things. First, it will add security to the data so the data cannot be corrupted. Second, by powering the registry with the blockchain, the public auditor will also make a real-time audit. So the auditor will audit the registry not once per year, but every 10 minutes [for example]. Third, it will reduce the friction in registration and the cost of property rights registration, because people could do this in the future using their smart phones. Blockchain will be used as a notary service.* » (**Shin, 2016**)

Cette chaîne de blocs cadastrale conservera de manière sécurisée et confidentielle la chaîne des titres de propriété et permettra aux acquéreurs intéressés de consulter l'historique et la nature des transactions. Ce cadastre numérique fait appel à une combinaison de chaînes privée et publique :

> « *... the details of the real estate transactions are placed on a private blockchain network run by known computers, and then, in order for citizens to verify the authenticity of certificates, that data can be turned into a cryptographic « hash» that's made public on the bitcoin blockchain which is run by thousands of computers worldwide. The hash is a type of digital fingerprint that enables anyone to verify that the data matches what's on the blockchain without seeing the data itself.* » (**Shin, 2017**)

Pareilles initiatives ont par ailleurs été lancées en Suède (**Kairos Future, 2017**), en Ukraine (**State Agency for eGovernance of Ukraine, 2017**), dans l'État d'Andhra Pradesh en Inde (**Andhra Pradesh, 2017**), au Brésil (**Records in the Chain Project, 2018**), dans le comté de Cook de l'Illinois (l'un des plus grands bureaux de registres fonciers aux États-Unis) (**Cook County Recorder of Deeds, 2017**) ainsi que dans la ville de South Burlington au Vermont (**Propy, Inc., 2018**).

Plus qu'un simple suivi des titres fonciers, les applications permettent désormais aux personnes intéressées de conclure directement un contrat de vente immobilière à partir de leur smartphones et de l'enregistrer en même temps en bonne et due forme sur une chaîne de blocs de manière permanente, sécurisée et confidentielle.

Par exemple :

> « *The Swedish system operates on a private blockchain. This has the land authority and others, like the banks, holding copies of the records. When a land title changes hands, each*

step of the process is verified and recorded on the blockchain. (…) The system acts as a highly secure and transparent verification and storage service for property transactions, but it stops short of a full-blown cryptocurrency where land can be bought and sold as easily as a bitcoin. » (**Wong, 2017**)

Éventuellement, ce cadastre numérique pourra être étendu à l'enregistrement des baux et hypothèques ainsi qu'aux dossiers de démolition ou d'expropriation.

Certes, le potentiel qu'offre un registre distribué de type chaîne de blocs pour assurer en toute sécurité et confidentialité la traçabilité des transactions horodatées s'avère très séduisante pour garantir la chaîne de titres et le bornage (limites des propriétés) si sensibles dans des litiges immobiliers ou pour troubles de voisinage. Cela étant, en matière de contrat de vente ou de donation d'immeubles, la loi peut exiger d'autres formalités qu'un simple accord de volontés telles qu'un acte notarié, un acte sous seing privé ou encore la publication officielle de l'acte pour rendre les contrats opposables aux tiers. Se pose ici un problème de validité des contrats conclus sur une chaîne de blocs sans avoir passé par un notaire, du moins dans les ressorts exigeant la présence d'un acte notarié. Ces contraintes juridiques, freinant la mise en œuvre de projets pilotes dans ce domaine au Québec par exemple, appellent éventuellement un assouplissement du cadre juridique pour assurer la cohérence des règles de droit applicables ou encore la neutralité du support technologique utilisé, du même style que la *Loi* [québécoise] *concernant le cadre juridique des technologies de l'information* (LRQ c C-1.1) ou encore l'article 2838 du *Code civil du Québec* prévoyant désormais qu' « [o]utre les autres exigences de la loi, il est nécessaire, pour que la copie d'une loi, l'acte authentique, l'acte semi-authentique ou l'acte sous seing privé établi sur un support faisant appel aux technologies de l'information fasse preuve au même titre qu'un document de même nature établi sur support papier, que son intégrité soit assurée ».

S'agissant données enregistrées sur une chaîne de blocs, l'État du Vermont a déjà pris l'initiative de préciser dans son Acte 157 H.868 (*An act relating to miscellaneous economic development provisions*), entré en vigueur le 1er juillet 2016, que sont présumées authentiques les données numériques enregistrées sur une chaîne de blocs maintenue dans le cadre de l'exploitation régulière d'une entreprise (Sec. I.1. 12 V.S.A. § 1913), notamment en ce qui concerne l'identité des parties contractantes, la date de conclusion et d'entrée en vigueur du contrat, les droits et obligations contractuelles ainsi que les transactions passées. Cette présomption d'authenticité peut toutefois être réfutée par la personne contre qui serait invoqué un fait litigieux.

De son côté, la Loi HB2417 *Signatures; electronic transactions; blockchain technology* de l'Arizona entérine d'ores et déjà la validité d'une signature ou contrat intégré sur une chaîne de blocs comme toute autre signature ou contrat électronique (art 5). La loi contient par ailleurs une définition détaillée de la technologie des chaînes de blocs et d'un contrat intelligent, à savoir :

« *E. For the purposes of this section :*

1. *"Blockchain technology" means distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data of the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth.*

2. *"Smart contract" means an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger.* »

3.3. La distribution de musique en ligne

Dans l'industrie culturelle, l'auteure-compositrice-interprète Imogen Heap, du Royaume-Uni, a lancé dès 2015 sa chanson *Tiny Human* sur la chaîne de blocs Ethereum avec le concours de la startup Ujo Music : « Les utilisateurs peuvent acquérir des licences pour des segments de l'œuvre (par exemple, la piste pour un seul instrument) ou pour la pièce musicale entière et pour un ou plusieurs usages (diffusion en continu, téléchargement, etc.). La technologie blockchain permet ensuite de répartir automatiquement chaque paiement, qui est envoyé directement à Imogen Heap et à chacun de ses collaborateurs. » (**Desjardins, 2016; voir aussi Pons, 2017**)

L'avantage de passer par une chaîne de blocs est de mettre en relation directe l'artiste et ses consommateurs, sans passer par des intermédiaires avec les droits de distribution très onéreux. Mieux qu'une simple carrière artistique en ligne rendue possible la révolution Internet (Napster), la chaîne de blocs garde en toute transparence une trace indélébile des transactions passées avec les conditions précises s'y rattachant tout en offrant une protection robuste contre les fraudes, les piratages et les reproductions non autorisées.

La plateforme Peertracks, dont le lancement est prévu en mars 2018, sera elle aussi intégrée sur la chaîne de blocs BitShares Music afin de permettre aux artistes et utilisateurs d'interagir entre eux en toute convivialité.

3.4. L'enregistrement et la vente aux enchères des noms de domaine

Tout à fait indépendamment de l'ICANN (*Internet Corporation for Assigned Names and Numbers*), le projet Namecoin a été le premier à proposer aux utilisateurs des noms de domaine se terminant en « .bit » à partir d'une chaîne de blocs, c'est-à-dire qu'« en réalité Namecoin ne gère rien d'autre que l'accès au système décentralisé, et que tous les noms de domaines [en « .bit »] sont en réalité contrôlés par les utilisateurs » (**Blockchain France, 2015a**). D'autres lui ont emboîté le pas, dont l'Emercoin (gérant les noms de domaine en « .coin », « .emc » et « .lib ») et l'Ethereum (gérant le « .eth »).

Depuis le 4 mai 2017, l'Ethereum Name Service (ENS) correspond au DNS (*Domain Name System*) d'Internet géré par l'ICANN. À la différence de ce dernier, « l'ENS n'est pas basé sur des serveurs racines, mais sur la multitude de serveurs/machines membres de la blockchain Ethereum » (**Benoist, 2017**). De plus, alors que l'achat d'un nom de domaine classique se fait en ligne à un prix prédéfini par le registraire de noms de domaine, l'enregistrement d'un nom de domaine se terminant en « .eth » se réalise au moyen d'une vente aux enchères :

> « Il s'agit d'un système d'enchères par le dépôt anonyme d'un nombre d'Ethers. En résumé, la demande d'un nom ouvre une période de 72 heures permettant à d'autres personnes d'enchérir. Une seconde période s'ouvre ensuite, d'une durée de 48 heures, durant laquelle chaque enchérisseur doit révéler son enchère. Le meilleur enchérisseur remporte l'enregistrement du nom et est remboursé de son enchère, moins la valeur correspondant à la

différence de montants entre les deux meilleures enchères. Ces fonds sont conservés dans un contrat pendant au minimum un an, et peuvent être retirés à l'issue de ce délai, sous réserve de libérer le nom. Si un nom ne fait l'objet que d'une seule enchère, le gagnant de l'enchère se voit rembourser les Ethers investis, sauf 0,01 Ether, correspondant à l'enchère minimale. Ce système permettrait selon les développeurs de l'ENS d'éviter la spéculation sur l'enregistrement de noms de domaine. » (**Benoist, 2017**)

Ainsi, plutôt que d'en confier la tâche à une autorité (centrale) comme l'ICANN, la chaîne Ethereum automatise l'attribution des noms à l'aide d'un programme informatique distribué et sécurisé.

Cela étant, n'ayant pas été intégré dans la base de données DNS supervisée par l'ICANN, les noms de domaine enregistrés en « .eth » (tout comme en « .coin », « .emc » et « .lib ») ne sont pas reconnus par les navigateurs dans leur version actuelle, à moins d'avoir installé une extension permettant de résoudre ces noms de domaine en faisant le pont entre le «°web Ethereum°» et l'Internet au sens large.

Ainsi donc, les noms de domaine en « .eth », « .coin », « .emc » ou « .lib » ne sont pas accessibles au grand public, mais uniquement sur les chaînes de blocs correspondantes Ethereum, Namecoin et Emercoin. Prenons encore une fois l'exemple de l'Ethereum Name Service (ENS) :

> « … l'usage premier de l'ENS est, comme l'est le DNS, de permettre à l'utilisateur de lire et retenir une adresse plus simplement en y donnant un sens. Le DNS permet de traduire une adresse IP en adresse lisible via le nom de domaine.
>
> L'ENS permet ainsi de traduire une adresse d'un utilisateur Ethereum (un portefeuille utilisateur) de type « f14955b6f701a4bfd422dcc324cf1f4b5a466265 » en « monprenom.eth°».
>
> Par exemple, lorsqu'un utilisateur souhaite envoyer de l'Ether à un autre utilisateur, il suffit de connaître son nom de domaine, et non plus son adresse utilisateur. Ces noms de domaine ont donc un usage assez limité, mais pourront par la suite être utilisés pour accéder à de futures applications Ethereum. » (**Benoist, 2017**)

À moins qu'elle ne soit faite sous contrôle de justice, la vente aux enchères n'étant soumise à aucune formalité stricte, l'intégrer sur une chaîne de blocs offrira aux parties une garantie de propriété plus robuste que la simple parole du vendeur en matière de biens meubles et minimisera le risque (et les conséquences) d'avoir vendu le bien d'autrui. Plus qu'une (simple) obligation de garantie de propriété incombant de plein droit au vendeur, ce sera la garantie elle-même qui bénéficiera d'office à l'acheteur, sans l'intervention du vendeur lui-même. Bien entendu, le cours des transactions s'en trouvera par ailleurs facilité avec l'automatisation – simultanée – du paiement et de la délivrance du titre de propriété.

3.5. La transmission des titres financiers et le financement participatif (*crowdfunding*)

De l'avis de plusieurs, les domaines financier et bancaire sont ceux où les contrats intelligents pourraient être le plus facilement appliqués : les caractéristiques inhérentes au monde numérique ne permettent que de coder des formules standardisées et des variables facilement mesurables

(**Cuccuru, 2017; FinTech Network, 2017**). À l'automne 2015, neuf banques d'investissement, dont les géants Goldman Sachs, JP Morgan et UBS, ont fondé un consortium regroupant plus de 70 grandes institutions bancaires autour de la start-up américaine R3 CEV, spécialiste du transfert d'actifs et de la sécurité cryptographique. Ce consortium s'est donné l'objectif de définir des standards communs pour le développement du concept des chaînes de blocs et son expérimentation sur différentes plateformes financières.

Au Delaware, les amendements adoptés au courant du mois de juillet 2017 ont également modifié le cadre juridique pour clarifier les usages permis en ce qui a trait à la gouvernance corporative, en approuvant notamment la tenue des registres des sociétés (p.ex. valeurs mobilières) et la transmission des communications d'actionnaires sur une plateforme distribuée faisant appel à la technologie des chaînes de blocs (voir aussi **Song, 2018**).

En France, c'est d'abord la possibilité d'inscrire l'émission et la cession de minibons « dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations » qui a été confirmée dans l'*Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse*, introduisant l'article L. 223-12 du Code monétaire et financier. Quelques mois plus tard, la Loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique habilite expressément le gouvernement à assouplir le transfert de certains titres financiers et valeurs mobilières au moyen d'un « dispositif d'enregistrement électronique partagé » (art 120(1°)). L'expression « dispositif d'enregistrement électronique partagé » est calquée de l'anglais *Distributed Ledger Technology* (DLT), que la Direction Générale du Trésor définit comme :

> « une technologie informatique innovante qui permet à des participants d'un réseau de valider par consensus des échanges et des transactions entre plusieurs participants sans faire intervenir d'organe central. Elle pourrait trouver de nombreuses applications, notamment pour l'enregistrement des transactions ayant lieu sur les marchés financiers de titres. » (**Direction Générale du Trésor, 2017**)

Plutôt que de référer uniquement aux « chaînes de blocs », l'expression « dispositif d'enregistrement électronique partagé » (DEEP) a été privilégiée afin de ne pas exclure de développements techniques ultérieurs, tout en couvrant les principales caractéristiques de la *blockchain*, à savoir : « sa vocation de registre et son caractère partagé » (***Rapport au Président de la République relatif à l'ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers*, 2017**).

Étant donné l'essor des *Fintechs* pour l'évolution du secteur financier, la Direction Générale du Trésor adopte une attitude d'ouverture vis-à-vis du recours aux technologies de l'information pour modifier les activités et les pratiques financières, en se fondant sur les principes suivants :

- dialogue et accueil des nouveaux entrants,
- attitude proactive d'identification des points de frottements éventuels entre nouveaux modèles et réglementations existantes, et de recherche des solutions appropriées,
- compréhension des risques et avantages associés aux nouveaux modèles pour anticiper leurs effets microéconomiques et macroéconomiques potentiels, tout en restant neutre

quant aux choix commerciaux et technologiques effectués. (**Direction Générale du Trésor, 2017**)

Au terme de deux consultations publiques menées auprès d'acteurs divers (banques, sociétés de gestion, techniciens de la *blockchain*, universitaires, cabinets d'avocats et de conseil), l'*Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers* fait de Paris la première place financière en Europe à permettre légalement le transfert de propriété de titres financiers par *blockchain* :

> « Sur le fond, l'ordonnance permet de conférer à l'inscription d'une émission ou d'une cession de titres financiers dans une « blockchain » les mêmes effets que l'inscription en compte de titres financiers. Elle ne crée pas d'obligation nouvelle, ni n'allège les garanties existantes relatives à la représentation et à la transmission des titres concernés. » (***Rapport au Président de la République relatif à l'ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers*, 2017**)

Cette réforme s'applique limitativement « aux titres financiers pour lesquels le droit européen n'impose pas de passer par un dépositaire central de titres, et en particulier les parts de fonds, les titres de créance négociables et aux actions et obligations non cotées » (**Direction Générale du Trésor, 2017a**). L'entrée en vigueur de l'Ordonnance est repoussée au 1er juillet 2018 au plus tard afin de ménager un temps d'élaboration des mesures d'application.

À l'échelle européenne, la Commission européenne a lancé, en date du 1er février 2018, l'Observatoire-forum des chaînes de blocs de l'UE afin de mettre en lumière les grandes évolutions de la technique des chaînes de blocs et encourager les acteurs européens de ce secteur. L'Observatoire-forum des chaînes de blocs est lui-même un projet pilote du Parlement européen et devrait étayer les travaux de la Commission sur les technologies financières (*FinTech*).

Sur le plan des initiatives terrain, la chaîne de blocs fait ses premiers pas exploratoires dans le marché des titres non cotés avec la conclusion, au printemps 2016, d'un partenariat stratégique entre BNP Paribas Securities Service (BP2S) et la plateforme d'investissement SmartAngels. Le projet consiste à mettre au point un registre de titres non cotés d'émetteurs (entreprises) financés via SmartAngels sur une chaîne de blocs privée :

> « Les investisseurs achetant ces titres verront leurs paiements traités immédiatement et des e-certificats leur seront émis instantanément. Les opérations financières réalisées sur la plateforme seront ainsi effectuées de manière simplifiée, rapide, sécurisée et à faible coût.
>
> L'intérêt pour les clients de SmartAngels est double dans un contexte de forte augmentation des volumes. La standardisation de l'inscription des titres permettra d'offrir aux investisseurs une plus grande sécurité informatique et de traitement des transactions. Quant aux émetteurs, la plateforme Blockchain opérée par BNP Paribas leur permettra de gérer leur actionnariat plus simplement. » (**BNP PARIBAS Securities Services, 2016**)

Cette plateforme conçue pour permettre d'enregistrer les opérations sur les marchés primaires et secondaires s'adresse « aux émetteurs, aux actionnaires, aux investisseurs (business angels,

investisseurs du capital risque et du capital développement), aux plateformes de crowdfunding, mais aussi aux avocats, notaires, experts-comptables et aux banques » (**SmartAngels, 2017**).

Parallèlement, quatre autres plateformes de financement participatif (Credit.fr, Enerfip, Lumo et Unilend) travaillent de concert pour sécuriser la gestion des bons de caisse de nouvelle génération sur une chaîne de blocs :

> « Dans un premier temps, les plates-formes partenaires inscriront sur une « blockchain » commune les transactions de leurs clients. Leur objectif est double : rassurer leurs clients sur leurs transactions grâce à un registre infalsifiable et en temps réel et, dans un second temps, créer grâce à un registre un marché secondaire d'échange de titres de dette entre PME. » (**Wajsbrot, 2017**)

La même année, la multinationale américaine IBM annonce, à l'occasion de la conférence Money 20/20 tenue à Copenhague, le lancement de la plateforme *Digital trade chain* (DTC) – rebaptisée we.trade – visant à faciliter le commerce national et international des petites et moyennes entreprises (PME) européennes. Ce projet, développé avec un consortium de sept banques (Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Société Générale et UniCredit) rejointes par Banco Santander, sera géré par une *joint venture* (JV) à être constituée en République d'Irlande et permettra « de connecter sans interférence les parties impliquées dans une transaction commerciale, l'acheteur, la banque de l'acheteur, le vendeur, la banque du vendeur et le transporteur » (**Société Générale, 2017**). La commercialisation de cette plateforme est attendue pour le second trimestre de l'année 2018.

4. Les enjeux juridiques inhérents à la mise en place des contrats intelligents basés sur des chaînes de blocs (*blockchains*)

Intégrer des contrats intelligents sur des chaînes de blocs soulève plusieurs enjeux juridiques liés à la gouvernance des chaînes de blocs (4.1), aux difficultés de remédier à une exécution incorrecte des contrats en raison de défaillances techniques (4.2), à l'irrévocabilité des opérations/transactions automatisées (4.3) ainsi qu'au choix de l'algorithme comme loi applicable aux contrats (4.4).

4.1. Gouvernance des chaînes de blocs

Si des contrats intelligents « traditionnels » – comme le distributeur automatique (de boissons gazeuses ou de titres de transport), l'imprimante payante ou les bornes de commande automatique de McDonald's – jouaient strictement un rôle de facilitateur de transactions sans modifier fondamentalement le régime classique de responsabilité civile du vendeur commerçant ou du fabricant, la gestion décentralisée d'une chaîne de blocs pose d'emblée la question de la responsabilité sous un angle nouveau.

De son héritage très cartésien, les régimes de responsabilité de tradition civiliste ou de common law reposent sur la notion de libre arbitre, supposant un (devoir de) contrôle personnel, par rapport à ses actes ou ceux d'autrui. Outre la responsabilité civile personnelle, l'on parle de l'obligation de diligence des parents dans la garde, la surveillance ou l'éducation de son enfant

(art 1459 CcQ), de l'obligation du propriétaire de réparer le préjudice causé par l'animal « sous sa garde » (art 1466 CcQ) ou la ruine de son immeuble (art 1467 CcQ), etc.

Or, qui contrôle une chaîne de blocs ? *A priori*, personne. Il s'agit d'une gouvernance assurée par consensus. L'exécution d'un contrat intelligent (ou toute autre transaction) sur une chaîne de blocs dépend non pas de la bonne volonté des cocontractants, mais du bon fonctionnement du code source et des algorithmes (**Murck, 2017**). Ces derniers prennent le contrôle et relègue les parties contractantes à l'arrière-plan.

4.1.1. Le devoir fiduciaire ou de loyauté des développeurs

Or, les algorithmes, quelqu'efficaces qu'ils soient, ne sont pas invincibles. À la suite d'un sensationnel détournement de 3,6 millions d'Ether par un pirate exploitant une vulnérabilité dans le code du programme DAO (*Decentralized Autonomous Organization*) de la plateforme Ethereum conçue spécifiquement pour exécuter des contrats intelligents (**Ore, 2016**), des juristes de common law proposent de reconnaître aux développeurs un devoir fiduciaire envers la communauté, dans la même veine que l'obligation de loyauté des administrateurs et des dirigeants vis-à-vis d'une entreprise :

> « *Generally, fiduciary duties include a duty of care (to act with competence), a duty of loyalty (to act in the interests of those they serve rather than in their own interest), and according to some schools of thought, a duty of good faith. Those who have invested in Ethereum, whether by buying ether or building on its blockchain, have likely expected this level of performance from the beginning*. » (**Walsh, 2016**)

Après l'incident de détournement, les développeurs, avec le concours des mineurs et d'autres utilisateurs, ont tenté de redresser la situation en « forçant » un *hard fork* dans la chaîne Ethereum, qui soit suffisamment importante pour « rétrodater » le système à la veille du piratage et retourner les fonds Ether à son propriétaire légitime.

Toutefois, des utilisateurs « récalcitrants », quoique minoritaires, continuent d'échanger avec l'ancienne unité de compte d'avant le *hard fork*, rebaptisée depuis Ethereum Classic (ETC). Les promoteurs d'Ethereum Classic (ETC) justifient leur maintien de la chaîne originale au nom de l'irréversibilité de principe des contrats intelligents exécutés sur une chaîne de blocs :

> « We believe the core value proposition of any blockchain is immutability; valid transactions can never be erased or forgotten. Individuals interacting on Ethereum Classic are governed by this reality; **Code is Law**. » (**Ethereum Classic**) [l'emphase dans l'original]

Avec une puissance de calcul extrêmement réduite, cette « obstination » semblait illusoire jusqu'à ce que certaines plateformes d'échange de cryptomonnaies (Poloniex, Shapeshift et Kraken) décident d'intégrer l'unité ETC en lui reconnaissant une valeur d'échange et en lui redonnant par là sa « raison d'être ».

De leur côté, les développeurs du Bitcoin ont décidé d'agir en amont en posant des points de contrôle (*checkpoints*) périodiques ou instantanés irréversibles de l'état du réseau à une date donnée, empêchant toute attaque des 51% pour les transactions passées avant cette date (**Laurie,**

2011 à la p 3). Le devoir fiduciaire des développeurs de chaînes de blocs serait donc envisageable, au risque d'empiéter sur la vocation décentralisée de la structure dans l'intérêt … communautaire.

4.1.2. Une structure tricamérale

Cet incident (parmi d'autres!) affectant la plateforme Ethereum (voir **Li et al, 2017**) soulève la question du degré ou de l'étendue de la responsabilité personnelle des développeurs lorsque le redressement de lacunes (involontaires ou imprévues) de programmation ne dépend pas que d'eux seuls, ni même du pirate initiateur de l'attaque malicieuse. Dans ce consensus disséminé sur une chaîne de blocs, certains y voient une structure tricamérale faisant intervenir les développeurs, mineurs et utilisateurs : « *All changes to the code and economics of Bitcoin need participation by all three constituencies to be implemented. Developers write the software that runs on the protocol, but miners and users must vote for the software by running it themselves.* » (**Tomaino, 2017**)

La question s'envisage différemment à l'égard d'une chaîne de blocs privée, où « le consensus est partagé entre un nombre restreint de nœuds identifiés (ex : une fédération d'entreprises d'un secteur d'activités) pour le calcul d'une blockchain dont les droits en lectures et écritures sont eux-mêmes contrôlés au lieu d'être totalement libres comme une blockchain publique » (**Lore, 2016 à la p 46**). Il ne s'agirait alors pas tant d'un consensus distribué *per se* que d'un pouvoir institutionnel autrement délégué en arrière-plan, substituant le contrôle – unilatéral – des décisions à celui – tout aussi unilatéral – des participations, avec les responsabilités (de garantie, de reddition de compte, du fait d'autrui) afférentes.

Cela étant, même sur une chaîne de blocs publique, des « concentrations de pouvoir » se créent *de facto* avec le regroupement des mineurs en coopératives et entreprises afin d'alimenter la puissance de calcul nécessaire pour valider les nouveaux blocs de transactions avec la preuve de travail. Dans cette optique, le devoir fiduciaire d'agir dans l'intérêt de la communauté pourrait être étendu aux plus gros mineurs : « *Treating the core developers and big miners of public blockchains as fiduciaries would set a clear standard for performance, make them accountable for actions that significantly impact other people, and ensure that they take their creation and operation of these public systems seriously.* » (**Walsh, 2016**)

Alors que le groupe d'assurance Axa enregistre chaque contrat d'assurance pour retard de vol (Fizzy) sur la chaîne de blocs publique Ethereum et que la Géorgie amorce un projet pilote pour enregistrer ses titres fonciers en faisant appel à la chaîne Bitcoin, cette question de responsabilité (partagée) est loin d'être hypothétique ou de n'impliquer que des cryptomonnaies. Qui est responsable, pour combien de temps et dans quelle mesure ?

Détaillons quelques cas de figure.

4.2. L'inexécution incorrecte d'un contrat intelligent intégré dans une chaîne de blocs

Advenant que survienne une défaillance technique ou attaque malicieuse rendant l'indemnisation des assurés incomplète ou inexécutable sur la chaîne de blocs. L'incident, quoique regrettable,

n'est pas en soi irréversible, en ce sens que cette inexécution par inadvertance n'affecte ni l'intégrité du contrat ni n'efface les obligations contractuelles afférentes. *A priori*, l'assureur demeure tenu de verser l'indemnité à ses assurés par tout moyen (dans ou en dehors de la chaîne de blocs, comme l'indemnisation Fizzy), à moins d'établir la force majeure ou encore ce que la doctrine anglo-saxonne appelle la « *'Code-as-law' Defence* » :

> « *... the original, unamended software design or a new software design that was the result of the agreed governance process may be considered* ***in a contractual claim*** *as a characteristic of the service or product. This is because contractual partners (...) have voluntarily chosen to use the code-based services and product as they are. For instance, in a proof-of-work census model the fact that consensus building takes up to 15 minutes is inherent to the model and not a breach of contract.* » (**Zetzsche et al, 2017 à la p 38**) [caractères gras dans l'original]

En d'autres termes, la chaîne de blocs faisant partie intégrante des engagements contractuels, les parties pourraient avoir accepté les risques et périls en toute connaissance de cause. Or, de par le fonctionnement décentralisé d'un tel système distribué se validant par vote majoritaire, les parties contractantes peuvent-elles avoir consenti de façon éclairée à parier sur ce qui serait au fond une course permanente entre les pirates et les honnêtes gens ?

De son côté, en droit civil québécois (par exemple), une force majeure est définie comme « un événement imprévisible et irrésistible »; y est par ailleurs assimilée « la cause étrangère qui présente ces mêmes caractères » (art 1470, al 2 CcQ). Pareille exonération est également prévue dans le Code civil belge, dont l'article 1148 dispose qu' « [i]l n'y a lieu à aucun dommages et intérêts lorsque, par suite d'une force majeure ou d'un cas fortuit, le débiteur a été empêché de donner ou de faire ce à quoi il était obligé, ou a fait ce qui lui était interdit ».

Qu'une défaillance survenue sur une chaîne de blocs publique puisse ou non être considérée comme une force majeure est sujet à débat, en tenant compte :

- de la perte subie par les assurés et l'assureur le cas échéant,
- du caractère « collectif » du redressement requis (coopération des plus gros mineurs), et
- de l'impact prévisible de cette décision sur d'autres contrats intelligents appelés à être intégrés dans une chaîne de blocs.

En effet, contrairement à un virement bancaire ou avec Paypal, même en toute bonne foi, ni la banque ni la plateforme de paiement tierce ni personne ne pourra corriger la situation par elle-même. Non seulement le défaut ne sera pas imputable à un individu en particulier, mais son redressement demandera le concours (majoritaire) des participants de la communauté *blockchain* pour « revenir dans le temps », comme en témoigne l'épisode du *hard fork* d'Ethereum.

Encore là, la possibilité de poser des *checkpoints* périodiques va vraisemblablement apaiser la controverse en renforçant, en amont, le devoir fiduciaire des développeurs. En outre, l'argument de la force majeure convainc de moins à moins à mesure que le nombre de nœuds diminue ou lorsque les défaillances surviennent sur des chaînes de blocs privées dont l'accès est contrôlé.

Dans des secteurs plus protégés comme en matière de protection du consommateur, les obligations de garantie renforcées du commerçant, le cas échéant, peuvent à cet égard faire échec à toute tentative d'exonération par force majeure : « Toute personne peut se dégager de sa responsabilité pour le préjudice causé à autrui si elle prouve que le préjudice résulte d'une force majeure, à moins qu'elle ne se soit engagée à le réparer. » (art 1470, al 1 CcQ) [nos soulignés]

Cela étant, l'intérêt d'intégrer un contrat intelligent sur une chaîne de blocs ne tient pas seulement à bonifier le fonctionnement d'un (simple) distributeur/exécuteur automatique, il réside avant tout dans la fonction d'authentification que peut assumer une chaîne de blocs en substituant un contrôle communautaire aux traditionnels tiers de confiance ou ancrage institutionnel.

4.3. L'authentification à l'épreuve de l'irréversibilité

La robustesse de la chaîne marquée par le caractère irréversible, c'est-à-dire infalsifiable des transactions confirmées, est l'un des attraits principaux de ce dispositif assurant l'intégrité des données enregistrées, « un système qui émet des moyens de preuves pour réglementer un régime de propriété grâce à la force de ses registres homogènes » (**Hummler, 2016**).

Quid d'une défaillance technique – (non) intentionnelle – rendant non seulement une obligation contractuelle inexécutable (sur la chaîne de blocs), mais altérant par ailleurs le contenu contractuel en y ajoutant des transactions erronées ?

Cette question se pose avec une acuité particulière lorsqu'on choisit de faire appel à une chaîne de blocs précisément pour son potentiel de traçabilité des transactions, comme pour la chaîne de titres immobiliers. Nous avons mentionné que des projets pilotes ont été menés à cet égard notamment en Illinois et en Suède. Toutefois, leurs rendus d'étape (**Kairos Future, 2017; Cook County Recorder of Deeds, 2017**), déposés au courant de l'année 2017, ne font pas état des préoccupations reliées au caractère irréversible des transactions (erronées) disséminées sur la chaîne de blocs. Plutôt, le bureau foncier du comté de Cook en Illinois relève le caractère très fiable des transferts de propriété immobilière opérés à l'aide de la cryptographie asymétrique et la possibilité – relativement aisée – de retracer les fraudes perpétrées en ligne :

> « Under current law and our paper-based system, a fraudster could create a fake deed using graphic design software, find the owner's signature on a prior public record like a mortgage, and create a new deed that appears as if the owner sold or gave their house to the fraudster. At this point, the scammer need only to mail it in to CCRD [Cook County Recorder of Deeds] and pay the recording fee (approximately $50). (…) If property conveyances were allowed only upon the entry of a public and private key, the unauthorized transfer of a property would be almost impossible. Even if the fraudster were able to hack or coerce the private key from the owner, the very fact that the transfer must happen on a computer makes it harder to cover one's tracks than is possible using U.S. mail. » (**Cook County Recorder of Deeds, 2017 à la p 38**)

Cela étant, la perte de la clé privée nécessaire pour l'identification d'une partie contractante peut devenir problématique lorsqu'il n'est plus possible de simplement « réinitialiser » son mot de passe dans un système qui ne sera géré par aucun administrateur (**Swanson, 2014**).

De plus, le caractère irréversible des transactions menées via *blockchain* s'avère toutefois une arme à double tranchant. Il exige des parties contractantes de spécifier explicitement et *ab initio* toutes les réserves limitatives ou éventuellement exonératoires de responsabilité ainsi que leurs conditions d'application, faute de quoi la cascade algorithmique de cause à effets ne pourra pas être freinée pendant la réouverture des négociations afin d'empêcher que ne soit causé un préjudice sérieux et irréparable à l'un des contractants (**Sklaroff, 2017 à la p 291**). Ce dispositif serait ainsi moins adapté pour des contrats à exécution successive ou différée à long terme.

Encore là, certaines adaptations pourraient être envisagées, telle l'interdiction – statutaire – de faire exécuter par un contrat intelligent des clauses pénales dépassant un certain seuil, ou en rendant « obligatoires les dommages et intérêts en cas de préjudice résultant de l'exécution d'une obligation nulle ou réputée non écrite » (**Akiobe Songolo, 2018**).

Une autre incertitude juridique liée à la conclusion des contrats intelligents – dans ou en dehors des chaînes de blocs – est la difficulté de vérifier la capacité de contracter des parties (**Giancaspro, 2017**). Cette préoccupation est connexe à la protection des parties plus vulnérables, comme les personnes aux prises avec des troubles mentaux, des personnes placées sous tutelle ou curatelle, ou encore très âgées.

4.4. Le choix de l'algorithme comme loi applicable aux contrats ?

L'histoire – ou plutôt le « manifeste » – d'Ethereum Classic (*supra*) laisse entrevoir le dilemme que pose l'émergence d'une *lex cryptographia*, dont l'automatisation algorithmique possiblement transfrontière pourrait facilement se soustraire au contrôle des législateurs nationaux (**Wright et De Filippi, 2015; Jeong, 2013**). À l'ère du « crypto-socialisme » (**Kosten, 2015**), des parties contractantes pourraient-elles, en toute connaissance de cause, se soumettre à loisir à cette loi « algorithmique » en écartant définitivement toute intervention des juridictions territoriales, et ce, quoi qu'il advienne ou indépendamment des circonstances ?

Tel serait, en effet, le message que tiennent à faire passer les fidèles à l'Ethereum Classic, qui préfèrent une « juridiction » régie par la « neutralité » algorithmique que d'être contraints de céder devant la primauté nécessairement « partisane » de l'intérêt commun/communautaire :

> « This does not necessarily mean that code *replaces* existing laws, or that *only* code is law (there are many geographical jurisdictions), but it gives users the opportunity to enter into a new blockchain-based jurisdiction where agreements are governed by code.
>
> By entering into contracts on Ethereum Classic, you can be certain that the network remains neutral. The outcome of transactions will be dictated by code you voluntarily interact with. Unless explicitly defined by the contract code, there are no reversals, no undos, no opt-outs.
>
> Transactions are final; applications are unstoppable. » (**Ethereum Classic**)

Les réserves sont surtout nombreuses notamment en matière de protection du consommateur. En plus de cette asymétrie d'information classique sur la qualité des produits ou des services offerts, l'exécution automatique des clauses dont la valeur juridique serait discutable pourrait

désavantager le consommateur en renforçant sa vulnérabilité par rapport aux grandes entreprises mieux avisées sur les plans juridique et technique : « *Are smart contracts maybe too smart for the ultimate users?* » (**Institute of International Finance, 2016 à la p 9**)

Conclusion

De ce qui précède, l'intérêt d'intégrer des contrats intelligents sur un registre distribué de type chaîne de blocs s'explique par la haute fiabilité des données numériques enregistrées sur une *blockchain*, rendant d'une part, leur intégrité assurée et, d'autre part, facilitant une exécution automatisée d'engagements contractuels « préprogrammés ». L'engouement pour les chaînes de blocs s'est avéré le mieux partagé dans les domaines financier et corporatif, où initiatives et projets pilotes foisonnent dans des secteurs peu réglementés en faisant bénéficier aux parties les avantages de l'automatisation sur les plan de la rapidité et de la sécurité des opérations bien définies.

La grande traçabilité et l'intégrité des transactions passées sur une chaîne de blocs la rendent également attrayante pour garantir la chaîne des titres immobiliers au même titre qu'un notaire ou contre une corruption bureaucratique endémique dans certains ressorts. La passation des contrats immobiliers directement sur une chaîne de blocs permettrait aux parties d'économiser sur les frais d'intermédiaires (commission au courtier et honoraires de notaire) tout en concluant plus rapidement et de manière sécurisée un contrat comportant les mêmes garanties d'authenticité. Toutefois, dans les ressorts requérant des formalités plus onéreuses pour la validité des contrats (de vente ou de donation) impliquant un immeuble, l'implantation des contrats dits intelligents sur des chaînes de blocs nécessite une adaptation des cadres juridiques applicables pour assurer la cohérence des règles, la neutralité des supports technologiques et une reconnaissance formelle d'authenticité des ententes conclues sur une chaîne de blocs au même titre qu'un acte notarié ou un document officiel. Les initiatives législatives en ce sens sont d'ores et déjà lancées dans l'État de Vermont et en Arizona.

Cela étant, les chaînes de blocs ne sont pas adaptées à tous les types de contrats ou d'engagements contractuels dans les cas où l'irréversibilité pèche par son excès de rigidité. Compte tenu de la difficulté, voire de l'impossibilité de modifier les engagements contractuels en cours de route même du consentement des parties, les contrats conclus à long terme, dont des engagements appellent une grande discrétion dans leur exécution ou fortement balisés par des préoccupations d'ordre public (p.ex. protection du consommateur), s'accommodent mal d'une automatisation peu adaptable aux circonstances imprévisibles, non prévues ou qui nécessitent des réaménagements plus motivés par l'équité que le souci d'efficacité.

Enfin, malgré les apparences, l'enjeu de la gouvernance (décentralisée) se pose moins que la perspective d'une liberté illimitée laissée aux parties de choisir d'être régies, en toute connaissance de cause, par la « loi algorithmique » plutôt que les lois nationales. Jusqu'où et dans quelle mesure la volonté ferait-elle office de loi des parties ?