croissanceplus GRANDIR ENSEMBLE PME FINANCE

KRAMER LEVIN
KRAMER LEVIN NAFTALIS & FRANKEL LLP

Gouvernance de la Blockchain

Les enjeux des chaînes de consensus pour la place financière de Paris

Recommandations/Réflexions :

- Création d'un marché dédié aux titres non cotés avec une expérimentation dans le cas des opérations de Règlement / Livraison de titres
- Encadrement de la migration des marchés financiers vers Blockchain
- Orientation du troisième Plan d'investissement d'avenir (PIA3)
- Donner à la *blockchain* la force de preuve authentique en droit français

Table des matières

Auteurs :

Hubert de Vauplane

Avocat associé chez Kramer Levin, Hubert de Vauplane (55 ans) a travaillé plus de 25 ans dans le secteur bancaire et financier, aussi bien en tant que juriste, banquier et opérateur en salle de marché. Avant de rejoindre le Barreau de Paris en septembre 2011, il était directeur juridique et de la conformité du groupe Crédit Agricole S.A. Il enseigne aujourd'hui à Sciences Po (Paris) après avoir été professeur associé à l'Université de Panthéon – Assas. Membre du Haut Comité Juridique de Place, il est expert auprès de l'AMF, de la Commission européenne, ainsi que du *Financial Market Law Committee* à Londres, après avoir été pendant 10 ans vice-président du *Europeean Financial Lawyers Markets Group* auprès de la de la Banque centrale européenne.

Jean Rognetta

Ancien journaliste, Jean Rognetta (50 ans) est délégué général de CroissancePlus et président de PME*finance*.

Economiste de formation (université de Turin) et bi-national franco-italien, il a été un observateur privilégié de la révolution numérique et du financement de l'innovation depuis le début des années 1990, qui ont progressivement libéré l'entrepreneuriat en Europe continentale. Il est notamment l'auteur de *La République des Réseaux* (Fayard, 2012).

Pierre-Alexis de Vauplane

Diplômé de l'Ecole Centrale Lyon et du Mastère Finance d'HEC, Pierre-Alexis de Vauplane (28 ans) travaille pour un family office renommé, où il est chargé des investissements en capital-risque et de la prospective.

Il a co-écrit en 2015 le rapport *Fintech 2020* de CroissancePlus/PMEfinance, qui a alerté les pouvoirs publics français et européens sur l'importance de la Blockchain et du retard accumulé dans les fintechs.

Introduction

Dans le rapport « *Fintech 2020* », publié en octobre 2015, CroissancePlus/PME*finance* a alerté l'Union Européenne et les pouvoirs publics français sur les enjeux économiques et de souveraineté liés à la technologie Blockchain. L'association considère nécessaire de favoriser l'essor d'un « écosystème blockchain » dans l'eurozone, pensé de telle manière que son déploiement progressif dans l'économie favorise la croissance des entreprises.

Par le biais des « blockchains », il est désormais possible de construire la confiance autrement que par les lois et la force de l'Etat. Grâce à ces protocoles, plusieurs entités non liées – ni toutes nécessairement de bonne foi – peuvent désormais se mettre d'accord, via une méthode de *consensus*, sur l'exactitude d'une information et rendre celle-ci vérifiable et/ou opposable à un tiers. La chaîne prend ainsi la forme d'un livre de transactions, un registre assimilable à un grand livre comptable, un cadastre ou un état-civil.

Appliquée aux paiements, la technologie Blockchain permet à une communauté de certifier l'absence de double-dépenses (c'est-à-dire qu'une personne tente d'utiliser un même euro, ou un même bitcoin, dans deux transactions différentes) et de bâtir un système de paiement plus flexible et – a priori – moins coûteux que l'actuel. C'est sur cette application que s'est construite la principale chaîne de consensus existante, fondée sur la cryptomonnaie Bitcoin.

Le succès de Bitcoin a provoqué un mouvement mondial de réflexion sur les applications financières de Blockchain. En France, il a notamment été mené par le groupe Caisse des Dépôts, qui a lancé fin 2015 une initiative de place qui vise à explorer, en mode « Do Tank », un certain nombre de cas d'usages par expérimentation[1]. Le gouvernement a également lancé des consultations sur un cadre dérogatoire qui permette d'expérimenter la Blockchain sur les bons de caisse. Enfin, la CSSPCE y consacre ses travaux et, en particulier, un colloque le 24 mars 2016. La présente note a été conçue dans ce cadre, pour présenter aux parlementaires les enjeux de la gouvernance des chaînes de consensus.

Puisque Blockchain offre la possibilité à une communauté de s'affranchir d'une autorité centrale pour certifier l'exactitude des transactions réalisées en son sein, sans pour autant les y enregistrer directement, son potentiel dépasse le seul secteur bancaire et financier. A terme, les modalités mêmes de l'échange économique peuvent être redéfinies par une technologie de certification automatique de toute transaction. CroissancePlus/PME*finance* considère que ce formidable potentiel pose des questions cruciales sur :

- à court terme, la compétitivité des places boursières, des banques, des compagnies d'assurances et en général des sociétés financières de l'eurozone ainsi que, par voie de conséquence, sur le financement des entreprises qui la composent ;
- à court-moyen terme, sur l'avenir de services publics comme le cadastre et l'état-civil ;
- à moyen-long terme, sur l'ensemble des transactions, et donc de la croissance des entreprises et simplement de la vie économique.

[1] Cette initiative regroupe, outre CroissancePlus-PME*finance*, des institutions financières comme Axa, BNP Paribas, le groupe BPCE, le Crédit Agricole et CNP Assurances ; des start-up, Blockchain Solutions, Cellabz et Paymium, ainsi que le CNAM et le pôle de compétitivité Finance Innovation.

I - La gouvernance, principal enjeu de la technologie Blockchain

Une première application concrète a été lancée en 2015 par le Nasdaq, via la plate-forme *Linq*, qui permet d'échanger des titres de sociétés non cotées. Les activités qui semblent en effet destinées à être touchées en premier par le déploiement de Blockchain sont celles des marchés financiers, en particulier les opérations négociées dans les bourses, ensuite dénouées dans un système de règlement-livraison de titres, puis conservées via un dépositaire central de titres auprès d'un intermédiaire financier teneur de compte. Pour cette initiative, le Nasdaq a fait appel à la société Chain[2] qui elle-même utiliserait la blockchain Bitcoin[3] comme architecture de base pour ses services financiers.

Blockchains publiques, blockchains privées : les enjeux de gouvernance

Pour ne pas être falsifiable, **une blockchain[4] requiert qu'aucun opérateur hostile ne détienne, à aucun moment, plus de la moitié de la puissance de calcul de la chaîne.** Une blockchain est dite publique dès lors que chacun peut la lire et l'utiliser pour réaliser des transactions mais aussi que chacun peut participer au processus de création du consensus. Il n'y a donc pas de registre central, ni de tiers de confiance. L'exemple le plus abouti de chaîne publique est Bitcoin[5].

La gouvernance des chaînes publiques, issue du mouvement *open source* et du *cypherpunk*, est simple : « *Code is Law* ». Dans ce système, c'est aux nœuds du réseau de valider les choix discutés et initiés par les développeurs en décidant d'intégrer ou non les modifications proposées. Son fonctionnement est fondé sur les « cryptoeconomics », la combinaison d'incitations économiques et de mécanismes de vérification utilisant la cryptographie. S'appuyant sur une approche communautaire, voire alternative, de l'économie, il a pourtant fait la preuve de sa solidité et de sa résilience.

En revanche, une blockchain est dite privée (ou semi-privée) dès lors que le processus de consensus ne peut être réalisé que par un nombre limité et prédéfini de participants. L'accès d'écriture est délivré par une organisation où les autorisations de lecture peuvent être publiques ou restreintes. Les « blockchain de place » évoquées dans plusieurs articles sont des exemples de chaînes privées. Dans ce cas, le processus de consensus est contrôlé par un ensemble présélectionné de nœuds. Vitalik Buterin[6] d'Ethereum décrit le cas d'un consortium de 15 institutions financières, dont chacune opère un nœud et dont 10 doivent signer chaque bloc pour que le bloc soit valide. L'accès à cette blockchain peut être public ou restreint aux participants selon un processus de cooptation.

Pour les détracteurs des chaînes privées, celles-ci sont à Blockchain ce que les intranets sont à Internet et elles sont, particulièrement, sujettes à un risque élevé de falsification. Leurs opposants voient Bitcoin comme un système impossible à réguler, opaque, lent à

[2] Start-up américaine, Chain.com a levé 30M€ en sept. 2015 auprès de Visa, Orange, Citi Ventures, Nasdaq et Fiserv.
[3] https://coincenter.org/2015/05/wall-street-is-using-bitcoin-not-just-the-blockchain/
[4] Utilisant une méthode de consensus de la preuve du travail
[5] La capitalisation boursière de Bitcoin est aujourd'hui environ 5Mds$
[6] Cf. Vitalik Buterin, "On public and private blockchains" : https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

transformer[7] et moins efficient techniquement que certains nouveaux protocoles[8]. A l'heure actuelle, le débat est loin d'être tranché entre chaîne publique et chaîne privée, avec, en sous-jacent, le débat entre système centralisé et décentralisé.

Il apparaît en tous cas clair que **le régulateur aura un rôle de premier plan à jouer dans la surveillance de la non-falsifiabilité des chaînes de consensus**. Il convient d'anticiper le conflit de compétences qui a émergé avec Internet entre le CSA et l'ART/Arcep et réfléchir dès aujourd'hui à la répartition des rôles entre les trois régulateurs français, AMF, ACPR et Banque de France, ainsi que leurs homologues européens.

Contrats intelligents : « killer app » de la blockchain ?

Parmi les nombreuses utilisations possibles de la blockchain, les développements les plus prometteurs résident dans les « *smart contracts* » (contrats intelligents). De quoi s'agit-il ? Ce sont des protocoles informatiques qui exécutent les termes d'un contrat (par exemple, un prêt d'argent, une émission obligataire ou d'action, mais aussi un vote, un mariage ou tout autre type de contrat) dont les caractéristiques sont standardisées[9]. L'objectif est de satisfaire les conditions contractuelles, comme les termes du paiement, de la livraison, mais aussi de la confidentialité, et même de l'exécution des obligations réciproques. Le caractère numérique et automatisé du contrat permet donc en théorie à deux partenaires de nouer une relation commerciale sans qu'ils aient besoin de se faire confiance au préalable, sans autorité ou intervention centrale. C'est en effet le système lui-même, et non ses agents, qui garantissent l'honnêteté de la transaction. Tel est le sens du projet Ethereum[10] qui doit permettre la création des *« smart contracts* » à grande échelle[11] en mettant en place une méthode de vérification entièrement dématérialisée qui peut être effectuée directement par les pairs sans l'interférence d'outils juridiques. Incorporés dans des objets physiques, ces contrats offriraient la possibilité, par exemple, de rendre le contrôle à la banque d'un véhicule acheté avec un crédit si l'emprunteur ne payait pas une mensualité. Ainsi, ces contrats intelligents sont des programmes capables d'exécuter automatiquement les conditions d'un contrat. Ils fonctionnent comme n'importe quelle instruction conditionnelle (« *if-then* ») d'un programme informatique, mais en interagissant avec des éléments du monde réel. Ces contrats intelligents pourraient permettre de construire des systèmes juridiques et financiers plus abordables et plus efficaces.

[7] Les débats sur la modification de la longueur des blocs de transactions sur Bitcoin ont pris plusieurs mois.

[8] Une des principales critiques étant liée à sa "scalabilité" puisque le système Bitcoin peut gérer aujourd'hui 7 transactions par seconde tandis que PayPal en gère 100 par seconde et Visa entre 2 000 et 7 000.

[9] Cf. S. Bourque & S. Fung Ling Tsui, "A Lawyer's Introduction to Smart Contracts", *Scienta Nobilitat Reviewed Legal Studies*, 2014.

[10] Start-up fondée par Vitalik Buterin en 2013 qui permet aux utilisateurs d'écrire des contrats intelligents ou des prêts. Le code utilisé dans le projet Ethereum est différent de celui utilisé par le bitcoin, même s'il s'en inspire. Le code a été réécrit de zéro. La principale différence par rapport à bitcoin est que les **transactions** stockées dans la blockchain ne sont pas limitées à envoyer et recevoir de l'argent. Ethereum dispose d'un quasi-langage de Turing et constitue donc un système de calcul réparti. Les pairs dans le réseau Ethereum ne se contentent pas de vérifier l'intégrité de la blockchain et d'ajouter de la monnaie, ils exécutent du code arbitraire, celui des applications qui sont développées et envoyées sur le réseau par n'importe quel tiers, qu'on appelle des « smart contracts ». Pour une explication technique du projet, cf. http://www.bortzmeyer.org/ethereum.html

[11] Comme tout système de registre décentralisé, la vérification coûte cher et les pairs doivent être incités à travailler ; d'où le développement des jetons (« token ») ou des points spécifiques à Ethereum, l'ether : il n'y a donc pas de mineurs contrairement au bitcoin qui sont rémunérés par des bitcoins.

Un deuxième enjeu de gouvernance dérive de la **compatibilité entre les normes anti-blanchiment et la structure du bloc où les transactions sont enregistrées** sous pseudonyme, à travers des clés publiques. L'anonymat des parties est aujourd'hui un risque évoqué par les régulateurs pour faire face au blanchiment d'argent.

Ce risque est encore mal perçu et évalué. Dans une blockchain publique, en effet, il est possible par croisement des données sur l'ensemble de l'historique de « localiser » et de surveiller les pseudonymes dont l'activité serait perçue comme suspecte. De ce point de vue, l'argent liquide et les cartes prépayées offrent de plus grandes possibilités pour financer des opérations illégales en plein anonymat.[12]

Mais pour les produits dérivés, notamment, il est nécessaire d'enregistrer non seulement l'identité des parties et le montant de la transaction, mais de nombreux détails sur celle-ci. Cela pourrait pousser à créer des chaînes privées, sous réserve de leur non-falsifiabilité et du remplacement de la validation algorithmique (« proof of work ») par un « proof of stake » sans risque de collusion.

Preuves de travail et de détention : le rôle du consensus dans l'édification des règles de gouvernance

La méthode historique de consensus, utilisée par Bitcoin, est la preuve du travail (« *proof of work* »). Cette méthode utilise l'énergie [13] comme moyen de vérification que le nœud (« mineur ») a bien réalisé un travail : ainsi, cela me coûte réellement du temps et donc de l'énergie de participer à la sécurité du réseau et je sais que cela coûte également aux autres participants du réseau. En conséquence, tous les participants ont un véritable intérêt à ce que le réseau fonctionne et garde une valeur. Le travail consiste à trouver un nombre x dont l'image f(x) par une fonction (de *hashage* appelée SHA-256) soit inférieure à un nombre fixé par avance par le réseau. La difficulté de travail étant liée à la probabilité de trouver ce nombre du premier coup. Sur Bitcoin, il faut répéter plusieurs centaines de milliards de fois l'opération pour espérer résoudre ce problème. Ainsi, seul un nœud ayant consommé beaucoup d'énergie sera capable de proposer un bloc de transactions. Les transactions inscrites dans ce nouveau bloc seront ensuite certifiées par le réseau à l'aide d'un protocole de vérification. Tant que plus de 50% de la puissance de calcul mise à disposition sur le réseau par l'ensemble des nœuds n'est pas sous contrôle d'un tiers malveillant, cette méthode est considérée comme inviolable[14].

Les deux principaux écueils généralement associés à cette méthode sont : le temps de latence nécessaire pour valider une transaction et le gain décroissant des mineurs[15]. Ces points sont discutés au sein de la communauté Bitcoin pour être améliorés, via une modification du code. Par ailleurs, la forte consommation d'énergie liée à cette méthode est également pointée du doigt.

---

[12] De la même manière que, dans le débat entre Apple et le FBI, il a émergé que l'achat de téléphones mobiles pré-payés et à usage unique s'avère plus efficace que le cryptage des données dans un smartphone.

[13] Soit une des trois des ressources physiques rares et infalsifiables à sa disposition : le nœud étant une puissance de calcul, il s'agit soit d'énergie, soit de temps, soit d'espace. Pour un nœud, l'énergie est obtenue en réalisant un nombre élevé de calculs (« minage »).

[14] Avec les volumes actuels, le coût du contrôle d'un bloc Bitcoin est estimé à plusieurs centaines de millions d'euros. Les blocs étant chaînés, ce coût initial augmente de manière exponentielle à mesure qu'on « remonte » dans la Blockchain et dans le temps.

[15] Ce gain décroissant pourrait réduire leur motivation, une forme nouvelle de la « Tragédie des Biens Communs »

Face à ces constats, la communauté blockchain débat sur l'utilisation d'autres méthodes de consensus qui ne seraient plus la preuve de travail mais par exemple la preuve de détention.

Depuis quelques mois, plusieurs sociétés tentent de mettre au point de nouvelles méthodes. Ainsi, la crypto-monnaie **Peercoin** utilise un mélange entre la preuve de travail et la preuve de détention (« *proof of stake* »[16,17]), c'est-à-dire qu'elle adapte la difficulté du travail en fonction de la « part » de chacun des nœuds. La « part » étant définie comme le produit du nombre de peercoin détenus et de l'âge de chacun de ces nœuds. Plus la « part » est élevée, plus la difficulté de la fonction de *hashage* est réduite[18] ; cela réduit ainsi mécaniquement la consommation d'énergie nécessaire pour miner.

Ethereum, qui utilisait la méthode de la preuve du travail en 2015, a annoncé sa décision de migrer progressivement vers la preuve de détention[19]. Cette migration pourrait cependant être remise en cause en raison de l'explosion récente du cours de l'Ether, qui a sextuplé de mi-janvier à mi-février pour passer devant Ripple en valeur.

Enfin, **Ripple** (crée en 2014) qui au sens strict n'est pas une blockchain et fonctionne via un système de vote itératif où 80% des serveurs doivent être d'accord sur une transaction pour qu'elle soit validée[20]. Ripple peut être utilisé comme système de règlement pour les banques.

Au final, ce débat autour de la méthode de consensus déterminera largement le choix de la gouvernance dans les technologies blockchain utilisée. C'est toute la question de l'apparition de nouveaux tiers de confiance, ce qui dans le domaine financier se révèle crucial par rapport au *business models* existants.

[16] L'idée derrière la preuve de détention est qu'au lieu de consommer une ressource physique, le mineur consomme la cryptomonnaie elle-même ; « *la preuve de détention a, elle aussi une elle aussi, une inégalité à satisfaire mais celle-ci concerne la quantité de monnaie qu'un utilisateur possède. La probabilité qu'un compte parvienne à confirmer le prochain bloc de transactions à ajouter à la blockchain est proportionnelle à la quantité de monnaie qui est sur ce compte* » (source : Finyear, Mars 2016, *Les consensus Proof of Work vs. Proof of Stake*)

[17] Les principaux avantages de cette méthode sont : la réduction de l'énergie consommée et la fin de la course à la puissance.

[18] Bitcoin Magazine: *"What proof of stake is and why it matters?"*

[19] http://cointelegraph.com/news/is-ethereum-vaporware

[20] https://ripple.com/files/ripple_consensus_whitepaper.pdf

II - Du règlement-livraison à la conservation : les enjeux sur les marchés financiers

Au-delà des cryptomonnaies, les marchés financiers constituent le terrain d'expérimentation naturel de la blockchain[21]. Les régulateurs ne s'y trompent pas. Ainsi par exemple, lors du dernier sommet du G20, le Forum de Stabilité Financière a décidé de suivre de près cette technologie et l'utilisation que pourraient en faire les marchés financiers[22]. Début mars 2016, quarante des plus grandes banques du monde, parmi lesquelles HSBC, Citigroup et BNP Paribas, ont formé un consortium, la société R3 CEV, qui teste notamment un nouveau système de transactions obligataires utilisant la technologie Blockchain. La suite logique de ce test est de développer cette technologie pour les opérations de règlement-livraison.

Or, ces dernières années, la France a perdu la maîtrise de la compensation (LCH/Clearnet) et la gouvernance du règlement-livraison et du dépositaire central (Euroclear, ex-Sicovam) alors même qu'elle dispose de « champions » mondiaux en matière de conservation de titres (BP2S, SGSS et CACEIS). Depuis la séparation du NYSE et d'Euronext, la place de Paris reste à la traîne des centres financiers, classée dorénavant à la 37ème place mondiale après avoir figuré dans les cinq premières places il y a une dizaine d'années[23]. La France est absente de la prise de décisions majeures qui transforment le monde de la finance, comme par exemple le projet de fusion le London Stock Exchange et Deutsche Börse.

Il semble donc très opportun de donner à la place de Paris un avantage technologique en y développant l'utilisation de la Blockchain. Comme à chaque fois que l'on se trouve face à une technologie émergente, les attentes sont extrêmement fortes. Certaines études récentes estiment que le coût pour les acteurs des marchés financiers pourrait diminuer de 20 milliards de dollars par an[24] et que Blockchain permettra d'assurer une quasi-instantanéité des opérations et surtout en supprimant le risque de contrepartie, au point, sans doute, de ne plus nécessiter de recourir à une chambre de compensation. Quoiqu'il en soit, la place financière qui introduira cette technologie la première gagnera une confiance parmi les investisseurs. Ceci pourrait les conduire à effectuer leurs opérations en priorité sur ce marché[25]. Certaines bourses comme le NASDAQ ou la Bourse de Sydney ne s'y sont d'ailleurs pas trompées en annonçant le recours à cette technologie.

---

[21] McKinsey Working Papers on Corporate & Investment Banking | No. 12 : *Beyond the Hype: Blockchains in Capital Markets* : http://www.the-blockchain.com/docs/McKinsey%20Blockchains%20in%20Capital%20Markets_2015.pdf

[22] Lettre du president du FSB au G20 des ministres des finances, 27 février 2016 : http://www.fsb.org/wp-content/uploads/FSB-Chair-letter-to-G20-Ministers-and-Governors-February-2016.pdf

[23] Cf. CCI Paris*, Paris Place financière des entreprises*, Octobre 2015.

[24] *The Fintech 2.0 Paper: rebooting financial services* : http://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf Plus récemment encore, Euroclear et Oliver Wyman ont publié un rapport sur l'utilisation de la blockchain dans les marchés financiers, mettant en avant ses avantages sur l'ensemble de la chaîne de valeur : du début de processus de transaction avec notamment la simplification des procédures de compliance (KYC/KYCC) jusqu'à la fin du processus la réduction des niveaux des appels de marge. Les risques opérationnels, de règlement ou de contrepartie se verraient considérablement réduits. Enfin, l'application de la blockchain permettrait l'auto-exécution de smart-contracts dans les activités « post marché », donnant ainsi la possibilité d'accélérer la création d'un écosystème innovant autour de cette technologie. https://www.euroclear.com/dam/Brochures/BlockchainInCapitalMarkets-ThePrizeAndTheJourney.pdf

[25] *Delivery versus payment on a blockchain* :

Il convient ici de distinguer les trois opérations de transaction, règlement-livraison et conservation[26], pour chacun des trois types de marché :

- règlementé, comme Euronext
- régulé mais non règlementé, comme Alternext
- hors marché ou OTC, comme le Marché Libre et les titres non cotés.

Les économies à réaliser semblent particulièrement importantes dans les opérations de règlement-livraison [27], où la mise en œuvre semble également la plus rapide. Par ailleurs, le Nasdaq Linq a montré qu'il était possible de développer une place de marché pour les titres non cotés en se basant sur une Blockchain, très probablement celle de Bitcoin[28]. En se prévalant d'expériences comme Euroquity de bpifrance, Place d'Echanges à Lyon, Alternativa et les initiatives de crowdfunding equity, la France semble bien placée pour utiliser **la Blockchain comme assise technologique pour la création de Bourses pour les titres non cotés**. Celle-ci pourra être progressivement vers les dérivés OTC, les transactions effectuées sur un marché réglementé et enfin pour les opérations effectuées chez un dépositaire central.

A ce stade, il s'agit surtout de donner à la France un cadre législatif favorable à l'utilisation de cette technologie. En adoptant la première la technologie Blockchain, Paris pourrait tenter de reconquérir son avance technologique, réelle jusqu'au rachat par Nyse, et devenir la place financière de référence en matière d'opérations post-marché et de règlement-livraison. Afin de réduire les risques inhérents au développement de cette technologie, la loi devrait déléguer à l'AMF le soin d'habiliter cette technologie utilisée par un système de règlement / livraison. Les conditions de sécurité et de transparence du registre décentralisé seraient fixées par un décret pris en conseil d'Etat.

Qu'est-ce que le post marché ?

En aval des transactions sur les marchés financiers, interviennent des activités dites de «post-marché» qui regroupent l'ensemble des opérations assurant la bonne fin des transactions. Après une phase de négociation où les ordres sont confrontés sur un marché, les titres faisant l'objet d'une transaction sont traités en deux étapes : une phase de «compensation» durant laquelle sont déterminés les soldes nets de titres à livrer, une phase de «règlement-livraison» se traduisant par la livraison des titres à l'acheteur et le versement des fonds correspondants au vendeur. L'étape de la compensation permet également de transférer les risques liés à la transaction vers la chambre de compensation/contrepartie centrale qui s'interpose entre acheteurs et vendeurs.

http://www.multichain.com/blog/2015/09/delivery-versus-payment-blockchain/

[26] cf. Annexe 2 : fonctionnement d'une Bourse

[27] 7 Ways Blockchain Technology Could Disrupt The Post-Trade Ecosystem, Kynetix White Paper (2015) : http://www.the-blockchain.com/docs/Seven%20ways%20the%20Blockchain%20can%20change%20the%20trade%20system.pdf

[28] On lira à ce propos "A Bitcoin Technology Gets Nasdaq Test Pilot to take place in fledgling Nasdaq Private Market", *Wall Street Journal*, 10/05/2015, http://www.wsj.com/articles/a-bitcoin-technology-gets-nasdaq-test-1431296886 et "Wall Street is using Bitcoin, not just the blockchain", CoinCenter, 12/5/2015, https://coincenter.org/2015/05/wall-street-is-using-bitcoin-not-just-the-blockchain/

Il devrait aussi être possible d'étudier ultérieurement l'utilisation de cette technologie dans les opérations effectuées au sein d'un Dépositaire central de titres afin d'authentifier les inscriptions en compte qui y figurent de la même manière qu'un écrit authentique. Cette reconnaissance des inscriptions en compte dans les livres ouverts chez un Dépositaire central de titres couplée à l'utilisation d'un système de règlement / livraison donnerait une sécurité à la circulation des titres, réduisant le risque de fraude et de manipulation.

Il est probable que le recours à cette technologie conduise à terme à amender la directive EMIR (« European Market Infrastructure Regulation ») et la directive MIF II (« Financial Instruments Directive ») afin de modifier l'obligation de participants à une transaction impliquant des produits dérivés de soumettre cette transaction à une chambre de compensation, dans la mesure où le recours à chambre de compensation ne présente plus le même intérêt dès lors que les opérations sont certifiées dans un grand registre. De la même manière, le recours à cette technologie ne devrait pas conduire à qualifier celle-ci de système de négociation au sens de la MIF II.

En conclusion, l'utilisation de la technologie de la blockchain dans les opérations de post marché présente les avantages suivants :

- Réduction du coût du risque et du coût opérationnel ;
- Réduction du *reporting* réglementaire ;
- Instantanéité des confirmations de bon dénouement des opérations ;
- Désintermédiation du marché ;
- Diminution drastique du risque de fraude et de manipulation ;
- Traçabilité totale des opérations.

III – Le droit applicable à la Blockchain

Qui est propriétaire de la Blockchain ?

Dans le monde du logiciel, il convient de distinguer logiciels ouverts de ceux qui sont protégés par des droits de propriété. Un logiciel est libre si et seulement si sa licence garantit les quatre libertés fondamentales : la liberté d'utiliser le logiciel, la liberté de copier le logiciel, la liberté d'étudier le logiciel, la liberté de modifier le logiciel et de redistribuer les versions modifiées. Les deux dernières libertés ne peuvent s'appliquer que si l'on a accès au code source qui est en quelque sorte la recette de fabrication du logiciel.

Qui est propriétaire de la blockchain ? Ici encore, la réponse dépend du type de blockchain utilisée. Dans une blockchain privée, la technologie développée par l'organisme en charge de la gestion de la blockchain est protégée par des droits de propriété intellectuelle, même si celle-ci utilise, pour une large partie, les codes sources versés librement lors de la création de la blockchain. Inversement, dans la blockchain publique, personne n'est « propriétaire » des codes sources, selon les principes communautaires de la théorie des biens communs.

Cette question de la propriété ou du contrôle des codes sources résonne de manière particulière dans l'industrie financière : il s'agit de la question de la protection des algorithmes utilisés dans certaines transactions financières et développés par des experts (les « quants ») dans la mesure où la plupart de ces algorithmes ne peuvent être protégés par des brevets ou droits d'auteur ; dès lors, ces algorithmes sont gardés secrets. Ceci n'est possible que dans une blockchain privée où les développements spécifiques apportés par l'éditeur ne sont pas toujours juridiquement protégés, mais dans ce cas, ils ne sont pas ouverts, pas même aux participants de la chaîne privée.

Force juridique des opérations réalisées dans la Blockchain

La Blockchain est une technologie. Dès lors :

- soit les opérations qui s'y traitent reflètent des transactions hors de la chaîne[29]. La chaîne de consensus constitue ici au mieux une preuve de la propriété, preuve qui n'est guère opposable aux tiers sans intervention du législateur pour étendre le régime de la preuve, un peu comme la signature électronique,
- soit elles constituent elles-mêmes des transactions (par exemple, le bitcoin).

L'enjeu du développement de la blockchain consiste ainsi à savoir comment lier les contrats « crypto » et les contrats « fiat », terme qui regroupe tout ce qui a trait à l'environnement juridique traditionnel[30]. C'est le problème de la cyberlaw et plus généralement de la relation entre cryptographie et opposabilité juridique[31,32].

---

[29] Il est désormais possible d'enregistrer sur la blockchain la preuve horodatée, irréfutable et indélébile de l'existence d'un document sans avoir à en révéler le contenu. L'expérimentation proposée par *proofofexistence* n'intègre pas le document lui-même dans le registre, mais une simple empreinte qui permet de prouver que le document existait à une époque donnée et qu'il est lié à une adresse précise. Empreinte qu'il est possible de confronter facilement à toute entité prétendant produire le document-source pour savoir s'il s'agit bien du même : la modification ne fût-ce que d'un caractère du document produit en effet une empreinte différente.

[30] cf. Quinn DuPont & Bill Maurer**,** « Ledgers and Law in the Blockchain **»,** The King's Review, 2015 : http://kingsreview.co.uk/magazine/blog/2015/06/23/ledgers-and-law-in-the-blockchain/

[31] Cf. Jean-François Blanchette, *Burdens of proof, Cryptographic Culture and Evidence Law in the Age of Electronic Documents*, Hardcover, 2012.

A l'heure actuelle, dans une blockchain ouverte, les opérations effectuées n'ont pas d'autre force juridique que la valeur que les participants à la chaîne veulent bien leur donner. Ainsi, dans le cas du bitcoin, les échanges de cette cryptomonnaie n'ont pas de valeur légale ; elles ne sont pas reconnues comme opposables aux tiers, mais uniquement entre l'acheteur et le vendeur. La situation est différente dans les chaînes privées puisque ces chaînes ne peuvent fonctionner qu'avec des règles internes opposables aux participants.

Un Etat peut légiférer sur la portée de ces chaines de blocs (publiques ou privées) et décider que ceux-ci constituent soit des preuves réfragables de propriété, soit des preuves irréfragables, voire même le titre de propriété lui-même. Mais dès lors que les opérations dépassent les frontières, les modalités de détermination de ce régime de preuve ne peuvent être élaborées que via une convention internationale. A défaut d'accord, on peut craindre la mainmise juridique par une puissance étatique plus forte que les autres sur la chaîne de consensus.

Le précédent de l'Internet et la mainmise des Etats-Unis, via la prédominance d'acteurs privés de droit américain (les fameux GAFA), doit ici servir d'exemple sur le risque de perte de souveraineté. On se souviendra utilement que l'essentiel des sommes investies jusqu'à présent dans les start-up Blockchain (estimées à 1 milliard de dollars) l'a été depuis Silicon Valley.

[32] La question de l'utilisation de la blockchain dans les opérations de règlement / livraison dans l'industrie financière illustre les bouleversements que cette technologie peut apporter : un registre décentralisée privée peut demain remplacer les dépositaires centraux tels que Euroclear, DTCC et autres, sous réserve de régler préalablement la question juridique du droit de propriété des titulaires de titres. Cf. Pascal Bouvier, "Distributed Ledgers Part II: Clearing, Settlements & Legal frameworks" : https://www.linkedin.com/pulse/distributed-ledgers-part-ii-clearing-settlements-pascal-bouvier-cfa?trk=mp-reader-card

Recommandation #1 : la Blockchain comme preuve authentique au regard de la loi

Et :

Recommandation #2 : pour un droit d'expérimentation dans le cas du règlement-livraison, particulièrement dans le cas de titres non cotés

Pour créer un écosystème français favorable à l'émergence de futurs leaders utilisant cette technologie, nous proposons de reconnaître la technologie Blockchain comme une preuve authentique au regard de la loi.

Tout en restant agnostique sur les choix technologiques réalisés par les nouveaux acteurs, l'Etat doit aider à la mise en place d'un écosystème favorable à cette technologie. Pour cela, nous proposons à très court terme :

(i) que le gouvernement lance une étude sur les risques et opportunités que constitue cette technologie pour l'Etat, à l'image du rapport publié par l'Etat du Vermont le 15 janvier 2016[33]

(ii) que la loi française reconnaisse la technologie Blockchain comme une preuve certifiante de même nature qu'un écrit sous la forme authentique pour le dénouement des transactions boursières.

En pratique, il s'agirait d'adopter une mesure législative pour les opérations de règlement-livraison sur titres en suite d'opérations de négociation réalisées sur un marché de gré à gré, à insérer dans le code monétaire et financier, selon laquelle l'authenticité[34] de l'opération (en l'espèce une vente) serait considérée comme un acte authentique dès lors que cet acte est enregistré dans un registre décentralisé recourant à une technologie considérée comme sécurisée et transparente. Ainsi, les transactions dénouées dans ces systèmes auront toutes les caractéristiques de l'acte authentique:

- **Date certaine** : l'acte authentique fait foi d'une date et celle-ci est incontestable. Elle peut donc servir de preuve ;
- **Le contenu est garanti par le registre décentralisé** : il garantit la validité du fond et de la forme de l'acte ;
- **L'acte a force probante** : l'acte authentique est un élément de preuve incontestable, il fait l'objet du plus haut niveau de preuve recevable en cas de litige ;
- **L'acte a force exécutoire** : la force exécutoire est de plein droit. De plus, elle est valable non seulement sur le territoire français mais également au sein de l'espace judiciaire européen. Cela signifie que l'acte a force exécutoire de plein droit, même ailleurs qu'en France.

[33] http://fr.scribd.com/doc/296118021/Blockchain-Technology-Opportunities-and-Risks

[34] L'acte authentique est défini par l'art. 1317 du Code civil comme étant « *celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises* ». Ce sont les actes notariés, les actes civils (acte de mariage, de décès,...). L'acte authentique est censé refléter la vérité, du moins pour les mentions correspondant aux constatations personnelles faites par l'officier public.

Ultérieurement, et au-delà de l'expérimentation sur les marchés financiers réglementés, il sera possible d'élargir le régime de la preuve par acte authentique recourant à la technologie de la Blockchain en complétant la loi du 13 mars 2000 sur l'adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique [35] .

Cette reconnaissance générale comme preuve légale authentique permettrait à la France de prendre une avance considérable dans le domaine[36] et faire émerger de nouveaux acteurs dans les domaines du « smart contracts ».

Recommandation #3 : 500M€ pour la blockchain dans le PIA 3

Entre 2009 et 2012, les gouvernements successifs ont mis en place deux Programmes d'Investissements d'Avenir (PIA) ; le montant total des programmes est de 47 milliards d'euros et selon Louis Schweitzer la totalité des fonds devrait être engagée d'ici mi-2017[37].

Le 12 mars 2015, François Hollande a annoncé une nouvelle vague d'investissements avec la création d'un PIA 3 qui devrait être doté de 10 milliards d'euros. Etant donnée le potentiel de la technologie blockchain, de son application dans l'ensemble de l'économie et de ses enjeux de souveraineté, nous préconisons qu'une part dédiée de 500M€ soit inscrite dans le prochain PIA.

Cet investissement pourra être ventilé dans la recherche, la formation ainsi que dans le financement de projets ou de jeunes entreprises utilisant cette technologie.

[35] Selon l'art. 1341 du code civil, « *doit être passé acte devant notaires ou sous signature privées de toute chose excédant une somme ou une valeur fixée par décret, même pour dépôt volontaire, et il n'est reçu aucune preuve par témoin contre ou outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors ou depuis les actes, encore qu'il s'agisse d'une somme ou valeur moindre* ».

[36] Seul l'Etat du Vermont, aux Etats-Unis, a adapté sa législation en ce sens.

[37] http://www.usine-digitale.fr/article/le-pia-3-mettra-l-accent-sur-l-agroalimentaire-la-formation-et-le-tourisme-previent-louis-schweitzer.N367148

Annexe 1 : Vermont Blockchain Draft Bill

BILL AS INTRODUCED H.737

Introduced by Introduced by Representatives Clarkson of Woodstock, Dakin of Colchester, Baser of Bristol, Botzow of Pownal, Carr of Brandon, Christie of Hartford, Eastman of Orwell, Kitzmiller of Montpelier, Marcotte of Coventry, O'Sullivan of Burlington, Parent of St. Albans Town, Scheuermann of Stowe, Sibilia of Dover, and Stuart of Brattleboro Referred to Committee on

Subject: Judiciary; commerce and trade; records; blockchain technology

Statement of purpose of bill as introduced: This bill proposes to address the validity and admissibility of, and presumptions relating to, records created with blockchain technology.

An act relating to recognizing blockchain technology. It is hereby enacted by the General Assembly of the State of Vermont:

Sec. 1. 12 V.S.A. § 1913 is added to read:

17 § 1913. BLOCKCHAIN ENABLING

(a) In this section "blockchain technology" means a mathematically secured, chronological, and decentralized consensus ledger or database, whether maintained via Internet interaction, peer-to-peer network, or otherwise.

(b) Presumptions and admissibility.

(1) Extrinsic evidence of authenticity as a condition precedent to admissibility in a Vermont court is not required for a record maintained by a valid application of blockchain technology.

(2) The following presumptions apply:

(A) A fact or record verified through a valid application of blockchain technology is authentic.

(B) The date and time of the recordation of the fact or record established through such a blockchain is the date and time that the fact or record was added to the blockchain.

(C) The person established through such a blockchain as the person who made such recordation is the person who made the recordation.

(3) A presumption does not extend to the truthfulness, validity, or legal status of the contents of the fact or record.

(4) A person against whom the fact operates has the burden of producing evidence sufficient to support a finding that the presumed fact, record, time, or identity is not authentic as set forth on the date added to the blockchain, but the presumption does not shift to a person the burden of persuading the trier of fact that the underlying fact or record is itself accurate in what it purports to represent.

(c) Without limitation, the presumption established in this section shall apply to a fact or record maintained by blockchain technology to determine:

(1) contractual parties, provisions, execution, effective dates, and status;

(2) the ownership, assignment, negotiation, and transfer of money, property, contracts, instruments, and other legal rights and duties;

(3) identify, participation, and status in the formation, management, record keeping, and governance of any person;

(4) identity, participation, and status for interactions in private transactions and with a government or governmental subdivision, agency, or instrumentality;

(5) the authenticity or integrity of a record, whether publicly or privately relevant; and

(6) the authenticity or integrity of records of communication.

(d) The provisions of this section shall not create or negate:

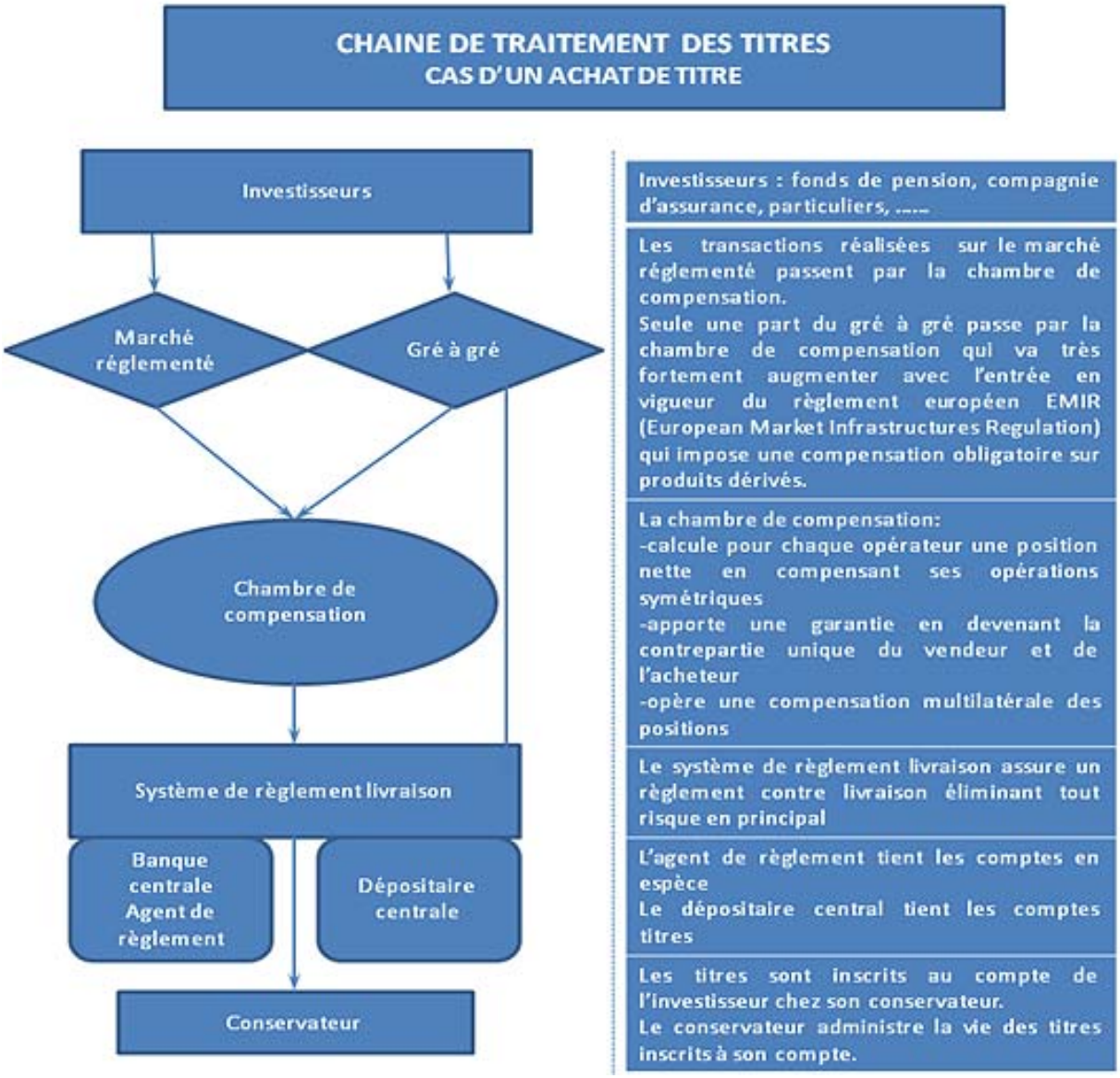
(1) an obligation or duty for any person to adopt or otherwise implement blockchain technology for any purpose authorized in this section; or

(2) the legality or authorization for any particular underlying activity whose practices or data are verified through the application of blockchain technology.

Sec. 2. EFFECTIVE DATE

This act shall take effect on July 1, 2016.

Annexe 2: Schéma Fonctionnement d'une bourse



Source : Banque de France[38]

[38] : https://www.banque-france.fr/stabilite-financiere/infrastructures-des-marches-financiers-et-moyens-de-paiement-scripturaux/infrastructures-des-marches-financiers/traitantlestitres.html?tx_cookiepolicybar_pi1%5Baction%5D=close&tx_cookiepolicybar_pi1%5Bcontroller%5D=CookieBar&cHash=1bdacdbf111f5a779a017cef527603bc