42 - **Le statut des plateformes de crypto-monnaies. –** Dès lors que les crypto-monnaies peuvent être qualifiées effectivement de monnaies, il est logique que les opérateurs soient considérés comme des prestataires de services de paiement, alors même qu'il n'y aurait pas nécessairement de mouvement libellé en monnaie ayant cours légal. Il s'agit du prolongement logique des analyses précédentes qui proposent de qualifier les crypto-monnaies de monnaies pouvant donner lieu à des opérations de paiement au sens du Code monétaire et financier. Cela rejoint l'analyse proposé par certaines institutions qui ont eu à connaître de la question. Ainsi, la cour d'appel de Paris a-t-elle confirmé le jugement du tribunal de Créteil qui avait considéré qu'une plateforme ayant une activité d'intermédiation pour le paiement de transactions en bitcoins ne pouvait invoquer le droit au compte [57]. Sans réellement prendre parti sur la nature des Bitcoins et sur la nature des opérations en cause, cette décision tend à considérer les opérations sur les crypto-monnaies comme des services de paiement. Dans le même ordre d'idées, l'ACPR a adopté une position énonçant que « dans le cadre d'une opération d'achat/vente de bitcoins contre une monnaie ayant cours légal, l'activité d'intermédiation consistant à recevoir des fonds de l'acheteur de bitcoins pour les transférer au vendeur relève de la fourniture de services de paiement » [58]. Le paradigme monétaire qui invite à qualifier les crypto-monnaies de monnaie véritables, les opérations sur ces monnaies de services de paiement, ou de monnaie électronique, et les établissements de prestataires de services de paiement, ou d'établissement de monnaie électronique le cas échéant, est bien plus cohérent que la position de la Banque de France qui considère que la qualification de moyen de paiement ne peut être retenue tout en considérant que l'activité de change/conversion des crypto-monnaies en devises ayant cours légal entre dans le champ de la réglementation bancaire [59]. La difficulté vient de l'originalité du système totalement décentralisé mis en place. Cela s'éloigne considérablement du schéma traditionnel. Pour autant, il n'est pas impossible de voir, avec M^me^ Pailler, dans la crypto-monnaie « un système de paiement électronique sans intermédiaire » [60]. Cette analyse permet de dépasser l'obstacle de la qualification monétaire et de mettre en évidence la vraie question de la sécurité des transactions qui peut conduire à se demander si le statut de prestataire de service paiement ou d'établissement de monnaie électronique est bien adapté au regard des risques présentés par ces activités. Ce n'est pas le lieu d'entreprendre cette étude mais il sera permis de regretter qu'elle n'ait pas été engagée lors de la discussion de la deuxième directive service de paiement [61].

43 - **Conclusion. –** Bien que l'avenir des crypto-monnaies soient des plus incertains et que les perspectives des monnaies locales, bien que réelles, restent limitées, les questions soulevées par les monnaies alternatives ouvrent de nombreuses et stimulantes perspectives. Parmi elles, il ne faut pas négliger l'intérêt renouvelé pour l'étude de la monnaie, phénomène économique et social essentiel mais étonnamment négligé. Au plan technologique, l'invention du système du blockchains suscitent déjà de nombreuses initiatives en dehors du domaine monétaire ; il se peut que ce soit là la véritable innovation ! Les manifestations pathologiques des monnaies alternatives restent encore assez limitées mais elles pourraient devenir plus nombreuses si le phénomène se développe : les premières analyses menées par les institutions et la doctrine auront alors largement identifier les voies possibles. Cependant, si les régulateurs et les juges souhaitent disposer d'outils cohérents et porteurs de solutions concrètes et cohérentes, ils devraient davantage porter leur attention vers le paradigme monétaire.

Mots-Clés : Instrument de paiement - Monnaies alternatives

57. *CA Paris, pôle 5, ch. 6, 26 sept. 2013, n° 12/000161 : JurisData n° 2013-024887 ; JCP 2014, 1091, note critique Th. Bonneau ; RD bancaire et fin. 2014, comm. 3, note Th. Samin et F.J. Crédot.* – Comp. avec *P. Pailler, Quelles règles pour l'encadrement de la crypto-monnaie en France : RISF 2014/4, p. 39, spéc. p. 40*, qui remarque que s'il est possible que le gestionnaire de la plateforme exécute des opérations de paiement « encore faut-il qu'il encaisse véritablement les fonds provenant de l'acheteur et verse les fonds au profit du vendeur, activité qui n'est pas nécessairement caractéristique pour la plate-forme de conversion, mais plutôt pour l'établissement de paiement associé ».
58. *Position ACPR, n° 2014-P-01.*
59. *Banque de France, Les dangers liés au développement des crypto-monnaies : l'exemple du bitcoin, préc.*
60. *P. Pailler, art. préc., spéc. p. 42.*
61. Comp. avec les propositions Outre-Atlantique, *V. Jamet, La « bitlicence » – Perspective nord-américaine d'un cadre juridique pour un « bitgeneration » encore en devenir : RISF 2014/4, p. 12.*

7 La blockchain défiera-t-elle la règle ?

Hubert de Vauplane, avocat, Kramer Levin LLP

Tout a été dit sur la blockchain... On rappellera qu'il s'agit d'une technologie de transfert et d'archivage d'informations permettant d'assurer un degré quasi parfait de fiabilité et de sécurité des transactions en répondant aux problèmes de la fiabilité des transmissions et de l'intégrité des interlocuteurs. D'un simple point de vue terminologie, le législateur français a défini cette technologie comme un *« dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations »*, préférant ainsi l'expression de « dispositif partagé » à celle de « registre distribué » [1]. Il est vrai que cette seconde expression résulte directement de la traduction française de Distributed Leger Technologie (DLT), expression retenue usuellement pour désigner la technologie de la blockchain même si celle-ci est plus étroite dans la mesure où elle ne vise qu'un certain type de registres distribués, généralement liés à une cryptomonnaies, et en particulier le bitcoin [2].

Si les développements pratiques de la blockchain sont potentiellement immenses (cadastre, livret médical, vote électronique, identité numérique, droits d'auteur, paiement, tenue de registre titres [3]...), il existe encore peu d'applications concrètes du fait de la complexité inhérente à cette technologie. Pour le juriste, les questions sont multiples : les plus « simples », comme celles relatives au droit applicable aux opérations dans la blockchain [4], aux plus complexes, comme la force juridique (probatoire ou force exécutoire) des informations inscrites dans la blockchain.

En fait, rien n'a été dit ! Bien sûr, chacun y va de son explication plus ou moins technique sur cette technologie. Et inévitablement, on parle du bitcoin. Plus rarement des autres crypto-monnaies. À regarder de près la littérature non spécialisée sur le sujet, blockchain et bitcoin semblent liés comme des frères siamois. Ce qui n'est pas totalement faux, mais qui n'est plus totalement vrai aujourd'hui. Pourquoi ? Parce que la première utilisation grandeur nature de la blockchain, et celle qui aujourd'hui fonctionne le mieux, est effectivement le bitcoin. À ce stade, on pourrait déjà considérer que le bitcoin est inhérent à la blockchain. Première erreur. Il n'existe pas une mais plusieurs technologies blockchain, selon le langage informatique utilisé. Deuxième erreur, ces différentes technologies n'utilisent pas toujours le bitcoin, mais parfois d'autres crypto-monnaies. Car l'une des particularités de cette technologie réside dans le mode de certification, de vérification, d'authentification d'une nouvelle transaction. Ce n'est qu'après cette validation qu'un maillon nouveau peut être ajouté à la chaine de blocs. C'est ce qui fait la force de ce système : toutes les transactions qui sont liées historiquement ont été validées de manière telle qu'elles sont considérées comme infalsifiables. Or, cette vérification est effectuée par une personne autre que celle qui a initiée l'opération, non pas selon une méthode centralisée où une personne (tiers de confiance) est supposée valider l'ensemble des opérations, mais selon une méthode de consensus qui permet d'éviter la fraude, faute de puissance de calcul suffisante pour renverser celle de la communauté des « valideurs » [5]. Il faut donc rémunérer ce travail de validation. En effet, vérifier un nouveau maillon de la chaine nécessite de réquisitionner beaucoup de puissance de calcul d'ordinateurs, ce qui a un coût. Ce sont ce que l'on appelle les mineurs (mining). Dans un système de blockchain comme le bitcoin, la validation d'une transaction nouvelle est rémunérée pour celui qui effectue cette vérification par l'attribution de bitcoins. C'est la méthode de consensus du Proof of Work ; Mais certaines chaines de blocs ont recours à d'autres crypto-monnaies. La plus connue après bitcoin, est l'éther, avec la chaîne Ethereum. Cependant, toutes les blockchains ne recourent pas à la méthode du consensus via la Proof of Work (PoW) mais parfois à une autre méthode, celle appelée de la Proof of Stake (PoS), où la validation est alors effectuée par des « forgeurs » (minting). Si la PoW permet d'exécuter plusieurs fois les algorithmes de « hachage » (fonction qui calcule une empreinte servant à identifier rapidement mais partiellement la donnée initiale) ou de calculer des puzzles mathématiques selon des algorithmes pour valider les transactions électroniques, la PoS est une méthode par laquelle une chaîne de blocs d'une crypto-monnaie vise à atteindre un consensus distribué. La différence ? Une question de méthode, car dans les 2 cas, il faut rétribuer le travail des « valideurs ». Mais comme toutes les blockchains ne sont pas publiques, il est apparu encore d'autres formes de consensus dans les chaines dites privées (celles dont l'accès et l'utilisation nécessitent l'accord d'une communauté (typiquement, les chaines développées par les banques entre elles, comme R3 en matière de paiement). Les blockchains privées ont des modèles très différents des chaines publiques car les « nœuds » (points de validation) sont connus et identifiés. Ces chaines ont alors recours à des techniques différentes de consensus, comme par

1. *Ord. n° 2016-520, 28 avr. 2016 relative aux bons de caisse. – C. mon. fin., art. L. 223-12.*
2. *ESMA, The distributeld Ledger Technology applied to securities markets, June 2006, § 4.*
3. *H. de Vauplane, quand le législateur s'intéresse à la blockchain pour les titres non cotés : Banque 2016, n° 798, p. 16.*
4. *H. de Vauplane, La blockchain et la loi : Banque 2016, n° 794.*
5. *H. de Vauplane, Blockchain, la question de la preuve par le consensus au cœur de la gouvernance : Banque 2016, p. 16.*

exemple la Preuve d'autorité (PoA), laquelle ne nécessite pas de recourir à une crypto-monnaie.
Pourquoi tous ces développements ? Simplement pour souligner qu'il existe aujourd'hui un grand nombre de blockchains, répondant toutes à la même logique qui est celle de transmettre et d'archiver des informations de façon sécurisée. Or, le sujet principal d'une blockchain (en dehors des aspects techniques, bien sûr), c'est de déterminer le fonctionnement du consensus. Ce qui permet facilement à un juriste de les différencier entre elles, c'est leur gouvernance : dis-moi comment fonctionne ton consensus, et je te dirai qui tu es !
Et à partir de ce moment-là, le juriste retrouve ses droits. Car derrière la question de la gouvernance, c'est celle de la « règle du jeu » qui se profile. Comment fonctionne une blockchain et encore plus une DAO (decentralized autonomous organization), ces organisations informelles qui fonctionnent grâce à un programme informatique fournissant des règles transparentes et immuables de gouvernance à une communauté car elles sont inscrites dans la blockchain ? Ne va-t-on pas vers ce que 2 auteurs ont appelé une lex cryptographia, c'est-à-dire des fonctionnalités administrées automatiquement via un « smart contract » ? [6] Mais alors, peut-on modifier ces règles et dans ce cas, qui peut décider de cette modification d'un « smart contract » ? On connait l'expression célèbre « code is law » de Lessing [7] selon laquelle la régulation des comportements passe moins par les normes juridiques que par l'architecture technique des systèmes informatiques ; ce qui conduit à considérer que ce qui est codé informatiquement constitue la règle (le code) entre les utilisateurs. Dès lors, il ne serait plus possible de modifier quoi que ce soit dans le code, même en cas d'erreur. Quand l'algorithme devient plus fort que les tables de la loi. Mais n'oublions pas que celles-ci ont été brisées [8].

6. *A. Wright and P. De Filippi, Decentralized blockchain technology and the rise of lex cryptographia, March 2015, SSRN : https ://ssrn.com/abstract=2580664.*
7. *L. Lessing, Code is law : Harvard Magazine, 2000.*
8. *Exode, 32, 16.*