Kramer Levin

Webinaire Blockchain & Risques : « *Responsabilité et Gouvernance* »

12 JANVIER 2021

Hubert de Vauplane

1/ Gouvernance & Blockchain

1/ Gouvernance & Blockchain

Définitions

- La *blockchain* se définit comme une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Elle s'apparente à un grand livre comptable décentralisé (en réseau pair à pair) enregistrant, à intervalles de temps réguliers, les transactions du réseau.
- Le fonctionnement décentralisé de la *blockchain* pose la question de sa gouvernance et de l'identification des acteurs de celle-ci.
- La gouvernance d'une chaîne de blocs concerne la manière dont celle-ci est initiée et gérée. Elle définit les règles et procédures concernant la validité des transactions, l'émission de nouveaux actifs, le règlement des litiges, le processus d'adoption des mises à jour du code, la protection contre les cyber-risques ou encore l'adhésion au réseau et la gestion des autorisations.
- Comme corollaire de cette décentralisation les modes de gouvernance sont très variés d'une *blockchain* à une autre (A). Cette gouvernance repose sur une multiplicité d'acteurs (B).

A. Des modes de gouvernance multiples

1. Gouvernance centralisée et gouvernance décentralisée

- **La gouvernance centralisée** fait référence aux *blockchains* privées, c'est-à-dire dont le nombre d'acteurs (les nœuds du réseau) est limité. Les *blockchains* privées regroupent toutes les solutions que les entreprises peuvent utiliser soit de manière partiellement décentralisée (*consortium*) soit avec une gouvernance totalement centralisée (*permissioned*).
  - Exemple : la *blockchain* Hyperledger développée par la Linux Fundation est une *blockchain* privée.
- Ce modèle de gouvernance centralisé sur une ou plusieurs entités juridiques ne présente pas de difficulté particulière quant à leur supervision par un régulateur.
- **La gouvernance décentralisée** fait référence aux *blockchains* publiques, c'est-à-dire dont le nombre d'acteurs (les nœuds du réseau) est illimité.
- La *blockchain* Bitcoin est l'archétype de la *blockchain* publique (*permissionless*). La gouvernance d'une telle *blockchain* repose essentiellement sur les mineurs qui effectuent le travail de vérification-sécurisation-enregistrement des blocs.
- Ce modèle de gouvernance décentralisé rend son appréhension par un régulateur beaucoup plus délicate.

2. Gouvernance « *on-chain* » et gouvernance « *off-chain* »

- La gouvernance ***« on-chain »*** signifie que le processus décisionnel et sa mise en œuvre s'effectue directement dans la *blockchain* par le code.

- A l'inverse, dans une gouvernance ***« off-chain »*** les décisions sont prises en dehors de la *blockchain* par un consortium de développeurs, organisé de manière informelle ou réunis dans le cadre d'une fondation voire d'une entreprise privée, avant d'être implémentées dans le code.

- Par exemple la *blockchain* Tezos a un système de gouvernance qui combine des éléments « *on-chain* » et des éléments « *off-chain* ». La maintenance et l'amélioration du code de Tezos sont principalement soutenues et financées par la fondation Tezos, immatriculée en Suisse (gouvernance « *off-chain* »). Tezos permet aussi à toute personne de proposer des modifications du code, qui font ensuite l'objet d'un « vote » sur la *blockchain*.

- La *blockchain* Ethereum s'appuie sur une méthode de gouvernance en partie « *off-chain* » : les modifications du code proviennent majoritairement de la fondation Ethereum (immatriculée en Suisse dans le canton de Zoug et dirigée par un groupe de développeurs proches des créateurs d'Ethereum). Des groupes concurrents et indépendants de cette fondation participent également au développement du protocole en proposant des améliorations.

2. Gouvernance « on-chain » et gouvernance « off-chain »

- La gouvernance de la *blockchain* Bitcoin repose en partie sur le logiciel *open source* Bitcoin Core dont la maintenance est principalement assurée par un nombre restreint de *core developers* qui ont un accès préférentiel au *repository* Github sur lequel est publié le code de Bitcoin Core.

- Les systèmes de gouvernance « on-chain » reposent essentiellement sur le consensus des utilisateurs par des mécanismes de vote. Pour simplifier, les utilisateurs manifestent leur adhésion aux propositions de modifications directement sur la *blockchain*.

    - Sur les *blockchains* reposant sur la preuve de travail (*proof of work*), seule la puissance de calcul (émanant des mineurs) dirigée vers la proposition de modification permet d'évaluer son degré d'adhésion.

    - D'autres *blockchains* comme celles fonctionnant sur la preuve d'enjeu (*proof of stake* – les transactions sont validées par les utilisateurs détenant de grandes quantités de *tokens*) peuvent s'appuyer sur des mécanismes de vote reposant sur l'adhésion des détenteurs de *tokens*, sans prise en compte de la puissance de calcul.

- Par exemple, dans le domaine de la finance décentralisée, la startup Compound a créé un jeton de gouvernance permettant à ses détenteurs d'émettre des suggestions, des propositions en code exécutable soumises au vote de la communauté pendant 3 jours.

B. Une multiplicité d'acteurs de la gouvernance

- La *blockchain* étant par nature décentralisée, les acteurs de sa gouvernance sont nécessairement multiples et diffèrent en fonction des protocoles :
  - Il peut s'agir de mineurs ou de pool de mineurs (Bitcoin, Ethereum…);
  - des utilisateurs finaux avec droit de vote ;
  - des développeurs ou pools de développeurs parfois organisés sous forme de fondation (Ethereum…);
  - d'une ou plusieurs entreprises pour les *blockchains* privées (ex : EOS développée par la société Block.one ; la société ConsenSys qui finance l'amélioration du code d'Ethereum ainsi que de nombreux projets de créations d' « infrastructures » facilitant l'utilisation d'Ethereum)
- Cet éclatement des acteurs de la gouvernance rend plus délicate la recherche d'une personne ou d'un groupe de personne responsable en cas de dommage.
- Dans le fond, la gouvernance des *blockchains* publiques est avant tout **communautaire**. Une communauté de parties prenantes aux rôles variables et évolutifs (mineurs, développeurs, entrepreneurs créant des produits utilisant la *blockchain*, traders et investisseurs, etc.) se constitue de manière progressive autour de chaque *blockchain* et travaille de manière collective pour la développer et la promouvoir.

2/ Responsabilité & Blockchain

2/ Responsabilité & Blockchain

- Malgré sa réputation de registre inviolable (« *tamper-resistant* »), l'écosystème *blockchain* et toutes les applications décentralisées qui viennent s'y greffer ne sont pas à l'abri de failles de programmation et donc de l'exploitation de ces failles par des « pirates ».

- L'exemple de **The DAO** et de son piratage est éloquent. En mai 2016, une organisation autonome décentralisée a été créée pour réunir des fonds, sous forme d'ethers, afin de financer des projets utilisant la *blockchain* Ethereum. Une faille du code du *smart-contract* sur lequel reposait The DAO a été exploitée par des pirates qui détournèrent près d'un tiers des encours réunis par le projet ce qui entraîna par la suite la scission (*fork*) de la chaîne Ethereum en deux *blockchains* distinctes. Sur la chaîne « *forkée* » les transactions correspondantes au piratage ont ainsi été inversées ou annulées.

- L'affaire **Tezos** a provoqué un retentissement équivalent. Cette *Initial Coin Offering* (ICO) a levé en 2017 l'équivalent de 232 millions de dollars en Bitcoin et en Ether. Suite à des rumeurs de désaccords entre les deux fondateurs pouvant affecter la gouvernance du projet, une class action réunissant des investisseurs a été lancé contre l'ICO. L'affaire s'est clôturée par une transaction de 25 millions de dollars le 26 août 2020.

- Ces différents risques pesant sur l'investisseur amènent une série de questions sur la nature de la responsabilité (A), sur l'identification de la personne ou du groupe de personnes responsables (B) et sur la détermination de la juridiction compétente (C).

A. Nature de la responsabilité

- La *blockchain* servant de support à de multiples transactions, la responsabilité peut être de nature :
  - **contractuelle** : certaines transactions ne sont que la représentation de contrats, parfois automatisés par le biais de *smart-contracts,* en *blockchain*. La responsabilité d'une plateforme d'échange de crypto-actifs vis-à-vis de ses utilisateurs sera également de nature contractuelle, notamment si la plateforme se fait « hacker » et perd les fonds déposés par ses clients.
  - **délictuelle** : en l'absence de liens contractuels, l'utilisateur final qui a subi un dommage du fait d'une attaque ou d'un dysfonctionnement de la *blockchain* peut théoriquement obtenir réparation sur le fondement de la responsabilité délictuelle. En droit civil comme en *common law* la responsabilité de principe est la responsabilité pour faute (*negligence*). La question se pose d'appliquer une responsabilité sans faute (*strict liability*) ou une responsabilité du fait d'autrui (*vicarious liability*) aux acteurs de la *blockchain* (développeurs, mineurs etc.).
  - **pénale** : financement du terrorisme, blanchiment, fraudes et arnaques, marché noir…

B. L'identification d'une personne responsable

- L'identification d'un responsable est rendue extrêmement difficile par la nature décentralisée de la *blockchain* et le pseudonymat des adresses qui ne permet pas d'identifier automatiquement les personnes qui les contrôlent.
- Pour les *blockchains* privées, les ICOs émises avec un *whitepaper* identifiant l'émetteur et les plateformes d'échange et de conservation de cryptoactifs, l'identification d'un responsable ne pose pas de difficulté.
- Il en va différemment pour les *blockchains* publiques (Bitcoin, Ethereum…) où l'identification du détenteur d'un portefeuille (*wallet*) est extrêmement difficile.
- Pour pallier ce manque quelques pistes de réflexion ont pu être avancées :
  - imposer à certains acteurs (pool de mineurs, développeurs etc.) une responsabilité de plein droit (strict liability). Cette piste présente l'inconvénient de brider l'innovation en augmentant fortement le coût de développement des logiciels alors même que la blockchain repose sur un code open source;
  - imposer à ces acteurs une assurance tierce obligatoire (comme le recommande le parlement européen concernant le droit civil de la robotique);

- Pistes de réflexion (suite) :
  - responsabiliser les réseaux sociaux classiques (Facebook, Instagram, etc.) et tout autre partie prenante (site internet, plateforme en ligne…) hébergeant de la publicité ou redirigeant les internautes vers des applications décentralisées ou des blockchains douteuses.
  - Certaines techniques sophistiquées de « data mining » et d'analyses « big data » permettent, dans certains cas, l'identification des détenteurs d'adresse grâce à l'analyse de la blockchain. Par ailleurs, la collecte d'informations « off-chain » (sur les réseaux sociaux, blogs, internet, etc.) permet parfois indirectement d'identifier le détenteur d'un « wallet ».

C. La détermination de la juridiction compétente

- Le droit international privé pose des règles de rattachement permettant de déterminer la loi applicable aux différents types de litige.
- Exemples :
  - en matière d'état et de capacité des personnes il s'agit de la loi nationale de la personne (ou éventuellement de son domicile);
  - le régime des biens corporels est soumis à la loi du lieu de leur situation;
  - en matière de responsabilité délictuelle il s'agira du lieu du fait dommageable, où pour les actes volontaires du lieu où ils sont passés;
  - en matière contractuelle, il s'agira le plus souvent, de la loi désignée par les parties;
  - en matière pénale il s'agit du lieu de commission de l'infraction et de la nationalité de l'auteur et de la victime du crime ou du délit.
- L'application de ces critères de rattachement à l'écosystème *blockchain* est particulièrement délicate compte tenu de la décentralisation de ses acteurs à l'échelle mondiale.
- Par exemple, un logiciel *open source* contenant certaines failles est déployé sur la *blockchain* par un développeur anonyme. L'exploitation de ces failles par un pirate causera des dommages à des investisseurs du monde entier. Le lieu du fait dommageable est ainsi démultiplié en autant de lieu que de domiciliation des victimes.

- Des critères de rattachement très divers peuvent être identifiés :
  - Pour le cas d'une ICO, le *white paper,* comme document contractuel, peut identifier une juridiction compétente. La localisation de l'émetteur est également un élément de rattachement. Dans l'affaire Tezos les défendeurs ont cherché à contester la compétence de la *U.S. District Court for the Northern District of California.* La question qui se posait était celle de savoir si le tribunal avait compétence sur la Fondation Tezos et la société Bitcoin Suisse, étant donné que l'ICO était émise en Suisse et censée s'adresser uniquement aux investisseurs hors des États-Unis. Recourant à un faisceau d'indices (site hébergé aux U.S. et rédigé en anglais, existence d'un employé en Californie etc.) la juridiction U.S. a reconnu sa compétence.
  - En l'absence de relation contractuelle d'autres critères de rattachement peuvent être évoqués comme la localisation des fermes de minage et des pools de mineurs; la localisation des fondations ou groupes de développeurs, etc.
  - Pour une infraction pénale la nationalité de la victime, ainsi que le lieu de résidence permettent d'identifier un juge compétent.

    Ex : L'article 113-2-1 du Code pénal dispose que « *Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République.* »

- Les autorités de régulation bancaires et financières nationales (SEC, FCA, AMF/ACPR…) disposent également de compétences larges pour assurer leur mission de protection de l'épargne.
- Dès lors que les épargnants d'un pays sont directement visés par certaines offres, les régulateurs nationaux peuvent agir en utilisant divers outils : mises en garde, listes noires, demandes de fermeture judiciaire de sites internet faisant la promotion d'offres illégales, engagement de poursuites judiciaires, etc.
- En 2019 la SEC, le gendarme boursier américain, s'est attaquée à l'ICO de Telegram. L'ICO d'un montant de 1,7 milliard de dollars a été jugée comme étant "une vente illégale de security tokens" et donc soumise à enregistrement préalable. Une transaction à été signée. Selon cet accord, Telegram s'est engagé à rembourser 1,224 milliard de dollars.

En conclusion, les régulateurs nationaux et les juridictions nationales disposent de nombreux outils pour se considérer comme compétents territorialement et appliquer leur propre droit à des infractions ou à des violations contractuelles liées à des blockchains publiques.