Breveter Bitcoin

par François Veltz

10 juin 2019

L'auteur recommande de lire la version originale en anglais.

Les chaînes de blocs sont là pour rester. Élaborées à partir des chaînes de blocs, des crypto-devises comme Bitcoin ou Ethereum peuvent connaître des destins différents, voire divergents. Une série de quatre articles analyse la question des brevets et des chaînes de blocs, également appelées registres cryptographiques. Les inventions mises en œuvre par ou dans des chaînes de blocs exigent de bonnes connaissances en mathématiques (cryptographie, théorie des graphes, etc.), une bonne perspective économique (théorie de l'entreprise, mesures d'incitation, etc.), une certaine compréhension de la théorie des jeux (dilemme du prisonnier, coopération, concurrence), ainsi que de solides compétences en informatique (développement de logiciel, mise en œuvre et infrastructure de matériel).

Le premier article tente de fournir des définitions techniques, en langage clair, des chaînes de blocs et des objets ou méthodes associés (par exemple, chaînes de blocs privées par opposition à publiques, vérification par preuve de travail, contrats intelligents, etc.). Le deuxième article aborde les questions de la brevetabilité (par exemple, à partir d'une perspective européenne et américaine, il examine la législation et la jurisprudence et fournit des exemples d'inventions). Le troisième article présente les activités de protection par brevet observées actuellement (par exemple, les cessionnaires, les objets revendiqués et les évolutions récentes). Le quatrième et dernier article traite des perspectives actuelles et futures (par exemple, opportunités et menaces, applications verticales, dépistage de la propriété intellectuelle, etc.). Les articles proposent des recommandations de rédaction des brevets. Bien qu'étant reliés entre eux, le lecteur peut passer directement à l'article présentant le plus d'intérêt pour lui.

Le premier article revient à l'essentiel, d'un point de vue technique. Il tente d'expliquer en termes simples mais précis en quoi consistent une chaîne de blocs, un contrat intelligent et d'autres objets ou composants proches. Les variantes de ces objets font aussi l'objet d'une discussion, sans perdre de vue la rédaction des brevets. Il fournit une description provisoire des problèmes techniques résolus par ces objets ou combinaisons d'objets. Les chaînes de blocs sont souvent associées à des modèles économiques de rupture, où la coopération et la concurrence peuvent coexister, jouant sur des nuances subtiles. Il est essentiel de comprendre les motivations techniques et/ou commerciales sous-jacentes afin de construire des architectures appropriées. L'article montre que la généalogie intellectuelle des chaînes de blocs présente des racines anciennes, notamment dans l'informatique distribuée, même si certains de ses derniers développements font appel à des techniques récentes (dont la physique quantique).

Le deuxième article examine dans le détail les questions actuelles et prévisibles quant à la brevetabilité. Les chaînes de blocs, mises en œuvre par ordinateur, présentent des aspects de brevetabilité connus et généralement maîtrisés (par exemple, détectabilité des mécanismes cryptographiques, présence de code source ouvert et de code fermé, etc.), mais mettent en avant certains points, comme les contrefaçons partielles, à examiner attentivement car les registres cryptographiques ont un caractère distribué du fait même de leur conception. L'utilisation de registres cryptographiques privés et/ou publics, parallèlement aux accords-cadres contractuels existants, aux tensions et aux évolutions entre les mécanismes centralisés (par exemple, un ou plusieurs nœuds pour la collecte de données et/ou le traitement), décentralisés et distribués (aucun nœud central, réseau de pairs) peuvent modifier les possibilités de brevetabilité et les manières de rédiger les revendications et les descriptions de demandes de brevet.

Le troisième article présente des analyses terminologiques portant sur les demandes de brevet publiées de fin 2017 à juin 2019. Pour l'instant, les chiffres montrent une présence élevée d'entreprises du secteur des technologies de l'information (IBM ou Amazon), alors que la présence du secteur financier (par exemple, Goldman Sachs, VISA, etc.) reste à un niveau nettement inférieur que celui qui était attendu. Les universités chinoises ont déposé de nombreuses demandes de brevets ces dernières années. L'article analyse les dépôts effectués réalisés par des sociétés comme nChain.

Le quatrième article traite des opportunités et des menaces en matière de brevets. Il semblerait que les mécanismes de base (comme ceux des consensus distribués) ont été largement brevetés ou divulgués, mais il reste toutefois de multiples autres points prometteurs à exploiter. En premier lieu, les applications verticales des chaînes de blocs présentent de nombreuses opportunités car les brevets pionniers (sinon essentiels) n'abordent pas pour l'instant les spécificités des domaines d'application (par exemple, en avionique, pour les dispositifs médicaux, quant à la gestion de la confidentialité, pour les voitures autonomes, les systèmes de positionnement par satellites GNSS, etc.). L'article propose provisoirement un examen systématique des opportunités manifestes, en faisant varier les échelles de temps et d'espace, entre autres. Enfin et surtout, il décrit certains aspects de la course à l'armement brevet concernant la crypto-monnaie Bitcoin.

À titre de conclusion provisoire, les chaînes de blocs et les contrats intelligents sont susceptibles d'avoir un avenir durable, y compris en ce qui concerne les brevets. On peut donc s'attendre à ce que les chaînes de blocs, qui permettent de résoudre des problèmes techniques très spécifiques, soient adoptées dans un grand nombre d'industries. Elles ne règlent pas tous les problèmes techniques mais peuvent cependant être appliquées à de nombreuses inventions (impliquant une pluralité d'objets et présentant un problème de confiance par endroits, comme la sécurité, la fiabilité, etc.). Concrètement, cela peut se traduire par la description de modes de réalisation comprenant une ou plusieurs chaines de blocs, et peut justifier dans certaines situations l'écriture de revendications dépendantes.

Pour protéger vos droits de propriété intellectuelle, contactez algopatent.com

I. Chaînes de blocs, systèmes de validation par preuve et contrats intelligents

Quelques recommandations pour rédiger des demandes de brevet portant sur des inventions impliquant des chaînes de blocs ou des contrats intelligents.

1. Blockchains

Une chaîne de blocs (« blockchain » en anglais) est une base de données distribuée et sécurisée par des techniques cryptographiques.

Les transactions échangées sont groupées en « blocs » à intervalles de temps réguliers, de manière sécurisée par cryptographie, forment ainsi une chaîne. Les différentes transactions enregistrées sont regroupées dans des blocs. Après avoir enregistré les transactions récentes, un nouveau bloc est généré et analysé. Si le bloc est valide (consensus distribué), le bloc peut être horodaté et ajouté à la chaîne de blocs. Chaque bloc est lié au précédent par une clé de hachage. Une fois ajouté à la chaîne de blocs, un bloc ne peut plus être ni modifié ni supprimé, ce qui garantit l'authenticité et la sécurité du réseau. Le chainage utilise des fonctions de hachage et des arbres de Merkle. Un arbre de hachage est constitué par un ensemble de sommes de contrôle interdépendantes. Des sommes de contrôles sont concaténées selon une structure en arbre. Un arbre de hachage permet de pouvoir vérifier l'intégrité d'un ensemble de données sans disposer nécessairement de la totalité des données au moment de la vérification. Les enregistrements dans une chaine de blocs sont protégés contre la falsification ou la modification par les nœuds de stockage : falsifier un bloc nécessite de falsifier l'ensemble de la chaîne, de sorte que le coût total devient prohibitif et garantit un niveau de confiance en la non-falsification de l'ensemble de la chaîne de blocs. Les transactions sont visibles dans l'ensemble du réseau (sauf élagage dit « pruning »).

Pour modifier une chaine de blocs, il est nécessaire et suffisant de prendre le contrôle de la majorité des nœuds composant la chaine. En pratique, c'est très difficile (mais pas tout à fait impossible, y compris pour des chaines de blocs publiques et étendues ; *in fine* c'est une affaire de moyens financiers et de logistique).

Le temps est un facteur important pour les chaines de blocs (e.g. notion de propagation, de latence, de percolation dans l'Internet des Objets, de coalescence, etc). Le consensus distribué implémenté dans les chaines de blocs est une réponse au problème des Généraux Byzantins, dans lequel des participants à un réseau ouvert doivent se mettre d'accord sur une stratégie concertée en sachant que certains des participants sont ennemis, compromis ou malicieux. Le consensus distribué permet de sécuriser un réseau non-sécurisé, mais cela prend un certain temps. Ce temps peut être minimisé ou optimisé en utilisant des chaines de blocs secondaires ou d'autres techniques lesquelles augmentent aussi les capacités de stockage.

Les nœuds « mineurs » ou de « minage » sont des entités dont le rôle est d'alimenter le réseau en puissance de calcul, pour permettre la mise à jour de la base de données décentralisée. Ces mineurs peuvent être rétribués par la distribution de jetons

cryptographiques (« *tokens* »). D'autres modes de compensation (en complément ou par substitution) prévoient des commissions sur les transactions.

Une chaîne de blocs peut être publique ou privée, ou selon des gouvernances intermédiaires, qui peuvent utiliser différentes barrières à l'entrée (validation par preuve de travail). Une chaine de blocs « publique » fonctionne sans tiers de confiance (modèle dit « *trustless* ») (ou distribué ou computationnel) par opposition au modèle de confiance « *trusted* » (centralisé, e.g. institutionnel). Une chaine de blocs publique ne définit généralement pas d'autre règle que celle du code constitué par la technologie protocolaire et logicielle qui la compose. Une chaine de blocs « privée » comprend des nœuds participants au consensus qui sont définis à l'avance puis authentifiés. Ses règles de fonctionnement peuvent être éventuellement extrinsèques.

2. Systèmes de validation par preuve de travail

Pour prévenir ou éliminer les courriels indésirables, il a été proposé de faire payer un prix unitaire très faible mais non nul. De la sorte, les *spammers* qui envoient des millions d'emails se seraient retrouvés dans une équation économique défavorable. Les systèmes de validation par preuve de travail poursuivent le même objectif : ce sont des barrières à l'entrée.

Dans le cadre du consensus distribué, pour répondre au problème technique du contrôle de l'admission dans un système distribué, il est possible voire fréquent d'utiliser cette validation par preuve de travail (« *proof of work* » en anglais). Du point de vue mathématique, une preuve de travail est « difficile à fournir mais facile à valider ». Les systèmes de validation par preuve sont généralement asymétriques : le calcul qui est requis en contrepartie d'une demande de service est couteux pour le demandeur mais demeure facilement vérifiable par un tiers.

Dans le cas de Bitcoin, la vérification par preuve de travail sélectionnée (système *Hashcash*) est extrêmement complexe. Ce type de preuve de travail brûle, littéralement, une gigantesque quantité d'énergie. Alors que la planète est en guerre à cause du pétrole, un tel mécanisme peut donner une image assez négative (en termes de communication, car la sécurisation des transactions est « utile » en soi).

Afin d'éviter ce que certains considèrent comme une catastrophe écologique, de nombreuses alternatives ont été proposées ou sont en cours d'élaboration. D'après ces alternatives, les calculs ont généralement pour but d'être « utiles » à la société, par exemple à des fins médicales (comme la recherche sur le cancer). Les articles économiques soutiennent toutefois que « l'utilité » reste un concept relatif (il n'existe pas de calculs universellement utiles).

La principale alternative au principe *hashcash* est celle de l'approche dite « preuve de participation » (*proof-of-stake* en anglais). Dans les systèmes par preuve de participation (ou preuve d'enjeu), le créateur du bloc suivant est choisi en fonction de différents critères (par exemple, sélection aléatoire, fortune, âge ou autre : c'est-à-dire, l'enjeu). Il est également possible d'utiliser des systèmes hybrides. Notamment, la « preuve d'activité » peut combiner la preuve de travail et la preuve de participation (dans ce cas, la preuve de participation intervient comme une extension dépendant de l'horodatage de la preuve de travail).

Du point de vue de la protection par brevet, il peut s'avérer intéressant d'étudier d'autres options que les systèmes axés sur la preuve de travail que celui reposant sur le *Hashcash* (par exemple, confer le brevet « Client-Puzzle » décrit dans US7197639). Du point de vue mathématique, il n'est pas évident de déterminer comment configurer des types de tâches de calcul qui ne peuvent pas être optimisées ou contournées par d'autres biais. Aucune documentation proche n'a été trouvée concernant les alternatives aux systèmes par preuve de travail (les exigences des systèmes par preuve de travail, tels qu'ils sont actuellement compris, sont : i) les solutions doivent être facilement vérifiables ; ii) la difficulté à trouver une solution doit être contrôlable.). Nombreux sont ceux qui disent qu'il n'existe pas d'alternatives « efficaces » (concept relatif). Malgré tout, l'obtention de brevets permet d'exercer un contrôle, que ce soit pour encourager ou décourager la substitution. L'opinion publique a également son importance et, si certains choix de société étaient réalisés, comme d'inclure d'autres formes d'utilité, ces alternatives pourraient finalement être adoptées et implémentées dans les protocoles standards.

3. Contrats intelligents

Les chaines de blocs peuvent être ou devenir *programmables* par l'emploi de « contrats intelligents » (« *smart contracts* » en anglais). Le domaine des contrats intelligents est émergent, complexe et riche.

Un contrat intelligent comprend des données et/ou du code exécutable. A ce jour, les contrats intelligents demeurent des scripts, i.e. des programmes très courts qui peuvent être implémentés dans certaines chaines de blocs. Dans le futur, tels que les imaginent les industriels, les programmes pourraient devenir substantiellement plus longs et donc comprendre des inventions mises en œuvre par ordinateur brevetées. Il est concevable de penser que la complexité des contrats intelligents va augmenter de bas en haut (« bottom-up »), en rendant de plus en plus complexes les scripts implémentés dans les chaines de blocs, et/ou de haut en bas (« top-down ») en « gravant dans le marbre » des chaines de blocs des logiciels déjà sophistiqués.

3.1. Exemple de contrat intelligent

Un exemple simple de contrat intelligent est celui d'un contrat de prestation entre deux personnes. Une partie A souhaite rémunérer une seconde partie B pour l'exécution d'une prestation. L'accord est formalisé par la création d'un contrat intelligent dans une chaîne de blocs. Lors de la formalisation de ce contrat, la partie A met en gage sur la chaîne de blocs le montant de la rémunération prévue pour B. Lorsque la prestation est réalisée, l'une des parties exécute le contrat. Celui-ci vérifie automatiquement que la prestation a bien été effectuée (manuellement par A, ou par intervention d'une tierce partie indépendante et préalablement autorisée, ou bien encore de manière automatisée au moyen de l'exécution d'un logiciel). Si tel est le cas, B reçoit la rémunération prévue. A défaut, la partie A récupère le montant de son gage.

En particulier, de façon remarquable, les contrats intelligents peuvent être créés, négociés et conclus par des machines entre elles (Internet des Objets).

3.2. Définitions

Un « contrat intelligent » ou (« *smart property* ») est un logiciel ou protocole informatique qui facilite, vérifie et exécute la négociation ou l'exécution d'un contrat (e.g. obligations, droits, contrôles, modalités de mise en œuvre, confidentialité, pénalités, etc.). Un contrat intelligent comprend un code logiciel qui est stocké et est exécuté sur/par une chaine de blocs et peut être déclenché par des données internes (e.g. date, heure) et/ou externes (e.g. température, cours de l'action, etc.) qui lui permet de modifier d'autres données, dans la chaine de blocs.

L'expression « contrat intelligent » désigne donc un ensemble de protocoles informatiques qui émulent la logique des clauses contractuelles classiques. Un contrat intelligent vise à émuler ou approcher la logique des clauses contractuelles (droit des contrats). Les contrats intelligents ne sont pas strictement équivalents à des accords contractuels. Ils contribuent à rendre la violation d'un accord coûteux car ils contrôlent un bien par le biais de moyens numériques. Un contrat intelligent peut non seulement définir les règles et les sanctions s'appliquant à un accord, de la même manière qu'un contrat traditionnel, mais il peut aussi appliquer automatiquement ces obligations. Pour ce faire, il saisit l'information comme une donnée entrante, attribue une valeur à cette donnée au moyen des règles énoncées dans le contrat et exécute les mesures exigées par ces clauses contractuelles. Les conditions de déclenchement de l'exécution du contrat peuvent inclure des faits (informations ou données d'entrée comme la température, les données météorologiques, le prix d'un bien, un événement, etc.) et/ou des règles logiques (par exemple, règles temporelles telles que l'expiration des délais, etc.). Elles peuvent être internes et/ou externes à une chaîne de blocs déterminée (par exemple, une chaîne latérale).

Dans certains cas, la vérification de l'exécution des clauses peut être effectuée par des hommes (par exemple, un tiers de confiance désigné) et/ou des machines. Il est possible d'utiliser des machines dites *Oracle*. Une machine *Oracle* agit comme un mécanisme permettant de déterminer si un test a réussi ou échoué, et s'il est en principe utilisé séparément du système testé. Elle peut utiliser une ou plusieurs heuristiques, caractéristiques statistiques, comparaisons de similarité, ou s'inspirer d'un modèle. Il est possible d'utiliser des mécanismes de vote.

3.3. Caractéristiques spécifiques

Contrairement aux logiciels standard, un contrat intelligent est *stocké et exécuté sur une chaîne de blocs*. Il hérite donc de ses propriétés, par exemple :

i) *l'immuabilité* du code correspondant (étant donné la réplication élevée des blocs enchaînés, il serait possible de corrompre un ou plusieurs nœuds, mais pas l'ensemble des codes répliqués dans les copies des blocs de la chaîne de blocs) ;

ii) la *vérifiabilité* du code (les instructions du code peuvent être lisibles par l'homme et/ou la machine dans certaines situations, mais la transparence/opacité peut être affinée par le cryptage et l'obscurcissement, etc. ;)

iii) *l'exécution garantie et fiable* par/sur la chaîne de blocs (même si de nombreux nœuds sont en panne ou attaqués, le programme sera exécuté et le consensus distribué fonctionnera : le résultat de l'exécution ne sera pas remis en cause) ;

iv) l'exécution *automatisée* (les conditions de déclenchement, telles que déterminées par les machines, seront satisfaites, l'intervention humaine n'étant pas forcément nécessaire).

Il a aussi des propriétés dont il faut soigneusement tenir compte : il se pourrait que le code du contrat intelligent, à moins qu'il ne soit anticipé, ne soit pas modifiable.

3.4. Caractéristiques communes au code logiciel conventionnel

Comme pour tout programme ou code informatique, différents langages de programmation sont disponibles, dont les modèles d'expressivité et de sécurité varient. Le langage « Solidity » en est un exemple.

En fait, la logique régissant l'exécution des contrats peut être variable. Outre la logique classique (celle des transactions entre humains), on peut mettre en place d'autres types différents (transactions de machine à machine, comme la *logique floue, ou intuitionniste, combinatoire, modale, propositionnelle, partielle, para consistante*, etc.).

Il est rappelé qu'un logiciel, donc un contrat intelligent, peut être mis en œuvre de différentes manières. Les contrats intelligents peuvent prendre différentes formes (par exemple, services Internet, agents, extraits, scripts, SOA, API, add-ons, plug-ins, extensions, etc.). Un contrat intelligent pourra utiliser des ressources locales et/ou distantes (traitement, stockage). Il pourra être distribué, utiliser ou proposer des interfaces de programmation (API) de contrôle ou de service, utiliser des services web, être mis en œuvre entièrement ou en partie en tant que matériel informatique (par exemple, un circuit FPGA placé dans un smartphone).

Les contrats intelligents, en tant que logiciels informatiques, peuvent être associés à divers mécanismes de *régulation*. Ils peuvent être indépendants ou interdépendants (enchaînés ou liés autrement). Les contrats intelligents peuvent être coopératifs ou non, concurrentiels ou non, convergents ou divergents, synchronisés ou désynchronisés, sécurisés ou non, formellement prouvés ou non, conformes ou non, congruents ou pas, etc. Certains programmes peuvent en régir d'autres (par exemple, le contrat-cadre). Des normes en cascade peuvent être mises en œuvre. Il est possible de structurer des couches de contrôle logiques (descendantes et/ou ascendantes) : depuis les couches de contrôle très proches des données (par exemple, les programmes manipulant les données au niveau de l'ensemble de celles-ci) jusqu'aux objectifs recherchés par le fournisseur de services ou l'opérateur contrôlant les contrats intelligents qui régissent le traitement des données.

Comme tout autre logiciel, un programme intelligent peut être lié ou associé à des parties en *code source ouvert* et/ou en code source fermé (par exemple, même si la plus grande partie du code peut être vérifiée, certaines parties sensibles ou critiques pour la sécurité du code peuvent se présenter sous la forme binaire, éventuellement masquées si elles ne sont pas renforcées). Dans un code source ouvert, les bugs ou les failles de sécurité peuvent être visibles de tous, mais ne pas être corrigés

rapidement. Un contrat intelligent peut être intégralement en open source, mais inclure aussi des parties en code binaire (le code source n'étant pas facile à obtenir par rétro-ingénierie, c'est-à-dire en mode sécurité par obscurité). Il combine ainsi le « meilleur des deux mondes » (vérifiabilité et confiance pour certaines parties du code, contrôle propriétaire pour d'autres).

Comme tout programme ou code, les contrats intelligents peuvent présenter une vulnérabilité importante en matière d'attaques. Ils doivent donc être « sécurisés » du point de vue de la sécurité informatique. Il est possible de développer des langages de programmation entièrement nouveaux pour l'encodage des contrats intelligents. Le langage « Solidity » en est un exemple. Un programme ou un contrat intelligent peut être sécurisé ou utiliser divers systèmes de *cryptage* (y compris, mais sans limitation, la cryptographie post-quantique, la cryptographie à sécurité quantique, la distribution de clé quantique, etc.). Outre le programme disponible en source ouverte et/ou fermée, on peut utiliser des mécanismes d'entiercement de code (c'est-à-dire, associés à un accès restreint, dans certaines conditions (automatisables) et/ou par une organisation humaine). De nombreuses contre-mesures peuvent être adoptées (code polymorphe, système pot de miel, etc.).

En ce qui concerne la forme, un programme ou un contrat intelligent est lisible par l'homme et/ou par la machine. Du fait de sa construction, un programme (exécutable) est lisible par la machine : les faits et les règles peuvent être traités par des machines. Les instructions lisibles à la machine ne peuvent pas être lues par l'homme. En général, les règles ou programmes lisibles par l'homme peuvent (souvent, mais pas toujours) être lus par des machines (par exemple, dans la pratique, les machines ne peuvent pas traiter certaines ambiguïtés du langage naturel, maintenant ou dans un avenir prévisible). Selon les applications, il peut s'avérer intéressant que les règles codées dans le programme soient lues par l'homme (pour des raisons de transparence, gouvernance, contrôle, etc.). Dans certains cas, le programme peut être écrit en pseudo-code exécutable, lisible à la fois par l'homme et par la machine. Dans d'autres situations, le code lisible par la machine peut être transcodé ou visualisé sous une forme compréhensible pour l'homme (par exemple, icônes lisibles par l'homme).

3.5. Validité et perspectives

Les contrats intelligents peuvent faire l'objet de nombreuses applications (verticales), dans différents domaines techniques. Bien entendu, les débouchés immédiats sont ceux du transactionnel et de la finance (e.g. instruments financiers comme les obligations, les actions et leurs dérivés, les contrats d'assurance - l'ère de « l'argent » programmable).

À notre connaissance, la validité des contrats intelligents reste encore largement à évaluer et à confirmer. Par exemple, des questions se posent en ce qui concerne la signature électronique. En principe, les lois la concernant exigent que la signature électronique du contrat soit « jointe ou *logiquement* associée » aux clauses du contrat. Des débats passionnés font rage actuellement au sein de la communauté Bitcoin à propos d'une technique d'élagage des données dite de « *segregated witness* » (surnom « Segwit »), consistant à séparer les données de la signature (témoin) des données de la transaction. Alors que l'objectif d'une telle technique d'élagage des données est d'augmenter la taille d'un bloc (qui est amplement répliqué dans le réseau

distribué) pour en obtenir une meilleure utilisation, il se pourrait que cette technique s'avère préjudiciable -voire incompatible- avec le droit des contrats (preuve de la chaîne de blocs). Les opposants à ce type d'option déclarent que le réseau deviendrait moins fiable. Ces techniques d'élagage des données pourraient mettre en danger des critères juridiques comme le « contenu reproductible », le « lien entre la signature et l'enregistrement pendant la transmission et le stockage », la « signature contenue dans et attachée à », et bien d'autres. Si certains nœuds spécialisés conservaient des données de signature, ils deviendraient des nœuds « fiables » ou privilégiés (donc des goulots d'étranglement, et au pire des « validateurs autorisés par la gouvernance »), ce qui serait antithétique vis-à-vis du système Bitcoin décentralisé non fiable. Il n'est pas facile de savoir ce que ces données représentent en termes quantitatifs car les parties signataires ont la possibilité de conserver leurs propres copies (et c'est donc un volume parfaitement gérable). La manière exacte dont les « clauses contractuelles » peuvent être stockées semble également discutable ou exiger une enquête (par exemple, lien avec des formulaires lisibles par l'homme, etc.).

En ce qui concerne l'évolution et la portée des contrats intelligents, des aspects comme la sécurité informatique et les réseaux de contrats intelligents sont à prendre en compte. Il faut notamment tester les chaînes ou les réseaux de contrats (par exemple, simulés, émulés, etc.). L'option de la vérifiabilité peut ainsi accroître la confiance dans le programme qui gère les collectes de données. L'exécution automatisée du contrat intelligent favorise des schémas d'automatisation plus importants et, notamment, le contrôle des flux de données. Les fonctionnalités financières intégrées donnent lieu à de nombreux autres développements, comme les micro-paiements (et les nano-transactions dans le monde de l'Internet des Objets) et au partage des revenus associé à l'accès aux données (monétisation). En ce qui concerne les réseaux de contrats intelligents, les considérations liées à la sécurité informatique sont de plus en plus complexes (par exemple, les risques systémiques).

4. Le système Bitcoin et les monnaies cryptographiques, construits à partir des chaînes de blocs

Une bataille fascinante, technologique d'abord mais aussi juridique, pourrait s'engager autour des crypto-monnaies et plus largement autour des applications renouvelées des technologies mobilisées par Bitcoin.

4.1. Le Bitcoin utilise des chaînes de blocs

L'histoire de Bitcoin est désormais bien documentée. Le lecteur intéressé pourra se reporter aux pages *Wikipedia* (en anglais), au document fondateur publié en 2008 par *Satoshi Nakamoto* intitulé "*Bitcoin: A Peer-to-Peer Electronic Cash System*", aux articles de Satoshi Nakamoto (« *The Book Of Satoshi: The Collected Writings of Bitcoin Creator* ») et aux articles de *Andrew O'Hagan* (« *The Satoshi Affair* »). Les livres de *Tapscott* et *Antonopoulos* peuvent aussi être recommandés.

Conceptualisée avant l'an 2000, née officiellement en 2008, signal faible en 2011 (revue *Wired*) puis devenue grand public en 2013, désormais appropriée par la Fintech, la crypto-monnaie Bitcoin a provoqué un choc industriel et financier palpable (e.g. activités de minage, transactions réelles, réflexions des régulateurs financiers, etc.).

Bitcoin vise au départ un projet politique libertaire, d'après une vision économique sous-jacente d'inspiration libérale. Bitcoin vise le « cash cryptographique » (au sens monétaire), i.e. une monnaie sans régulateur institutionnel (donc sans possibilité d'intervention étatique) mais selon un modèle informatique objectif et non-manipulable (ou alors difficilement), avec des garanties en matière de vie privée et de liquidité (ces techniques sont brevetables ou brevetées). Bitcoin se veut donc être du *cash* mathématique sûre, rare, sans aucun contrôle institutionnel et donc non manipulable politiquement (« *real hard money* »). Plus profondément, Bitcoin vise à remplacer la « *credit-based economy* » par l' « *equity-based economy* », ce qui conduit à des horizons de modèles d'affaires radicalement différents (et généralement brevetables). Les débats sont nourris quant au statut juridique et fiscal de ce nouvel objet (e.g. unité de compte ou commodité plutôt que monnaie) et à sa régulation (e.g. en matière de taxation)

Du point de vue technique (en gardant à l'esprit la question des droits de propriété intellectuelle associés à Bitcoin et aux chaînes de blocs), Bitcoin repose sur des fondations cryptographiques bien maîtrisées, mais qui continuent d'évoluer. Techniquement, Bitcoin est une intégration de technologies informatiques éprouvées et anciennes. La généalogie intellectuelle de Bitcoin remonte à la B-money of Wei Dai 1999, Nick Szabo en 2005, voire probablement à des périodes antérieures (milieux cyberpunk puis cypherpunk des années 1980).

En 2018, Bitcoin est à un point d'inflexion de son histoire. Bitcoin représente aujourd'hui une fraction infinitésimale des échanges monétaires mondiaux et le nombre de transactions par seconde est encore très faible. La communauté cherche activement la mise à l'échelle (« *Bitcoin needs to scale* »), ce qui nourrit des débats passionnés sur les options techniques à prendre, et à conduit récemment à des *forks* (scission de projets en open source) forts médiatisés (Bitcoin Cash en ABC et SV). Les variantes de Bitcoin, appelées « AltCoins » (e.g. Litecoin, Namecoin, Swiftcoin, Primecoin, Blackcoin, Dash, Ethereum, Zcash, etc) poursuivent des compromis différents, en matière de modèle (inflationniste ou autre), d'accès, de validation par preuve de travail, de signatures, etc. Pour les tenants de Bitcoin, ces variantes sont souvent perçues comme étant préjudiciables (abandon de souveraineté, perte de libertés, déperditions d'énergie en termes d'efforts de développement logiciel, ressources matérielles perdues en matière de réseau, etc.).

4.2. Protection par brevet de Bitcoin

De nombreux dépôts de brevets font référence à Bitcoin dans leurs spécifications, parfois même dans leurs revendications. Certains semblent concerner directement des monnaies cryptographiques, alors que d'autres ont une portée plus étendue. Nous étudions ci-après le portefeuille de la société nChain.

Les technologies qui fondent Bitcoin, et par dérivation les « AltCoins » (monnaies cryptographiques alternatives à Bitcoin), sont pour la plupart des techniques de l'informatique distribuée, qui intéressent depuis longtemps de nombreux domaines industriels (Internet, télécommunications, calcul scientifique, robotique, productique,

etc.). Par exemple, le problème du consensus distribué est un problème connu en théorie du calcul distribué, qui remonte aux années 1970 (e.g. brevets IBM).

Actuellement, toutes les composantes technologiques utilisées pour les crypto-monnaies sont susceptibles d'être sophistiquées et donc de donner lieu à des dépôts de demandes de brevets. Récemment les signatures *Boneh-Lynn-Schacham* ont été considérées en remplacement des signatures *Schnorr* ou élliptiques ECDSA. Les méthodes de validation par preuve de travail sont également susceptibles d'évoluer rapidement.

En ce qui concerne le cas spécifique de Bitcoin et de ses déclinaisons (par exemple Bitcoin Cash, ou ses dérivés ABC ou SV), Bitcoin présente l'avantage d'être le premier arrivé, mais il est notoire que les choix d'implémentation présentent des défauts (par exemple, pas de gouvernance intégrée, facteurs limitant son évolutivité, etc.). Bitcoin a fait naître des forces hostiles à son encontre, mais aussi des foules qui lui accordent leur soutien. À notre avis, une question importante qui se pose est celle de la course aux brevets entre les géants de la finance et les géants des technologies de l'information. Les opérateurs financiers, comme les banques ou Goldman Sachs, peuvent constituer de nouveaux portefeuilles de propriété intellectuelle, mais cela prendra des années. Pour l'instant, les acteurs de la finance ont déposé un nombre étonnamment faible de demandes de brevet. En revanche, IBM et les principaux acteurs des technologies de l'information ont beaucoup plus de brevets que la Fintech ne pourra jamais en espérer. À elle seule, l'entreprise IBM compte plus de 120 000 demandes de brevets publiées, dans de nombreux domaines différents (du consensus distribué à la cryptographie fondamentale). Au milieu des géants des technologies de l'information et de ceux de la finance, les start-up et d'autres acteurs peuvent tenter d'influencer certaines orientations technologiques en déposant des demandes de brevet. Ils ont probablement des chances limitées, mais raisonnables, a fortiori sur la base d'alliances stratégiques (par exemple, Google, des banques). Si des sites marchands (comme Amazon) fournissent le pouvoir de hachage requis pour mettre en place la crypto-devise et si, en même temps, l'utilisation de la cryptographie se répand rapidement, Bitcoin pourrait effectivement devenir imparable. Facebook, Google ou les géants Chinois pourraient aussi pénétrer le secteur. Bien entendu, les dirigeants de ces grands groupes, et pas uniquement les gouvernements nationaux et les banques centrales, suivent de très près les évolutions des crypto-monnaies et des chaines de blocs. Les brevets peuvent jouer un rôle majeur dans les équilibres entre les différentes forces en puissance. C'est un paradoxe, étant donné les origines de Bitcoin (qui rejette les institutions). A n'en pas douter, parallèlement aux évolutions technologiques, les batailles juridiques concernant les chaines de blocs et les crypto-monnaies seront épiques.

II. Brevetabilité des inventions liées à la chaîne de blocs

Comme les inventions *logicielles*, les inventions de brevets liées à Bitcoin, aux monnaies cryptographiques et à la chaîne de blocs sont (dans la pratique) brevetables. Leur caractère technique, hérité d'une forte empreinte cryptographique, est favorable à la brevetabilité. Cependant, certaines inventions pouvant être qualifiées de *méthodes commerciales* (pratiques administratives, économiques, etc.) sont en général exclues de la brevetabilité. La frontière entre les brevets logiciels et les méthodes commerciales est poreuse : le savoir-faire en rédaction de brevets peut faire toute la différence (par exemple, la terminologie et certains ajustements apportés à l'invention, si nécessaire). Les parties suivantes traitent spécifiquement de la brevetabilité en Europe. Les autres parties décrivent les spécificités aux États-Unis.

Les inventions actuellement publiées présentent des particularités intéressantes, à la limite de plusieurs points délicats en matière d'exceptions à la brevetabilité : i) les brevets de logiciel ii) les actes mentaux et les méthodes intellectuelles, ii) les méthodes d'affaires, iv) la représentation d'informations. Chacune des exceptions peut conduire à des ajustements de langage. Les sections suivantes passent en revue le cas particulier des chaînes de blocs par rapport aux critères communément considérés pour chaque type d'exemption à la brevetabilité.

1. Méthodes mises en œuvre par ordinateur

Les inventions Bitcoin, ou apparentées, soulèvent les problématiques classiques que posent désormais la majorité des inventions mises en œuvre par ordinateur, mais les aggravent quelque peu du fait de l'emploi des chaines de blocs et de contenus chiffrés.

La présence de brevets et donc de contrefaçon peut se produire à différents niveaux :

- à l'intérieur des chaines de blocs, les contrats intelligents sont pour l'instant des scripts courts mais ils sont susceptibles d'évoluer vers des programmes complexes, hautement répliqués dans l'ensemble de la base de données distribuée. Il est donc concevable que les programmes complexes mettent en œuvre des inventions i.e. des procédés brevetables et/ou brevetées;

- les chaînes de blocs, par leur nature, peuvent en théorie être revendiquées en elles-mêmes et pour elles-mêmes (en tant que combinaisons de briques technologiques connues et/ou nouvelles et inventives, par exemple des systèmes de validation, des schémas de signature, des techniques d'élagage, des architectures spécifiques, etc.). De nouveaux types de chaînes de blocs apparaissent régulièrement sur le marché (nano-transactions pour M2M, etc.);

- selon la perspective la plus large, les inventions mises en œuvre par une chaîne de blocs peuvent inclure une ou plusieurs chaînes de blocs, connues ou spécifiques, ainsi qu'une pluralité d'autres objets (matériels ou logiques) extérieurs à ces chaînes de blocs : ces inventions, si elles sont revendiquées et brevetées, peuvent elles aussi être reproduites ;

Les parties suivantes traitent succinctement des caractéristiques spécifiques aux inventions implémentée par chaîne de blocs : i) la détectabilité et ii) la contrefaçon.

1.1. Détectabilité

Une problématique juridique majeure des inventions mises en œuvre par ordinateur tient à la *détectabilité* de ces inventions. Cette détectabilité peut évoluer au cours du temps (via le produit logiciel lui-même, sa forme e.g. *open source*, et sa documentation). A un instant donné, elle peut être immédiate ou peut requérir de l'ingénierie inverse. La détectabilité n'est aucunement appréciée par les examinateurs de brevet mais elle constitue est un facteur critique pour l'appréhension de la contrefaçon (e.g. saisies-contrefaçons et l'interprétation par les juges et/ou les jurys). Elle fait également écho à la lisibilité des inventions pour les tiers adverses, e.g. les conseils en propriété industrielle qui effectuent des études de liberté d'exploitation.

Comme toute invention de nature logicielle, la détectabilité des inventions utilisant des chaînes de blocs est à appréhender avec attention. Les « *blockchain-related inventions* » se caractérisent généralement par une détectabilité plutôt faible. Les centres de données ne sont presque jamais publics, voire a contrario sont très difficiles d'accès (e.g. nécessité d'opérations de saisie-contrefaçon, d'injonctions, etc.). Par ailleurs, l'usage intensif de la cryptographie amoindrit la détectabilité des inventions. De plus, dans les chaînes de blocs, les données peuvent être stockées en texte clair, mais aussi en texte chiffré.

Les portefeuilles de crypto-monnaie (*wallets*) comprennent des interfaces graphiques, lesquels *frontends* sont détectables (et de valeur du point de vue de leur détectabilité), mais elles ne représentent d'une petite partie de la technologie, laquelle se déroule essentiellement sur le *backend (« patents buried deep in data centers »)*. Par construction, les chaînes de blocs, ou une partie d'entre elles, sont répliquées dans de nombreux nœuds du réseau, mais ces données peuvent rester peu informatives. Les logiciels de traitement des valeurs de hash peuvent être implémentés localement (accessibles), mais aussi dans des endroits réservés du réseau (e.g. caches non accessibles).

S'agissant d'informatique dans les nuages (« Cloud computing »), on pourra veiller à prévoir certes des boucles ouvertes (avec intervention de l'utilisateur, donc des étapes visibles et détectables) mais aussi à l'automatisation - à terme - de ces boucles de rétroaction (i.e. selon des boucles fermées, et en donnant les critères quantitatifs permettant une prise de décision logique par la machine).

1.2. Contrefaçon

À ce jour, il ne semble pas y avoir de litige juridique en matière de brevets dans le domaine émergent des chaines de blocs, à l'exception des scissions de code ouvert (« forks »).

Historiquement, les architectures de type « Cloud computing » ont souligné que la contrefaçon pouvait résulter de l'action conjointe de plusieurs parties. Le droit américain parle de « divided infringement » ou de « contributory infringement ». Les droits nationaux ont différentes approches (contrefaçon indirecte, fourniture de

moyens, contrefaçon conjointe, complicité, etc), qu'il n'est pas possible d'approfondir ici. La « divided infringement » désigne une forme de responsabilité en matière de contrefaçon de brevet qui se produit lorsque plusieurs acteurs sont impliqués dans l'exécution de la contrefaçon revendiquée d'un brevet de méthode et qu'aucune partie n'a seule effectué toutes les étapes de la méthode. Les *mashups* et autres applications composites impliquant une pluralité de serveurs situés dans différents pays ont amené les conseils en propriété industrielle à rédiger des revendications selon des tournures linguistiques particulières, visant généralement un fournisseur principal d'un service, ou pouvant être lues sur plusieurs entités.

Les chaînes de blocs semblent ajouter des problèmes juridiques nouveaux et entièrement différents à ces difficultés existantes.

Un trait saillant des inventions liées aux chaînes de blocs est la nature *distribuée* de ces dernières. De nombreuses parties prenantes étant impliquées, il est très facile, en raison de leur construction, de détecter d'éventuelles contrefaçons : par la saisie d'un seul nœud, qui réplique toutes les données et/ou tous les programmes intégrés dans la chaîne de blocs. En même temps, il peut s'avérer très difficile d'appréhender une multitude de contrefacteurs, car la base de données est répliquée à très grande échelle.

En d'autres termes : si chaque nœud du réseau a la même copie de données et de programmes, il est nécessaire et suffisant de mettre la main sur un seul nœud pour évaluer la contrefaçon (si celle-ci n'est pas chiffrée). Cependant, même dans le cas où celle-ci est prouvée, que peut-on faire contre des milliers de contrefacteurs ?

La taille du code est un autre facteur essentiel. À l'heure actuelle, les contrats intelligents sont des scripts courts et il est peu probable que ces scripts puissent mettre en œuvre des procédés brevetés. A l'avenir, des programmes complexes, c'est-à-dire des codes logiciels significatifs, pourraient bien mettre en œuvre une pluralité d'inventions (par exemple dans le domaine complexe de l'Internet des objets, de l'auto-régulation de véhicules autonomes, etc.).

Certains facteurs peuvent toutefois apporter des nuances à ce qui précède. En effet, il existe habituellement *des tensions entre les mécanismes de centralisation, de décentralisation et de distribution*. La centralisation et la décentralisation font référence au fait d'avoir plus ou moins de « centres » dans une architecture déterminée. La distribution désigne les systèmes qui correspondent théoriquement à des systèmes de pair à pair, chaque nœud étant égal, c'est-à-dire qu'il n'y a pas de nœuds privilégiés. En réalité et dans la pratique, les systèmes distribués purs sont rares : en raison de compromis techniques et/ou commerciaux, certains nœuds peuvent jouer des rôles particuliers (par exemple, l'indexation, la fiscalité, la mise en cache, etc.), les étapes de traitement et les données suivantes pouvant être évaluées différemment dans certains nœuds particuliers, qui auraient plus de responsabilités que d'autres. Par exemple, dans les chaînes de blocs privées, le nombre d'acteurs reste assez limité et il est concevable de déterminer la contrefaçon d'une méthode brevetée. La collecte et la possession de « big data » (pour réaliser des analyses à valeur ajoutée) sont souvent en jeu, car certaines parties sont disposées à lutter durement pour avoir un accès privilégié aux données. Par exemple, dans la gestion de la confidentialité à l'aide de chaînes de blocs, elles peuvent souvent constituer un

intermédiaire de choix, détenant des clés de chiffrement. De plus, la présentation des interfaces de programmation API peut exposer et conduire à la divulgation des étapes de méthodes brevetées.

Il n'en demeure pas moins que, outre la détectabilité (complexe) des inventions mises en œuvre par une chaîne de blocs, il peut devenir extrêmement difficile de détecter une contrefaçon, puis de faire appliquer la loi. Comme dans le cas des brevets logiciels, les rédacteurs de brevets doivent essayer de rédiger les revendications de manière ingénieuse, c'est-à-dire d'après une perspective centrée sur les parties prenantes (par exemple, quelles étapes manifestes du procédé la partie B exécute-t-elle dans son interaction avec A et C ?). Dans le cas de chaines de blocs privées, ce qui est souvent le cas dans le cadre industriel, le nombre d'acteurs est moindre et les analyses peuvent être plus simples.

1.3. Logiciel en open source

Des instructions de code ouvert ne restreignent pas nécessairement la possibilité de breveter une ou plusieurs technologies sous-jacentes. Le fait que certains logiciels soient *open source* ne signifie pas forcément que les inventions mises en œuvre seront découvertes (il peut être très difficile d'évaluer un code *spaghetti*).

Selon les cas, il peut être recommandé d'annoter - ou pas - un code ouvert. A contrario, le code peut être obfusqué, voire durci ou blindé/hardened (chiffré et plus encore).

En ce qui concerne les contrats intelligents, le caractère open source de ces objets peut aussi souligner la *lisibilité* de ces contrats intelligents (cf. l'article précédent).

2. Acte mental et méthodes intellectuelles

Tout d'abord, proche des mathématiques car impliquant des méthodes cryptographiques en leur cœur, la « flaveur » des revendications de ce type d'invention est *a priori* défavorable. On ne peut pas breveter les mathématiques. Un langage mathématique trop marqué attire en général des objections d'abstraction ou d'acte mental.

A contrario, pour prospérer, une revendication doit généralement utiliser des mots les plus « techniques » possibles (ce qui s'apparente *in fine* à des exigences sociales). C'est essentiellement en raison de son expérience qu'un rédacteur de brevets sait quel est le compromis efficace.

Dans le cas des inventions Bitcoin, il peut être recommandé de souligner - et si possible de développer- les aspects de système, matériels et tangibles. On ne s'en tiendra donc pas par exemple aux seuls processeurs génériques (confer *infra*), mais selon les cas on soulignera les modes de réalisation par processeurs spécialisés FPGA, des modes de calcul distribués et spécifiques aux inventions, l'utilisation de processeurs *multi-cœurs* ou *many-core* à des fins d'optimisation. Il pourra être approprié de souligner des aspects propres à l'automatisation de tâches, par exemple en ce qu'elles ne sont pas réalisables manuellement (e.g. méthodes haute fréquence, temps-réel, etc.).

3. Méthodes de commerce

Les inventions dans la mouvance Bitcoin présentent souvent des modèles économiques en émergence ou en rupture radicale avec les pratiques existantes. Ces modèles d'affaires se traduisent généralement en mots, i.e. sont généralement étroitement imbriqués dans les étapes de procédé revendiquées. Ces mots sont par exemple des mots ou expressions tels que « *merchant* », « *commission* », « *peer-to-peer lending* », etc.

En Europe, la théorie veut que les plans, principes et méthodes dans l'exercice d'activités intellectuelles, en matière de jeu ou dans le domaine des activités économiques, sont des « non-inventions » au sens de l'article 52(2) et (3) CBE. Néanmoins, une implémentation par ordinateur peut rendre une méthode commerciale brevetable (si l'amélioration procurée par le dispositif ne se trouve pas uniquement dans le secteur économique)

Les termes importés du domaine du commerce, de la gestion des affaires et de la finance doivent être dans la mesure du possible évités, et à défaut définis dans les termes les plus quantitatifs possibles. Si seules des définitions sont possibles (i.e. des périphrases précisant ce qui est entendu ou couvert par un mot donné), il convient de garder à l'esprit que ces définitions sont susceptibles d'être introduites dans les revendications : un soin extrême, le même que celui apporté aux termes des revendications, doit être apporté quant à leur formulation.

En Europe, et particulièrement ces dernières années, la clarté des revendications selon l'Article 84 CBE devient de plus en plus impérative. Par exemple, un terme imprécis comme « *visibility* » dans l'expression « *visibility of a smart contract* » est susceptible de soulever des objections.

En pratique, il s'agit essentiellement d'une question de terminologie, qu'il faut rendra la plus technique possible (si cela est possible). Le vocabulaire à connotation économique sera avantageusement remplacé par du vocabulaire considéré comme « technique ».

Des termes techniques tels que « *message* », « *réseau* », « *nœud* », « *clé* », « *partie* » sont largement acceptés par les examinateurs de brevets. Dans la mesure du possible, il est préférable d'éviter le langage commercial ou administratif utilisant des mots comme « *marchand* », « *prix* » ou « *paiement* ». De tels objets peuvent être résumés par des mots comme « *entité* » ou « *machine* » ou « *serveur* » (parce que la caractéristique de « marchand » n'est pas technique). En Europe tout au moins, il faudrait utiliser, au mieux, le nombre minimum de termes propres au champ cible. Par exemple, les termes « *part* » ou « *paiement* » ont une connotation financière marquée et il faut limiter leur utilisation. Ils peuvent être avantageusement remplacés par des synonymes adéquats. Les dictionnaires WordNet, et d'autres, indiquent, par exemple, les synonymes suivants pour « part » : *portion, partie, pourcentage, portion du capital-actions, parcelle et contribution*. Certains synonymes peuvent convenir ou pas et, dans certains cas, il n'y a pas d'alternative réelle. L'expression « *contrat intelligent* » est une inclusion relativement récente, aux frontières flottantes ou floues (malgré les pages Wikipedia, on peut estimer que la terminologie n'est pas stable). Cette

expression peut être instanciée dans un « *programme* » ou un « *protocole* ». Même si, *a priori*, certains termes pourraient être acceptés, il est plutôt recommandé de rester en dehors du domaine des affaires. Par exemple, les systèmes transactionnels sont généralement brevetables (secteur du tourisme) mais, par sécurité, il est préférable de remplacer le terme « *transaction* » par « *transmission de messages* » ou autre terme équivalent, afin de souligner les caractéristiques techniques sous-jacentes.

Au-delà du choix des mots i.e. du seul choix terminologique (constitutif de la « flavor » des revendications), il peut être recommandé d'insister sur les caractéristiques dites *technique*s de l'invention et des *relations* entre les mots soigneusement choisis.

Le caractère technique peut notamment être renforcé par l'emploi de définitions soigneusement écrites (ces définitions constituant en soi des revendications « de second rideau », en ce qu'elles peuvent aboutir à remodeler les revendications déposées). Ensuite, concernant les relations entre mots, une approche généralement fructueuse consiste à considérer une pluralité d'objets manipulés. Par exemple, manipuler une pluralité de contrats intelligents soulève presqu'instantanément des questions passionnantes. Le fait d'avoir une pluralité d'acteurs économiques peut se traduire techniquement par la mise en œuvre de « *multi-party computing* » ou de mécanismes d'optimisation par exemple multi-objectifs. De manière générale, une revendication étant représentable par un graphe (relations entre objets), on pourra étudier les diverses modalités d'interaction ou de régulation associées aux objets en interaction (exemples de questions: *où sont les points de contrôle du système ? le système est-il contrôlable ? quels sont les risques systémiques le cas échéant ? quelle régulation ou interface homme/machine* ? (e.g. déclenchements automatiques, seuils).

En périphérie de l'invention, pour renforcer le caractère technique de certaines inventions, il peut être approprié d'épuiser les d'échanges (e.g. protection par biométrie, sécurisation par chiffrement, routage, base de données centralisées ou distribuées, etc.). L'exigence de caractère technique peut aussi inviter à étudier de nombreux aspects sous-jacents, notamment les types de logiques mis en œuvre. Par exemple, les modes de *« commissions »* ou les *« incentives »* (incitations de marché) peuvent parfois être traitées dans la perspective de l'application de règles logiques de diverses natures, de modalités de déclenchements, d'effets systémiques, de régulation « cybernétique », d'apprentissage, etc.

4. Interfaces utilisateur et représentation d'informations

En matière d'interfaces et de représentation d'informations (qui est non-brevetable dans la plupart des juridictions), la frontière est parfois complexe entre fond et forme. Avec suffisamment de savoir-faire en matière de rédaction de revendications, la description et les revendications en matière de représentation d'informations peuvent être formulées de telle manière que la situation en matière de brevetabilité s'améliore. La jurisprudence Européenne a évolué en 2012 et considère désormais plus favorablement les inventions améliorant les prises de décision ou déchargeant la charge cognitive associée à l'utilisation d'interface homme-machine.

L'invention peut même parfois être développée, sur le fond, à cause de ces raisons de nature juridique. Par exemple, on pourra essayer de quantifier le plus possible la représentation de données. Par exemple, une « symbologie » et l'affichage de

symboles peut être développée selon des propriétés de « superposabilité ». Les déclenchements d'actions (causes) et les règles logiques de gestion de l'affichage (conséquences) seront avantageusement explorés, développés, décrits et revendiqués. De manière générale, il est utile de décrire et revendiquer la logique sous-jacente gouvernant les actions effectuées par la machine, en quoi consistent les actions en elles-mêmes, la façon dont ces dernières s'inscrivent plus largement dans le procédé, etc. On aura toujours bénéfice à souligner les synergies éventuelles entre les interfaces logiques et les systèmes physiques (e.g. système « *force touch* » créant des subtilités dans les commandes, e.g. une vitesse de gestuelle indiquant indirectement l'état de l'utilisateur lors de la saisie de données. Ces considérations peuvent être adjacentes au cœur de l'invention mais permettent généralement d'obtenir des positions brevetables et bloquantes pour les tiers.

Les demandes de brevet publiées mentionnent parfois une validation d'étape ou de résultat intermédiaires « machine et/ou humaine ». Au sens du droit Européen, les revendications avec des boucles ouvertes (avec intervention humaine) sont malvenues et il est prudent de prévoir des versions en boucle fermée explicitant les critères quantitatifs de décision.

5. Prise en compte de règlementations additionnelles

Pour compliquer encore le tableau, les technologies en rapport avec les chaines de blocs ou les contrats intelligents concernent souvent des domaines industriels (e.g. médical, avionique, robotique, etc.) qui sont *déjà* inscrits dans des cadres règlementaires contraignants.

Les règles et normes applicables structurent leurs marchés. Par ricochet, les règlementations structurent les revendications des demandes de brevets (une invention pour être commercialisable doit respecter la règlementation en vigueur). Ces normes (qui constituent d'ailleurs le socle de l'état de la technique) se traduisent souvent par des caractéristiques techniques concrètes. La présence d'un régulateur limite l'espace des possibles. Si une invention est trop différente des exigences réglementaires, elle ne pourra pas être implémentée et restera de fait spéculative. Si une invention se déduit directement de la règlementation publiée, alors elle ne sera pas brevetable.

Par exemple, dans le domaine médical, les inventions répondent aux règles de la FDA (mondiales de fait). Le pancréas artificiel (en boucle fermée) n'est pas encore autorisé, ce qui se traduit outre l'intervention du patient dans la réalité de la thérapie par des étapes de confirmation ou d'infirmation d'injection d'insuline dans les revendications de brevet. L'usage de chaînes de blocs soulèvera de nombreuses questions de nature technique mais aussi de nature règlementaire.

Dans le domaine de l'aéronautique, l'avionique est structurée par la FAA. La certification des aéronefs impose des délimitations entre matériel de type avionique (monde « fermé ») et de type non-avionique (monde « ouvert »). En pratique, cette distinction peut être quantifiée, selon des critères de fiabilité (par exemple) qui se retrouvent dans les revendications de brevet. L'avionique peut faire de multiples

usages de la *blockchain* pour compléter ou se substituer en partie aux modèles de confiance existants. L'intelligence artificielle « explicable », qui pourrait reposer sur une couche de confiance type chaine de blocs, compliquera encore l'écriture de revendications de brevets. Les dépôts en la matière devront donc encore se sophistiquer.

Les banques - qui utilisent de manière croissante des inventions de type Bitcoin ou qui s'y préparent – vont prochainement devoir respecter la directive GDPR, fortement structurante en Europe. Entre autres exigences, le droit à l'oubli imposera un traitement particulier - et héritable - des droits en lecture/écriture. En poussant encore les recherches, il apparaît que des chaines de blocs « modifiables » peuvent être construites (ce qui est paradoxal), incorporer des mécanismes de gestion des droits (DRM). L'information classique étant toujours copiable, des propriétés quantiques (e.g. non-clonabilité, fuites quantiques) pourraient être invoquées, par exemple en matière de gestion du droit à l'oubli.

Dans un autre domaine, les inventions sur les voitures autonomes pourraient impliquer des régimes de responsabilité encodés dans des contrats intelligents.

La prise en compte des exigences réglementaires - présentes et futures - s'ajoutera donc nécessairement aux considérations techniques et juridiques de la gestion dans et par les chaînes de blocs, qui sont abordées ici. Autrement dit, les inventions fondées sur les chaînes de bloc pourront conduire à adapter des mécanismes de régulation qui leur sont propres, en fonction du domaine d'application de destination. La complexité règlementaire va donc impacter directement les revendications de demandes de brevet. A terme, il est également possible de penser que des domaines techniques auparavant distincts pourront se rejoindre (hybridation de domaines techniques).

6. Brevetabilité aux Etats-Unis

Certaines décisions de la Cour Suprême ont façonné le paysage américain en ce qui concerne les méthodes commerciales et les brevets logiciels.

En 1998, la décision « *State Street Bank & Trust Co contre Signature Financial Group* » a établi que les méthodes commerciales pouvaient être brevetables, ce qui a provoqué une vague de dépôts de demandes de brevets. En 2014, la décision « *Alice Corp Pty Ltd contre CLS Bank* » a jugé que les méthodes commerciales financières mettant en œuvre une « pratique économique fondamentale » étaient probablement des idées abstraites non brevetables, sauf si elles incluaient des progrès « technologiques ».

À ce jour et dans la pratique, un test en trois étapes est réalisé, la troisième étape étant critique. Il faut tout d'abord déterminer si l'invention (c'est-à-dire, les revendications) concerne une catégorie statutaire (par exemple, un procédé ou un système). Cette étape est rarement bloquante. On analyse ensuite si l'invention porte sur une exception judiciaire (une idée abstraite), par exemple sur une invention pouvant être exécutée mentalement (comparer et/ou organiser des données) ou par une personne utilisant un stylo et du papier. Compte tenu des algorithmes mathématiques, c'est généralement le cas. Enfin, la troisième étape consiste à déterminer si les revendications apportent « significativement plus » que l'idée abstraite. Plusieurs

sous-critères peuvent être exploités. En général, l'utilisation d'un ordinateur générique (par exemple, architecture de Von Neumann) ou d'un simple dispositif d'affichage ne suffit pas à satisfaire à la troisième étape du test (« niveau de généralité élevé », « interface connue », etc.). Le temps passant, les exigences peuvent même s'intensifier. Dans certains de nos dossiers, il a même été allégué qu'un appareil d'IRM (Imagerie par résonance magnétique) est un appareil « générique ». Les limitations à des domaines d'utilisation spécifiques (par exemple, les applications médicales, de logistique) peuvent également ne pas suffire, même si le « risque » pour l'Office des brevets de délivrer un brevet trop étendu est considérablement limité. Les finalités ou le champ d'utilisation limitant la portée des revendications ne doivent pas donner « vie, sens et vitalité » (« *life, meaning and vitality* ») aux revendications. Pour qu'elles soient significativement plus importantes qu'une idée abstraite, ces limitations à des domaines d'utilisation spécifiques doivent être « significatives », c'est-à-dire qu'elles doivent présenter une relation complexe, étroite ou autrement profonde avec le domaine envisagé (« limiter l'idée abstraite à une application utile particulière » - « *confining the abstract idea into a particular useful application* »). Dans la pratique, à nouveau, on constate que l'accumulation de limitations (dispositifs tangibles pour l'exécution de l'invention, spécification des domaines d'utilisation, effets de synergie) peut conduire à un objet revendiqué brevetable.

Les demandes de brevet concernant des chaînes de blocs peuvent être considérées comme des brevets de logiciels. Une invention qui améliore le fonctionnement technologique ou les procédés d'un ordinateur peut être brevetable. La jurisprudence américaine semble de plus en plus conforme à la pratique européenne, mettant l'accent sur le caractère technique et les effets techniques (et non sur les effets économiques indirects).

7. Brevetabilité dans d'autres juridictions

À notre connaissance et d'après notre expérience, les poursuites en Chine sont très similaires à la pratique européenne. Une demande de brevet rédigée pour l'Europe pourrait être acceptée aux États-Unis, alors que l'inverse ne sera pas forcément vrai (notamment, en raison de l'absence de mentions sur les effets techniques associés aux caractéristiques revendiquées).

Pour les autres juridictions (par exemple, Japon, Corée, Canada, Australie, etc.), il est conseillé de consulter un conseil en brevets national.

III. Analyse des demandes de brevets publiées, relatives aux chaines de blocs (3/4)

10 juin 2019

Depuis quelques années, les dépôts concernant les briques technologiques de Bitcoin s'accroissent significativement (e.g. chaînes de blocs, validation par preuve de travail, signatures cryptographiques).

Différents groupes d'intérêts se constituent, corrélativement à l'accroissement des enjeux politiques, économiques et financiers. Des entreprises du secteur bancaire déposent des demandes de brevet (e.g. *Bank of America, Visa*). Les géants de la finance (e.g. Goldman Sachs) prennent position et déposent également. Des entreprises dans des secteurs connexes comme Amazon ou IBM spécialisent leurs dépôts. Le capital-risque alimente de nombreuses startups qui codent en dur et cherchent des droits exclusifs. Les positions des régulateurs, e.g. FED et BCE, s'affinent régulièrement. Des Etats-nations envisagent la création de crypto-monnaies nationales (e.g. crypto-rouble or crypto-yuan). Des groupements de brevets voient le jour (e.g. la « *Blockchain Patent Sharing Alliance* » en Octobre 2017). Certaines sociétés comme nChain font du dépôt de brevet leur activité principale et vise à influencer le marché (en faveur de Bitcoin Cash et dorénavant de son « fork » Satoshi Vision). En première approche, il est quelque peu paradoxal que les défenseurs de Bitcoin, qui vise à exister indépendamment des Etats, cherchent à obtenir des droits de brevet qui sont des mécanismes de propriété institués par les Etats. En réalité, pour simplement exister et réussir à percer auprès du grand public, cela participe certainement de compromis qui semblent se réaliser sur beaucoup de plans (gouvernance, traçabilité et taxation, normalisation, collisions, congruences, compatibilités, etc.).

1. Faits et chiffres

1.1. Nombre de demandes publiées

Factuellement, les outils de recherche dans les bases de données de brevet permettent de mettre clairement en évidence l'augmentation des dépôts, confirmant les volontés de contrôler le secteur.

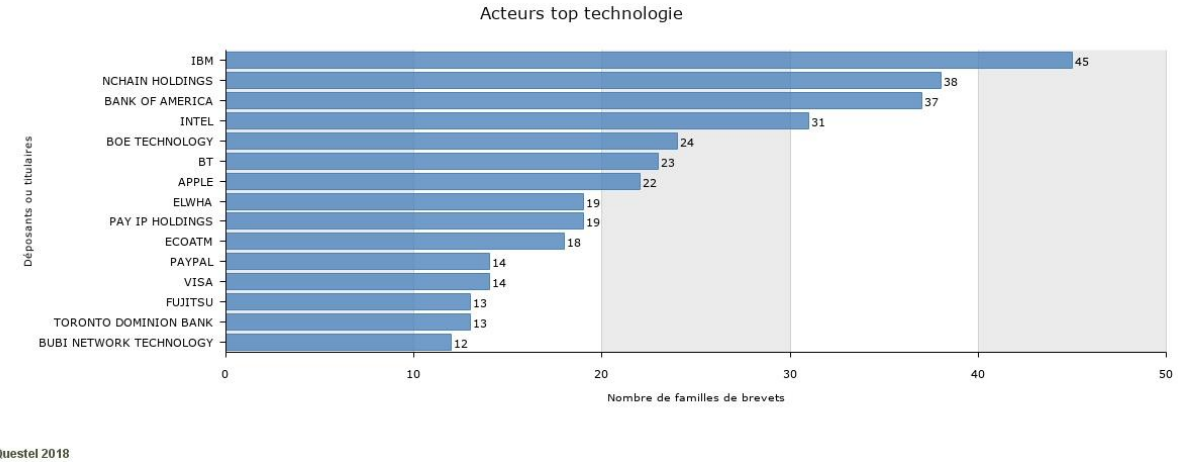
Mot-clef	*En revendications* **(nombre de demandes publiées)**			**En** *description* **(incluant les revendications) (nombre de demandes publiées)**		
	Fin 2017 (Nov.)	Mi 2018 (Juillet)	Mi 2019 (Juin)	Fin 2017 (Nov.)	Mi 2018 (Juillet)	Mi 2019 (Juin)
"**bitcoin**"	29	207	305	1527	2433	3768
"**blockchain**"	123	626	**1776**	512	1777	**4168**
"**smart contract**"	33	245	**1143**	226	764	**3303**

Source: Questel Orbit, entre Novembre 2017 et Juin 2019 (18 mois)

Les chiffres ci-dessus, en plus de rapports de recherche, semblent indiquer que les termes “blockchain” et “smart contract” sont entrées dans le corpus brevet, et en particulier dans le corpus des revendications. Bitcoin est largement cité, mais comme on peut s’y attendre, ne figure pas souvent dans les revendications. Bien que les définitions apparaissent comme stables dans Wikipédia, et comprises par les examinateurs, il reste recommandé de préciser les définitions en description (les propriétés des objets manipulés restant remarquables ; exécution en parallèle des contrats intelligents, diversité des types de chaines de blocs, etc).

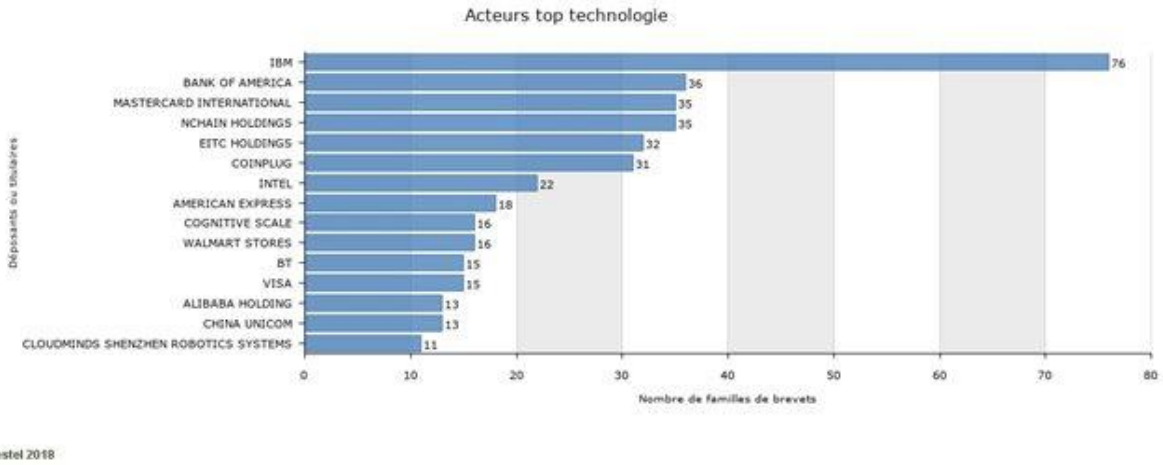
1.2. Demandeurs

Entre novembre 2017 (début de la rédaction de cet article) et juillet 2018, on remarque les dépôts massifs de la part des universités chinoises (si elles étaient cumulées, elles dépasseraient allègrement 300 dépôts).



« bitcoin » n’importe où dans le cahier des charges, nombre de familles par demandeur, Questel, juillet 2018

Certains autres demandeurs à souligner sont (sélection) : WALMART (11), MASTERCARD (10), NOKIA (10), UPS (10), ALIBABA (8), COINBASE (7), AMAZON (5), BITMAIN (10), NASDAQ (5), SAMSUNG (3), GOLDMAN SACHS (2), MICROSOFT (2), AMADEUS (1), ID QUANTIQUE (1)



« chaîne de blocs » n'importe où dans le cahier des charges, nombre de familles par demandeur, Questel, juillet 2018

Les demandes Bitcoin relèvent généralement de la grande classe IPC G06F (traitement de données), G06Q 30/00 (commerce électronique) et G06Q 40/00 (finance, fiscalité).

L'étude des demandes de brevet publiées à ce jour semble autant porter autant sur le cœur du projet (e.g. les « sidechains », qui pour certains dévoient l'idée fondatrice), que sur des perfectionnements qu'ils soient significatifs (par exemple pour programmer les chaînes de blocs) ou accessoires (dépôts opportunistes sur les interfaces des « *wallets* »). Une myriade d'applications verticales peut également être détectée.

A ce jour, il est désormais clair que le potentiel technique - et donc de brevets - de cette famille de technologies est substantiel. En premier lieu, le secteur des crypto-monnaies en tant que tel est en effervescence et continue d'inventer à rythme soutenu. A l'instar d'une véritable explosion évolutive précambrienne, de nombreuses technologies de base utilisées par les inventions Bitcoin évoluent rapidement.

Par exemple, la substitution des algorithmes originels « Proof-of-Work » (reposant sur la notion d'investissement) par des algorithmes « Proof-of-Stake » conduit à des systèmes substantiellement différents. Par ailleurs, par effet transversal, de nombreux domaines techniques réincorporent, en les modifiant parfois, les briques de Bitcoin. Des domaines techniques connexes ou éloignés s'hybrident rapidement avec les briques de base de Bitcoin (e.g. gestion des données personnelles, Internet des Objets, systèmes transactionnels, etc).

Pour le futur, on peut attendre des fertilisations croisées en augmentation. Dans le secteur de l'IT (Information Technology), les portefeuilles de brevets d'IBM et des GAFA totalise des centaines de milliers de demandes et brevets délivrés (le seul portefeuille IBM est de l'ordre de 50 000 titres en vigueur). Une fraction de ces inventions est susceptible d'être utilisée dans les technologies actuelles Bitcoin. Le raisonnement « en silos » des Offices de brevet devrait permettre pendant quelques temps d'opérer des transpositions brevetables (applications aux industries du voyage, de la santé, de l'avionique, etc.).

2. Exemples d'inventions

Les exemples suivants ne représentent pas la grande diversité des sujets abordés dans les demandes publiées.

Premier exemple : en lieu et place de publicités sur les navigateurs Internet, souvent jugées intrusives, en échange d'un accès à un contenu souhaité, il est possible d'exécuter localement un code logiciel dans le navigateur web client pour créer de la crypto-monnaie afin de rémunérer le créateur de contenu. De fait, des extensions pour les navigateurs, eu lieu de filtrer les publicités sont déjà proposées pour tenter d'empêcher l'exécution de ce type de code. L'exécution du code côté client coûte à ce dernier de la puissance de calcul, donc du matériel et de l'énergie. Des variations permettent d'envisager nombre de schémas différents : type de calcul (e.g.

folding@home et autres projets de recherche médical ou non) et/ou l'allocation aux bénéficiaires (e.g. répartition entre créateurs, producteurs, etc). La rentabilité économique et l'acceptation sociale de ce genre de système ne semble pas testée.

Deuxième exemple : le fondateur d'*Ethereum* donne un exemple pour « ubériser Uber »: avec les chaines de blocs et les contrats intelligents, Uber serait décentralisé en une collection de services unitaires, cherchant à maximiser leur efficacité individuelle ou collective, ou en étant en compétition les uns avec les autres. La mise en relation d'offres et de demandes de covoiturage pourrait être organisée de manière totalement algorithmique (cette dernière pouvant d'ailleurs être multi-critères, e.g. tenir compte de facteurs tels la proximité, le tarif, les conditions d'assurance, la réputation du conducteur et/ou du passager, etc.). De même, et plus largement, la mise en orchestre de services distincts (e.g. système d'interface utilisateur, système de recherche, système d'optimisation de routes, système de paiement, systèmes GPS, système d'assurances) pourrait être mise en œuvre via des contrats intelligents, temporaires mais objectifs. Les contrats intelligents promettent donc des « *mashups* » ad hoc, opportunistes, flexibles et éphémères. La question de la régulation, de l'existence et de la gestion de risques systémiques, classiques dans ce type de système complexe, restent des questions ouvertes.

Les chaînes de bloc et les contrats intelligents devraient également jouer un rôle dans l'Internet des objets en fournissant une infrastructure programmable et programmée pour faire interagir un grand nombre d'appareils. Or l'Internet des Objets (IoT) recèle de nombreuses promesses industrielles (par exemple en logistique, productique mais aussi dans le domaine de la maintenance aéronautique). Etant un levier de l'IoT, les chaînes de blocs et les contrats intelligents promettent de programmer et reprogrammer les chaînes de valeur.

3. Pourquoi protéger par brevet ? Différentes utilisations des brevets

3.1. Généralités

Les brevets peuvent être offensifs ou défensifs (ou les deux). Les brevets délivrés confèrent des droits exclusifs, c'est-à-dire le droit d'en exclure d'autres. Un brevet est une forme de contrôle, c'est-à-dire de pouvoir de décision, d'options facultatives. Pour un contrôle efficace, il faut souvent multiplier le nombre de titres. La force d'un portefeuille de brevets est généralement supérieure à la somme de la force de ses membres. Les demandes de brevet présentent aussi des avantages, en ce sens qu'elles constituent des menaces planantes significatives à l'encontre des parties adverses (analyse de liberté d'exploitation). Les demandes de brevets incluant de la matière non-revendiquée peuvent représenter autant de « munitions », pour modeler les revendications en cours d'examen. Une bonne connaissance des procédures en vigueur dans les différentes juridictions permet d'optimiser les voies de procédure à suivre (par exemple, Traité de coopération sur les brevets (PCT), dépôts nationaux, etc.). Il existe même des « astuces », comme l'utilisation de voies secondaires pouvant échapper au radar des conseils en propriété industrielle adverses.

Lorsqu'une invention générique est publiée, il est généralement toujours possible de breveter des inventions spécifiques. Le générique n'anticipe pas le spécifique (mais le contraire est vrai). Des brevets de perfectionnement restent généralement possibles

après un dépôt pionnier : des déposants adverses peuvent se neutraliser mutuellement (dépendances mutuelles).

En complément ou en substitution des droits de brevet, il est possible de recourir à la publication défensive. La publication entrave la brevetabilité. Une publication défensive sophistiquée peut impliquer la participation d'un conseil en propriété industrielle, qui sera par exemple attentif aux éventuelles améliorations adjacentes à l'invention de départ. Même s'il est possible d'utiliser des publications électroniques, il est toutefois préférable de recourir aux « canaux » officiels (par exemple, publication des demandes, en amont, auprès des offices de brevets, procurant une indexation native des contenus).

De très nombreux autres paramètres sont à prendre en compte. Les brevets peuvent changer de mains. Un brevet défensif peut finir par être acheté par une entité agressive, par exemple un *patent troll*. Le paysage technologique peut changer rapidement. La qualité de la rédaction d'un brevet peut s'avérer très importante. La jurisprudence peut changer, et de manière radicale. Une demande de brevet dont la description est riche pourra être mobilisée de manière plus ou moins adéquate afin de rivaliser avec des documents cités par les examinateurs et allégués comme étant en collision avec l'invention. La période d'examen (par exemple, la fin de l'année) peut jouer un rôle important dans certaines juridictions. Et la liste est longue.

3.2. Demandes d'inventions relatives à une chaîne de blocs

Bitcoin est (aussi) une affaire politique.

Il peut s'avérer utile de breveter des développements technologiques souhaités. Mais il peut aussi s'avérer tactique de breveter des orientations technologiques qui, au départ, *ne sont pas* souhaitées. Il est possible de breveter une situation défavorable, pour en évincer tout tiers, notamment un compétiteur. Par exemple, les demandes de brevet visant à *sécuriser* l'affichage des publicités sur les dispositifs électroniques (en contournant les bloqueurs de publicité) peuvent être déposés par des annonceurs (pour empêcher ces bloqueurs de publicité) ou, au contraire, par des opposants à la publicité en ligne pour réserver des droits exclusifs et en évincer les annonceurs.

Tout brevet déposé peut être utilisé en faveur, ou en défaveur, de Bitcoin. Les aspects fondamentaux de la protection par brevet sont importants, mais les caractéristiques secondaires peuvent l'être tout autant (par exemple, chaînes secondaires, interface utilisateur, etc.). Le brevetage des chaînes latérales ou l'extensibilité hors chaîne, même s'il s'agit de technologies indésirables pour certains, peut favoriser le contrôle et permettre de (ré)orienter le marché (voir, par exemple, l'affaire US2016330034).

4. Le cas particulier de nChain Holdings (nCrypt, auparavant EITC Holdings)

La société nChain Holdings (anciennement connue sous le nom de EITC Holdings) dépose de nombreux brevets dans le domaine des Bitcoin, depuis 2014. Constituée sous le nom de nCrypt (Société à responsabilité limitée) et elle est censée être financée à hauteur de 300 millions de dollars.

La société nChain a publié 156 demandes (jusqu'en juillet 2018). Déposées après 2014, 35 demandes au moins mentionnent M. Wright au titre d'inventeur. Dans le corpus des *arbres de revendications* publiés déposés à ce jour, si l'on exclut les noms communs (comme ordinateur, système, message, etc.), on constate que les termes significatifs suivants ont été employés (nombre d'occurrences entre parenthèses) :

nœud (528 fois), transaction (525), public (396), privé (304), script (237), hachage (227), valeur (149), chaîne de blocs (147), maître (146), secret (130), partie (126), métadonnées (114), jeton (114), déterministe (102), contrat intelligent (101), crypto-monnaie (95), cryptographique (84), invitation (81), registre (81), rachat (81), épisode (75), adresse (66), générateur (65), paiement (65), contenu (58), contrôle (41), conditions (34), inscription (34), P2P (32), amorce (30), elliptique (27), code (25), diffusion (22), boucle (20), bitcoin (18), trafic (15), attaquant (13), portail (13), licence (13), profil (12), routage (12), flux (11), fiable (10), portefeuille (10), authentification (9), paie (8), booléen (7), taux (7), automate (6), chaîne (6), séquestre (6), Honeynet (6), système pot de miel (6), monnaie fiduciaire (5), aléatoire (5), anneau (5), risque (5), arbre (5), influence (4), falsifié (4), interface (3), numérisation (3), topologie (3), contrôleur (2), irréversible (2), emprunt (2), Turing (2), Merkle (2), Shamir (1).

Les titres incluent des termes ou expressions comme :

système de comptage, vote sécurisé, transactions Turing complètes, , secret commun, sécurité réactive, sécurité préventive, théorie du choix, portefeuille, P2P, émission de jetons, paiement en temps réel, remboursements, web de confiance, paie, contrats intelligents d'application en chaîne de blocs, prêts de pair à pair, transactions symétriques équitables, fonctionnalité de portail logique, contrôle de performance d'un contrat, distribution de contenu numérique, vérification du propriétaire du logiciel, tableau de hachage distribué, registre distribué de pair à pair.

Même si d'autres publications sont attendues dans un avenir proche, celles existantes fournissent déjà un aperçu préliminaire du portefeuille en constitution.

Alors qu'il semblerait que le protocole de base soit provisoirement breveté, certains termes sont clairement absents des revendications, comme « sidechains ». Les publications futures pourraient inclure ces termes.

Dans « L'affaire Satoshi », A. O'Hagan mentionne que nCrypt envisageait de « ... *retravailler les services financiers, sociaux, juridiques ou médicaux* ». Toutefois, peu d'applications verticales semblent émerger dans le corpus publié, à l'exception de la gestion des droits numériques. De même, il manque de nombreux mots-clés stratégiques en technologies de l'information, comme : « *advertisement* » (Google), « *cloud* » (Amazon) - qui n'est curieusement cité que dans sept demandes -, ou « *social* » (Facebook).

L'article suivant présente des indications quant à des opportunités de prises de brevet.

IV. Perspectives concernant les inventions liées à la chaîne de blocs

Après avoir fourni des définitions, rappelé la législation sur les brevets et la jurisprudence et analysé rapidement les nouvelles demandes de brevet, quelques conclusions temporaires peuvent être proposées concernant les perspectives des inventions mises en œuvre par une chaîne de blocs (opportunités et questions ouvertes).

1. Opportunités manifestes

Les remarques suivantes doivent bien entendu être considérées avec la plus grande prudence.

D'après les recherches conduites, il semble qu'il reste encore des opportunités de prise de brevet en matière de technologie fondamentale (par exemple, les chaînes latérales ou secondaires). Certains domaines adjacents qui profitent des améliorations des technologies cœur (par exemple, les techniques de chiffrement) pourraient bénéficier de la protection par brevet, par fertilisation croisée des domaines techniques. Dès à présent, certaines inventions spécifiques concernant des applications verticales de ces technologies sont succinctement présentées.

1.1. Lacunes dans les technologies fondamentales

L'activité de protection par brevet sur Bitcoin étant précoce, *modulo* la période de secret de 18 mois, il semble que des mots-clés importants font défaut dans les revendications publiées (qui définissent les limites de la protection).

Le cas du mot « sidechain » est intéressant. Afin d'étendre l'utilisation de Bitcoin et d'accroître sa vitesse, des « chaînes secondaires » ou « chaînes latérales » sont parfois mises en œuvre, en parallèle des chaînes principales. Certains soutiennent que ces chaînes latérales nuisent à la sécurité et font augmenter les coûts de transaction. D'autres expliquent que ces types de chaînes introduisent la déflation (car ils font augmenter la fourniture « d'argent », la réserve bancaire fractionnée, la destruction du facteur de rareté, etc.). Les chaînes latérales ou « l'extensibilité hors blocs » sont donc rejetées par certains dans la communauté Bitcoin. Des requêtes dans le corpus brevet incluant par exemple le mot « sidechain » (dans les revendications), ou des variantes de celle-ci, donne très peu de résultats positifs (par exemple, l'affaire US20160330034, par Blockstream, inventeurs Gregory Maxwell, développeur de Bitcoin Core, et Adam Back, inventeur prétendu de *Hashcash*, voir aussi l'affaire US2016035358165).

Cet exemple semble indiquer qu'il est tout à fait possible que des brevets pionniers puissent encore être délivrés sur des principes génériques ou généraux (par exemple, élagage de la chaîne de blocs, mécanismes de consensus décentralisés, contrats intelligents avancés, etc.). Comme il a été dit, il est également possible d'élaborer des variantes, des améliorations, des solutions de rechange ou des alternatives aux systèmes de vérification par preuve de travail.

1.2. Importation et adaptation de schémas cryptographiques connus

La cryptographie est une composante majeure du système Bitcoin et des chaînes de blocs. Les améliorations de la cryptographie peuvent probablement être « importées » dans Bitcoin (c'est-à-dire, modifiées et associées pour répondre à des problèmes techniques spécifiques), ce qui peut donner lieu à de nouveaux brevets. En d'autres termes, il peut être judicieux d'analyser attentivement des portefeuilles en cryptographie (et, par exemple, d'étudier quelles sont les inventions applicables, comme c'est le cas dans les systèmes de crypto-monnaie, et ce qui peut être adapté à l'économie sous-jacente des crypto-monnaies).

En tant que science, la cryptographie inclut de nombreuses sous-catégories, comme la cryptographie par code, la cryptographie par hachage, la cryptographie basée sur les treillis. La cryptographie est principalement classée dans la classe américaine 380 ou CPC H04L 9/00. Cette dernière classe inclut 2 242 documents de brevet. Une partie des mécanismes décrits dans ces brevets pourrait être réutilisée et adaptée à des systèmes de crypto-monnaie.

La liste des sujets à examiner est longue. Une sélection dans le désordre : *signatures multiples, partage du secret de Shamir, calcul sécurisé multi-partie, sécurité théorique de l'information, sécurité sémantique, cryptage homomorphe, protocoles de vote, schémas de signature Merkle, chiffrement éphémère, cryptage à préservation de format*, etc.

Il convient d'accorder une attention particulière à l'informatique quantique. À ce jour, l'avènement des ordinateurs quantiques n'est pas encore certain, mais il ne faut pas l'écarter. Les articles de nChain indiquent que, même dans un tel cas (par exemple, algorithme de Shor), le système Bitcoin ne serait pas menacé. Cela vaut toutefois la peine d'étudier la manière d'utiliser les techniques post-quantiques émergentes, par exemple la *Distribution quantique des clés* (afin de prévoir les défaillances de mise en œuvre, qui sont une triste réalité). Il semble sage d'inclure dans les descriptions de demandes de brevet des développements sur des algorithmes post-quantum.

1.3. Autres technologies adjacentes (IP scouting)

Les portefeuilles des fournisseurs de *technologies de l'information* peuvent être explorés en profondeur et, le cas échéant, adaptés aux nouveaux paradigmes. Afin d'améliorer les systèmes existants, diverses technologies adjacentes peuvent être associées aux éléments fondamentaux de Bitcoin (par exemple, pour améliorer la *vitesse* et la *sécurité* de Bitcoin).

Certains domaines essentiels incluent la sécurité de la mise en œuvre du code, la gestion du réseau, la gestion de l'alimentation, les interfaces d'utilisateur et les technologies permettant l'émergence de marchés dérivés.

La *mise en œuvre du code logiciel* de Bitcoin peut s'avérer essentielle pour la sécurité et on peut donc s'attendre à ce que les brevets traitent la façon dont les dénis de service sont abordés, ainsi que les éclatements de transactions, l'introduction d'erreurs, les transactions fausses, mal réalisées ou malveillantes, etc. Dans le

domaine de la *sécurité informatique*, on peut associer des principes génériques ou spécifiques à des sous-systèmes Bitcoin existants pour générer une nouvelle propriété intellectuelle. Le système Bitcoin doit résister aux attaques réalisées au niveau du protocole (par exemple, attaques dues à l'intervention humaine).

L*'évolutivité* du réseau Bitcoin peut inclure ou requérir une gestion spécifique du réseau. Les caractéristiques brevetables peuvent concerner des inventions liées au matériel informatique, par exemple la gestion de l'alimentation, le calcul par le GPU, les technologies FPGA, etc. À l'origine, Bitcoin n'avait pas de limites en ce qui concerne la taille des blocs. Afin d'éviter les attaques DDoS, une limite a été introduite, relevée par la suite, et à l'heure actuelle elle reste un facteur restrictif.

Les *interfaces d'utilisateur* sont essentielles pour la facilité d'utilisation de Bitcoin (c'est-à-dire, la vitesse de la monnaie). De plus, les brevets concernant les interfaces d'utilisateur sont détectables. Les interfaces utilisateur des portefeuilles sont actuellement reconnues comme étant défectueuses ou ne donnant pas entière satisfaction. Les portefeuilles diversifiés et l'expérience acquise dans les activités de brevetage des fournisseurs de technologies de l'information seront probablement mis à profit pour des applications liées à Bitcoin et à la chaîne de blocs. Compte tenu de l'irréversibilité des transactions, certaines méthodes pourraient être développées pour inverser, interrompre, reprendre, annuler ou sécuriser une transaction (contre les erreurs, les abus, le vol d'identité, etc.).

Il se pourrait bien que des *marchés dérivés* soient créés à partir de Bitcoin. Ils doivent l'être et ils le seront. Ces marchés peuvent correspondre à des mécanismes spécifiques. Les techniques utilisées dans le secteur financier depuis des décennies peuvent être reproduites « en l'état » ou spécifiquement adaptées. Par analogie, les techniques et l'expérience acquises en finance algorithmique ou en *High Frequency Trading* peuvent, de même, être avantageusement réutilisées et/ou adaptées. Les brevets portant sur la finance peuvent être revus à la lumière de Bitcoin (voir, par exemple, l'affaire US9704143).

En tant que principe général, *l'informatique* brevetée peut faire l'objet d'explorations dans un grand nombre de directions. Par exemple, parmi les documents de brevets ayant IBM pour demandeur, 62 d'entre eux incluent le terme « *consensus* » dans les revendications et 481 dans les descriptions. Les techniques de consensus distribué peuvent vraisemblablement être sophistiquées (Des mécanismes de virtualisation ou de conteneurisation peuvent être explorés afin d'abstraire Bitcoin de la méta-gestion des crypto-monnaies en concurrence entre elles (économie darwinienne)

1.4. Chaînes de blocs et inventions spécifiques aux applications verticales

La protection par brevet de chaînes de blocs spécifiques et/ou de leurs applications peut favoriser « l'Internet de la valeur » (Internet pour la communication, chaîne de blocs pour la valeur). Les possibilités de prises de brevet concernant les applications des technologies discutées ici semblent rester amplement ouvertes.

Les chaînes de blocs et technologies associées peuvent être utilisées dans différents secteurs et pour divers usages. À ce jour, la liste sans cesse croissante des applications des chaînes de blocs destinées à différents secteurs inclut d'éventuelles

applications dans : les réseaux sociaux, la production (par exemple, avionique, journaux de bord), la robotique, les services publics (par exemple, gestion de réseaux intelligents), les médias (par exemple, gestion des droits numériques, distribution de contenus), les services (par exemple, assurances), le secteur touristique (par exemple, billetterie), les services juridiques (par exemple, négociation électronique), l'éducation, les soins de santé (par exemple, gestion des dossiers des patients), les gouvernements ou les services publics, la sécurité personnelle, l'identité ou la sûreté, la logistique (par exemple, transports), les télécommunications et même les jeux (paris sur Internet, les casinos étant à l'origine de Bitcoin)

Chacune de ces applications verticales (sectorielles) peut recourir à des combinaisons spécifiques de technologies, dont certaines peuvent être brevetables. Dans certains cas, une partie de ces développements spécifiques peuvent enrichir, à leur tour, les principes généraux.

Par exemple, un Internet des objets reposant sur des chaînes de blocs peut poser des problèmes techniques très spécifiques et, par conséquent, impliquer des solutions brevetables. Ces solutions peuvent recourir à des nano-transactions, utiliser des *fonctions impossibles à cloner physiquement* (PUF), etc.

Les techniques de gestion de la confidentialité reposant sur des chaînes de blocs peuvent mettre en œuvre un ou plusieurs mécanismes comme *k-Anonymity, l-diversity, Virtual Party Protocols, Secure Sum Protocols, differential privacy, exponential mechanism, quasi-identifiers, or Statistical Disclosure Control*. Nous pourrions citer de nombreuses autres applications, par exemple en matière d'analyse des données, d'apprentissage automatique (approfondi, fédéré, etc.).

Un autre domaine d'intérêt est celui de la propriété industrielle des sites « marchands », comme celui d'Amazon (voir l'affaire US8719131), ou de Wal-Mart. Les sites marchands sont encouragés à fournir l'option de hachage nécessaire pour gérer correctement les chaînes de blocs (ils souhaitent être rémunérés). Il semblerait que, pour leur part, le nombre de demandes de brevets augmente rapidement.

2. Questions ouvertes et perspectives

Bitcoin et les technologies émergentes connexes soulèvent nombre de questions fascinantes. Dans le désordre :

Perspectives de mise à l'échelle. Si, selon la conjecture de Moore, la mise à l'échelle de Bitcoin a effectivement lieu, des millions de chaînes de blocs pourraient-elles rivaliser entre elles ou plutôt coopérer (mesures de similarité, etc.) ? Des systèmes hybrides de chaînes de blocs décentralisées et « centralisées » (c'est-à-dire, des bases de données de sens commun) pourraient émerger et être brevetées. L'intelligence artificielle et, dans la pratique, l'apprentissage automatique, reposent souvent sur des « big data ». Comment les chaînes de blocs se rattachent-elles à l'intelligence artificielle et/ou aux mégadonnées ? L'intelligence artificielle a-t-elle besoin de données sécurisées par une chaîne de blocs ?

Perspectives minimalistes. Les méthodes et les systèmes de la chaîne de blocs peuvent-ils être appliqués aux échelles de calcul les plus faibles, dans l'espace et/ou le temps (par exemple, au niveau des instructions dans un CPU) ? L'Internet des objets peut également utiliser des types spécifiques de chaînes de blocs ou de systèmes par preuve de travail.

Perspectives méta. Les monnaies sont inextricablement liées à leurs protocoles (OSS). Serait-il possible de structurer les monnaies (monnaie directrice, etc.) ?

Perspectives amont. Certaines techniques cryptographiques existantes peuvent-elles être revisitées en fonction des nouvelles perspectives actuelles, afin de mieux adapter les besoins actuels ?

Perspectives aval. Quelles sont les possibilités d'analyse des chaînes de blocs, c'est-à-dire d'observation de celles-ci ?

Perspectives business. De nouveaux modèles commerciaux, désormais à caractère cryptographique, peuvent surgir et devenir brevetables (micro-transactions, nouveaux types d'intermédiaires ou de courtiers en données, etc.).

Perspectives politique. Les nations et les gouvernements promulguent des lois. Alors que certains pays sont favorables aux monnaies numériques (Bitcoin a reçu la bénédiction officielle du Japon en avril 2017), beaucoup d'autres leur tournent le dos (comme la Chine). La diversité des attaques ne cesse de s'accentuer (récemment, il a été dit que la chaîne de blocs Bitcoin inclut des hyperliens vers des vidéos à caractère pédophile). Le système Bitcoin, et plus largement les chaines de blocs, doivent se frayer un chemin à travers de nombreuses législations, comme la réglementation bancaire, l'acceptation sociale, la pertinence économique et écologique. Les lois sur les brevets peuvent être modifiées, de même que la jurisprudence, en faveur des crypto-monnaies (par exemple, « caractère technique», aspect tangible) mais aussi contre elles (par exemple, actuel « reduction to practice »).