# *Blockchains* pour la défense

## Blockchain for defense

Alexis Poindron[1]

[1] Unité d'Economie Appliquée, ENSTA Paris, Institut Polytechnique de Paris, France, alexis.poindron@ensta-paris.fr

**RÉSUMÉ.** Nous discutons des possibilités d'usage de la *blockchain* pour la défense, avec un accent particulier sur la question de l'innovation dans les secteurs duaux. Nous nous prononçons en faveur d'une *blockchain* tenue par la défense, à plusieurs niveaux de confidentialité, où des appels d'offres seraient formulés par des contrats intelligents. Nous soutenons que cet environnement catalyserait l'innovation duale en favorisant, non seulement les rencontres entre la défense et l'innovation civile, mais encore entre les entreprises elles-mêmes, qu'elles soient civiles ou militaires.

**ABSTRACT.** We discuss the potentialities of blockchains used for defense, with an emphasis on innovation in dual sectors. We argue in favor of defense guided by blockchain, with multiple levels of confidentiality, where public tenders are formulated with smart contracts. We argue that this environment would catalyze dual innovation, not only between defense and the civil sector, but also between enterprises, be they civil or military.

**MOTS-CLÉS.** *blockchain*, innovation, défense, contrats intelligents.

**KEYWORDS.** blockchains, innovation, defense, smart contracts.

### 1. Introduction. Une brève histoire de la *blockchain*. Quel rapport entre la *blockchain* et la défense ?

La *blockchain* est un registre distribué et décentralisé, organisé en blocs contenant les listes d'opérations. La première *blockchain* fut conceptualisée, introduite et présentée par [NAK 08] en tant que technologie sur laquelle est fondé le *Bitcoin*. Le registre distribué en question était alors cantonné à une liste de transactions partagées en *peer-to-peer*. La *blockchain* est donc historiquement liée aux cryptomonnaies : elle propose fournir un cadre de coordination sécrétant, pour ainsi dire, la monnaie comme son propre sang, mais elle n'y est donc pas cantonnée, n'étant que la technologie que sous-tend les cryptomonnaies.

L'existence d'un système de validation différencie une *blockchain* d'un registre distribué classique. Dans une *blockchain* publique de type *Bitcoin* ou *Ethereum* 1.0, la validation se fait par preuve de travail. D'autres *blockchains* utilisent d'autres systèmes de validation. Par exemple, *Tezos*, *Cardano* et *Ethereum* 2.0 utilisent une preuve d'enjeu[1].

Si *Bitcoin* ouvrit la révolution des *blockchains*, le deuxième pas significatif fut marqué par l'implémentation des contrats intelligents sur la *blockchain*. *Ethereum* [BUT 13] et *Tezos* [GOO 14] développèrent concomitamment cette technologie, implémentant sur les *blockchain*s un langage *Turing complete* (c'est-à-dire capable de faire tourner n'importe quel programme qu'un ordinateur peut faire tourner) que n'était pas le programme *Bitcoin*, cantonné aux transactions financières.

Un contrat intelligent est un programme informatique codifiant un contrat entre deux parties, et s'exécutant automatiquement lorsque les conditions d'exécution du contrat sont remplies. Ou plutôt, le contrat est exécuté par les validateurs du réseau, c'est-à-dire, dans le cas d'une *blockchain* publique, par les mineurs qui sont rémunérés pour cette tâche, soit que des pièces soient créées pour eux, lorsque la *blockchain* en question est animée par sa propre cryptomonnaie, légèrement inflationnaire, soit que

[1] Tel semblait être le souhait du co-auteur d'*Ethereum*, Vitalik Buterin, depuis la création d'*Ethereum*, bien que la conversion de la preuve de travail à la preuve d'enjeu fût longue. Dans la preuve d'enjeu, les mineurs engagent d'importants dépôts de garantie, et leur probabilité de valider les blocs est proportionnelle à leur dépôt - ce système est conçu pour rendre la fraude absurde, puisque la perte du dépôt de garantie, sanction consécutive à la fabrication d'un faux bloc, rendrait le coût de la manœuvre supérieur aux bénéfices.

 

l'émetteur de la transaction, qui s'acquitte des frais de transaction, soit l'unique source de financement du minage.

Dans la lignée de la *blockchain Bitcoin* qu'il complète, le contrat intelligent permet donc de se passer d'un tiers de confiance. De même que *Bitcoin* peut se passer de banques, le monde de la justice est remplacé par celui de l'informatique. Avec le *Bitcoin*, le réseau validait les transactions du bitcoin par un système de validation par preuve de travail. Avec les contrats intelligents, là encore, un système de validation quelconque (preuve de travail ou d'enjeu) vérifie les conditions et fait tourner les contrats intelligents. Ceux-là constituent donc une suite naturelle à cette *blockchain* primitive.

Bien que les contrats intelligents se greffent naturellement sur la *blockchain*, et qu'ils peaufinent la technologie primitive du bitcoin pour porter son potentiel à maturation, néanmoins il n'est pas inepte de considérer séparément nos deux piliers, de distinguer des applications *blockchain*s la dimension "*Bitcoin*" (c'est-à-dire la technologie pair-à-pair, avec un système de minage) de la dimension "contrat intelligent". La deuxième nous intéressera davantage.

En deux mots, la *blockchain*, au sens large, est donc à regarder comme un écosystème, un lieu de coordination et d'échanges commerciaux et financiers.

En dépit d'une architecture bien qualifiée par son nom, il ne serait peut-être pas abusif, cependant, de désigner par "*blockchain*" toute sorte de communication dont l'authenticité est garantie par un système de validation plus ou moins horizontal : qui dit *blockchain* sous-entend résilience. Que la destruction ou corruption d'un nœud ne paralyse pas le réseau - plus de routeurs, plus de serveurs, mais une toile organique de millions de témoins mutuels - suggère bien d'autres utilisations de la *blockchain* que de simples transactions. On comprendra aisément que cette technologie n'ait pas manqué de susciter bien des attentes et des espérances quant à ses applications, et notamment de la part de la défense. C'est ce point qui nous intéresse plus particulièrement dans cet article, où nous nous proposons un état des lieux des applications défense de la *blockchain*.

Cet article est organisé comme suit. Puisqu'ils sont appelés, à notre sens, à jouer un rôle central dans un environnement coordonné, nous discutons en Section 2 l'utilisation générale des contrats intelligents. La Section 3 campe le paysage de la *blockchain* dans une visée de coordination au sens large, en discute quelques aspects techniques. Enfin, puisque c'est vers celle-ci que tendait notre section dévolue à la coordination, la Section 4 peut enfin proposer la *blockchain* comme lieu de rencontre et d'émulation entre secteurs civil et militaire. L'architecture de la *blockchain* étant la plus prometteuse en tant qu'elle "met en relation", un accent particulier sera mis sur l'innovation dans les secteurs duaux. La Section 5 conclut.

## 2. Un écosystème de contrats intelligents

Le contrat étant le coeur des activités économiques, et qu'ils exigent le plus de confiance et de transparence possible, le contrat intelligent devait se situer naturellement au coeur des transactions. Le contrat étant donc l'implémentation concrète de la confiance entre des parties, il était naturel d'implémenter des contrats intelligents sur la *blockchain*. L'authenticité du contrat intelligent est alors garantie par la technologie des *blockchain*s: tous les nœuds du réseau peuvent vérifier les conditions d'application du contrat. Le réseau fait tourner les contrats intelligents comme il valide les transactions.

### 2.1. *Ce n'est pas une révolution conceptuelle …*

L'idée du contrat intelligent est immémoriale. Comme la *blockchain* dans sa version la plus simple, la version *Bitcoin*, touchant directement aux origines de la monnaie ("j'utilise le bitcoin que m'a donné Pierre, qui le tient de Jacques, qui le tient de Jean, etc."), le contrat intelligent constitue une solution technique révolutionnaire à des questions millénaires. Il ne s'agit en effet, au fond, que d'une mise en informatique des ordonnances hébraïques, dans la forme de ceux du Pentateuque. Quant au *peer-to-*

*peer*, il s'agit d'un système de témoins généralisés. On peut éventuellement dire que, si nouveauté conceptuelle il y a, elle se trouve dans l'unification de l'ordonnance et du témoignage, dans l'élargissement de l'assemblée de témoins à une communauté entière, exécutrice des contrats. Si révolution il y a, elle est purement technique.

### 2.2. *… c'est une révolution technique*

Mais c'est déjà énorme. Il n'est plus besoin de vérifier manuellement que les conditions d'application du contrat sont bien remplies. Parce que, selon les mots d'Edouard Klein, ils remplaçent trente bureaucrates par quelques lignes de code, les contrats intelligents sont déjà utilisés par la gendarmerie nationale. Ainsi *Tezos* est-il utilisé par le C3N (unité nationale de lutte contre la cybercriminalité de la Gendarmerie), qui grave sur une *blockchain* les dépenses dont elle doit rendre compte auprès d'Europol [FAV 20]. Les contrats intelligents peuvent donc court-circuiter une paperasse laborieuse et inefficace en ménageant une liste de conditions. Le "contrat" - il convient de mettre des guillemets, car le sens de ce mot est considérablement élargi par l'usage, un contrat intelligent n'étant pas forcément un contrat au sens économique du terme - est validé lorsque toutes les parties ont donné leur feu vert.

Un champ de nouvelles possibilités s'ouvre pour résoudre des affaires qui naguère semblaient impossibles à mettre en pratique à cause des frais de gestion, de la complexité ou de la difficulté d'évaluer les externalités. Des systèmes de facturation ou de pénalités complexes deviennent possibles, spécifiées et implémentées par un maillage de contrats qui s'appellent les uns les autres, où les digues s'ouvrent et se ferment, déterminées par l'activité des parties en jeu. Par exemple, la diffusion des œuvres artistiques et intellectuelles peut être entrée sur des contrats intelligents [BAS 20]. Sous cet angle, le *smart contract* fonctionne tout-à-fait comme un réseau de Pétri, comme l'a remarqué [ZUP 20], en cela qu'il ouvre ou ferme les digues, exactement comme les réseaux de Pétri par leur système de jetons. La paternité d'une œuvre et sa valorisation commerciales sont unifiées, le dépôt du *hash* sur la *blockchain* publique pouvant être associé à un contrat intelligent chargé de délivrer en direct la lecture de l'œuvre (stockée par exemple sur une *blockchain* privée communiquant à la *blockchain* publique) au souscripteur.

Les vieux problèmes du monopole naturel, de l'interopérabilité des fournisseurs de services et l'entreprise de travaux de télécommunications peuvent se résoudre par des contrats intelligents. Alors que les infrastructures seraient encore à construire, les utilisateurs souscriraient à un abonnement "à condition que dix millions de personnes minimum y souscrivent" [ROH 74], [KAT 85], [KAT 86]. On ne risque alors plus de se retrouver seul avec un téléphone qui ne peut appeler personne. Quand un entrepreneur audacieux, qui tisse un réseau dans un pays où tout est à construire, proposait une collaboration à un partenaire, ce dernier pouvait craindre que les promesses du premier ne soient fondées que sur du sable. Avec le contrat intelligent, des conditions telles que celles-ci peuvent être ménagées : "si l'entrepreneur reçoit la subvention qu'il attend, et si X, Y et Z consentent eux aussi à prendre part au projet, et si la banque consent au prêt, alors…".

Des conditions extérieures peuvent même être ajoutées comme véto ou condition nécessaires. À la faveur d'oracles qui communiquant à la *blockchain* la température extérieure, tel contrat intelligent sera déclenché, ruisselant de proche en proche. L'information sur ce tissu organique se répercute à tous les degrés du système.

### 2.3. *Exploiter à la source*

Si l'on entend partout répéter que la *blockchain* "permet de se passer des tiers", toutefois on entend rarement remarquer que la *blockchain* permet de se passer de bases de données intermédiaires, qu'elle permet une communication directe, une osmose entre les individus et/ou les entreprises, au sujet desquelles on collecte des données, et l'exploitation de ces données. Plus généralement, un écosystème de *blockchains* semble faciliter la communication entre toutes sortes de données et l'analyse des données. Il n'est plus besoin de bases de données élaborées séparément : tout communique et on

 

pioche directement les données à la source. Si donc, selon Nick Szabo [SZA 16], les contrats intelligents faciliteraient la recherche sur le cancer, c'est, pensons-nous, dans la mesure où elles offrent une osmose entre les données anonymisées des patients, et leur exploitation directe et sans filtre par la recherche médicale. Tout l'intérêt de ce système d'échanges et de contrats (action) repose sur la possibilité de puiser directement avec les bases de données (information) sans avoir besoin de construire une base de données intermédiaire privée, *ad hoc*, jetable et conditionnée à une mission ou une recherche particulière. Tous les chercheurs travaillant sur des données empiriques s'en sont rendu compte : construire une base de données est long, et cette dernière doit être rentabilisée par la publication de plusieurs papiers. Avec la *blockchain*, cette élaboration serait considérablement facilitée.

C'est en vérité tout la recherche scientifique qui semble avoir à y gagner. On peut ainsi dresser, par exemple en mathématiques, un "réseau des problèmes ouverts", de leurs applications supposées, et des "problématiques connectées". La centralisation au sein d'un seul écosystème, et de préférence un écosystème centré sur l'intérêt national, permettrait de gagner un temps considérable, et surtout, que des chercheurs indépendants n'ont pas besoin de rebâtir éternellement pour leur propre compte (activité qui constitue le gros du temps consacré à la recherche empirique).

Pour l'instant, la recherche scientifique avance sans architecture globale, par une succession de "*lucky guesses*" disait René Thom. Et s'il est vrai, par exemple en mathématiques, que le hasard et la confrontation à des bases de données de formules permet de tisser des liens insoupçonnés qui font avancer la recherche par d'heureuses surprises, que les avancées profondes en matière de recherche scientifique ne se font pas par des appels d'offres, et que la sérendipité (pénicilline) et la recherche fondamentale (laser) jouent un rôle capital dans les recherches solides et de longue haleine, néanmoins il convient à court terme de garder un œil sur les problématiques brûlantes. La *blockchain* pourrait offrir une meilleure visibilité et, contrairement à ce qu'on pourrait penser de prime abord, un catalyseur de sérendipité. Car c'est lorsque l'encyclopédie se déploie sous nos yeux que les analogies, que la reconnaissance de constantes, de motifs, de séries déjà-vues et que l'on retrouve en feuilletant l'encyclopédie des formules …

De même, la valorisation des inventions serait facilitée par le transfert de bases de données brevets sur la *blockchain*, par l'appel direct des données brevets depuis les contrats intelligents. Ces bases de données directement analysables et exploitables court-circuitent l'élaboration laborieuse de bases de données "faites à la main".

Que l'on songe maintenant que cette *blockchain* soit, comme nous le suggérerons par la suite, tenue par la défense, que celle-ci puisse vaguement faire connaître la direction de ses besoins (donner une "direction linéaire" à la recherche), et laisser la recherche et l'invention aller s'y diriger. Une part d'aimantation et une part de sérendipité se mêlent pour chacun faire éclore l'autre en un cercle vertueux. Tout cela peut être géré par des contrats intelligents.

### 2.4. *Digestion des sacs de nœuds*

Les contrats intelligents, en s'appelant les uns les autres, pourraient permettre de digérer des sacs de nœuds. À ce titre, ils offrent une méthode. La rigueur d'une validation pas-à-pas des points d'accords, des décalages de vocabulaire, ou la mise entre parenthèse des accidents historiques, pourraient être traités plus rigoureusement, permettant aux différentes parties de clarifier les litiges et de s'extirper de la logique du chaudron. Le contrat intelligent peut constituer un appui technique pour résoudre des schismes, en remontant pas-à-pas jusqu'à la source du désaccord, et aboutir à une réunification dogmatique comme on repousse les nœuds jusqu'au nerf de tous les nœuds. Les contrats intelligents constituent donc un outil de clarification, de pacification qui pourrait grandement aider les litiges à se résorber.

 

### 2.5. *De la remontée automatique. Une nouvelle ère juridique*

Au lieu de lister les devoirs des deux parties, le contrat intelligent remplace le devoir et la violations par des listes de conditions, qui implémentent automatiquement les conséquences de toutes les situations possibles. Le contrat intelligent contient la sanction, non comme une sanction légale, punitive, mais comme une simple disposition du contrat. Il suggère un recours aux instances juridiques en aval plutôt qu'en amont, en cas de litige et non à titre d'opérateurs de validation. En vérité, il n'y a plus de sanctions du tout : si je ne paye pas mon loyer, la porte ne s'ouvre plus, mon dépôt de garantie est saisi, etc. c'est là une simple modalité du contrat. On ne paye plus une amande pour avoir violé la loi, on achète le droit de commettre un acte répréhensible. C'est toute une vision juridique qui se trouve retrempée dans ce paradigme, qui devra être un jour sérieusement discutée.

### 2.6. *Des contrats plus ciselés deviennent possibles*

Avec le contrat intelligent, des sanctions et facturations complexes deviennent possibles. À mesure que les coûts de transaction diminuent, plus l'offre et la demande se trouvent facilement, et plus les contrats se flexibilisent - c'est-à-dire se fragilisent (au moindre concurrent légèrement plus efficient, on change de fournisseur ou d'employé) ou plutôt, se transforment. À l'échelle individuelle, on travaille un jour pour un employeur, un autre pour un autre: tout est dicté par les conditions pré-spécifiées auxquelles nous avons consenties. En septembre aux vendenges, en hiver au tourisme de montagne. À l'échelle de la défense, les fournisseurs de la BITD (base industrielle et technologique de défense) entreront, sortiront au gré des besoins.

## 3. Blockchains pour la défense : un organe de coordination d'utilisation bien spécifique

> « Many people look blockchains as databases. But blockchain is not about data; it is about coordination » (Arthur Breitman, co-fondateur de Tezos).

On entend dire, à juste titre, de la *blockchain* qu'elle est un organe de coordination. Pour autant, il serait trop simple d'attendre d'elle toutes les solutions aux besoins de coordination. Les applications d'un registre distribué en matière de cyber-résilience suscitent un intérêt compréhensible, bien que pour l'instant, les attentes de la défense semblent reposer sur la magie des mots ("coordination", "cyber-résilience", etc.) plutôt que sur des bases solides. C'est pourquoi, ayant brièvement rappelé dans quelle mesure cet outil de cyber-résilience peut évidemment intéresser la défense, nous ouvrirons une section de discernement général en matière de *blockchain*.

### 3.1. *Un outil de cyber-résilience*

La *blockchain* présente quelques applications évidentes pour la défense :

- Sécurité des communications, par exemple entre plusieurs bases militaires, par un mécanisme de validation horizontal. Sécurisation des systèmes de commande des missiles. [USD 20]
- Gestion des chaînes de distribution par l'utilisation de contrats intelligents, simplification des procédures de validation, d'approvisionnement, de traçabilité.

Mais dans les cas susmentionnés, où se recommande une *blockchain* publique, la défense prend le réseau entier à témoin. Il ne s'agit pas d'une *blockchain* en vase clos.

De façon générale, la *blockchain* est un outil de coordination, appréciable au sein d'un consortium d'entreprises ayant besoin de communiquer et de coordonner leurs opérations en s'appuyant sur un environnement unique facilitant les opérations logistiques, mais également au sein d'une entreprise unique, lorsque les intérêts des participants ne sont pas alignés. Il serait inepte de proposer une *blockchain* hermétique, interne à la défense - où les intérêts sont par définition alignés et où les falsifications volontaires sont déjà contrôlées par les procédures ordinaires - sauf si l'on regarde le registre distribué comme un moyen de prévenir les erreurs de manipulation, auquel cas les contrats

 

intelligents greffés sur la *blockchain* agiraient à la manière d'une "*Multi-party authorization*", non pour se garantir des *hackers*, mais pour s'assurer qu'aucune étape n'a été accidentellement brûlée.

Tout ceci est fort bien, mais c'est encore modeste. Recourir à une *blockchain* publique, déjà existante ou non, ou construire une *blockchain* privée, c'est s'enfermer d'emblée dans un carcan. Un environnement intelligent est un environnement malléable et aussi complexe que nécessaire.

### 3.2. *Discernement général sur l'utilisation d'une* blockchain

Si la technologie de la *blockchain* est recommandée comme outil de communication ultra-fiable, quoique lente, notamment pour commander des exécutions sensibles, elle n'est pas recommandée pour irriguer un tissu d'objets à faible puissance de calcul, même en utilisant d'autres systèmes de validation que la preuve de travail. L'emploi d'une *blockchain* n'est véritablement justifié que dans les cas suivants :

- Besoin d'un archivage fiable (infalsifiabilité des données).
- Besoin de coordination complexe et dans différents états du monde (utilisation de contrats intelligents).
- Besoin d'interopérabilité (d'un environnement permettant de communiquer facilement avec d'autres *blockchain*s).

Le dernier point est un peu à part. Il s'agit d'une simple question technique proposant d'aligner les échanges sur une technologie universelle, à dessein de faciliter l'interopérabilité de diverses institutions qui, si elles n'ont pas directement besoin d'une *blockchain*, ont besoin de communiquer fluidement avec des partenaires[2]. De sorte que, si l'emploi *blockchain* est parfois difficile à justifier dans telle ou telle circonstance, le fait que la *blockchain* offre une standardisation des moyens de communication, d'écriture et de transactions, justifie l'adoption de cette technologie par une entreprise ou une institution soucieuse de communiquer facilement avec d'autres environnements que le sien.

Dans le cas de la défense, on est en droit d'espérer une osmose, non seulement entre couches de *blockchain*s de divers caractères d'intimité, mais aussi avec des *blockchain*s purement civiles, d'un Internet de toutes les *blockchain*s, civiles et militaires. Par exemple, la mise en relation de plusieurs entreprises (*blockchain* de type consortium) préconise une *blockchain* pour tracer l'histoire d'un produit tout au long de sa conception, jusqu'à sa distribution. C'est bien le caractère infalsifiable de la *blockchain* qui est mobilisé ici : l'enregistrement de chaque mouvement facilite considérablement le traitement des litiges - et, en fait, supprime beaucoup de litiges, puisque tout est plus clair.

L'intérêt foncier de la *blockchain* repose donc sur deux piliers, à savoir, son infalsifiabilité, et la possibilité d'organiser la chaîne de commandements ou de commandes sous forme de contrats intelligents - deux avantages lorsqu'il s'agit d'assurer une chaîne fiable de transmission des directives. En revanche, lorsqu'il s'agit d'en user pour mettre en rapport divers composants d'un système intrinsèque, par exemple, une *blockchain* en circuit fermé dans une entreprise, ou pour coordonner des nuées de drones - c'est-à-dire, remplacer la cryptographie par la preuve de travail pour se garantir contre le *hacking* -, c'est bien souvent écraser la mouche avec un tank.

### 3.3. *L'aimant réaligne la limaille*

[SIL 16] attribue à la DGA et la BITD un rôle de gouvernance et de direction économique. Pour emprunter une image à Julien Gracq, l'aimant réaligne la limaille: en orientant la R&D, la défense dirige indirectement des entreprises concurrentes et/ou complémentaires dans des directions semblables, ce qui favorise leurs rencontres, l'harmonisation de leurs techniques - de manière quasi-

[2] Ainsi de même se justifierait l'utilisation des "stable coins", qui constituent à première vue une absurdité, le sens des cryptomonnaies étant, justement, de s'affranchir de la main étatique sur la monnaie.

 

inappréciable, sans doute, et difficile à détecter par l'économétrie, comme il en va des harmonies bien huilées où l'allure du contrefactuel devient inconcevable -. On peut ainsi espérer l'émergence d'une synergie, même tacite, même involontaire, entre plusieurs entreprises qui ne se connaissent pas, issues de plusieurs secteurs d'activité.

De plus, en cas de guerre, la mobilisation du tissu industriel sera immédiate : irriguée déjà par les intérêts nationaux et une mainmise de la défense, la conversion des échanges sur la *blockchain* en effort de guerre sera facile.

### 3.4. *Une cryptomonnaie "battue" par la défense ?*

Si comme le rappelle [FAV 20] la défense est une institution en laquelle les français ont confiance, et si la monnaie est incarnation de confiance, alors comment manquerions-nous de pousser la logique jusqu'à une défense nationale battant sa propre monnaie ?

Une parenthèse peut être ouverte sur la question d'une cryptomonnaie de la défense. Dans une économie libre, l'émission de monnaie est une activité économique à part entière et rien n'interdit à personne de battre sa propre monnaie. Puisque nous nous intéressons ici à la défense, nous pourrions penser que les cryptomonnaies ne nous intéressent pas (sinon par l'utilisation des cryptomonnaies pour conclure des accords secrets, ou pour dépenser des *Bitcoins* saisis par des actions anti-terroristes). Pourtant, une *blockchain* battant sa propre cryptomonnaie n'est pas forcément une sottise. Si l'on songe que cette *blockchain* doit être reliée aux capacités de production industrielle et de R&D, et qu'une partie de cette production est exportée à des clients étrangers, il serait bon sans doute d'envisager ce moyen par lequel l'armée pourrait tracer, contrôler l'utilisation qui sera faite de sa monnaie, et y associer des conditions à l'usage (de même que l'extraterritorialité du droit américain interdit l'usage du dollar dans certaines transactions). Cette cryptomonnaie, plus ou moins attachée à l'euro - ce "plus ou moins" jouant selon nous un rôle de battement qui permettrait à la défense de s'immuniser, et d'immuniser son contrat, contre les actions de la BCE à l'échelle européenne, dont les intérêts ne sont pas forcément alignés avec ceux de la défense - serait un puissant outil de direction économique, diplomatique et stratégique.

En somme, de même que le système de "monnaie tracée" et de contrats intelligents, le concept de nations sur *blockchains* remonte aux origines de la société, dont la confiance était le ciment.

### 3.5. *Si l'on opte pour un système de validation centralisé, quel intérêt d'utiliser une* blockchain *?*

On confond souvent public avec *permissionless* et privé avec *permissioned*, mais [ACH 19] opère entre les *blockchain*s une discrimination plus fine : on peut être à la fois privé et *permissionless* (ex : restriction à l'écriture, lecture publique), ou public et *permissioned* (ex : écriture publique et restrictions à la lecture). Toutes les configurations peuvent être ciselées pour se conformer aux besoins des organismes.

Si tout le monde comprend à peu près l'intérêt d'une *blockchain* publique, celui d'une *blockchain* privée est plus délicat. Pourquoi recourir à une architecture en blocs, si la validation des opérations est députée à un noyau central ? L'infalsifiabilité des données (donc la résistance à la perte, aux mauvaises manipulations et aux *crashs* ...) font de la *blockchain* l'outil de stockage parfait pour des données à la fois sensibles et très peu volumineuses (dont la taille n'est pas très supérieure à celle du *hash*). Le passage à l'échelle demeure un problème, du moins dans le cadre des *blockchain*s publiques, de sorte que le stockage de bases de données sur la *blockchain* ne semble pas possible aujourd'hui. Les données d'un passeport, par exemple, sont déjà trop lourdes si la *blockchain* est à l'échelle du monde.

Or, il n'est pas évident que l'armée doive absolument opter pour une *blockchain* privée, comme on pourrait spontanément le croire. À ce paradoxe bon marché, [FAV 20] objecte que la sécurité est aujourd'hui mieux assurée par les *blockchain*s de type publique et "*permissionless*", à cause du grand

 

nombre de validateurs non concertés, à plus forte raison à mesure que l'anonymat semble de mieux en mieux assuré sur les *blockchain*s publiques. Cette proposition audacieuse et fondamentement juste à notre sens doit toutefois être nuancée de quelques réserves. Premièrement, le risque d'une rebellion ou de l'hostilité d'une large population envers la défense, expose celle-ci au risque, inexistant pour les autres utilisateurs, d'une majorité du réseau décidant de refuser de valider les transactions de l'armée. Deuxièmement, la *blockchain* publique est grevée de difficultés techniques difficilement surmontables. À cause du problème de passage à l'échelle, on n'y dépose que des *hashs* de documents, à des fins, par exemple, de garantie de propriété intellectuelle ou d'authentification, non des données : voilà qui est embarrassant, car nous aurions aimé y stocker des documents cruciaux. Il semble que les recherches en cours sur le découpage des données en un nombre restreint de nœuds ne soient pas encore au point et que ce casse-tête, insoluble sur la *blockchain* publique, appelle tout simplement le passage à un écosystème de *blockchain*s communicantes.

La solution du problème est une affaire de malléabilité. Nous avons besoin d'une *blockchain* évolutive, à plusieurs couches de confidentialité (*side chains*) pour maintenir plusieurs niveaux de dialogue auprès de différents partenaires civils. C'est ce que nous nous proposons d'examiner dans la section suivante.

## 4. La *blockchain* comme catalyseur à l'innovation duale

### 4.1. *À la recherche de ponts. Superposer des environnements. Exporter des structures observées d'un domaine à un autre*

Jadis, la défense était le moteur de l'innovation. Par exemple, les financements militaires français dans le domaine de l'aéronautique ont-ils ruisselé naturellement vers les applications civiles. La recherche militaire coûte cher, et sa valorisation dans des activités civiles était une nécessité économique. Ainsi, [HER 15] mentionne l'importance des exportations pour maintenir l'activité économique des entreprises de défense. Cette nécessité économique ne va pas sans risques stratégiques et montre l'importance, du point de vue de la nation, pour les entreprises de défense d'exercer dans le secteur civil, un débouché où les ventes ne se retournent pas, ou moins, contre la nation.

Aujourd'hui encore, certes, les activités de défense demeurent dans le monde des partenaires essentiels aux entreprises stratégiques. Ainsi le ministère de la défense des USA, qui a financé des recherches pour disposer d'un réseau sécurisé pour ses télécommunications, qui donnèrent Internet, continue t-il de soutenir la *high tech*. La cryptographie, également, un domaine en pleine expansion, au cœur des communications et des questions de stratégie, concerne aussi bien les civils que les militaires.

Mais le temps où la défense était la locomotive de l'innovation est révolu. Loin de prétendre soutenir ou concurrencer les entreprises privées, la défense aujourd'hui s'assoit discrètement sur le côté pour assister au déroulement de l'innovation, comme attrapant les occasions au vol. Comment réamorcer un vraie synergie ?

Bien que la part des brevets mis au secret soit tout-à-fait marginale, il n'est pas inintéressant de mentionner un doublon, significatif, dans la procédure de déclaration d'une invention auprès de la défense. Le candidat au brevet doit, en déposant son invention[3] signaler celle-ci à la défense, alors que l'INPI transmet lui aussi la demande à la défense nationale. Non seulement l'innovation et le "droit préemption" par l'armée, si marginal soit l'exercice de ce droit, sont décoordonnés (l'inventeur propose, l'armée dispose), mais il semble encore que la défense surveille mal l'innovation civile, puisqu'il lui faut prendre deux précautions plutôt qu'une.

[3] Nous parlons bien ici des candidats au brevet ; quid de ceux qui souhaitent tenir leur invention au secret ? il est difficile de trouver des informations sur les devoirs des inventeurs vis-à-vis de la défense, en matière de divulgation et d'exploitation des inventions ne postulant pas à un brevet.

Ce manque de concert appelle une solution plus coordonnée. L'importance serait cruciale, de part et d'autre, civil et militaire, de se trouver facilement, et de façon automatisée, dans un environnement où les outils de cartographie ou de *text mining* peuvent être utilisés : que le secteur civil connaisse les besoins de la défense et, réciproquement, que la défense puisse continûment faire connaître ses besoins aux inventeurs. Il est temps de refonder la trame de l'innovation, afin que la dualité s'y déploie avec le plus d'efficacité, pour que les besoins civils et militaires se trouvent. Nous avons besoin d'un environnement capable de nous suggérer mécaniquement de nouvelles associations technologiques, et d'opérer des ponts entre des domaines. Par exemple, s'il s'agit de lier les graphes de coocurrences technologiques aux graphes de coocurrences de classes scientifiques dans les articles de recherche, alors - moyennant peut-être une agrégation des nœuds du graphe le plus gros, en cas de déséquilibre - on pourra faire coller au mieux la topologie de l'un et de l'autre. Puis, constatant les liens manquants sur l'un, suggéré par les liens sur l'autre, de nouvelles pistes de recherches sont ainsi suggérées. Certes, une *blockchain* n'est a priori pas nécessaire pour cela; mais c'est parce que la *blockchain* implémente des contrats intelligents, eux-mêmes puisant directement dans des bases de données pour adapter leurs stratégies aux évènements du monde, que les *blockchain*s offrent un terrain unifié permettant de mettre aisément en rapport les domaines les uns avec les autres, de constater sur les uns des structures, comme des associations technologiques ou des citations, qu'on pourra tenter d'exporter et appliquer aux autres.

Ce qui achève de plaider pour un environnement plus flexible, où le civil et le militaire ne seraient pas essentiellement séparés, c'est que les contours de la dualité sont eux-mêmes mal délinéés. Lorsque des législations distinguent clairement deux secteurs qui, sur le plan de l'innovation, ne le sont pas, alors s'instaure inévitablement une incitation à contourner la loi, puisque rien n'empêche, techniquement, illégalement, d'enregistrer un brevet dans un autre pays. De plus, le flou des frontières entre les applications civiles et militaires complique la tâche de faire respecter les normes.

### 4.2. *S'appliquer au mouvement du train*

Exploiter les complémentarités, les synergies, par un environnement favorable aux rencontres, c'est, d'un point de vue économique, internaliser des externalités.

De quelles externalités parle t-on au juste ? Des combinaisons d'invention, de l'émulation, de toutes les externalités de découvertes - toute l'affaire de la recherche, qu'elle soit théorique, appliquée, ou, justement, qu'il s'agisse de jeter des ponts entre les deux pans. La question des externalités peut se formuler dans un contexte d'innovation : l'innovation des uns profite aux autres, et tout l'art de la défense pourrait être de jouer le rôle de catalyseur d'externalités en matière d'innovation. Cette machine, qui se place à l'échelle de toutes les externalités susceptibles de s'opérer entre des activités diverses, est donc massive, de taille à se ranger dans la catégorie des "monopoles naturels". L'innovation, par sa nature intrinsèquement multiplicative, peut être regardé comme une vaste économie qui, s'il est vrai qu'on ne peut la planifier, peut être néanmoins orientée de loin, en canalysant des ressources dans certaines directions.

Toute l'affaire de la défense sera donc d'exploiter les externalités en sa faveur et dans le sens de l'intérêt général.

Alors que le monde "s'uberise", c'est-à-dire que l'offre et la demande n'aspirent qu'à se mettre en relation directement, en supprimant les tiers de confiance. C'était l'objectif de la *blockchain*. Cet objectif s'intégrait dans une visée de construction d'une économie parallèle, inaccessible aux gouvenements [BAR 15].

Une réflexion sur l'avenir de la défense s'impose. Celle-ci doit s'appliquer au mouvement et, prenant le courant, tirer profit de l'uberisation du monde et s'intégrer à cette vaste "permaculture". Par la *blockchain*, la défense pourrait de nouveau jouer un rôle central dans l'innovation : innovation par la *blockchain*, et innovation dans la technologie des *blockchain*s.

### 4.3. *Des contrats intelligents pour l'innovation : rencontre de l'offre de la demande*

[MOU 12] indique la difficulté souvent rencontrée, en pratique, pour les distributeurs de remonter le processus de leurs produits - et en 2021, le problème semble demeurer : même dans le cas de la défense, les sous-traitants des entreprises sont mal connus au sein de la BITD. Puisque, selon [CAH 13], 190 000 contrats sont conclus chaque année entre le ministère de la Défense et les PME, on conçoit l'importance de remettre à neuf les mécanismes de traçage. On attend donc de la *blockchain* un environnement offrant une meilleure traçabilité des produits et de poster facilement des appels d'offres pour permettre aux innovations duales de se développer conformément aux besoins de la défense.

Nous l'avons mentionné plus haut : les bases de données, anonymisées ou non, pourront être directement appelées à l'intérieur des programmes de contrats intelligents. Il existe certes déjà le répertoire SANDIE des statistiques annuelles sur la défense. Que l'on imagine désormais qu'au lieu d'importer une base de données sur notre ordinateur, des couches de confidentialité produisent des bases de données plus ou moins fournies, malléables, vivantes pour ainsi dire, et puisées directement, de manière automatisée, à l'intérieur des échanges économiques, assurés par des contrats intelligents.

S'il existe des intérêts purement militaires sans applications civiles, les entreprises exerçant une activité militaire sont généralement duales. Cette dualité est mal prise en compte par la gestion actuelle de l'innovation défense[4], que ce soit d'un point de vue légal ou d'un point de vue commercial. L'inventeur doit premièrement être capable d'estimer la teneur de son invention, de son potentiel défense, ainsi que des intérêts de la défense en général, ce qui est beaucoup lui demander. Cette appréciation (plus ou moins subjective et floue, car certaines inventions sont difficiles à discerner comme intéressant l'armée, de sorte que faire le choix de ne pas breveter son invention présente un risque légal et commercial) suggère que la *blockchain* pourrait être utilisée systématiquement pour que la défense (qui aura un regard même les inventions que les inventeurs souhaiteraient garder secrètes, sans déposer de brevet) valide ou non son intérêt pour l'invention.

La traçabilité offerte par la technologie des *blockchains*[5] - laquelle inclut celle des contrats intelligents et des oracles - offre une garantie de respect des normes, ce qui est particulièrement appréciable dans des pays gangrenés par la corruption. Ici, aucun pot de vin ne peut plus falsifier les données : un produit peut être tracé tout au long de sa chaîne de production et jusqu'à sa distribution dans les commerces au détail. En matière de lutte contre le terrorisme, le recours au *text mining* et autres outils de l'intelligence artificielle recommandent la mise à disposition du secteur civil des bases de données, afin que ces entreprises ne puissent se mettre accidentellement en rapport avec des clients terroristes : les services anti-terroristes, branchés sur la même toile, pourront interrompre les transactions. Les services de compliance auront tout à gagner de cette toile. L'environnement de la *blockchain* est propice à l'intégration des outils d'intelligence artificielle. Un rapport de la commission européenne [COM 21] enveloppe les deux outils, IA et *blockchain*, dans un seul cadre : les deux sont appelés à se développer conjointement. Les outils intelligents seraient de grand secours, par exemple, pour détecter les ventes massives de produits à double usage disséminés en plusieurs petites ventes à des hommes de paille dispersés. Une simple analyse de flux dans les réseaux suffit à tirer la sonnette - et tout est plus simple lorsqu'un environnement unique permet de découvrir ce qu'on ne cherchait pas.

Tout le monde gagnerait à cette meilleure coordination. Seul un environnement où toutes les données communiquent permet un telle fluidité, et d'agir en temps réel pour contrer en amont de telles transactions. Meilleure coordination dit moins de mauvaises surprises (ventes bloquées), moins de blocage bureaucratique, des collaborateurs qui se trouvent plus facilement …

[4] Pour une étude sur la dualité, et notamment de la distinction entre dualité et biens à double usage (le premier relevant de l'industrie, le second étant une notion juridique, relative à l'usage qu'on en fait), voir [MEU 16].

[5] La *blockchain* semble descendre des EDI (Echange de Données Informatisées) qui permettaient déjà, en traçant les flux logistiques de matières, de gérer les productions en flux tendus.

 

### 4.4. *Catégorisation automatique des données*

Si aujourd'hui la recherche en économie de l'innovation tourne déjà son regard, même si ces outils demandent à être perfectionnés, vers une topologie des brevets sur la base de leur contenu sémantique [LEB 21], cette pratique pourrait se généraliser pour rechercher des clients, fournisseurs, ou bien pour connaitre, tant dans le domaine de l'industrie que de celui de la recherche scientifique, quels sont les problèmes ouverts (l'industrie et la science communiquant par surcroît par l'intermédiaire de la *blockchain*).

Un argument fort veut qu'une classification *ex ante* se cuirasse contre les artefacts auxquels les approches de type boîte-noire sont exposés. Les régularités statistiques ne sont pas forcément significatives (c'est toute la différence entre une approche par variables spécifiées, et une analyse en composantes principales) et, bien que les derniers algorithmes de réseaux de neurones semblent étonnamment capables de conceptualiser les objets qu'on leur fait apprendre, on peut à juste titre émettre un avis mitigé, ou s'inquiéter d'une approche boîte noire de l'invention. C'est dans cette veine également que [MIS 21] s'inquiète d'un traitement automatisé des *Big Data*.

En sens contraire, si vraiment dualité il y a, et ruissellement d'un secteur sur un autre, alors n'est t-il pas ridicule et inefficace de scléroser les inventions dans ces catégories ?

Cette objection, il est vrai, demeure suspecte de par sa coloration nominaliste. La querelle des universaux, rempaillage de l'antique querelle de l'existence des formes, semble avoir trouvé dans une épistémologie économique étroite un troisième et bien faible souffle. À en croire les partisants, cette voiture-là, de cette marque, diffèrerait essentiellement d'une autre voiture, celle-là, d'une autre marque. Amalgamer deux marques de voitures sous l'étiquette de "voiture", c'est déjà agir en planificateur central, c'est déjà préjuger de la fonction d'utilité d'autrui.

Si le bon sens verse en sens contraire, la position nominaliste n'est toutefois pas dénuée d'une certaine vérité. Si un four est un four, une voiture une voiture, et un parapluie le même parapluie, qu'il pleuve ou que le soleil brille, la complexification des inventions invite cependant à plus de prudence et moins de dénigrement du nominalisme. Cette objection contre le rassemblement des objets sous l'ombre de classes d'équivalences peut sembler ridicule de prime abord, mais quand l'économie se complexifie, elle remet sérieusement sur la table la querelle des universaux, enfin du sens qu'il se trouve à définir telle classe d'équivalence, tel macro-état "voiture" rassemblant sous son aile les multiples micro-états que sont les marques. Sans doute en va t-il de même de l'invention : elle consiste à assembler des technologies inattendues, à distinguer ce qui paraissait identique, à identifier ce qui n'en laissait rien paraître.

Nous entendons donc que la *blockchain* permette à l'invention de s'automatiser dans une certaine mesure. Une approche "boîte noire" des classifications de brevets n'est certainement pas à dédaigner. Cela peut se faire par analyse en composantes principales - ces axes malléables et digérées par l'évolution technologique jouant le rôle de classes de plus en plus fines - ou par des procédés d'intelligence artificielle (ex : proximité sémantique, comme évoqué plus haut) ou par une proximité calculée par l'usage (on constate que tel ou tel brevet sont souvent utilisés conjointement: pourquoi ne pas les mettres dans une même classe ? et pourquoi un brevet ne pourrait-il pas appartenir à plusieurs classes à la fois ?). Certaines associations technologiques suggérées pourraient alors diriger la recherche dans des directions que l'on ne soupçonnait pas forcément. Il existe déjà une classification flexible des brevets: la structure de classification inter-brevets CIB, dont la nomenclature est stable, s'oppose à la nomenclature CCB, nomenclature "pépinière" (où se doivent guetter les "vraies" inventions, les bonds en avant inaccessibles aux modèles linéaires). Lorsque les inventions deviennent assez standard et largement utilisées, elles peuvent se figer dans la nomenclature stabilisée. Ce processus d'ankylose, ou de sédimentation, est tout-à-fait celui des *blockchain*s; mais paradoxalement peut-être, la *blockchain* peut se renouveler sans cesse par ses nouveaux blocs. L'ankylose des blocs passés - c'est-à-dire la fiabilité des données - est la condition de la flexibilité de ce monde de sociétés

 

qui se fonde sur elle. On songe alors à des bases de données qui, même achevées, pourraient encore s'ordonner selon des catégories flexibles, digérées dans l'architecture par les besoins actuels en inventions. C'est parce que les anciens blocs se sclérosent, qu'en contrepartie le monde des *blockchain*s peut être aussi souple.

Ainsi s'intègre, non seulement le brevet à la *blockchain*, mais aussi l'utilisation elle-même qui en sera faite. Poussant cette logique à son terme, des oracles puisent directement dans les bases de données les conditions des contrats intelligents. De même que l'art rupestre de la préhistoire exploitait les accidents du support pour les intégrer au dessin, de même une exploitation en profondeur de la *blockchain* doit jouer sur une sémantique conforme à la *blockchain*, un fond et une forme qui tendent à s'harmoniser, afin d'exploiter au mieux, en s'appliquant à ses mécanismes les plus élémentaires, toutes les potentialités de la *blockchain*.

### 4.5. *Accès gratuit à la cartographie des brevets comme incitation à s'inscrire sur la* blockchain

Nous nous sommes prononcés en faveur d'un environnement où la défense prendrait aisément connaissance des activités civiles, et pourrait ouvrir auprès des entreprises des contrats intelligents. Il faut encore que les entreprises aient une incitation solide à venir sur la *blockchain*, même celles qui ne proposent pas d'applications militaires, que les mailles du tissu industriel soit plus serrées, que les entreprises se trouveraient mieux, bref, que lier les rayons de la roue au moyeu les rapproche les uns des autres. La défense orienterait, infléchirait la R&D dans une telle ou telle direction (tout en gardant présent qu'une intervention trop invasive tuerait la sérendipité). Synchronisant les activités sans être directive, la défense agirait comme le moyeu, inclinant la recherche autour des intérêts nationaux par un système d'appels d'offre sous forme de contrats intelligents.

La publication en *open source* de la cartographie des brevets [CAI 21], véritable "Google Earth" de l'invention, serait "*Pareto-improving*". Selon Frédéric Caillaud, 80% des connaissances techniques sont contenues dans les bases brevets. Selon ce directeur de l'innovation à l'INPI, les bases brevets permettent de : (i) surveiller et détecter ses concurrents; (ii) prévoir ce qui se passera à l'avenir, détecter les tendances de développement dans le secteur où l'on est impliqué; (iii) détecter des concurrents potentiels et de notre liberté d'exploitation; (iv) détecter des opportunités technologiques. Mais surtout, elle serait utile à la défense, qui posterait sur cette carte les brevets virtuels correspondants à ses besoins, lesquels déclencheraient automatiquement des contrats entre la défense et l'innovateur.

Cette cartographie, qui repose aujourd'hui sur une proximité sémantique des brevets[6], constitue une approche futée pour contourner l'obstacle des non-citations volontaires de technologies. De ces grappes de brevets, de ce "vaste jeu de go" [CAI 21], les dépositaires de brevets tendent à émerger de cette géographie : ainsi qu'il en va de tout bon algorithme de *text mining*, comme ceux de reconnaissance d'images qui parviennent à "trouver eux-mêmes" le concept de roue, ou d'une analyse en composantes principales qui tend à manifester des variables interprétables, ainsi la cartographie des brevets trouve elle-même les grands groupes d'innovations, dont les brevets apparaissent par grappes éparses sur la carte[7].

[6] « [...] nous avons eu recours à la base de donnée DWPI (Derwent World Patent Index). [...] le résumé de chaque nouveau brevet est réécrit et traduit en anglais par un des cinq cents experts de Clarivate Analytics de façon à lui donner du sens, de le classer sur la base d'une ontologie et d'un vocabulaire prédéfini. [...] Chaque nouveau brevet est analysé afin de le rattacher comme nouveau membre à une famille existante si l'invention est déjà protégée ou, dans le cas contraire, devient le brevet de priorité d'une nouvelle famille. Une famille DWPI correspond à une invention » [CAI 21].

[7] C'est sans doute encore un sophisme que d'énoncer que, un brevet étant par définition original, on voit mal comment l'intelligence artificiel pourrait le reconnaître. Mais puisque l'homme est capable de reconnaître son ignorance tout en détectant du sens, sans doute sera-t-il possible de déléguer la validation des brevets à l'intelligence artificielle. Cela étant, un homme devra toujours rester dans la boucle. Comme le remarque Didier Lebert, il existe tout un art littéraire de la rédaction de brevets, consistant à le rédiger juste assez

 

Une analyse boîte-noire des brevets, suggérant des associations de technologies disparates apparemment étrangères les unes aux autres, semble désapprouver une classification figée des brevets, pour les raisons évoquées plus haut. De même que les modèles génératifs de *deep learning* peuvent remonter à contre-courant, non pour reconnaître des images mais pour en produire, de même avons-nous besoin d'un environnement où les données de protection intellectuelle peuvent être utilisées pour suggérer de nouvelles associations de brevets.

Tout invention est alors déclarée sur la *blockchain* et devient visible si la demande de brevet est acceptée. Les entreprises utiliseraient cette gigantesque base de données pour découvrir de nouvelles associations technologiques. Ici, les outils restent à construire. Nous avons, pour notre part, dans [POI 21], proposé un outil d'inférence par maximal de coordination qui pourrait, exporté dans le contexte des bases de données brevets et technologiques, fournir un procédé exploratoire propice à suggérer des "associations naturelles de technologies", c'est-à-dire - si l'on regarde un brevet comme un assemblable (original) de technologies - de nouveaux brevets. L'utilisation du principe de coordination maximal se place dans la droite ligne des techniques d'analyse des associations de technologies en termes de cohérence [ANS 57].

### 4.6. *De quoi l'avenir sera fait*

[FAU 21] distingue trois types de diffusion technologique, que nous pourrions qualifier en ces termes :

- Le phénomène d'amplification ("1 puis 10 puis 100"), où la technologie enfle exponentiellement ; on pense bien sûr au numérique.
- Le phénomène cumulatif ("A, puis AB, puis ABCDE") où les technologies s'amassent dans le silo à connaissances.
- Le phénomène "A, puis AB, puis ACDE" que nous appellerons bond du cavalier d'échecs, pour emprunter une expression de Claude Lévi-Strauss, à laquelle aussi bien Jared Diamond aurait pu recourir pour illustrer ses pages sur l'écriture, montrant comme certaines inventions "prennent" et d'autres meurent.

La dernière classe est plus subtile. Ces "procédés combinatoires non cumulatifs" se passent le relais. Sont-ils oubliés pour autant ? Lors même qu'on n'utiliserait plus le papier et le crayon, ils auraient tout de même servi à concevoir l'informatique : un produit fini passe dans les produits intermédiaires, et sa trace demeure à jamais, invisible.

Cette classification, toutefois, suppose une certaine continuité de l'innovation, même dans le cas de l'amplification. Les discontinuités, les révolutions échappent à toute classification. Si pour les entreprises "normales" l'approche brevet permet d'orienter la recherche technologiques par petits bonds adaptés à leurs besoins, la défense, elle, pense sur le long terme et ne se contente pas d'améliorations à la marge : la sûreté du pays dépend des grands bonds, qu'il ne faut pas laisser passer.

### 4.7. Wanted *: exploration d'une zone de la carte des inventions*

Lorsque les technologies sont en symbiose, il faut imaginer un système de coordination, une sorte de lieu intelligent qui favoriserait leurs rencontres. Il s'agirait de centraliser les informations et orienter leur synchronisation autour des intérêts nationaux, par un système d'appels d'offre, de bonus pour l'utilisation de telle ou telle association de briques technologiques ... En synchronisant les activités, non seulement horizontalement (la *blockchain* comme lieu de rencontre) mais aussi verticalement, la défense donnerait le diapason de la recherche en l'inclinant autour des intérêts nationaux.

---

précisément pour se conformer à l'exigence de réplicabilité, mais avec assez d'obscurité toutefois pour brouiller nos traces. Il n'y aura jamais de solution satisfaisante pour rendre justice de chaque invention par rapport aux autres : toujours quelque critère devra s'appliquer pour décider des degrés de paternités entre brevets.

Aujourd'hui, l'Etat fait déjà appel à des entreprises privées, formule des appels d'offres publics, régis par le code du marché public. Il ne s'agit pas, en "blockchénisant" les contrats défenses avec les industriels, de bouleverser la toile fragile des contrats confidentiels, mais au contraire d'offrir une articulation plus souple entre plusieurs petits comités, sélectionnés par la défense, à qui la défense a donné droit de répondre à l'appel d'offre, comme c'est déjà le cas, et à qui elle fera connaître ses besoins plus précisément qu'aux autres. Ici, les outils traditionnels de l'économie (par exemple l'algorithme de Gale-Shapley [GAL 62]) pourront être plus facilement implémentés, pour ordonner les fournisseurs et clients par ordre de préférences, qui passeront progressivement les différentes couches de confidentialité au fil des contrats.

### 4.8. *Remplacement/complétion du monopole que confère le brevet par un système de dédommagement ?*

Une capillarité entre les deux mondes, civil et militaire, ne peut prendre corps que dans un environnement prenant en compte les externalités de R&D et des productions industrielles. Les contrats intelligents pourraient-il offrir une valorisation alternative, du moins complémentaire au brevet ?

Remarquons tout de même que, les *blockchain*s étant infalsifiables, elles semblent en fait déjà offrir par elles-mêmes, potentiellement, une alternative au brevet, par un système de rétribution qui remplacerait le monopole. Le graphe de citations évoqué à la sous-section précédente, dont les flux de rétributions seront calculés sur le modèle d'une centralité des citations, relèveraient d'une obligation légale, à laquelle toutefois il faudra ajouter des mécanismes incitatifs pour inviter positivement les inventeurs à citer leurs sources.

Il ne serait pas inopportun de profiter des bases de données brevets pour implémenter, par ce système de rétribution, de permettre à la défense d'agir concrètement comme une vaste main orientant de loin la recherche dans la direction de ses besoins. Ces "contrats intelligents ouverts", cette pose de brevets virtuels, se présentent sous la forme de simples ensembles au sens mathématique du terme, d'associations de techologies "pressenties" pour répondre à un certain besoin pratique, ce qui serait d'autant plus pratique que ces technologies pressenties seraient flexibles, partiellement automatisées, comme nous l'avons dit plus haut, par une approche boîte-noire et malléable de la classification des brevets.

Ces brevets virtuels "remplis" seraient plus ou moins rétribués, accompagnés ou non d'un engagement de la part de la défense envers tel ou tel inventeur proposant telle ou telle solution. Outre la flexibilisation du monde de l'innovation - aujourd'hui soumis à des jeux assez pervers de préemption et de dépôts massifs de brevets pour contrôler des zones entières de la carte - permettrait en outre d'articuler la valorisation de la propriété intellectuelle (si je valorise mon invention, je rémunère le propriétaire du brevet que je cite) avec des contrats intelligents (je peux allier ces rémunérations légales à des arrangements avec mes clients, concurrents, etc.). Cette souplesse, ce rapprochement de la propriété intellectuelle et des arrangements financiers entre les entreprises, offre un cadre évidemment plus propice à l'innovation que les jeux de monopoles.

Toutes les transactions commerciales se feraient sur la *blockchain* et, redisons-le, un seul environnement enveloppera des activités variées : recherche scientifique, invention, innovation, valorisation et échanges commerciaux, statistiques, etc. ce, afin de faire apparaître les synergies et de leur offrir un lieu d'échanges où elles pourront respirer librement.

### 4.9. *Sur les diverses manières de valoriser la propriété intellectuelle. Comment la défense peut orienter la recherche*

Des systèmes de citations de brevets, de calcul de centralité (mettons de côté la difficile question des incitations et des biais de citations, et supposons pour faire simple que les citations sont rapportées honnêtement) offrent un cadre plus riche aux stratégies de valorisation intellectuelles, moins arbitraires

 

et moins viciées que le monopole. Les rétributions pouvant être alors alors commise à des entreprises privées très semblablement à des systèmes d'assurances, qui produiraient pour l'inventeur des modèles de contrats à soumettre à ses clients, l'inventeur étant lui-même soumis aux conditions des inventeurs qu'il cite, etc. La valorisation de l'invention, fluctuante, sera fixée par ce maillage, et la valorisation intellectuelle serait entièrement dictée par l'offre et la demande pour l'utilisation des inventions en question. Ainsi, une forte centralité d'invention serait inutile sans application industrielle (d'où viendrait l'argent ?). La centralité des inventions agirait donc comme une charge, mais l'innovation seule, c'est-à-dire l'utilisation de l'invention, déverserait des capitaux de l'industrie vers les inventeurs. L'invention serait rétribuée à la mesure de l'innovation - toujours en recourant à des contrats intelligents - qui citerait les brevets qu'elle utilise. Par exemple, si mon brevet F cite le brevet E, qui cite les brevets C, D qui eux-mêmes citent les brevets A, B, et si une entreprise utilise mon invention, alors elle me rétribue automatiquement, et une partie de mes bénéfices sera reversée aux détenteurs de chacun de ces brevets antérieurs, proportionnellement à la centralité des noeuds du graphe de citations inter-brevets[8], dans l'esprit d'un indice de Katz, Bonacich ou PageRank[9]. Une autre approche, plus simple, consiste à appliquer la formule $\mathbf{x}'=G\mathbf{x}$, où $\mathbf{x}$ est le vecteur des utilisations de chaque brevet par les industries (calculées d'une manière que nous ignorons), et $G=(g_{ij})$ la matrice des citations, avec $g_{ij}$ la part qu'occupe le brevet i dans le brevet j, avec $\sum_i g_{ij}=1$, et $\mathbf{x}'$ le vecteur corrigé par les citations inter-brevets.

C'est alors qu'on peut imaginer un système de rétributions/subventions par citations, qui serait géré par la défense. Celle-ci peut y ajouter des "biais de subventions", des appels d'offres sous forme de contrats intelligents qui signifieraient: "Si quelqu'un trouve une solution technologique à ce problème, nous lui offrons telle récompense / tel contrat de production...". La défense pourrait même biaiser ce calcul en introduisant des "bonus" pour les inventions regroupant certaines briques technologiques, conformément à ses besoins. Alors, tenant compte des ruissellements d'innovation, la défense pourrait alors utiliser les outils de l'analyse des réseaux pour calculer les rétributions optimales à attacher aux brevets virtuels, ces appels d'offre à l'attention des entreprises aussi bien civiles que militaires, ou déverser carrément et sans contrepartie des subventions dans le monde de l'invention et de l'innovation.

### 4.10. *La* blockchain *au service de l'autonomie stratégique*

La *blockchain* ne pourrait-elle coordonner des projets industriels de dimension européenne ? favoriser la formation de collaboration de l'ampleur de celle d'Airbus dans les domaines stratégiques ? Qui dit autonomie stratégique dit hiérarchie : tout produit peut en définitive entrer dans le domaine stratégique, mais l'affaire est de quantifier cette importance. Quantification d'autant plus délicate que les entreprises sont inter-connectées dans des processus de productions complexes, qui se définissent les uns par les autres, "à la Léontieff", et que la localisation des entrées du processus n'est pas forcément évidente. Ces entrées, que doit détecter une analyse inputs-outputs, définissent à la fois les secteurs où l'investissement sera le plus rentable et les points faibles de l'autonomie de la nation.

Certes, avant de considérer la *blockchain* à l'échelle européenne, il convient premièrement de réaliser à quel point elle simplifierait la gestion de la BITD, mais surtout, que cette gestion doit se comprendre dans une perspective d'autonomie stratégique. Il ne s'agit pas forcément de récréer aujourd'hui une industrie nationale pour tous ces secteurs clefs, mais au moins de savoir comment la créer en cas d'urgence, et de pouvoir le faire rapidement. Il ne s'agit pas de produire des masques quand il n'y a pas de pandémie, mais de savoir qui produit des élastiques, qui produit du textile de tissage serré. Idem pour les produits à usage militaires - et de trouver des débouchés civils à ces inputs

[8] Qui est en fait un hypergraphe, puisqu'un brevet peut être regardé comme un assemblage de briques technologiques. Voir [BUS 14]; [TUD 21] pour les questions de centralité (et donc l'agrégation des citations inter-brevets) dans les hypergraphes.

[9] Puisque la *blockchain* garde trace de l'état du monde à chaque bloc, il est aisé, en cas de fraude (non citation de brevets) ou d'oublis, de recalculer les montants dus, en remontant la *blockchain* à l'époque où le lien aurait dû être opéré.

 

en questions, en temps de paix. Ce que nous disions plus haut des brevets virtuels, exprimés comme union de briques technologiques, vaut ici pour les produits militaires ou d'importance vitale tels que les outils pour faire face à des pandémies, toujours menaçantes dans un monde dont on fait le tour en quelques heures.

## 5. Conclusion

C'est à une échelle concrète que la *blockchain* offre à la défense de bâtir un environnement où l'innovation serait non seulement enregistrée (bases de données brevets sur la *blockchain*) mais aussi exploitée, parce que des contrats intelligents interagiraient directement avec ces bases de données brevets. La défense et le civil se retrouveraient ici et passeraient leurs contrats sur un environnement toujours en mouvement, où tout va plus vite, où tout est plus fluide. Ici, on enregistre, on pose des appels d'offres, on signe, on déclenche une collaboration, on fait des transactions, tout ça au même endroit. Et bien sûr, en cas de conflit, la défense pourra instantanément mobiliser le tissu industriel.

La mise en place d'une *blockchain* tenue par la défense - qui délivrerait les droits de lecture et d'écriture à chaque niveau d'intimité - devrait présenter selon nous les caractéristiques suivantes :

- Plusieurs niveaux de confidentialité sur la *blockchain*. Il convient en effet que l'armée ne fasse pas connaître ses besoins ni ses faiblesses au monde entier. Ces niveaux ne sont d'ailleurs pas forcément comparables ; il s'agirait d'un ensemble partiellement ordonné de niveaux d'intimité, plutôt que d'une pyramide : ce qui est découvert à certains civils ne l'est pas forcément à d'autres, et réciproquement.
- La *blockchain* serait à entendre au pluriel. Il s'agit d'un environnement de *blockchain*s communicantes, elles-mêmes en communication avec le monde des *blockchain*s civiles : un vaste assemblage de *side-chains* interagissant les unes avec les autres. La frontière entre l'environnement-*blockchain* de la défense et les *blockchain*s civiles existantes serait d'ailleurs assez floue. Dans la part publique de cette *blockchain*, la validation des blocs est assurée par une preuve par l'enjeu. Les mineurs en questions (ou "boulangers" si l'on reprend le terme de *Tezos*) sont rémunérés par les émetteurs des contrats pour leur travail de boulange ; il convient en effet, à ce niveau où plusieurs entreprises civiles sont en compétition, et où les intérêts ne sont pas forcément alignés, que la *blockchain* soit la plus conforme possible aux mécanismes du marché. Dans ses parties les plus privées, la validation des opérations serait dévolue à la défense nationale (le choix du processus de validation s'impose généralement de lui-même. Celui que nous avons proposé peut être discuté. À l'heure où l'on voit - *Ethereum* 2.0 - la preuve d'enjeu se substituer à la preuve de travail, et considérant que la preuve de travail et beaucoup trop horizontale pour se proposer sérieusement à la défense - une bureaucratie inefficace ne ressemble-t-elle pas à une preuve de travail ? -, il est évident que ce point demandera une réflexion particulièrement approfondie).
- L'entrée sur la partie publique de la *blockchain* donnerait accès à la cartographie des brevets.
- Pour manifester ses besoins, la défense peut dessiner des brevets virtuels, construits sous la forme d'ensembles de briques technologiques, éventuellement associées d'un carnet des charges et d'une rémunération des entreprises proposant une telle solution technologique. Si cette invention possède des applications civiles, la défense pourra, à titre incitatif, surévaluer la rémunération des inventeurs existants ou virtuels (appels d'offres) pour tirer la couverture dans sa direction. Ces brevets virtuels sont associés à des contrats intelligents, déclenchant une collaboration avec l'inventeur dont le brevet a été validé par les organes de propriété intellectuelle (lesquels devront rétroactivement être partiellement contrôlés par la défense, pour éviter des jeux de blocage qui la paralyseraient).

Ce système de *blockchain* nationale gérée par l'armée présenterait les avantages suivants :

- Elle constitue un outil de centralisation qui bénéficierait même au civil, dans la mesure où elle offrirait une plateforme de contrats intelligents où les entreprises civiles, duales et militaires pourraient coordonner leurs activités. D'un point de vue industriel, cette *blockchain* n'est pas même compromis entre le libre-échange et les intérêts de la défense nationale : ce serait un outil de coordination dont tout le monde bénéficierait.
- Un avantage stratégique. Dans un contexte de hauts risques liés au terrorisme, il importe que l'armée puisse s'adapter rapidement à des situations d'urgence et mobiliser les entreprises clefs pour la défense nationale. Ce qui était initialement une base de données brevets / contrats avec la défense, peut être rapidement converti en opération militaire (ici on retrouve l'idée de la base de données immédiatement mobilisable, on l'on pioche directement, sans besoin de construire une base de données intermédiaires, appliquée aux intérêts de sécurité nationale).

Pour ce qui est de la défense orientant l'innovation par l'ouverture de brevets virtuels (attachés à des contrats intelligents) et, éventuellement, des subventions, ce système de moyeu est-il grevé de biais et de vices ? Est-il souhaitable, sur le plus strict plan de l'innovation ? Cette question, bien sûr, demandera à être minutieusement discutée.

Il sera sans doute possible, un jour, lorsque les *blockchain*s seront plus découpées, de stocker des bases de données sur la *blockchain* et de les exploiter ; c'est dans ce domaine, soit dit en passant, que la défense pourrait redevenir *leader* de l'innovation. En proposant une *blockchain* à la mesure de ses besoins complexes, elle boosterait la recherche sur des *side chains* plus ou moins communicantes, selon les externalités engagées.

## Remerciements

Je dois aux discussions avec Didier Lebert et Richard Le Goff un grand nombre conseils, orientations et idées décisive qui ont bien plus qu'étoffé cet article. Mes remerciements vont à toute l'équipe de l'UEA pour ses retours et critiques, indications. Je remercie Demelza Hays pour plusieurs conversations sur les *blockchain* dont j'ai tiré ici une partie de la matière. Je dois Teona Melitauri plusieurs perspectives juridiques de la *blockchain*, dans la Section 2 sur les contrats intelligents et dans la conclusion. Je suis redevable à l'Agence Innovation de Défense, AID-2020-65-0057 pour son soutien dans le cadre du projet FireBall. Je remercie enfin Dorgylès Kouakou, dont les recherches sur l'autonomie stratégique apportent un éclairage important sur les questions de coordination qui nous intéressent dans le cadre de ce projet.

## Bibliographie

[ACH 19] ACHARYA V., YERRAPATI A.E., PRAKASH N., *Oracle blockchain services quick start guide*, 2019.

[ANS 57] ANSOFF H.I., « Strategies for diversification », *Harvard Business Review*, p. 113-124, 1957.

[BAR 15] BARON J., O'MAHONY A., MANHEIM D., DION-SCHWARZ C., *National security implications of virtual currency: examining the potential for non-state actor deployment*, Rand Corporation, 2015.

[BAS 19] BASHIR I., *Mastering blockchains*, third edition, 2020.

[BUS 14] BUSSENIERS E., *General centrality in a hypergraph*, 2014.

[BUT 13] BUTERIN V., *Ethereum whitepaper*, 2013.

[CAH 13] CAHUZAC-SOAVE O., DE MAUPEOU M., *PME et marchés de défense en France : le SIA Lab, une initiative au service de l'accès des PME aux marchés de la défense*, 2013.

[CAI 21] CAILLAUD F., STERNBERGER C., « La carte d'état-major des inventions brevetées : un avantage concurrentiel majeur pour innover », *Technologie et Innovation*, vol. 6, n° 2, 2021.

[COM 21] EUROPEAN COMMISSION, *Artificial intelligence, blockchain and the future of Europe: how disruptive technologies create opportunities for a green and digital economy*, Main report, 2021.

 

[DEB 63] DEBREU G., SCARF H, « A limit theorem in the core of an economy », *International Economic Review*, vol. 4, n° 3, 1963.

[FAU 21] FAUCONNET C., « Les graphes de cooccurrences technologiques pour l'analyse de l'innovation », *Technologie et Innovation*, vol. 6, n° 2, 2021.

[FAV 20] FAVIER J., FONTANA E., « La *blockchain*, au service de la sécurité », *RES Militaris – Revue Européenne d'Etudes Militaires - European Journal of Military Studies*, vol. 10, n° 1, 2020.

[GAL 62] GALE D., SHAPLEY L.S., « College admissions and the stability of marriage », *American MathematicalMonthly*, vol. 69, p. 9-14, 1962.

[GOO 14] GOODMAN L.M., *Tezos, a self-amending crypto-ledger*, white paper, 2014.

[HER 15] HERAULT P., « La base industrielle et technologique de défense à l'âge de la globalisation », *Revue Défense Nationale*, n° 784, p. 95-100, 2015.

[KAT 85] KATZ M., SHAPIRO C., « Network externalities, competition, and compatibility », *The American Economic Review*, vol. 75, 1985

[KAT 86] KATZ M., SHAPIRO C., « Technology adoption in the presence of network externalities », *Journal of Political Economy*, 1986

[LEB 21] LEBERT D., « Les apports des techniques structurales à l'analyse des processus d'innovation : une introduction », *Technologie et Innovation*, vol. 6, n° 2, 2021.

[MEU 16] MEUNIER F.-X., *Innovation technologique duale : une analyse en termes d'influences et de cohérence*, Thèse de doctorat, Université Paris 1 Panthéon-Sorbonne, 2016.

[MOU 12] MOURA S., « La base industrielle et technologique de défense : identification et caractéristique », *Ecodef : Le Bulletin de l'Observatoire Economique de la Défense*, n° 58, 2012.

[NAK 08] NAKAMOTO S., *Bitcoin: a peer-to-peer electronic cash system*, 2008.

[POI 21] POINDRON A., *The maximal coordination principle*, 2021.

[MIS 21] MIS J.-M, *Pour un usage responsable et acceptable par la société des technologies de sécurité*, Rapport au Premier ministre, vol. 1, 2021

[ROH 17] ROHLFS J., « A theory of interdependent demand for a communications service », *The Bell Journal of Economics and Management Science*, 1974

[SIL 16] CORREA SILVA R., *Défense et dynamiques industrielles : la restructuration de l'industrie de défense brésilienne*, Master professionnel, 2016.

[SZA 16] SZABO N., *Smart contracts: 12 use cases for business and beyond: a technology, legal and regulatory introduction*, 2016.

[TUD 21] TUDISCO F., HIGHAM D. J., *Node and edge eigenvector centrality for hypergraphs*, 2021.

[USD 20] U.S DEPARTMENT OF DEFENSE, *Potential uses of blockchain*, 2020.

[ZUP 20] ZUPAN N., KASINATHAN P., CUELLAR J., SAUER M., « Secure smart contract generation based on petrinets », *Blockchain Technology for Industry 4.0*, pages 73–98, 2020.

 