Note n°07/24

4 mars 2024

Nathalie Devillier

Chercheuse associée, Fondation pour la recherche stratégique

FONDATION *pour la* RECHERCHE STRATÉGIQUE

Les enjeux de la technologie de la blockchain pour la cyberdéfense française

La technologie blockchain (chaîne de blocs) est une base de données distribuée et décentralisée : une technologie de stockage et de transmission des informations qui y sont codées, sans organe central de contrôle. Or, la capacité des forces armées à l'emporter dans un environnement hautement contesté est de plus en plus dictée par son aptitude à défendre les systèmes d'information et les données qu'ils contiennent contre la compromission et la manipulation. Dans le top dix des menaces identifiées par l'agence de l'Union européenne (UE) de la cybersécurité figurent d'ailleurs la compromission de la chaîne d'approvisionnement, les campagnes avancées de désinformation, les attaques ciblées *via* les données des appareils connectés (Internet des objets) et l'utilisation de l'intelligence artificielle (IA)[1].

Face à une cybermenace en croissance, un modèle entièrement nouveau de stratégie de cyberdéfense pourrait émerger avec les blockchains et repose sur son caractère immuable, l'automatisation, l'auditabilité des blocs, la décentralisation et sa sécurité. En effet, la technologie blockchain est sécurisée en transparence et repose sur une structure de données cryptographiques qui rend la falsification à la fois exceptionnellement difficile et immédiatement évidente[2]. Surtout, les réseaux blockchains sont résilients et résistent notamment aux attaques

[1] L'IA peut être utilisée pour renforcer de nombreuses activités néfastes telles que la création de désinformation et de faux contenus, l'exploitation de biais, la collecte de données biométriques et autres données sensibles, la création automatique de mails d'hameçonnage (ENISA, Artificial intelligence and cybersecurity research, *ENISA Research and Innovation Brief*, 2023, DOI: 10.2824/808362).

[2] La technologie de la blockchain est décentralisée : elle repose sur un très grand nombre d'ordinateurs (nœuds) dans le monde ; les algorithmes de consensus rendent difficile la manipulation du système sans l'approbation de la majorité du réseau et puisque toutes les transactions sont cryptographiquement liées entre elles, toute modification d'une transaction entraînerait une modification de la chaîne entière, ce qui serait immédiatement détecté.

par déni de service[3]. Il est indiscutable que les ipséités de la blockchain en font un atout face à la « *fragilité native du numérique* »[4], notamment pour renforcer la défense et la cyberdéfense militaire.
Cette technologie est souvent qualifiée de disruptive car elle est un élément fondamental du web 3.0 et ouvre des possibilités bien au-delà des monnaies virtuelles (Bitcoin, Ethereum…), des créations artistiques (jetons non-fongibles, NFT) ou des contrats intelligents, pour s'étendre à l'identité, à la santé, aux sciences, aux monnaies réelles, aux actifs numériques et à la preuve numérique. Cette technologie révolutionnera-t-elle les affaires militaires aussi dans l'espace ? Contrairement aux idées reçues, le droit ne constitue nullement un obstacle au développement des innovations reposant sur cette technologie, bien au contraire : le cadre juridique de la blockchain contribue à son expansion.

Néanmoins, les blockchains ne sont pas une solution miracle et doivent être utilisées de manière réfléchie et en conjonction avec d'autres mesures de sécurité pour une défense complète contre les menaces cybernétiques. Combinée aux autres technologies émergentes et de rupture[5], la démocratisation des blockchains fait naître des scénarios inconnus de menace cyber.

Renforcer la défense et la cyberdéfense

Les technologies numériques ont transformé les armes, les tactiques et les stratégies militaires. Des essaims ou flottes de milliers de drones (aériens, terrestres, maritimes) seraient capables de se coordonner de manière autonome pour se déployer sur tout un territoire[6]. Les cas d'usage dans le secteur de la défense sont bien connus dans le domaine de la cybersécurité[7] :

- ⇒ Sécurisation des communications militaires en garantissant l'intégrité des messages et en empêchant leur interception ou leur modification non autorisée et renforcement de la sécurité des données de renseignement, autres données sensibles, en garantissant leur intégrité et leur confidentialité ;
- ⇒ Garantir l'authentification des documents militaires tels que les ordres de mission
- ⇒ Garantir la résilience et la sécurité des réseaux et des données des systèmes de commandement militaire[8].

[3] Dinesh Kaluram Choudhary, Shanthi Bhatt, « Blockchain in National Defence », *International Journal for Scientific Research & Development,* vol.6, n° 4, 2018, pp. 1505-1511 ; Bruno Rodrigues, Thomas Bocek, Burkhard Stiller, « Multi-domain DDoS Mitigation Based on Blockchains », *in* Daphne Tuncer, Robert Koch, Rémi Badonnel, Burkhard Stiller (eds.), *Security of Networks and Services in an All-Connected World*, AIMS 17 juin 2017, Lecture Notes in Computer Science [10356], Springer, Cham.
[4] Philippe Dejean, Patrice Sartre, « La cyber-vulnérabilité », *Études*, vol. 7-8, n° 1, 2015, pp. 21-31.
[5] Systèmes généraux d'intelligence artificielle, systèmes autonomes, systèmes hypersoniques, IA génératives, 5G, 6G, technologies quantiques, renforcement humain et biotechnologique.
[6] Appel à projets AMASS (*Autonomous Multi Domain Adaptative Swarm of Swarms*) pour un budget de 78 millions de dollars par la DARPA, www.sam.gov, 30 janvier 2023. Pour une analyse des champs opérationnels possibles en France, voir Pierre Vallée, « Le rôle des drones aériens dans les conflits actuels et futurs », Cahier Armée de l'Air et de l'Espace, *Revue de Défense Nationale,* Hors-série, n° 11, juin 2023, pp. 102-110.
[7] Alessia Cornella, Linda Zamengo, Alexandre Delepierre, Georges Clementz, « Blockchain in defence: a breackthrough? », FINABEL, European Army Interoperability Center, www.finabel.org, septembre 2020 ; Wojciech Mincewicz, « Blockchain technology and national security. The ability to implement a blockchain in the area of national security », *De Securitate Et Defensione. O Bezpieczeństwie I Obronności*, vol. 6, n° 2, 2020, pp. 114-129.
[8] La sécurité est le segment qui compte le plus grand nombre d'acteurs : États-Unis : Boeing, IBM, Galaxy Digital, Microsoft Azure Blockchain ; Chine: 360 Total Security, Alibaba, China Aerospace Corporation (CASC), China Electronics Corporation (CEC), China Information Technology Security Evaluation Center (CNITSEC), Tencent, Zhongan Technology ; Union européenne : Airbus, Distributed Ledger Technology (DLT) Malta, Guardtime, Leonardo, NXTsoft, Thales Group, Vottun ; Russie : Bitfury Group, Kaspersky Lab, National University of Science and Technology « MISiS », RusBITex.

Les déclinaisons de la blockchain à des fins d'optimisation en termes de gestion sont également connues[9] :

⇒ Gestion des chaînes d'approvisionnement militaires pour garantir la traçabilité, la transparence et la sécurité des produits et des pièces de rechange militaires tout au long de leur cycle de vie car l'historique des transactions est visible ainsi que l'identité de l'acheteur. Cela contribue à réduire les risques de contrefaçon et de fraude[10] ;

⇒ Gestion des identités numériques et de l'accès pour les militaires et le personnel de sécurité, garantissant que seules les personnes autorisées ont accès aux ressources sensibles (Guardtime, Digital Bazaar, Waves)[11] ;

⇒ Gestion des actifs militaires : les véhicules, les armes et l'équipement sont convertis en actifs intangibles (« tokens » dans une blockchain), améliorant ainsi l'efficacité de leur utilisation et de leur maintenance ;

⇒ Gestion des contrats et des approvisionnements : les contrats intelligents basés sur la blockchain (« smart contracts ») peuvent automatiser le paiement d'une clause pénale, ce qui réduit les risques de non-respect des accords, donc les litiges et les coûts administratifs (Airbus, R3, Boeing, IBM, Lockheed Martin, Rostec, China Electronics Corporation)[12].

Les caractéristiques de la blockchain en font *a priori* un solide support à des fins de cyberdéfense[13]. Immuable et inviolable, la blockchain stocke les données qui sont cryptographiquement sécurisées et ne peuvent pas être modifiées une fois enregistrées. La gestion sécurisée des identités numériques limite les usurpations d'identité et renforce l'authentification, et en termes de protection des données, les utilisateurs gardent le contrôle de leurs propres données et décident quelles informations ils partagent et avec qui. La collecte, le stockage et le partage sécurisé de renseignements entre les agences gouvernementales et les partenaires de la cyberdéfense améliorent ainsi la coordination et la réponse aux menaces cybernétiques. Néanmoins, l'avènement de l'informatique quantique remet en cause les caractéristiques de la blockchain[14]. En effet, la sécurité des algorithmes cryptographiques d'une blockchain repose sur la difficulté de résoudre certains problèmes mathématiques. Or, les ordinateurs quantiques, en utilisant des principes de la mécanique quantique, pourraient résoudre ces problèmes beaucoup plus rapidement que les ordinateurs classiques. Cela signifie que les signatures numériques actuellement considérées comme sécurisées pourraient être compromises par des attaques quantiques, mettant ainsi en danger les éléments intégrés dans la blockchain.

[9] Ministère des Armées, « La transformation numérique dans l'armée de Terre », www.defense.gouv.fr, 27 septembre 2023. Pour une description des différents types de blockchains (publique, privée ou de consortium) dans ce contexte, voir « La blockchain pour appuyer les projets innovants de l'Armée de Terre – le cas de FIBR2EO », www.archives.defense.gouv.fr, 22 juin 2021.

[10] Jérôme Verny, Ouail Oulmakki, Xavier Cabo, Damien Roussel, « Blockchain & Supply chain: towards an innovative supply chain design », *Projectique*, vol. 2, n° 26, 2020, pp. 115-130.

[11] L'individu a un contrôle total sur son identité numérique : il peut choisir avec qui il partage ses informations et quels aspects de l'identité sont révélés dans différentes situations.

[12] Konstantinos Christidis, Michael Devetsikiotis, « Blockchains and Smart Contracts for the Internet of Things », *IEEE Access*, vol. 4, 2016, pp. 2292-2303.

[13] Dorian Belz, « Blockchain: a cyber defence force multiplier », *Global Security and Intelligence Studies*, vol. 7, n° 1, 2022, pp. 195-201.

[14] Lu Gan, Bakhtiyor Yokubov, « A performance comparison of post-quantum algorithms in blockchain », *The Journal of the British Blockchain Association,* vol. 6, 2023, pp. 1-10.

La décentralisation des blockchains (elles ne sont pas contrôlées par une seule entité) rend plus difficile pour les cybercriminels de cibler une seule source de données ou de compromettre un point central de contrôle. Cette décentralisation rend les blockchains résistantes aux pannes et aux attaques DDoS[15], ce qui garantit une disponibilité continue des données et des services et renforce la résilience des infrastructures.

La transparence de l'enregistrement des transactions (elles sont accessibles à toutes les parties autorisées) permet une meilleure visibilité des activités et aide à détecter les comportements suspects[16]. Le recours au consensus distribué pour valider les transactions (la majorité des participants doivent être d'accord pour qu'une transaction soit acceptée) réduit le risque de transactions malveillantes. La blockchain peut être utilisée en complément des SIEM car elle apporte immutabilité, traçabilité et contrats intelligents alors que les SIEM se concentrent sur la collecte, l'analyse et la réponse aux événements de sécurité. Combinées, ces technologies offrent une approche robuste pour la sécurité de l'information.

La blockchain et la militarisation de l'espace : nouveau paradigme des affaires militaires ?

A priori, la blockchain ne révolutionne pas les affaires militaires, elle est un moyen de les sécuriser et de renforcer leur efficacité. Elle sera une révolution si elle mène à des avancées ou des nouveautés qui lui sont propres et si elle est mise en œuvre dans tous les secteurs de la défense. Qu'en est-il dans le domaine spatial ?

Au-delà du *New Space*, des ressources spatiales sont tokenisées dans une blockchain par des entreprises privées : satellites, orbites, appareils, débris spatiaux, astéroïdes et autres objets peuvent être intégrés à une blockchain[17]. Les satellites peuvent être utilisés comme nœuds de la chaîne – soit en tant que nœuds participants qui stockent les données, soit en tant que nœuds de validation qui valident et ajoutent des données. Cela signifie que les réseaux satellites peuvent être utilisés comme infrastructure où stocker des données et à travers laquelle effectuer des transactions.

Le premier satellite à utiliser la blockchain fut lancé en 2017 par la société Blockstream pour distribuer le bitcoin dans le monde entier. Du côté de la sécurité, SpaceChain a été conçu en 2018 pour un système de blockchain basé sur un satellite. La société avait annoncé son intention de lancer une constellation de satellites pour prendre en charge un système d'exploitation basé sur la blockchain. En avril 2023, elle a rejoint le programme de startups de Google pour développer des applications de traitement sécurisé des données à bord des satellites en orbite basse et pour les futurs lancements de charges utiles.

[15] Attaques en déni de service ou en déni de service distribué. Un exemple notable d'attaque DDoS est celle dont a été victime Google le 1er juin 2022 : l'infrastructure et les services de Google ont été perturbés lorsque l'attaquant a utilisé plusieurs adresses pour générer plus de 46 millions de requêtes par seconde, soit 76 % de plus que le record précédemment signalé.

[16] Les blockchains publiques sont sans permission et permettent à tout le monde de les rejoindre ; les blockchains privées ou fermées sont sous le contrôle d'une entité qui détermine quels nœuds peuvent voir, ajouter ou modifier des données et dans les blockchains de consortium, les procédures de consensus sont contrôlées par des nœuds prédéfinis. Elles disposent d'un nœud validateur qui initie, reçoit et valide les transactions et les nœuds membres peuvent recevoir ou initier des transactions.

[17] Elizabeth Howell, « How blockchain can change the space industry », www.space.com, 9 avril 2020.

La demande d'innovations blockchain basées dans l'espace va croissant, notamment avec le développement d'applications cloud et d'actifs critiques dans l'espace (satellites, systèmes spatiaux, terres rares présentes dans les astéroïdes). Planetary Resources (une société minière d'astéroïdes) a été acquise en 2018 par ConsenSys (une importante société de blockchain). Cet accord ouvre la porte à la prise en charge par la blockchain de l'extraction d'astéroïdes en utilisant le processus de tokenisation. En effet, selon le droit luxembourgeois, les ressources de l'espace sont susceptibles d'appropriation[18].

L'espace est plus que jamais une plateforme d'innovation commerciale grâce à la blockchain. Dans le même temps, cette dernière s'infiltre dans tous les champs de l'activité humaine d'autant que le cadre légal est propice à son expansion.

Un cadre juridique propice à l'expansion des blockchains

La blockchain pourrait bien inonder l'espace numérique sans que l'utilisateur ne s'en aperçoive du fait des réglementations nationales ou régionales. Alors que le facteur réglementaire est souvent présenté comme un frein, si ce n'est un obstacle, à l'innovation, certaines législations nationales « crypto-friendly » en termes de fiscalité sur les plus-values se situent au Salvador, à Singapour et dans quelques pays européens : Slovénie, Portugal, Suisse, Allemagne, Malte, Estonie, Pays-Bas, mais aussi au Canada[19]. Ces cadres juridiques permissifs facilitent le lancement d'activités basées sur la blockchain.

Aux Etats-Unis, c'est le scandale FTX qui a amené la révision de la réglementation fédérale *Uniform Commercial Code* (UCC) en juillet 2022. Son article 12 reconnaît à présent les transactions de financement garanties par des actifs numériques (cryptomonnaies ou NFT)[20].

Enfin, en septembre 2023, malgré une position stricte de la Chine sur les opérations de crypto-monnaie, le Tribunal populaire de Chine a publié un rapport complet qui clarifie le statut juridique des monnaies virtuelles dans le pays (« Identification des attributs de propriété de la monnaie virtuelle et élimination des biens impliqués dans l'affaire »). À Hong Kong, la Chine a aussi approuvé un plan complet pour les actifs numériques qui fait de la cité-État un *hub* crypto. Une analyste observe : « *Tant que l'on ne viole pas les résultats financiers, pour ne pas menacer la stabilité financière de la Chine, Hong Kong est libre d'explorer sa propre voie dans le cadre du principe 'Un pays, deux systèmes'* »[21]. Cette décision s'inscrit dans la lignée d'un jugement du 31 mars 2023 du Tribunal de première instance d'Hong Kong, qui fut le premier à reconnaître que les cryptomonnaies peuvent faire l'objet d'un droit de propriété[22].

Dans l'Union européenne, le cadre législatif se construit de façon réticulaire à travers différents instruments juridiques : politique commerciale, protection des données et surtout l'identité numérique. En 2017, le Parlement européen y voyait déjà le moyen de renforcer et améliorer les politiques commerciales de l'Union (accords de libre-échange et de reconnaissance mutuelle) et

[18] Loi du 20 juillet 2017 sur l'exploration et l'utilisation des ressources spatiales, *Journal officiel du Grand-Duché de Luxembourg*, 28 juillet 2017, mémorial A674.
[19] Ahad Waseem, « 10 best countries for cryptocurrency – Crypto laws, taxes & adoption », www.management.org, 3 août 2023.
[20] Uniform Law Commission, Uniform Commercial Code, www.uniformlaws.org, 28 septembre 2023.
[21] Emily Tonelli, « China's court says crypto, digital assets are legally protected », www.cryptobriefing.com, 1er septembre 2023.
[22] *Re Gatecoin Limited (In Liquidation),* [2023] HKCFI 914, www.legalref.judiciary.hk, 31 mars 2023.

les décisions relatives au caractère adéquat des données ainsi que les mesures de défense commerciale compatibles avec les accords de l'Organisation mondiale du commerce (OMC)[23].

Mais l'Union européenne voit plus loin : « *À l'avenir, tous les services publics utiliseront la technologie de la chaîne de blocs* »[24]. Pour éviter la fragmentation du paysage de la blockchain et favoriser la collaboration entre les États membres, un partenariat européen a été lancé en 2018. Il se concentre principalement sur la construction de l'infrastructure européenne de services de chaîne de blocs afin de rendre les services publics transfrontaliers plus efficaces. Le partenariat prend la forme d'un bac à sable technologique et réglementaire et a pour but de permettre aux décideurs politiques européens d'acquérir des connaissances sur le fonctionnement de cette technologie, son potentiel et ses risques.

Les registres distribués sont soumis au droit européen de la protection des données à caractère personnel (RGPD) car le règlement est technologiquement neutre. La contradiction apparente entre le caractère inaltérable de la blockchain et le droit à l'effacement ou le principe de limitation de la conservation des données reconnus par le RGPD a été résolue par la CNIL elle-même[25]. La blockchain peut être particulièrement utile pour remplir certaines obligations issues du RGPD telles que la traçabilité et la preuve du consentement. Néanmoins, le choix d'un type de blockchain peut avoir un impact, à la hausse ou à la baisse, sur les risques aux droits et libertés des personnes concernées.

Le recours à la preuve (technique) à divulgation nulle (« zero knowledge proof ») est ainsi préconisé pour générer des preuves sur des données à caractère personnel tout en préservant l'anonymat du fournisseur de preuve. L'autorité européenne a aussi clarifié que l'émetteur de crypto-actifs est un responsable de traitement et à ce titre réalise une étude d'impact sur la protection des données avant d'amorcer le traitement des données sur une blockchain[26]. Le règlement sur les marchés de crypto-actifs (MiCA), qui établit un cadre réglementaire harmonisé pour les crypto-actifs au niveau de l'UE, vient d'être approuvé par le Conseil : les règles portent sur la supervision et l'autorisation des transactions, la transparence et la divulgation de l'incidence environnementale des crypto-actifs[27].

Un autre obstacle a été levé au même moment concernant l'adéquation entre le *Data Act*[28] et les contrats intelligents. Initialement, leur manque d'adéquation semblait miner le partage de données prôné par le texte et entraver l'intégration et la collaboration entre les systèmes. Le projet de règlement européen établit justement des règles et des normes claires pour les contrats intelligents utilisés pour automatiser le partage de données. Les institutions

[23] Parlement européen, Résolution du 13 décembre 2018 sur la chaîne de blocs : une politique commerciale tournée vers l'avenir, P8 TA(2018)0528.
[24] Commission européenne, « Déclaration créant le Partenariat européen sur la blockchain et instituant l'infrastructure européenne de services de chaîne de blocs (EBSI) », www.digital-strategy.ec.europa.eu, 10 avril 2018.
[25] CNIL, « Premiers éléments d'analyse de la CNIL – Blockchain », www.cnil.fr, septembre 2018.
[26] European Data Protection Supervisor, « Avis sur la proposition de règlement sur les marchés de crypto-actifs et modifiant la directive (UE) 2019/1937 », www.edps.europa.eu, 24 juin 2021.
[27] Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) no 1093/2010 et (UE) no 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 (Texte présentant de l'intérêt pour l'EEE), JOUE L 150, 09/06/2023, 40-205.
[28] Proposition de règlement européen fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), COM(2022)68.

européennes sont parvenues en juin 2023 à un accord politique sur les principales dispositions de la législation, y compris celles sur les contrats intelligents[29].

Enfin, la stratégie européenne « Façonner l'avenir numérique de l'Europe » met l'accent sur la nécessité d'investir dans les infrastructures de connectivité (y compris la 5G) et les technologies émergentes telles que l'IA, les technologies quantiques et la technologie blockchain. La création d'une « identité électronique publique universellement acceptée » facilitera et sécurisera l'accès transfrontalier des citoyens à des sites en ligne sur le territoire de l'Union européenne[30]. Cette identité numérique européenne (eID) prendra la forme d'un portefeuille numérique sur le téléphone mobile. La fourniture de registres électroniques figure parmi les services de confiance qualifiés[31]. Des schémas de certification garantiront la conformité de ces portefeuilles en termes de cybersécurité[32].

La blockchain est donc en passe de devenir la clé d'une identité numérique centrée sur l'utilisateur pour tous les citoyens de l'Union européenne. Ceci pourrait provoquer un effet domino en lien avec les objectifs de la « boussole numérique », selon laquelle tous les services publics clés doivent être disponibles en ligne d'ici 2030[33].

Conclusion et recommandations stratégiques

S'agissant d'une technologie dite « émergente ou de rupture » (OTAN, Commission européenne)[34], les impacts de la technologie blockchain sur la vie économique et quotidienne des citoyens seront autant invisibles que majeurs. Invisibles car cette technologie de web 3 s'effacera derrière une application mobile ou un site Internet (web 2), et majeurs car s'étant infiltrée dans tous les aspects de la vie courante, sa défaillance entraînera des répercussions immédiates et à impact fort. Ce qui conduirait à des scénarios inédits de menace cyber. Plusieurs actions seraient à envisager :

1. Intégrer l'impact de la blockchain dans les réflexions du Sénat sur l'intelligence économique en tant qu'outil de reconquête de notre souveraineté[35].

2. Examiner, dans le cadre du Comité français de l'intelligence artificielle générative, l'interaction entre la blockchain et les manipulations de l'information qu'elle implique ainsi que ses conséquences pour le public et les forces armées.

[29] Conseil de l'Union européenne, « Règlement sur les données : le Conseil et le Parlement parviennent à un accord sur l'équité de l'accès aux données et de l'utilisation des données », www.consilium.europa.eu, 27 juin 2023.
[30] Règlement n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, JOUE L 257, 28/08/2014, 73-114.
[31] Présidence du Conseil, « Le Conseil et le Parlement parviennent à un accord sur une identité numérique européenne », www.consilium.europa.eu, 29 juin 2023.
[32] Présidence du Conseil, « Le Conseil et le Parlement parviennent à un accord sur une identité numérique européenne », www.consilium.europa.eu, 29 juin 2023. .
[33] Commission européenne, « Une boussole numérique pour 2030 : l'Europe balise la décennie numérique », www.eur-lex.europa.eu, 9 mars 2021.
[34] OTAN/NATO, Advisory group on emerging and disruptive technologies, Annual report 2020, www.nato.int, 2021 ; European Commission, Directorate-General for Justice and Consumers, Liability for artificial intelligence and other emerging digital technologies, Publications Office, www.op.europa.eu, 2019.
[35] Sénat, Proposition de loi visant à faire de l'intelligence économique un outil de reconquête de notre souveraineté, texte n° 928, (2022-2023) de Mme Marie-Noëlle Lienemann, MM. Jean-Baptiste Lemoyne, Babary et Franck Montaugé, déposé au Sénat le 21 septembre 2023.

3. À l'initiative de la France avec d'autres États membres, obtenir un projet important d'intérêt européen commun (PIIEC) auprès de la Commission européenne pour soutenir le développement industriel des blockchains en lien avec l'objectif de l'UE : une transformation numérique résiliente et souveraine, respectueuse des libertés individuelles.

4. Faire une étude de droit substantiel de la blockchain appliquée à la défense, à la sécurité et à la cybersécurité pour déterminer les conditions de sa compatibilité avec les considérations de sécurité et les normes et politiques de sécurité, par exemple les données classifiées et sensibles, dans un contexte post-quantique.

5. Face à la militarisation de l'espace, actualiser le droit international de l'espace (COPUOS Nations unies), afin de coordonner les organisations spatiales nationales et régionales et les acteurs privés à une gouvernance globale pour contrecarrer la course aux armes spatiales et protéger les ressources naturelles spatiales, en particulier les orbites.

Fondation pour la Recherche Stratégique (FRS)

55 rue Raspail 92300 Levallois-Perret

Fondation reconnue d'utilité publique par décret du 26 février 1993

Directeur de la publication : Bruno Racine

ISSN : 2273—4643

WWW.FRSTRATEGIE.ORG