GOUVERNEMENT

Liberté
Égalité
Fraternité

LES VERROUS TECHNOLOGIQUES DES *BLOCKCHAINS*

SYNTHÈSE

Avril 2021

cea

Institut Mines-Télécom

Inria

Directeur de la publication : Thomas Courbe

Édition : BCom de la DGE

Dépôt légal : avril 2021

ISBN : 978-2-11-162212-8 (version en ligne)

Direction générale des Entreprises – 67 rue Barbès – BP 80001 - 94201 Ivry-sur-Seine Cedex

AVERTISSEMENT

La méthodologie de cette étude ainsi que les résultats obtenus, les conclusions et recommandations qui en sont tirées sont de la seule responsabilité des chercheurs missionnés. Ils n'engagent ni la Direction générale des Entreprises ni le ministère de la Recherche, de l'Enseignement supérieur et de l'Innovation (MESRI), ni aucun des membres du Comité de pilotage.

MEMBRES DU COMITÉ DE PILOTAGE

Côme BERBAIN	DINSIC
Hélicia CLAUDE	DGE
Blandine DUSSER	DGE
Marie-Christine PLANÇON	MESRI/DGRI
Michel RAYNAL	Université Rennes 1
Olivier ROUXEL	DGE
Benoit WINTREBERT	Ministère des Armées

INSTITUTS

CEA-LIST, INSTITUT EN RECHERCHES SUR LES SYSTÈMES NUMÉRIQUES INTELLIGENTS

Tél. : +33 (0)1 69 08 08 00

www-list.cea.fr

INSTITUT MINES-TELECOM

Tél. : +33 (0)1 75 31 92 00

www.imt.fr

INSTITUT NATIONAL DE RECHERCHE EN SCIENCES ET TECHNOLOGIES DU NUMÉRIQUE

Tél. : +33 (0) 01 80 49 40 00

www.inria.fr/fr

CHERCHEURS RÉDACTEURS DU PRÉSENT RAPPORT

Stéphane DALMAS, Conseiller innovation auprès de la direction générale Inria
Patrick DUVAUT, Directeur de l'innovation au sein de l'IMT
Georges GONTHIER, Chercheur senior au sein d'Inria
Gilles JACOVETTI, Ingénieur de recherche à l'IMT Atlantique au sein de l'IMT
Agnès LANUSSE, Ingénieure chercheuse senior au CEA LIST
Gérard MEMMI, Professeur et chef de département à Télécom Paris au sein de l'IMT
Sara TUCCI-PIERGIOVANNI, Cheffe de laboratoire au CEA LIST

SOMMAIRE

RÉSUMÉ ANALYTIQUE

Présentée le 15 avril 2019, la stratégie nationale blockchain, qui vise à faire de la France une « nation de la blockchain », est le fruit d'un travail mené par la Direction générale des Entreprises avec l'ensemble de l'écosystème de la blockchain en France. Dans le cadre de l'axe 2 de cette stratégie, « *être à la pointe des enjeux technologiques* », le ministre de l'Économie des Finances et de la Relance, la ministre de l'Enseignement Supérieur, de la Recherche et de l'Innovation et le secrétaire d'État chargé du Numérique ont confié au CEA, à l'IMT et à Inria une mission visant à « définir avec précision l'ensemble des verrous technologiques et techniques » autour de la blockchain.

Cette mission a été conduite de juin 2019 à janvier 2020 par une équipe composée de Sara Tucci-Piergiovanni (chef de laboratoire au CEA LIST), Gérard Memmi (professeur et chef de département à Télécom Paris au sein de l'IMT), Agnès Lanusse (ingénieur chercheur senior au CEA LIST), Gilles Jacovetti (ingénieur de recherche à l'IMT Atlantique au sein de l'IMT), Georges Gonthier (chercheur senior Inria), Patrick Duvaut (directeur de l'innovation à l'IMT) et Stéphane Dalmas (conseiller innovation auprès de la direction générale Inria).

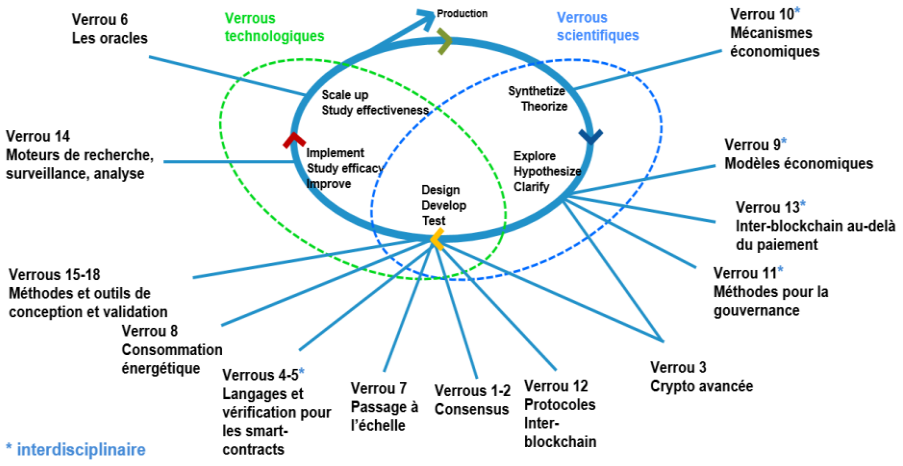
Le rapport issu de cette mission décrit en détail les verrous que nous avons identifiés et propose un ensemble de recommandations pour favoriser la levée de ces verrous, et plus généralement le développement des technologies blockchain au bénéfice de la société et du monde économique. Trois cartographies appuient nos travaux : la première sur les laboratoires de recherche travaillant dans le domaine de la blockchain, la seconde sur les offres d'enseignement aujourd'hui en France, incluant une comparaison avec ce qui se fait dans les plus grandes universités mondiales et la dernière sur les *start-up* françaises les plus actives sur ces technologies.

Les verrous

Une des contributions majeures de ce rapport est la méthodologie d'analyse que nous proposons, qui a pour but de construire une feuille de route pour les années à venir. À cette fin, nous avons d'abord identifié les verrous en les traitant par « préoccupation » (sécurité, passage à l'échelle, interopérabilité, etc.) et nous les avons ensuite classés selon leur maturité et leur potentiel de rupture. Dans une dernière étape, grâce aux cartographies réalisées, nous avons pu analyser la capacité de l'écosystème français à les lever.

Verrous et maturité

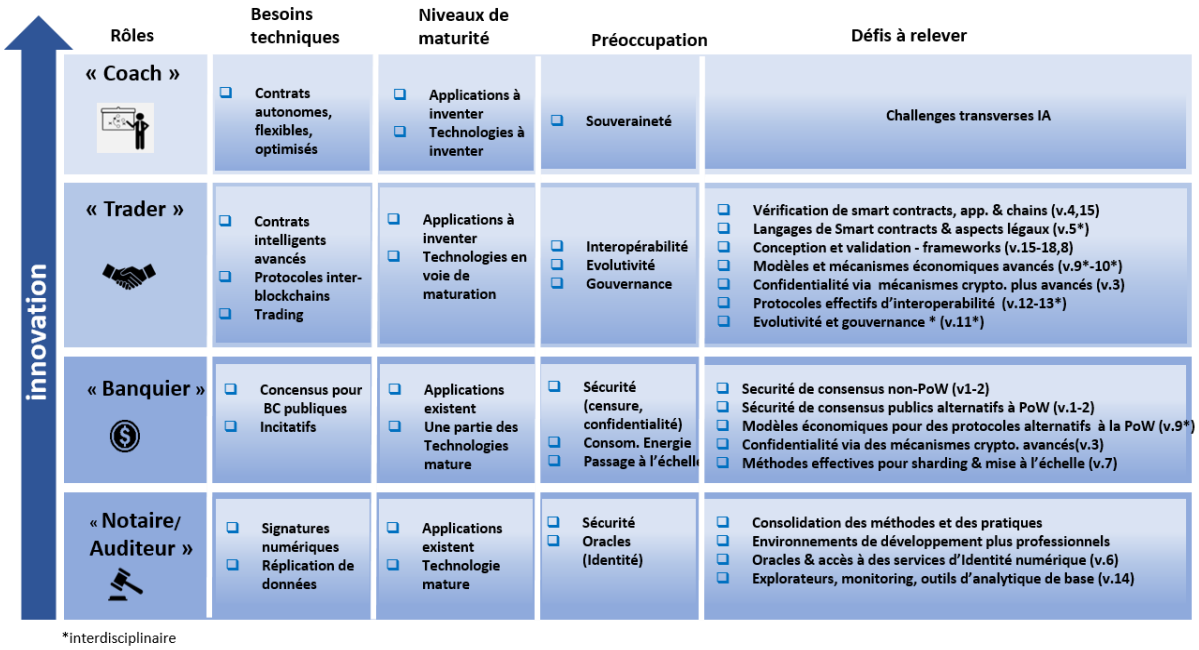
La figure suivante présente succinctement les différent verrous identifiés en les positionnant sur un cycle recherche & innovation, en fonction de la maturité de la recherche sur ces sujets.



Notre analyse positionne la majorité des verrous dans la phase « *Design, Develop, Test* ». Dans cette phase, le cadre théorique et des solutions existent mais n'ont pas encore été appliqués à la blockchain (applications qui sont évidemment non triviales). Cette phase est charnière, ici la levée d'un verrou nécessite un dialogue entre la recherche et d'autres acteurs de l'écosystème d'innovation, comme des *start-up*, qui peuvent à ce stade incuber certaines solutions et les porter à maturation.

Verrous et innovation

Pour ce qui concerne le potentiel de rupture, nous avons réparti les verrous selon l'innovation apportée par leur levée. Cette innovation dépend de l'usage que les applications font de la blockchain : du plus élémentaire, « Notaire » (archivage et traçabilité), au plus élevé « *Coach* » (optimisation et analyse décisionnelle), en passant par le niveau « Banquier » (échange d'actifs) et « *Trader* » (contrats intelligents avancés, places de marché, assurances, etc.). Cette répartition est présentée dans la figure suivante (le « potentiel de rupture » est croissant de bas en haut).



*interdisciplinaire

Notre analyse nous amène à considérer comme prioritaires les verrous au niveau « *Trader* » : accéder à ce niveau d'innovation signifie créer une vraie rupture technologique. Nous reconnaissons également l'intérêt des verrous au niveau « Notaire », parce qu'il s'agit de verrous de nature plutôt technologique dont la levée est envisageable à court terme : leur levée permettrait une accélération de la productivité de solutions à ce niveau et contribuera à l'adoption des blockchains.

Verrous et acteurs français

Grace à nos cartographies, nous avons identifié que, pour les verrous liés à la vérification des *smart contracts* et aux langages formels, nous sommes en avance par rapport à l'international : nous avons une recherche de haut niveau et des *start-up* actives dans le domaine, avec des compétences recherchées à l'étranger. Sur les verrous liés à la cryptographie, la recherche française, pourtant bien reconnue dans ce domaine, est finalement peu impliquée sur ses applications à la blockchain ; les réalisations les plus importantes se font aux États-Unis et en Israël. Pour les verrous sur les modèles et mécanismes économiques, interopérabilité et gouvernance, nous ne sommes pas en retard. Toutefois, une recherche active se poursuit partout dans le monde en nous mettant en forte compétition avec l'international. Sur les verrous autour du génie logiciel (outils et méthodes de conception et validation), nous ne sommes pas en retard, nous avons des compétences fortes sur le sujet et un vrai besoin industriel. Le marché des outils d'aide à la conception et à la validation est vierge, avec une forte demande. Sur

les verrous reliés au consensus et au passage à l'échelle, nous ne sommes pas en avance, mais nous avons des compétences fortes en algorithmique distribué, des chercheurs impliqués sur la blockchain et de belles collaborations avec des *start-up*.

Les recommandations

Nous énonçons 14 recommandations dans ce rapport, issues des auditions que nous avons menées, de l'analyse des verrous identifiés et des forces et des faiblesses françaises. Nous les avons voulues pragmatiques mais ambitieuses. Ces recommandations sont résumées dans la suite.

Sur la recherche

En ce qui concerne les recommandations en matière de recherche, nous proposons de favoriser les actions interdisciplinaires, de valoriser les compétences françaises sur les aspects langages, d'amplifier les recherches sur le sujet de la confidentialité et de la gestion des données personnelles ou sensibles (*privacy*), et de focaliser une partie des compétences en génie logiciel sur les problèmes spécifiques des applications et des infrastructures blockchains (cf. la grande action d'innovation que nous proposons). Nous suggérons également d'étudier la création d'un Institut International Interdisciplinaire de la Blockchain, pour dynamiser la recherche française, encourager l'interdisciplinarité et donner à notre pays une meilleure visibilité internationale.

Sur l'innovation

Nous proposons le lancement d'une grande action d'innovation sur les sujets de conception, de validation et de *benchmarkin*g, avec pour objectif de créer les outils, manquants aujourd'hui, qui faciliteront l'adoption des technologies blockchain par le développement plus simple de solutions fiables.

Cette grande action, qui durerait idéalement entre 4 et 5 ans, lancera des projets ciblés, conduits par de (petits) consortiums associant typiquement des *start-up* et des laboratoires de recherche (avec d'autres acteurs si besoin), sur des durées assez courtes (12 à 18 mois), avec des objectifs concrets bien définis. Nous envisageons que le sujet puisse être couvert par une vingtaine de tels projets.

Sur la confiance numérique

Sur la question de la confiance numérique, en lien avec les blockchains, nous recommandons que l'ANSSI s'empare du sujet blockchain, qu'une réflexion soit menée sur la certification (des acteurs et/ou des applications et services) spécifique.

L'identité numérique est la base de la confiance. Nous proposons la création d'un véritable service public de l'identité numérique, pour les personnes physiques comme pour les personnes morales, qui soit modulaire, évolutif, utilisant des technologies cryptographiques avancées (en lien aussi avec les recherches mentionnées plus haut sur le sujet *privacy*). Ce serait, pour nous, une mesure phare pour favoriser l'innovation dans la blockchain en France. Un tel projet, qui pourrait associer État et recherche publique, serait à même de stimuler efficacement la recherche et la création d'entreprise dans ce secteur.

Sur l'appui aux politiques publiques

Pour appuyer les politiques publiques et les projets de l'État dans ce domaine, qui reste encore assez mal compris aujourd'hui, nous suggérons fortement la mise en place d'un comité consultatif issu de la recherche publique, avec des chercheurs en activité sur le sujet, capables de mobiliser d'autres collègues si nécessaire. Ce comité serait saisi sur les questions technologiques des projets de l'État et sur la mise au point des réglementations et de la législation sur le sujet.

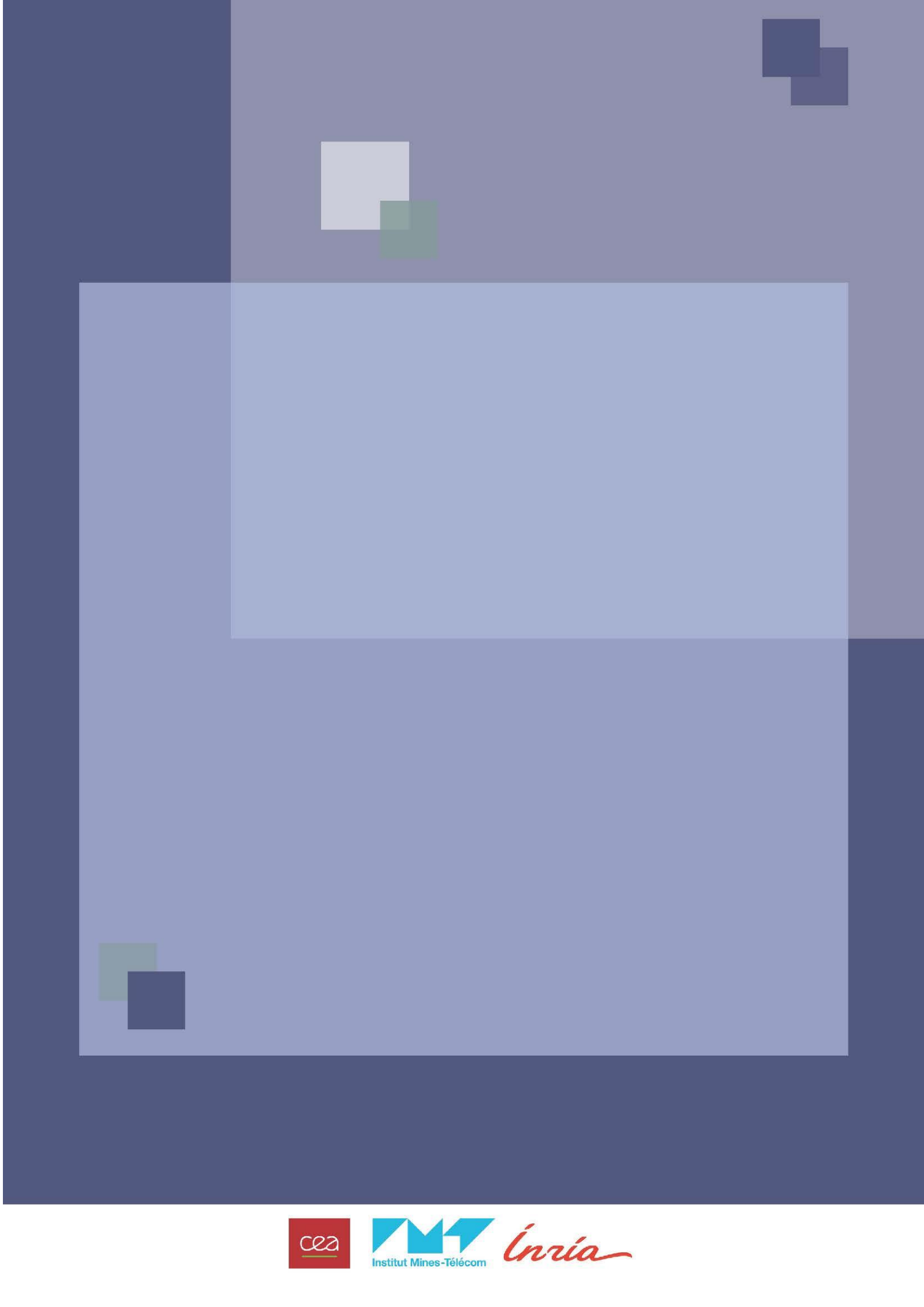
Sur les liens entre recherche publique et *start-up*

Nous recommandons de promouvoir la collaboration entre la recherche publique et les *start-up* dans le but de faciliter l'accès aux compétences et aux résultats de recherche les plus avancés en termes de calcul distribuée, cryptographie, vérification et certification de contrats intelligents, de finance et d'économie. La grande action d'innovation que nous proposons sera un moyen opérationnel de créer des liens plus forts entre ces deux mondes.

Sur l'enseignement

La cartographie des offres d'enseignement montre clairement le besoin d'augmenter le nombre de formations aux technologies blockchains. Nous proposons la mise en place de formations spécialisées, au niveau master, par les organismes d'enseignement supérieur (pour former deux types de profils : des ingénieurs R & D spécialisés et des ingénieurs d'application). Favoriser la formation en alternance dans des laboratoires de R & D du domaine nous apparaît comme une idée intéressante pour permettre aux avancées de la recherche de pénétrer plus vite les entreprises. Enfin, une offre cohérente de MOOC[1] sur le domaine (hébergée par la plateforme FUN) devrait être élaborée.

1 **MOOC** : *Massive Online Open Course* (en français **FLOT** Formation en Ligne Ouverte à Tous)


cea
Institut Mines-Télécom
Inria