GOUVERNEMENT

*Liberté*
*Égalité*
*Fraternité*

# LES VERROUS TECHNOLOGIQUES DES *BLOCKCHAINS*

RAPPORT

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

# 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 et des Finances, 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 (cheffe de laboratoire au CEA-LIST), Gérard Memmi (professeur et chef de département à Télécom Paris), Agnès Lanusse (ingénieure chercheuse senior au CEA-LIST), Gilles Jacovetti (ingénieur pédagogique à l'IMT Atlantique), 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).

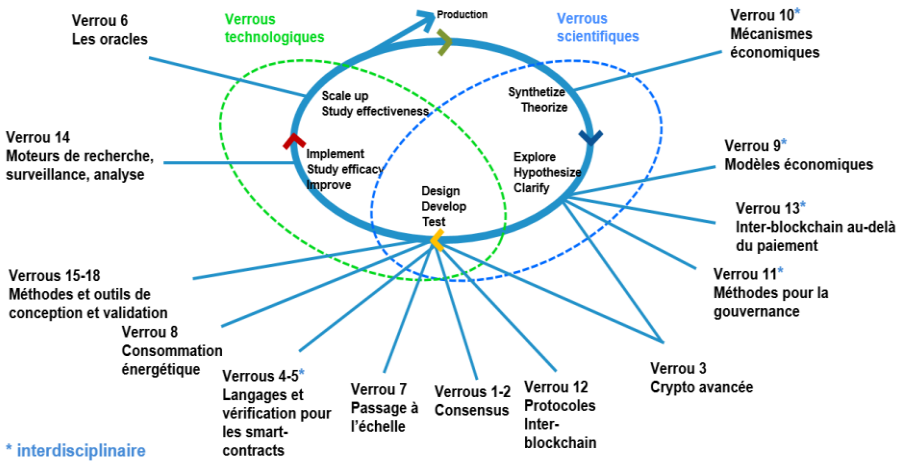
Le rapport issu de cette mission décrit en détail les verrous que nous avons identifiés et propose un ensemble de recommandations pour favoriser la levée de ces verrous, et plus généralement le développement des technologies blockchain au bénéfice de la société et du monde économique. Trois cartographies 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 traitants 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

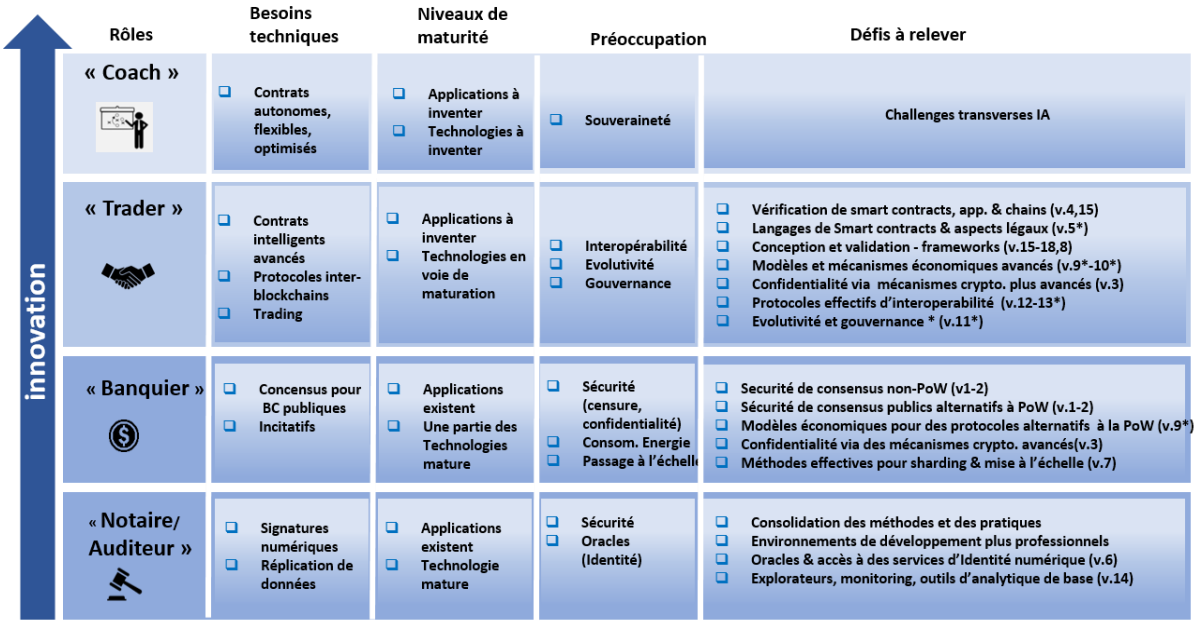
La figure suivante présente succinctement les différents verrous identifiés en les positionnant sur un cycle recherche & innovation, en fonction de la maturité de la recherche sur ces sujets.




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

Grâce 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 distribuée, 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 *bechmarking*, 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 le lancement d'une réflexion entre l'ANSSI et les entreprises du secteur sur la certification spécifique des acteurs et/ou des applications.[1]

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

1 À la suite de cette recommandation et sous l'impulsion de la Direction générale des Entreprises, un cycle d'échanges entre *start-up* blockchain et équipes de l'ANSSI a été mené à bien sur la certification de produits/services utilisant la blockchain. L'objectif de ces échanges est une meilleure compréhension des enjeux d'une telle certification par les deux parties.

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[2] sur le domaine (hébergée par la plateforme FUN) devrait être élaborée.

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

# Sommaire

# Table des verrous

# Table des recommandations



# Table des figures

# INTRODUCTION

## 1.1 Portée de la mission

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 et des Finances, 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, cheffe de laboratoire au CEA-LIST
- Gérard Memmi, professeur et chef de département à Télécom Paris
- Agnès Lanusse, ingénieure chercheuse senior au CEA-LIST
- Gilles Jacovetti, ingénieur pédagogique à l'IMT Atlantique
- Georges Gonthier, chercheur senior Inria
- Patrick Duvaut, directeur de l'innovation à l'IMT
- Stéphane Dalmas, conseiller innovation auprès de la direction générale d'Inria

Le présent rapport rend compte de nos travaux. Il décrit en détail les verrous que nous avons identifiés. Nous y formulons également 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.

### 1.1.1 Verrous technologiques

Nos investigations sur les verrous technologiques de la blockchain se sont concentrées sur la technologie elle-même, dans une acceptation assez large de ce qui est appelé communément blockchain ou technologies de registres distribués (Distributed Ledger Technology, abrégé en DLT, en anglais). Les questions réglementaires, économiques ou d'acceptation sociale, par exemple, ont été considérées hors du périmètre de notre mission.

Par verrou nous entendons un problème ouvert (dont la solution n'est pas disponible dans l'état de l'art) et qui s'oppose à la réalisation de certaines applications (avec certaines caractéristiques ou spécifications) ayant au moins un intérêt pratique potentiel. Les verrous auxquels nous nous sommes intéressés sont plus scientifiques que technologiques au sens où ils demandent une activité de recherche scientifique pour être levés, même si *in fine* ils interviennent bien dans la réalisation d'un objet technologique. La section 2.1.4 expliquera la différence que nous ferons,

dans ce rapport, entre verrous scientifiques et technologiques, en fonction des implications de la levée d'un verrou dans un cycle de recherche et d'innovation.

Notre lettre de mission a orienté nos travaux sur cinq grands sujets :

- la souveraineté : sur tous les risques liés à l'utilisation de blockchain pour des usages publics et « critiques » ;
- la sécurité : sur tous les problèmes de sécurité liés aux blockchains (consensus, protocoles, cryptographie…) ;
- l'interopérabilité et l'évolutivité : sur les problèmes liés à l'interopérabilité entre blockchains et à leurs évolutions (typiquement évolution des protocoles et questions de gouvernance associées) ;
- l'énergie : sur les questions de consommation d'énergie par les blockchains; essentiellement celles qui utilisent la preuve de travail et les solutions alternatives envisageables ;
- les modèles économiques : sur les incitations à la participation (fourniture de moyens de calcul et de stockage) aux blockchains publiques.

Notre analyse des verrous nous a amené à structurer notre rapport d'une manière un peu différente mais le lecteur pourra facilement retrouver nos réflexions et conclusions sur ces différents sujets dans la suite du texte.

### 1.1.2 La blockchain au-delà des crypto-monnaies

Il est bien entendu difficile de parler de blockchain sans parler de monnaie électronique. La création d'une monnaie électronique est l'application qui est à l'origine de la blockchain, avec Bitcoin. Et cela reste encore l'application principale et (trop ?) emblématique de ces technologies aujourd'hui.

Dans le cadre de notre mission, nous avons considéré les crypto-monnaies (au sens de monnaies électroniques utilisant de la cryptographie) comme une application de ces technologies, au même titre que toutes leurs autres applications. Nous ne nous sommes donc pas spécifiquement intéressés aux verrous technologiques liés à l'implémentation d'une crypto-monnaie mais uniquement aux verrous qui interviennent dans les technologies sous-jacentes possibles de blockchain.

L'utilisation de la blockchain pour implémenter une crypto-monnaie ou plus généralement pour créer et échanger des jetons (*tokens*) porteurs d'une valeur économique en lien avec des actifs matériels ou immatériels (la « digitalisation des actifs ») pose également beaucoup de questions riches et complexes, de nature économique, juridique ou réglementaire, que nous n'avons donc pas abordées dans le cadre de cette mission.

### 1.1.3 La maturité technologique

De très nombreuses offres technologiques existent aujourd'hui (Bitcoin, Ethereum, Tezos, Hyperledger, R3 Corda, pour n'en citer que quelques-unes), certaines avec un support fort de grands acteurs des services informatiques (IBM et Hyperledger) ou de fondations disposant de dotations conséquentes (parfois de plusieurs centaines de millions d'euros) pour aider à leur développement.

Indépendamment des verrous technologiques qui resteraient à lever, la question de la maturité des technologies existantes se pose naturellement. Nous entendons par maturité technologique la capacité à concevoir, réaliser et maintenir des services basés sur ces technologies, avec des coûts maîtrisés, des performances et une fiabilité suffisantes (par rapport à l'état de l'art).

Les opinions sur cette question de la maturité technologique de la blockchain sont assez diverses. Nous pouvons citer, par exemple, une prédiction récente de Gartner[3] qui fixe à 2023 l'horizon d'obtention de plateformes blockchain suffisamment stables (en particulier en termes de performances et d'interopérabilité) pour avoir un véritable impact (mise en production d'applications et de services), à partir de 2028.

La question de la maturité technologique n'est pas une question centrale dans un rapport essentiellement tourné vers le futur de ces technologies. Et ce n'est donc pas une question à laquelle il faut s'attendre à trouver une réponse simple en lisant le reste de ce rapport. C'est aussi une question plus complexe qu'il ne peut y paraître : les blockchains sont constituées de plusieurs composants qui ont parfois des niveaux de maturité différents et la maturité elle-même ne peut s'apprécier vraiment que dans le contexte d'une application. Ces sujets sont notamment abordés dans le chapitre 3 (Les verrous et l'innovation).

### 1.1.4 De l'intérêt des technologies blockchain

« *Blockchain technologies have not yet lived up to the hype and most blockchain projects are stuck in experimentation mode* » (Avivah Litan, distinguished analyst and research vice-president chez Gartner). C'est une opinion assez largement partagée aujourd'hui.

Les raisons pour lesquelles ces technologies n'ont pas encore pu démontrer clairement leur réel potentiel (hormis en matière de crypto-monnaies et d'objets spéculatifs) sont certainement multiples et liées à leur complexité intrinsèque et à un certain nombre de verrous que nous identifions dans ce rapport (temps de transaction, passage à l'échelle, interopérabilité, évolutivité, absence de certains outils de génie logiciel, etc.).

Mais au-delà de ces considérations, nous ne pouvons pas occulter la question de l'intérêt réel ou de l'utilité de la blockchain par rapport à d'autres solutions plus éprouvées ou plus spécifiques. Il est vrai qu'un grand nombre des preuves de concept lancées ces dernières années ont cherché à résoudre, *via* la blockchain, des problèmes qui n'étaient pas forcément les mieux adaptés pour démontrer sa réelle utilité (qui auraient pu être souvent résolus plus efficacement par d'autres moyens, parfois avec des solutions plus spécifiques mais aussi souvent avec des solutions bien éprouvées). Un énorme « effet de mode » autour de la blockchain a, sans aucun doute, poussé un certain nombre d'organisations à vouloir monter trop rapidement des démonstrateurs et certains à s'interroger sur le fait que la blockchain était aujourd'hui plutôt une solution en quête d'un problème. Tout cela a contribué à entretenir aussi une certaine image injustement négative de ces technologies.

La mission est bien entendu persuadée qu'une blockchain ou plutôt une « plateforme blockchain » fournit un ensemble de fonctionnalités qui peuvent trouver de belles applications (et d'encore plus belles applications lorsque certains des verrous que nous avons identifiés seront levés) hors des aspects crypto-monnaies et spéculatifs qui lui font parfois une assez mauvaise publicité. Savoir quelles applications sont les mieux adaptées à une telle plateforme n'était pas

3 https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-

dans le champ d'investigation de notre mission même si quelques pistes peuvent être trouvées dans ce rapport.

## 1.2 Méthodologie

Le travail présenté dans ce rapport sur les verrous technologiques de la blockchain est le résultat d'auditions avec un certain nombre d'acteurs, publics et privés (dont la liste est présentée en Annexe C) et des compétences et de l'expertise des membres de la mission, composée en majorité de chercheurs actifs dans le domaine.

Dans le temps imparti à la mission, nous avons dû faire des choix parfois difficiles sur les personnes et les organisations à auditionner et nous avons privilégié celles et ceux qui avaient une expérience claire des verrous technologiques de la blockchain (parfois au détriment de ceux qui auraient eu une expérience plus applicative mais certainement tout aussi intéressante).

Les recommandations que nous formulons dans ce rapport sont le fruit de nos auditions et de nos réflexions et discussions. Elles n'engagent bien évidemment que les membres de la mission.

Les sections sur les cartographies recherche, formations et *start-up* présentent leurs méthodologies particulières.

## 1.3 Remerciements

Nous tenons à remercier l'ensemble des personnes que nous avons auditionnées, dont la liste se trouve en Annexe C, pour leur disponibilité et la qualité des échanges (pour des auditions qui ont très rarement duré moins de deux heures). Nous remercions également le comité de pilotage qui nous a accompagnés tout le long de cette mission, pour la richesse de nos discussions. Ce comité était composé de Michel Raynal (Université Rennes 1), Côme Berbain (DINSIC), Marie-Christine Plançon (MESRI/DGRI), Olivier Rouxel (DGE) et Benoit Wintrebert (ministère des Armées).

# 2 LES VERROUS TECHNOLOGIQUES DES BLOCKCHAINS

## 2.1 Méthode d'identification des verrous

Les systèmes numériques du futur seront massivement distribués. Il ne s'agit plus de communiquer des données entre deux dispositifs ou plus, mais il s'agit de numériser la coopération et l'échange entre un grand nombre d'utilisateurs : des systèmes de vote, des places de marché, la gestion de chaînes d'approvisionnement étendues. Ces applications peuvent se réaliser à l'échelle d'Internet, mais pour ce faire il faut construire ce qu'on appelle de la confiance décentralisée : rendre possible les coopérations entre acteurs qui ne se font pas confiance, sans passer par une tierce-partie. La blockchain est une technologie en rupture, appelée souvent la « machine à confiance », elle incarne aujourd'hui la première concrétisation de la confiance décentralisée.

La blockchain a vu le jour avec l'apparition de Bitcoin en 2009, toutefois son potentiel a été vraiment dévoilé un peu plus tard avec la naissance d'Ethereum et la notion de « contrat intelligent » (*smart contract*) : on ne s'échange pas que de la monnaie, mais n'importe quel actif numérisé, et on peut le faire selon des règles complexes.

Aujourd'hui, la blockchain a suscité de l'intérêt dans presque tous les secteurs industriels à commencer par ceux qui souffrent d'un manque de transparence et qui impliquent un grand nombre d'acteurs : l'alimentaire en est un exemple emblématique, avec des *start-up* désormais actives dans le domaine. Toutefois, l'utilisation des blockchains en production par notre industrie demeure très limitée et les investissements restent relativement timorés. Au-delà des difficultés à trouver des nouveaux modèles économiques pour valoriser un service rendu par une blockchain (modèles qui commencent à émerger avec la tokenisation), les technologies blockchains sont encore très peu matures alors qu'elles doivent répondre à des exigences de sécurité très élevées. Pour apporter de la confiance, la blockchain doit se comporter comme un système sans défaillances. Remplacer une banque, ou un notaire, un auditeur, par un protocole informatique exécuté en réseau signifie requérir de la blockchain des exigences de sécurité proches des systèmes logiciels critiques. Est-ce que les blockchains répondent aujourd'hui à ce niveau d'exigences ? La réponse est non. Est-ce que nous disposons de méthodes et outils pour pouvoir atteindre ce niveau d'exigences ? La réponse est non.

Cette section présente les verrous à surmonter pour répondre à ces enjeux.

Les retombées, une fois ces verrous levés, impacteront drastiquement différents secteurs de la société. Dans des interactions sociétales, industrielles et économiques en perpétuelle mutation, les échanges directs entre utilisateurs selon des règles auto-établies, évolutives, transparentes et vérifiables à tout instant, ouvriront de nouveaux marchés et services, tout en augmentant la qualité des services et produits échangés.

Nous commencerons par présenter une brève introduction à la blockchain, son évolution et sa classification habituelle (blockchain publique, privée et de consortium) ainsi qu'une architecture de référence pour identifier les briques technologiques qui concourent à constituer un système blockchain générique. Nous présentons ensuite notre méthode d'identification et de classification des verrous.

### 2.1.1 Blockchains en bref

Les blockchains ont comme objectif premier la réalisation d'échanges entre utilisateurs dans un environnement où les participants sont « pairs » (tous les utilisateurs sont « égaux ») et ne se font pas *a priori* confiance. La sécurisation des échanges, au lieu de passer par un organe central de contrôle, qui joue le rôle de garant où « tierce partie », passe par le maintien d'un registre partagé qui enregistre l'historique des échanges.

Chaque utilisateur maintient sa propre copie du registre et chaque nouvelle transaction est validée localement par l'utilisateur, avant d'être enregistrée, à l'aide d'un protocole informatique. Comme chaque utilisateur a une copie locale, il va de soi que le registre sera hautement disponible car redondé, en principe sur un grand nombre de nœuds.

> ***Zoom technique : la vérifiabilité publique***
>
> *Techniquement la révolution blockchain repose sur le concept de « public verifiability », c'est-à-dire, un système technique qui permet à quiconque de vérifier de manière autonome l'exactitude de l'état du système. Dans un grand livre distribué, tout observateur peut vérifier que chaque action modifiant l'état du système est valide : conforme à l'ensemble des règles, acceptées par tous, qui régissent le système. Cette vérifiabilité est possible seulement si les informations nécessaires à la validation sont disponibles, vérifiables dans un temps raisonnable, et que les actions effectuées soient observables.*

L'application de mécanismes cryptographiques simples, garantit également qu'il soit très difficile, déjà localement, de modifier le contenu du registre sans rendre le contenu invalide aux yeux des autres participants. Pour ce faire, il faudrait reconstituer le contenu du registre à partir de l'enregistrement modifié et corrompre les autres participants pour leur faire adopter le contenu régénéré. Si l'on considère cette éventualité comme quasiment impossible ou non raisonnable, alors la modification accidentelle ou malveillante demeure quasiment impossible, délivrant une bonne propriété d'intégrité du registre.

Le fonctionnement d'une blockchain commence par son « cœur » constitué des algorithmes de consensus qui permettent aux participants de maintenir la cohérence des copies du registre distribué. Le consensus porte sur l'historique du registre : les copies maintenues par des participants honnêtes doivent être cohérentes entre elles et les enregistrements doivent être valides. La validité d'un enregistrement dépend de l'application, par exemple en Bitcoin, un enregistrement est valide si il n'y a pas de double dépense et le payeur possède le montant déclaré dans sa transaction.

Pour adapter cette notion de validité à des applications qui vont au-delà des systèmes de paiement, les *smart contracts*, ou contrats intelligents, sont souvent déployés dans les blockchains. C'est grâce à ces contrats intelligents qu'il est possible de créer des règles d'enregistrement auto-établies par les participants, comme par exemple des validations complexes incluant des calculs et, *in fine*, rendre les blockchains programmables.

Enfin, il ne faut pas oublier que les utilisateurs interagissent avec la blockchain *via* des *wallets* ou portefeuilles numériques. Un portefeuille numérique fournit à son l'utilisateur un couple de clés (privée et publique). Chaque enregistrement est signé par son émetteur avec sa clé privée. Les autres utilisateurs peuvent lire l'enregistrement à l'aide de la clé publique de l'émetteur et l'accepter s'il s'agit d'un enregistrement valide. Une signature numérique valide donne au lecteur une très bonne raison de croire que l'enregistrement a été créé par son émetteur (authenticité) et que l'enregistrement n'a pas été modifié (intégrité). Les signatures numériques fournissent également une propriété de non-répudiation, ce qui signifie que le signataire ne peut pas affirmer

qu'il n'a pas signé, tout en prétendant que sa clé privée reste secrète. À chaque portefeuille est associé un ensemble de jetons (le contenu du portefeuille). Seul le propriétaire du portefeuille, à l'aide de la clé privée, a le droit de transférer les jetons associés. Les contrats intelligents peuvent également disposer d'un portefeuille numérique associé, qui sert également d'identifiant du contrat intelligent dans le système. Les utilisateurs, en effet, paient le contrat pour qu'il soit exécuté.

### 2.1.2 Classification et évolution des blockchains

#### Classification

La technologie blockchain continue d'évoluer en ce qui concerne la façon dont les chaînes sont construites, accédées et vérifiées, mais nous pouvons classer les blockchains en trois grandes catégories :

- Blockchain *publique*, ouverte à tous pour lire, envoyer, ou recevoir des transactions, et permet à tout participant d'être partie prenante du consensus pour décider des ajouts et des transactions valides ;
- Blockchain dite *de consortium*, qui impose certaines restrictions aux autorisations d'écriture, de sorte que seul un ensemble présélectionné de participants au réseau peut influencer et contrôler le processus de consensus, même si la lecture est ouverte à tout participant du réseau ;
- Blockchain *privée*, dont les autorisations d'écriture sont strictement limitées à un seul participant (ou organisation), même si ses autorisations de lecture sont ouvertes au public ou limitées à un sous-ensemble de participants du réseau.

Bien qu'elles diffèrent dans la vitesse du consensus et si une ou plusieurs autorités de confiance[4] sont utilisées, ces trois catégories de blockchains partagent certaines propriétés communes :

- elles utilisent toutes des réseaux pair-à-pair, gérant des transactions de manière décentralisée ;
- elles exigent toutes que chaque transaction soit signée numériquement et ajoutée au registre global distribué des transactions, et que chaque nœud validateur conserve une réplique du registre ;
- elles s'appuient toutes sur un consensus pour synchroniser les répliques à travers le réseau.

#### Évolution

Bien que Bitcoin soit sorti en 2009 en tant que premier système de monnaie numérique pair-à-pair, les concepts cryptographiques et d'algorithmique répartie sous-jacents (l'utilisation d'arbres de Merkle pour son optimisation, par exemple, ainsi que l'utilisation des *Byzantine quorums* pour la validation de transaction) ont été proposés au début des années quatre-vingt-dix. Au cours des dix dernières années, la technologie blockchain a évolué au-delà de la monnaie numérique (Blockchain 1.0), vers des contrats intelligents ou des blockchains programmables (Blockchain 2.0), puis vers une vision de formes avancées de collaborations décentralisées, tant d'un point de vue économique que juridique (Blockchain 3.0). La Figure 1 montre l'évolution des blockchains au cours du temps. On remarque la naissance des blockchains programmables avec la publication d'Ethereum. La programmabilité des blockchains a suscité l'intérêt de quasiment tous les secteurs

4 Les entités qui délivrent et gèrent les accès des participants.

industriels : les propriétés d'un « *cryptographic ledger* » pouvaient en effet servir à d'autres applications que les transferts des jetons (cf. 2.1.3).

Ces trois dernières années ont vu une multiplication de preuves de concept ou expérimentations dans des secteurs comme l'énergie, l'alimentaire, la mobilité, le contrôle de la pollution, l'administration, etc., mais souvent avec des ambitions limitées et des investissements timorés. Le passage à une blockchain 3.0 demande de surmonter des obstacles d'ordre technique, c'est-à-dire, les verrous que nous allons traiter dans ce document.

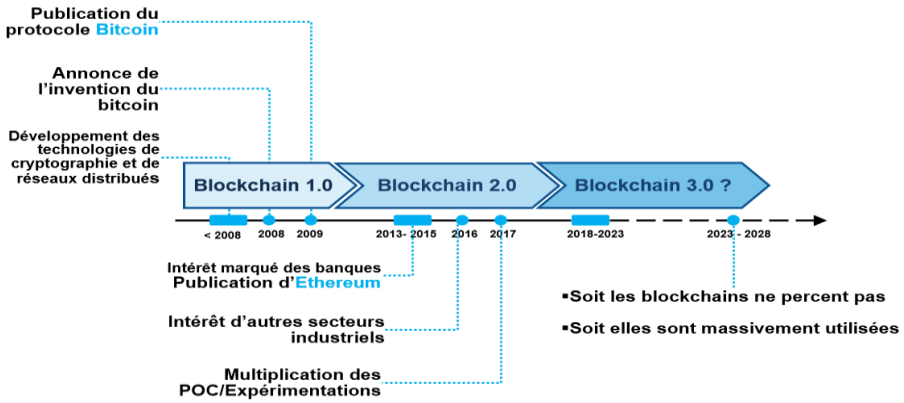



Figure 1 - Évolution des technologies blockchain

## Architecture générique

La Figure 2 montre une architecture blockchain générique organisée en niveaux[5]. Les composantes représentées par des rectangles bleus font partie des technologies Blockchain 1.0. Les composantes représentées par des rectangles blancs sont développées dans le contexte des évolutions suivantes. Bien que les composantes de la Blockchain 2.0 s'appuient sur des concepts de base déjà bien établis, elles montrent un niveau de maturité globalement encore assez modeste.

5 Architecture inspirée de l'article *Security and Privacy on Blockchain*, Rui Zhang, Rui Xue et Ling Lui, ACM Computing Survey, juillet 2019.

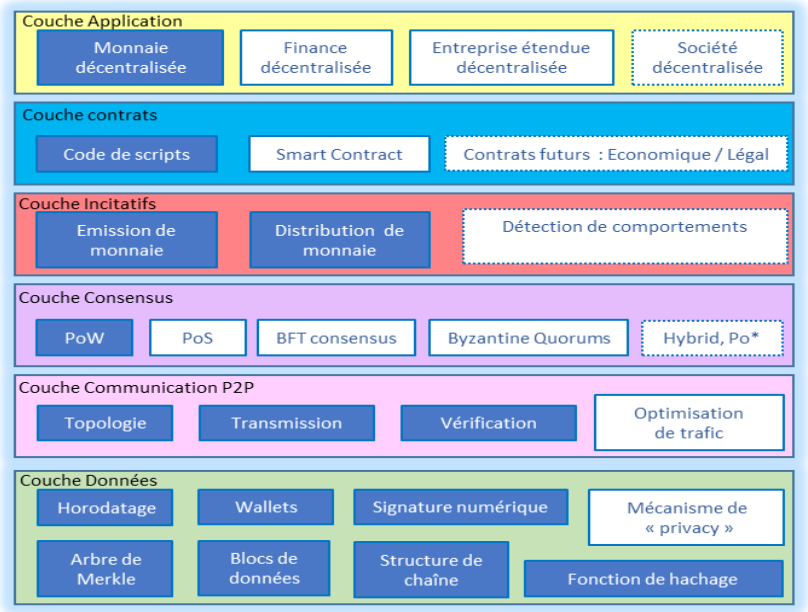



Figure 2 - Architecture générique d'un système Blockchain

Les composantes en pointillés sont encore très prospectives, évoquant des sujets de recherche pour les années à venir qui seront naturellement explorés une fois les verrous que nous avons identifiés levés.

### 2.1.3 Les applications et le rôle de la blockchain

La mission a opté pour un référentiel des usages adapté à l'analyse des verrous. Le choix s'est porté sur le référentiel décrit dans l'article « Panorama des applications des blockchains à l'énergie », de Gilles Deleuze & Sara Tucci-Piergiovanni, paru dans la « Revue de l'Électricité et de l'Électronique, Numéro 2, 2018 ». Ce référentiel présente une cartographie des applications attendues par l'utilisation de chaînes de blocs.

Les applications y sont classées sur l'axe vertical en fonction du niveau d'innovation apporté. Du bas en haut la complexité des validations et calculs requis exécutés par la blockchain augmente. Cette complexité dérive du rôle joué ou usage, qui va de simple Notaire (ou Auditeur) sur le premier niveau, à Banquier, *Trader* et jusqu'à *Coach* pour des gouvernances décentralisées et leur optimisation. Sur l'axe horizontal, les applications sont classées en fonction de la complexité de l'interaction nécessaire pour réaliser le rôle joué dans l'application donnée. Les questions de sécurité se durcissent potentiellement de gauche à droite.

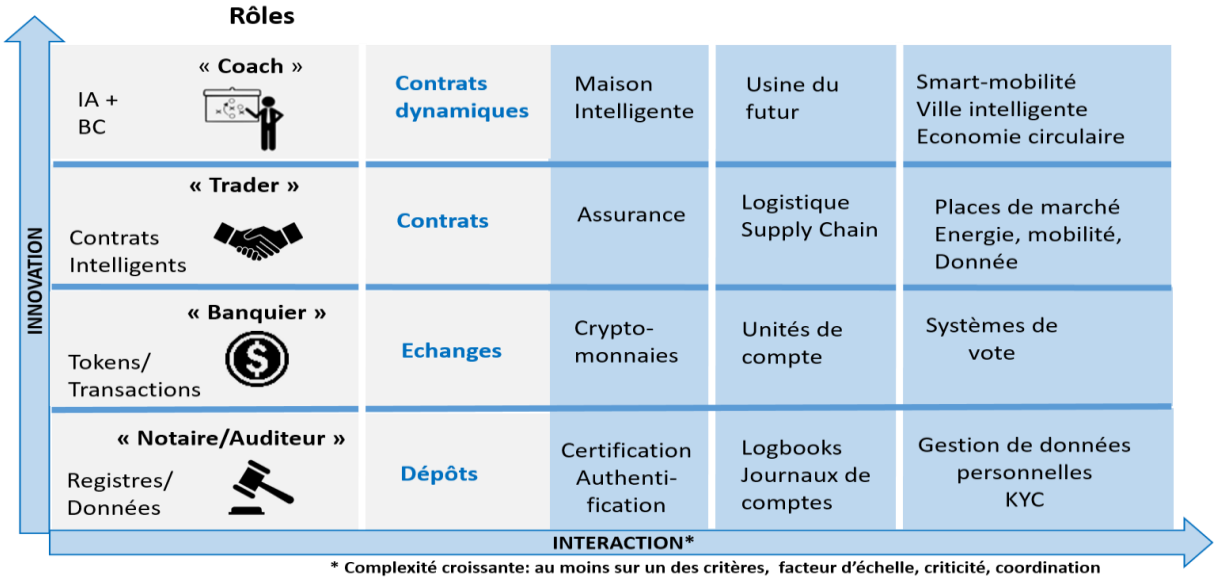



Figure 3 - Cartographie des usages

Aujourd'hui, les blockchains sont utilisées à un niveau assez élémentaire, « Notaire », comme moyen de traçabilité où la blockchain a un rôle de coffre-fort hautement disponible. Souvent, on y enregistre des données à archiver ou des empreintes (signatures) de ces données, comme pour des diplômes ou des actes notariaux, par exemple. La blockchain n'a pas un rôle actif dans ce cas, la validation d'un enregistrement consiste à vérifier uniquement la validité de la signature de l'émetteur. Pour aller un peu plus loin, certaines applications à ce niveau emploient des *smart contracts* élémentaires pour effectuer des opérations de régularisation ou facturation, par exemple. Ces opérations sont faites sur des flux des données enregistrés. Ces flux (par exemple une production ou une consommation) sont souvent produits par des sources externes (appelées oracles). La plupart des usages actuels se placent à ce niveau.

Le niveau « Banquier » se caractérise par le déploiement de crypto-monnaies comme alternative à d'autres systèmes de paiement. Il correspond aussi à la création de crypto-monnaies dédiées au financement et à la promotion de moyens de production particuliers pour des services et produits. Des usages de blockchains existent à ce niveau mais ils demeurent encore très limités. Les transactions entre utilisateurs se généralisent à tout type d'échange d'actifs représenté par un équivalent numérique (ce que l'on appelle la *tokenisation*). Les échanges entre types d'actifs se placent également à ce niveau.

Le niveau « *Trader* » prévoit l'utilisation de contrats intelligents avancés pour gérer des conditions de facturation complexes et l'application des termes et conditions d'un contrat. Un contrat intelligent à ce niveau peut couvrir également la phase de négociation entre utilisateurs, qui mènerait à un accord entre parties. Cela signifie que, par exemple, les utilisateurs pourraient conclure des marchés sur la base d'offres et demandes variables, ou au travers d'enchères.

Le dernier niveau « *Coach* » remplit des fonctions d'optimisation et d'analyse décisionnelle, éventuellement à base d'intelligence artificielle distribuée. Les utilisateurs, au travers des algorithmes d'intelligence artificielle, pourront modifier des règles et des comportements pour améliorer les objectifs globaux d'une communauté, par exemple. Pour ce faire les contrats intelligents devront intégrer des capacités d'auto-adaptation, d'où le lien avec l'intelligence artificielle.

### 2.1.4 Méthode de classification des verrous

Dans ce rapport, nous proposons une méthode d'analyse et de classification des verrous illustrée dans la figure 4 ci-dessous.

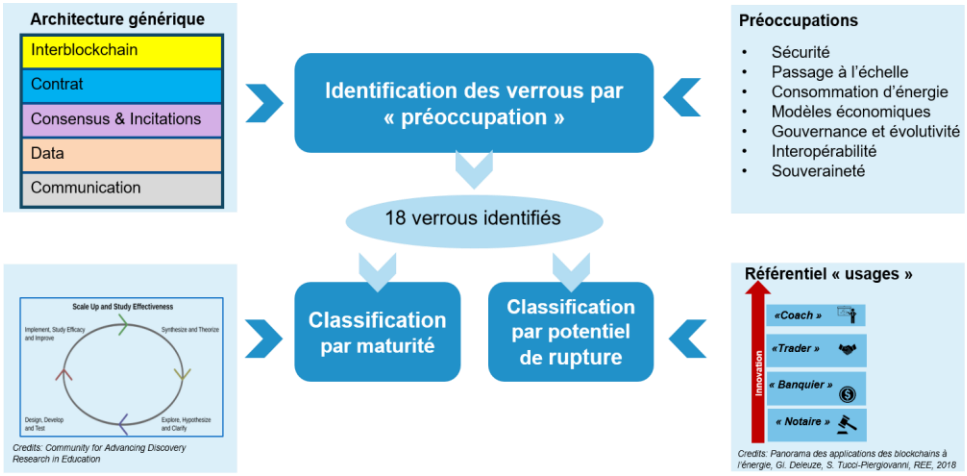



Figure 4 - Méthode de classification des verrous

Nous appellerons *préoccupation* (*concern* en anglais) les notions suivantes :

- sécurité,
- passage à l'échelle,
- consommation énergétique,
- modèles économiques,
- gouvernance et évolutivité,
- interopérabilité,
- souveraineté.

Nous appellerons *composante technique* les composantes de l'architecture en Figure 2. Nous ne traiterons pas directement la couche application, mais nous identifierons les verrous des composantes techniques support (*enabling*) à ce niveau : les protocoles entre blockchains et oracles (les sources d'information externes aux blockchains). Voici donc les composantes traitées :

- données,
- consensus,
- incitations,
- smart contracts,
- protocoles entre blockchains.

Chaque préoccupation sera déclinée sur une ou plusieurs composantes techniques, selon la pertinence. Cette déclinaison donnera lieu à un ou plusieurs verrous.

Un verrou peut être ensuite décliné en scientifique ou technologique selon son positionnement dans le graphique en Figure 5 (origine *Community for Advancing Discovery Research in Education*).

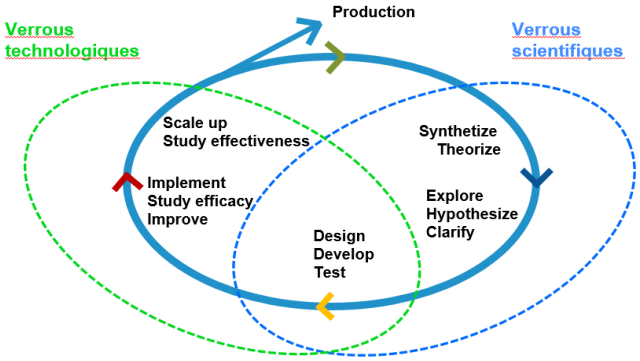



Figure 5 - Cycle de Recherche et d'Innovation

Un verrou qui se positionne dans les deux premières phases du cycle de R & I nécessitera surtout l'implication des scientifiques et de la recherche de base pour être levé, il est donc qualifié comme scientifique.

Pour la troisième phase « Design, Develop, Test », le cadre théorique et les solutions existent mais n'ont pas encore été appliquées au domaine d'intérêt — dans notre cas à la blockchain. Nous verrons que la plupart des verrous identifiés se positionnent dans cette phase. C'est une phase charnière, ici la levée d'un verrou a besoin à la fois de la recherche (qui se fait ici de manière plus appliquée par rapport aux phases précédentes), mais également de la forte implication 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, ainsi que des industriels. Dans cette phase, un verrou peut-être qualifié à la fois de scientifique et technologique.

Dans les dernières deux phases, nous qualifierons les verrous comme technologiques, car il s'agit plutôt de passer d'un prototype à un produit ou service commercialisé.

Il est important de souligner que ce qui est présenté est un chemin de principe et que finalement l'intervention de différents acteurs dans tout le cycle est beaucoup plus fluide en réalité : certains grands groupes industriels peuvent disposer d'une R & D avancée bien impliquée dans la levée de verrous plus scientifiques, ou alors être uniquement utilisateurs de technologie et intervenir plus tard dans la phase « *scale-up* », par exemple. Nous pensons, toutefois, que ce chemin de principe nous permet d'analyser plus aisément les verrous en termes d'intensité de la recherche, d'horizon temporel et d'acteurs à mobiliser.

Une fois les verrous identifiés, nous allons les projeter sur le cycle de R & I dans la section 2.10. Puis nous les évaluerons par rapport à leur potentiel d'innovation dans le chapitre 3. Pour ce faire, nous allons les positionner dans la cartographie des usages proposée dans la Figure 7. Cela permettra de mieux comprendre la portée de la levée d'un verrou en termes de rupture tout en suggérant leur priorisation.

## 2.2 La sécurité

La sécurité est une préoccupation majeure. Une blockchain par sa nature doit remplir son rôle de manière décentralisée, une blockchain de confiance doit le faire sans défaillances. Cela signifie qu'il est demandé à une blockchain, à partir de son usage le plus élémentaire, i.e. « Notaire », de :

1. servir des communautés étendues et ouvertes en réseau ;
2. être disponible et cohérente : répondre à un utilisateur dans un temps raisonnable et sans erreur logique ;
3. préserver la confidentialité des échanges et l'identité des utilisateurs, tout en permettant aux échanges d'être vérifiables.

De plus, l'interaction avec d'autres blockchains ou oracles doit être également sécurisée.

On juge la première capacité « servir des communautés étendues et ouvertes en réseau » comme indispensable. Sans cette capacité, les technologies décentralisées de confiance ne pourront pas atteindre le niveau de rupture promis. Autrement dit, les technologies qui ne visent pas à remplir cette capacité au niveau de leur conception ne sont pas jugées en rupture.

Par la suite, nous abordons les verrous de sécurité liés aux algorithmes de consensus du point de vue essentiellement de leur disponibilité et de leur cohérence, aux contrats intelligents et aux oracles. Les verrous liés aux mécanismes cryptographiques qui sont utilisés pour garantir la confidentialité sont également présentés.

### 2.2.1 Consensus

Le consensus est clairement la clé de voûte d'un système de chaîne de blocs. Dans cette section, nous examinons les consensus en les comparant principalement en fonction de leurs garanties en termes de cohérence et de disponibilité. Les questions liées à la consommation d'énergie du consensus à base de preuve de travail sont abordées en Section 2.4. Cependant, nous constatons que pour que les chaînes de blocs puissent percer dans l'industrie, dans une vision développement durable de la société, des alternatives convaincantes à la preuve de travail doivent être trouvées. La recherche se concentre donc naturellement sur ces alternatives à la preuve de travail, et c'est pourquoi nous nous sommes concentrés dans ce rapport sur les verrous liés à ces alternatives.

Les questions de concentration du pouvoir de vote sont spécifiques au type de consensus utilisé (preuve de travail, preuve d'enjeu, etc.). Elles sont longuement discutées dans l'Annexe A, où nous abordons les questions d'équité et censure des transactions, et sont reprises dans le contexte de la souveraineté en Section 2.8 et des modèles économiques en Section 2.5.

## Les mécanismes de consensus dans les blockchains

VERROU 1 : Des preuves de sécurité pour les alternatives à la preuve de travail.
*Verrou scientifique dans la phase « design, develop, test »* (cf. Figure 5).

Chaque technologie blockchain propose un mécanisme de consensus différent, d'où la difficulté d'être exhaustif et de pouvoir les comparer. À savoir qu'un mécanisme de consensus idéal combinant toutes les propriétés souhaitées ne peut exister à cause du théorème CAP[6] et donc des compromis doivent être trouvés entre cohérence, disponibilité et tolérance aux partitions. Dans cette section nous présentons de manière succincte les avantages et les inconvénients des solutions existantes, la description détaillée de ces solutions et leur relation au théorème CAP sont présentées en Annexe A. Dans notre analyse, nous avons également pris en compte la maturité de ces technologies.

### Les technologies à preuve de travail

**Avantages :**

- servent des communautés étendues et ouvertes en réseau ;
- bonne maturité technologique pour Bitcoin.

**Inconvénients :**

- temps de réponse longs, volume de transactions servies limité ;
- la sécurité dépend de comportements socio-économiques de prédiction difficile, mais des études sont disponibles[7] et le système fonctionne en pratique ;
- la non fiabilité du réseau de communication peut compromettre la cohérence du registre ;
- consommation énergétique.

### Les technologies à preuve d'enjeu

**Avantages :**

- servent des communautés étendues et ouvertes en réseau ;
- résolvent le problème de la consommation énergétique ;
- un meilleur temps de réponse.

**Inconvénients :**

- la sécurité dépend de comportements socio-économiques qui n'ont pas été suffisamment étudiés ;
- la non fiabilité du réseau de communication peut compromettre la cohérence du registre;
- en cours de développement.

6 Nancy Lynch and Seth Gilbert. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. 2002

7 Bruno Biais et al. The Blockchain Folk Theorem. 2018

### Les technologies à base de consensus BFT

**Avantages :**

- la corruption du registre ne dépend pas de la fiabilité du réseau de communication ;
- maturité technologique atteinte pour certaines solutions (Hyperledger Fabric, par exemple).

**Inconvénients :**

- ne servent pas des communautés étendues et ouvertes en réseau. Cela implique que ces technologies sont déployées sur réseau privé ou de consortium de petite taille.

### Les technologies à base de consensus BFT couplés à la preuve d'enjeu

**Avantages :**

- servent des communautés étendues et ouvertes en réseau ;
- sécurité assurée par des « comités de validateurs », où le bloc est produit au travers d'un algorithme de Consensus BFT : la corruption du registre ne dépend pas de la fiabilité du réseau de communication.

**Inconvénients :**

- la sécurité dépend de comportements socio-économiques qui n'ont pas été suffisamment étudiés ;
- en cours de développement.

### Conclusions

L'analyse de l'état de l'art (voir Annexe A) permet de constater que les solutions alternatives à la preuve de travail émergent avec des principes de conception intéressants mais elles doivent encore être validées. Plus particulièrement, la mise en œuvre de la sélection et du renouvellement des comités de validateurs est aujourd'hui un défi majeur de ces solutions en ce qui concerne leur sécurité. À cela s'ajoute la difficulté de comprendre l'impact des mécanismes d'incitations sur le comportement des comités dans le temps (point en lien avec les verrous 9 et 10 de la section Modèles et mécanismes économiques).

### 2.2.2 Réplication légère

VERROU 2 *:* Réplication « légère » dans un environnement dynamique.

*Verrou scientifique dans la phase « design, develop, test »* (cf. Figure 5).

Par réplication légère, nous entendons une réplication qui puisse être réalisée sur un réseau asynchrone[8]. Il faut bien noter que n'importe quel objet informatique (ou type de donnée) peut être répliqué en utilisant un algorithme de consensus, toutefois un algorithme de consensus tolérant aux pannes ne peut pas être implémenté sur un réseau asynchrone (résultat d'impossibilité FLP[9]). La recherche de types de données[10] qui ne requièrent pas de résoudre le problème du consensus, tout en étant pertinent pour la construction des applications blockchains est donc d'actualité. Cependant il faut mitiger la portée des résultats atteints jusqu'ici. Les algorithmes de réplication légère fonctionnent bien si l'ensemble des nœuds (répliques) est fixé. Dans un environnent dynamique, la question des performances et de la sécurité de ce type de réplication reste un problème ouvert.

### 2.2.3 Mécanismes cryptographiques

VERROU 3 : Méthodes cryptographiques avancées pour la protection de la privacy et la confidentialité.

*Verrou scientifique entre les phases phase « explore, hypothesize, clarify » et « design, develop, test »* (cf. Figure 5).

Dans les blockchains de première et seconde génération, la vérifiabilité publique des transactions (voir 2.1.1) repose principalement sur leur *reproductibilité*, ce qui impose que les données correspondantes soient *publiées sur la blockchain*. Ceci entre en conflit avec d'une part la réglementation européenne (RGPD) lorsqu'il s'agit de données personnelles – comme les pièces d'identité exigées par les mesures contre la corruption – et d'autre part avec les intérêts stratégiques lorsqu'il s'agit de données commerciales sensibles, comme un inventaire ou un carnet de commande.

Les acteurs que nous avons auditionnés traitent ces conflits soit en délégant le traitement des données sensibles à un tiers de confiance, soit en optant pour une blockchain privée (en particulier dans les cas des données commerciales). Ces palliatifs ne permettent donc pas de réaliser entièrement la promesse de transparence et de confiance associée aux blockchains.

Ce verrou est en fait dû à l'utilisation limitée de la cryptographie dans les blockchains actuelles : hachage et signature électronique, qui permettent seulement d'assurer l'intégrité du registre distribué et l'authenticité des ordres de transaction. Il semble possible de le lever en ayant recours

8 Un réseau asynchrone est un réseau dans lequel aucune hypothèse n'est faite sur le temps maximal de diffusion des messages (il est fini mais pas connu par les nœuds du réseau).

9 Fischer, Lynch, Patterson. *Impossibility of Distributed Consensus with One Faulty Process,* 1985

10 Le registre est un type de donnée, la crypto-monnaie est un type de donnée, ainsi que les contrats intelligents (l'objet répliqué est soit le contrat soit les données manipulées par le smart contract).

à des techniques cryptographiques plus sophistiquées, qui permettent de vérifier la correction des transactions sans avoir accès à leurs données sensibles. On peut citer :

- la **preuve sans divulgation** (*zero-knowledge proof - ZK*)[11], qui permet d'avoir une garantie probabiliste de l'existence d'une preuve d'une affirmation (par exemple, la nationalité d'une personne) sans rien révéler de cette preuve (par exemple, l'identité de la personne) ;
- le **transfert aveugle** (*oblivious transfer - OT*)[12] qui permet d'accéder à une base de données sans révéler la donnée lue ;
- le **calcul multi-parties** (*multi-party computation – MPC*)[13] qui permet d'effectuer un calcul combinant les données de plusieurs entités sans révéler aux unes et aux autres, autre chose que la partie du résultat qui les concerne ;
- la **vérification probabiliste de preuve** (*probabilistically checkable proof*)[14] qui permet de produire un certificat de validité probabiliste *de taille constante* d'une preuve arbitraire.

Bien que beaucoup de ces techniques soient trop coûteuses à mettre en œuvre pour être appliquées directement aux blockchains, des travaux plus récents ont identifié des combinaisons plus efficaces. En particulier, les ZK-SNARKs (*zero-knowledge succint non-interactive arguments of knowledge*)[15] fournissent des certificats compacts vérifiant la correction de transactions simples. Cette technologie est utilisée pour réaliser le paiement confidentiel dans la blockchain Zcash, et est ou va être supportée par les *smart contracts* Ethereum et Tezos – de ce fait elle entre plutôt dans la phase « implement, study efficacy, improve » (cf. Figure 5).

Cependant, la technologie SNARK a quelques limitations : d'une part elle impose de limiter *a priori* la taille des calculs de vérification (Zcash utilise un mécanisme auxiliaire pour contrôler l'absence de double dépense), et pour des raisons d'efficacité, elle utilise un aléa pré-calculé (*common reference string – CRS*) qui fixe la taille des transactions en plus d'être une faiblesse potentielle (Zcash le calcule par MPC avec des ordinateurs qui sont ensuite détruits par le feu !). La recherche scientifique visant à lever ces limitations est toujours très active. Parmi les nombreuses nouvelles propositions on peut citer :

- les preuves récursives, implémentées dans Coda[16], qui appliquent les SNARK à eux-mêmes ;
- les STARK (*succint transparent argument of knowledge*)[17] qui utilisent aussi un schéma récursif, mais ce schéma ne fait plus appel aux courbes elliptiques et est donc résistant aux ordinateurs quantiques ;
- les engagements de Pedersen (*Pedersen commitments*)[18], implémentés dans le protocole Mimble-Wimble, qui permet de garantir plus simplement la confidentialité des transactions purement monétaires.

---

11 S. Goldwasser, S. Micali, C. Rackoff. « The knowledge complexity of interactive proof-systems. » STOC '85.

12 G. Brassard, C. Crépeau, J.-M.Robert. « All-or-nothing disclosure of secrets. » CRYPTO '86.

13 A. C. Yao. « How to generate and exchange secrets. » SFCS '86.

14 S. Arora, S. Safra. « Probabilistic checking of proofs: A new characterization of NP. » JACM 1998.

15 Parno, Howell et al. « Pinocchio: nearly practical verified cryptography. » Cryptology ePrint Archive 2013.

16 Bowe, Sean et al. « Halo: Recursive Proof Composition without a Trusted Setup. » Cryptology ePrint Archive 2019.

17 Ben-Sasson, Nemtov et al. « Scalable, transparent, and post-quantum secure computational integrity. » Cryptology ePrint Archive 2018.

18 Fuchsbauer, Orrù, Seurin. « Aggregate Cash Systems: A Cryptographic Investigation of Mimblewimble» Cryptology ePrint Archive 2018.

Si la recherche française est bien active sur ces sujets (en particulier, Mimble-Wimble est une proposition française), elle est loin d'avoir l'envergure de ses concurrents américains ou israéliens. En outre, les sociétés que nous avons auditionnées ne semblent pas très sensibles à l'émergence probable de ces technologies et courent donc le risque de se faire doubler par des concurrents sur ce sujet. Ceci serait d'autant plus regrettable que plusieurs ont souligné que la réglementation européenne créait de fait un vrai marché pour des solutions blockchain plus respectueuses de la confidentialité.

Nous n'avons pas retenu comme verrou la question de la protection et de la récupération des clés cryptographiques, parfois soulevée lors de nos auditions, parce qu'elle n'est pas spécifique aux blockchains, et qu'elle est résolue par l'état de l'art – la société française Ledger est même un *leader* du secteur. De même nous n'avons pas retenu la résistance aux ordinateurs quantiques, qui n'est pas encore d'actualité et n'est pas non plus spécifique aux blockchains.

### 2.2.4 Contrats intelligents

VERROU 4 : La vérification de la correction des contrats intelligents.

*Verrou technologique entre la phase « design, develop, test » et « implement, study efficacy, improve »* (cf. Figure 5).

VERROU 5 : Des langages pour les contrats intelligents plus expressifs.

*Verrou scientifique entre la phase « explore, hypothesize, clarify » and « design, develop, test »* (cf. Figure 5).

Les *smarts contracts*, ou *chaincodes* sont des programmes informatiques exécutés dans la blockchain. Leur particularité est d'être immuables une fois déployés. En effet un *smart contract*[19] une fois inséré dans un bloc ne pourra plus être modifié ni supprimé. Cette propriété engendre des problèmes de sécurité importants, car un *smart contract* mal codé pourrait être vulnérable à des attaques informatiques. Cela a été le cas pour le célèbre *theDAO* qui a été attaqué en causant la perte d'une somme de crypto-monnaie considérable. Si la correction des *smart contracts* est donc un verrou majeur, il est important de souligner que la plupart des attaques ont ciblé des bogues ou des vulnérabilités de la plateforme d'exécution[20]. La question de la sécurité des *smart contracts* est d'autant plus importante que les applications industrielles seront encodées sous formes de nombreux *smart contracts*.

Pour aller au-delà d'une preuve de concept, il sera opportun de considérer le développement des *smart contracts* avec des précautions similaires à celles prises pour le développement des codes critiques. Une plateforme pour des applications critiques aurait d'un point de vue technique besoin d'un langage d'entrée vérifiable ainsi que d'une chaîne de compilation prouvée et d'un environnement d'exécution sécurisé.

Les tests sont déjà omniprésents dans ce domaine mais les techniques de vérification formelles en sont encore à leurs balbutiements en ce qui concerne leur application aux langages de *smart*

19 Nous adopterons cette orthographe dans la suite pour souligner qu'il s'agit d'un objet spécifique.

20 N. Atzei, M. Bartoletti, and T. Cimoli. A survey of attacks on ethereum smart contracts sok. In Conference on Principles of Security and Trust -2017.

*contracts*. La plupart des tentatives ciblent Solidity, un langage pour la plateforme Ethereum mais aucun cadre de vérification entièrement fonctionnel n'est toujours disponible. De plus, Solidity et Ethereum ne sont pas les cibles idéales pour la vérification car il n'y a pas de sémantique claire prédéfinie pour Solidity, et même pour le EVM (Ethereum virtual machine), les tentatives de définition de la sémantique formelle ne sont que des avancées très récentes[21].

En termes de sûreté, les langages fortement typés sont sûrement à privilégier. Dans cette catégorie nous pouvons citer Michelson, le langage de *smart contract* de bas niveau de Tezos qui est un langage fonctionnel statiquement typé dont le système de type et l'implémentation de son interpréteur ont été validés à l'aide d'outils OCaml. Cependant, l'écriture et l'audit des programmes de Michelson sont considérés comme laborieux par la plupart des utilisateurs et plusieurs langages de plus haut niveau sont en cours de développement.

Dans la catégorie des langages fortement typés, nous pouvons également citer Plutus, le langage de *smart contract* de la plateforme Cardano, qui est un langage purement fonctionnel.

Par rapport aux langages pour l'écriture de smart contract, aujourd'hui nous devons admettre qu'il y a un écart considérable entre un contrat rédigé ou compris par un juriste et un *smart contract*. Un *smart contract* est un morceau de code écrit dans un langage de programmation (généraliste comme Java, Go ou spécialisé comme Solidity), bien loin des concepts juridiques. Les contrats intelligents sont d'ailleurs largement surestimés dans la compréhension générale, car ils sont considérés comme un mécanisme potentiel pour appliquer automatiquement un contrat au sens juridique du terme (*enforceability*), mais, de ce point de vue, les contrats intelligents ne sont pas plus puissants qu'une simple journalisation de preuve. Les *swap atomiques* (cf. Annexe B) sont plus puissants de ce point de vue car ils peuvent assurer qu'un transfert est fait si seulement si un autre transfert (par exemple d'un autre actif numérisé) est vraiment réalisé. Toutefois, ces mécanismes sont capables d'appliquer des conditions encore rudimentaires et la recherche est à poursuivre pour avoir des langages de *smart contract* qui les rapprochent de vrais contrats.

Ces langages pourront/devront cibler l'écriture d'applications qui s'exécutent sur plusieurs blockchains (comme pour les *swaps atomiques*), cette piste de recherche est en lien également avec le verrou 15 qui vise à lever le verrou de la validation des applications ou services distribués.

21 E. Hildebrandt et al. Kevm: A complete Formal Semantics of the Ethereum Virtual Machine. 2018.

### 2.2.5 La question des oracles

VERROU 6 : Des oracles avec des méthodes de redondance et de vote.

*Verrou technologique dans la phase « scale up, study effectiveness »* (cf. Figure 5).

La liaison monde réel (oracles) et blockchain est vulnérable. Un capteur défaillant, par exemple, pourrait engendrer l'enregistrement d'une donnée « fausse » qui pourrait ensuite avoir des répercussions sur tout le système (par exemple mauvaise facturation ou prise de décision). À noter que ce point est général à tout système cyberphysique et qu'il est potentiellement aggravé par les éventuelles implications financières d'une transaction et le manque de preuves de la capacité d'un *smart contract* à gérer des défaillances d'oracle. Des solutions de redondance et de qualification des données sont connues[22], et doivent être appliquées de manière systématique. Il s'agit de consolider les pratiques et créer des bibliothèques de *smart contract* standards, qui sachent gérer cette liaison. De plus, un service d'identité numérique pourrait permettre de certifier les sources.

## 2.3 Le passage à l'échelle

VERROU 7 : Des approches de passage à l'échelle à consolider.

*Verrou scientifique dans la phase « design, develop, test »* (cf. Figure 5).

Par passage à l'échelle, nous entendons ici la capacité d'un système à modifier la taille ou le volume de ses ressources pour s'adapter à la charge de travail générée par les utilisateurs.

Dans les blockchains, cette charge est représentée par le volume de transactions, tandis que les ressources sont les validateurs et/ou les blocs[23]. Dans Bitcoin, par exemple, les validateurs sont les mineurs qui traitent les transactions en les validant et en les incluant dans des blocs. Il convient de noter que dans Bitcoin, étant donné que la vitesse de création et la taille de blocs au fil du temps ne changent pas, le système ne traite pas le passage à l'échelle en tant que tel. Une stratégie de passage à l'échelle consisterait à multiplier les ressources et à répartir la charge sur les ressources disponibles.

Nous décrivons dans la suite deux types d'approches : les approches par « *sharding* » d'une part et les approches par « chaînes latérales » d'autre part.

#### Le sharding

Dans les approches dites « de *sharding* par les comités » (Omniledger, RapidChain, Elastico, par exemple) une ressource est un groupe de validateurs appelé comité. Un protocole de *sharding* crée des comités, attribue chaque nœud à un comité et supprime des comités. La charge globale est ainsi éclatée en morceaux (*shard*) et chaque transaction est dirigée vers son comité. L'inconvénient de ces approches est la gestion de transactions « *cross-shard* » : les transactions

22 Gurcan et al. *An Industrial Prototype of Trusted Energy Performance Contracts Using Blockchain Technologies*, 2018.

23 Plus précisément les « ressources » sont toutes les ressources impliquées dans le mécanisme de consensus lui-même.

qui doivent être validées par différents comités. La mise en cohérence de ces transactions se fait selon un protocole spécifique (de type « *atomic commit* »), ce qui représente une difficulté supplémentaire de mise en œuvre et une potentielle perte de performances.

Une autre approche, dite de « sharding par les chaînes » consiste à multiplier les chaînes pour s'adapter à la charge. Lorsque la charge augmente la chaîne est fractionnée et ensuite, lorsque la charge diminue, les fragments sont fusionnés[24]. Ces approches, qui consistent d'une certaine manière à imiter le comportement de la chaîne Bitcoin, tout en adaptant les ressources, ne présentent pas les problématiques liées au traitement des transactions en conflit du *sharding* par comité.

Globalement, le *sharding* semble une bonne piste de travail, cependant les protocoles par comité sont complexes à concevoir (à cause de la gestion des transactions « *cross-shards* ») et il serait donc bon d'analyser avec précision si les propriétés de sécurité sont toujours bien respectées.

Les approches de *sharding* par les chaînes sont intéressantes, plus simples et plus innovantes. Il serait intéressant de voir si ces approches s'appliquent à des chaînes construites *via* des mécanismes de consensus plus économes en énergie que la preuve de travail.

### Les chaînes latérales

Ces approches sont complémentaires aux approches précédentes. Il s'agit ici de réduire la charge en en détournant une partie sur d'autres chaînes connectées, dites latérales. L'état de l'art de ces protocoles, qui est analysé dans l'Annexe B et dans la section 2.7.1, met en exergue l'immaturité de ces protocoles et l'absence de validation.

## 2.4 Consommation énergétique

VERROU 8 : Des méthodes de mesure de la consommation énergétique.

*Verrou scientifique/technologique dans la phase « design, develop, test »* (cf. Figure 5).

La sécurité d'une blockchain à preuve de travail repose sur le *minage*. Cette activité, consommatrice en énergie, a suscité une série d'articles alarmistes. Par exemple, les experts du média américain Digiconomist[25] estiment que chaque transaction en Bitcoins aurait une empreinte carbone de 314 kg de $CO_2$ et que la consommation du seul réseau Bitcoin serait de 73.12 TWh par an, comparable à celle de l'Autriche.

Cette polémique doit cependant être nuancée[26]. Premièrement, il n'y a pas d'estimation aisée et précise de cette consommation. Digiconomist, par exemple, fonde son calcul sur le hashrate (GH/s) et le cours du BTC. Il suppose que lorsque le BTC grimpe, le nombre de fermes de minage augmente, ce qui n'est pas prouvé. De plus, il ne semble pas prendre en compte la diminution régulière de la puissance électrique requise pour un GH/s, liée à la loi de Moore. L'estimation est très sensible à la proportion entre les types de matériels. Pour une année donnée, l'écart entre la performance d'un hardware standard d'un hardware dédié, tous deux à état de l'art, est de l'ordre de 1000. La seule présence de 1 % du *hardware* dédié change complètement la consommation

24 Anceaume et al. Sycomore : a Permissionless Distributed Ledger that self-adapts to Transactions Demand. 2018

25 https://digiconomist.net/bitcoin-energy-consumption

26 Deleuze & Tucci-Piergiovanni. Revue de l'Électricité et de l'Électronique, Numéro 2, 2018.

d'énergie. Ainsi, une estimation plus récente, qui considère que seules des fermes de minage équipées de *hardware* de dernière génération fonctionnent durablement à une date donnée, serait plutôt de autour de 9 TWh.

Deuxièmement, cette consommation d'énergie s'inscrit dans la hausse globale des besoins en énergie des technologies numériques. Il est également intéressant de rapporter cette consommation à celle de l'ensemble de ces technologies. Selon le rapport « The Cloud begins with Coal »[27], l'informatique « dans les nuages » représente à elle seule 416 TWh, soit à peu près l'empreinte carbone de toute l'industrie aéronautique, et elle croît rapidement : elle double sa consommation d'énergie tous les quatre ans. D'ici 2030, celle-ci pourrait atteindre 1400 TWh par an et dépasser la Chine et les États-Unis, les plus gros consommateurs d'électricité au monde.

Le véritable point faible des blockchains publiques à preuve de travail n'est en fait pas la consommation globale, mais la consommation par transaction. Pour le Bitcoin, avec une estimation basse à 250 MW de consommation globale et un volume entre 4 et 7 transactions par seconde, la consommation par transaction varie entre 10 et 18 kWh. Il est intéressant de noter aussi que ce coût pourrait être réduit par des techniques de *sharding* telles que présentées dans la section 2.3 sur le passage à l'échelle.

Ce court état de l'art met en exergue que nous ne disposons pas de modèles précis de consommation et que donc établir des méthodes précises pour l'estimation de la consommation énergétique pour les blockchains, et plus généralement pour les technologies numériques, est certainement un verrou à lever. Cela permettra de comparer plus aisément et sans biais des solutions blockchains entre elles et vis-à-vis de technologies centralisées plus traditionnelles.

D'un point de vue plus applicatif, il sera intéressant de dresser des profils énergétiques de tout *smart contract* s'exécutant de multiples fois à des fins de maîtriser et optimiser cette consommation.

Cette question de la consommation énergétique prendra aussi une importance considérable quand il s'agira d'opérer des applications blockchain sur des nœuds qui doivent absolument la minimiser, typiquement dans l'Internet des objets (IoT)

27 *The Cloud begins with Coal*, Digital Power Group, 2013.

## 2.5 Modèles et mécanismes économiques

### 2.5.1 Les modèles

VERROU 9 : Des modèles économiques pour les blockchains.

*Verrou scientifique entre la phase « synthesize, theorize » et « explore, hypothesize, clarify »* (cf. Figure 5).

Par modèle économique, nous entendons un modèle mathématique qui peut prédire certains paramètres d'intérêt (prix d'une crypto-monnaie, consommation d'énergie, coût de transaction, etc.). Par exemple, les crypto-monnaies sont des objets plus complexes à modéliser que les monnaies fiduciaires, en raison de la présence de facteurs techniques tels que les vulnérabilités et les attaques.

La recherche de modèles prédictifs a intéressé à la fois les économistes et les informaticiens, mais d'une manière différente. Tous deux ont analysé les chaînes de blocs avec leurs méthodes préétablies, qui ne pouvaient sans aucun doute que modéliser finement certains aspects, et moins bien d'autres. Cela explique, au moins en partie, pourquoi les économistes ont été principalement intéressés par Bitcoin, et beaucoup moins par les chaînes de blocs qui utilisent des protocoles de consensus plus complexes, difficiles à analyser sans l'aide d'informaticiens. Parmi les travaux disponibles sur Bitcoin, on peut citer les travaux visant à confirmer la stabilité du mécanisme de son consensus ou la prédiction de sa consommation énergétique. La question de la prédiction du cours d'une crypto-monnaie est également un sujet d'étude actif.

Les informaticiens ont exploré des aspects plus proches de leurs préoccupations, comme la question de l'équité ou de la censure des transactions. L'équité est considérée d'un point de vue informatique comme la capacité du système à traiter toutes les transactions émises par des clients honnêtes, évitant ainsi que certaines transactions soient rejetées. Il n'est pas surprenant que ces travaux aient confirmé que Bitcoin n'est pas « *fair* » de ce point de vue : les mineurs ont en effet tendance à choisir les transactions qui leur rapportent le plus de bénéfices, au détriment d'autres transactions. Des études provenant du monde de la cryptographie ont souligné que les mineurs peuvent non seulement choisir les transactions les plus intéressantes pour eux, mais aussi «voler» des transactions déjà confirmées rapportant des bénéfices majeurs, créant ainsi une branche de la chaîne.

Sur un plan plus théorique, les modèles économiques modélisent un agent comme stratégique (il suivra les règles d'un protocole seulement si cela maximise son gain), alors que dans le calcul réparti un agent est soit obéissant (il suit les règles) soit corrompu (il en dévie de manière arbitraire). Une harmonisation de ces concepts dans un modèle unique est une voie à poursuivre.

En conclusion, la recherche (interdisciplinaire) sur ces nouveaux modèles est assez récente et elle doit être poursuivie. Elle permettra d'analyser plus finement non seulement Bitcoin mais également d'autres blockchains publiques émergentes qui utilisent des alternatives à la preuve de travail (en lien avec le verrou 1) ainsi que des applications/*smart contracts* multi-blockchains évolués (en lien avec le verrou 15).

### 2.5.2 Les mécanismes

VERROU 10 : Des mécanismes économiques pour les blockchains.

*Verrou scientifique entre la phase « synthesize, theorize »* (cf. Figure 5).

Dans ce rapport, nous tenons à souligner que trouver un modèle pour prédire un phénomène est certes fondamental, mais il n'est pas totalement satisfaisant. Du point de vue d'un ingénieur, qui doit concevoir un nouveau mécanisme d'incitation et de vote pour une blockchain, un modèle pourra confirmer ou non la qualité de sa solution, mais il ne lui donnera pas une méthode pour trouver une autre solution plus satisfaisante. La branche de l'économie qui cherche un mécanisme pour atteindre un certain objectif est appelée *théorie des mécanismes d'incitation* (« *mechanism design* »). De toute évidence, puisque cette branche de l'économie s'est développée dans un contexte où le mécanisme est parfaitement mis en œuvre (par un gouvernement par exemple, ou par un arbitre), en ce qui concerne les blockchains cette théorie devra tenir compte du fait que le mécanisme sera implémenté de manière décentralisée. Ce verrou scientifique est le plus amont que nous avons identifié et il mérite une attention toute particulière ; le concept de *smart contract* sera central dans la mise en œuvre des mécanismes trouvés.

Nous soulignons que la capacité à lever ce verrou résidera uniquement dans la collaboration entre économistes, informaticiens et mathématiciens.

## 2.6 Gouvernance et évolutivité

VERROU 11 : Des méthodes pour la gouvernance des communautés.

*Verrou scientifique entre la phase « explore, hypothesize, clarify » et la phase « design, develop, test »* (cf. Figure 5).

L'objectif principal de la gouvernance dans les blockchains est d'améliorer la confiance entre les différents utilisateurs d'une blockchain. Bien que les blockchains soient souvent qualifiées de «réseaux sans confiance» car les transactions sont gérées par le système, en réalité la confiance est un facteur critique dans le succès d'une blockchain. Au lieu de faire confiance aux institutions, les utilisateurs doivent faire confiance aux parties prenantes, aux développeurs et à ceux qui sont techniquement qualifiés pour vérifier le code de la blockchain et des *smart contracts* utilisés. Il faut donc s'assurer que les utilisateurs et les fournisseurs de services blockchain sont d'accord sur les règles de gouvernance. Une blockchain sans gouvernance est peu susceptible d'atteindre ses objectifs commerciaux à long terme.

Techniquement, ce qui est désormais appelé *gouvernance de blockchain* est la façon dont les humains prennent les décisions qui affectent les chaînes de blocs, par le biais de mécanismes tels que les mises à jour de code informatique dont certaines peuvent entraîner des modifications de la chaîne (des éléments rajoutés à la blockchain après la mise à jour). Cette gouvernance peut être totalement centralisée et conservatrice (comme dans Bitcoin), ou plus décentralisée et ouverte (comme dans Ethereum), elle peut être *off-chain* et suivre des mécanismes variés et non préétablis

(comme dans Ethereum) ou alors *on-chain via* des mécanismes formalisés qui s'exécutent à l'intérieur de la plateforme elle-même, comme dans le cas de EOS et Tezos[28].

L'avantage des approches *on-chain* réside dans la transparence du processus d'évolution de la chaine et de sa démocratie potentielle. Pour bien comprendre la différence entre les deux approches, nous prenons l'exemple de la récompense de bloc Ethereum[29] : sur Ethereum les développeurs – institution de gouvernance – ont annoncé en septembre 2018 que, lors de la prochaine mise à jour, la récompense par bloc miné serait abaissée de 3 à 2 ETH. La communauté a dû accepter cette décision, même si les mineurs auraient préféré avoir la possibilité de voter ce choix. Dans EOS et Tezos, en revanche les modifications sont discutées et votées. Si la modification est acceptée alors chaque mineur appliquera la mise à jour.

Cependant, la question de garantir un processus démocratique et efficace dans les systèmes de gouvernance *on-chain* reste ouverte. Le théorème d'Arrow[30] par exemple souligne la difficulté de la prise de décision collective lorsqu'il existe au moins trois propositions alternatives. L'abstentionnisme est également un problème à gérer car cela peut réduire la légitimité de la proposition gagnante. La délégation du pouvoir de vote peut palier en partie ce problème, mais les mécanismes de délégation sont encore peu étudiés et il est difficile d'en prédire le comportement.

Il convient aussi de mentionner que les chaînes latérales (cf. Annexe B) promues par Ethereum (avec le projet Plasma) offrent un mécanisme pour faire évoluer les blockchains sans faire appel à un vote explicite *on-chain*. Une chaîne latérale enfant peut en effet être créée par quelques développeurs à partir d'une chaîne principale parent comme moyen d'explorer une nouvelle fonctionnalité. Si cette nouvelle fonctionnalité de la chaîne enfant s'avère populaire, la chaîne principale peut éventuellement être abandonnée en déplaçant tous les actifs vers la chaîne enfant, qui peut devenir la nouvelle chaîne principale.

En conclusion, plusieurs solutions sont proposées au travers de projets comme Ethereum, EOS et Tezos, cependant, il n'y a pas encore une méthode de gouvernance qui fasse l'unanimité, c'est pour cela que nous identifions un verrou à ce niveau. Il serait intéressant de poursuivre des études technico/sociales sur les comportements des communautés blockchains pour y voir plus clair et établir des méthodes de gouvernance décentralisée, efficaces et résilientes.

Il est également important de souligner que l'établissement des méthodes d'évolution de codes blockchains implique un certain niveau de modularité de l'architecture et du logiciel (cf. 2.9) pour que la proposition d'une évolution soit possible et « *backward* compatible ». Cette modularité est typiquement mise en avant dans la plateforme Tezos, par exemple.

28 Nous traitons dans cette section que les blockchains publiques, bien évidemment les blockchains privées et de consortium peuvent établir des règles formalisées de gouvernance *off-chain*.

29 Gouvernance des blockchains : Vitalik Buterin (ETH) VS Dan Larimer (EOS), Journal du Coin, 2018. https://journalducoin.com/altcoins/gouvernance-blockchains-vitalik-buterin-dan-larimer/

30 Arrow. A Difficulty in the Concept of Social Welfare.1950.

## 2.7 Interopérabilité

Aujourd'hui, l'industrie de la blockchain est cloisonnée entre de nombreuses plateformes et protocoles différents. De plus, comme déjà observé dans le rapport Deloitte[31] : « aucune solution unique n'a émergé comme le gagnant clair ; par conséquent, aucune norme technique ou de processus n'est encore en place, empêchant certaines entreprises de développer des plans d'affaires clairs ou de pouvoir collaborer avec des partenaires de l'écosystème pour une adoption massive ».

Ces difficultés ont été confirmées au cours de nos auditions. Le manque de référentiel technique sera probablement comblé par les travaux de standardisation à l'ISO mais il faudra attendre plusieurs années de travail pour obtenir des résultats concrets, alors que la technologie ne cesse d'évoluer et de se diversifier.

Le manque d'interopérabilité de la blockchain a trois conséquences majeures. Tout d'abord, il est très difficile d'échanger de la valeur entre des actifs créés sur différentes plateformes. Échanger un jeton ERC-20 contre, par exemple, un *altcoin* basé sur le protocole Bitcoin nécessite un intermédiaire centralisé agissant comme une chambre de compensation.

Deuxièmement, il est difficile voire impossible d'échanger entre des applications créées sur différentes plateformes. Étant donné que diverses applications sont lancées sur des protocoles complètement différents, il n'y a aucun moyen standard pour eux de communiquer ou d'échanger des données ou une logique. Cela empêche de nombreuses applications et contrats intelligents d'optimiser leurs propres fonctionnalités et valeur.

Enfin, l'état cloisonné de l'industrie de la blockchain limite la mutualisation des développements. Alors que pratiquement tous les projets de blockchain sont open source, la technologie développée sur un protocole ne peut pas être partagée avec ou adoptée par d'autres protocoles. De nouveaux développements sur un protocole peuvent fournir de l'inspiration ou des idées pour un autre, mais le code lui-même n'est jamais compatible ou réutilisable entre différents protocoles. Si l'industrie était plus unie, chaque progrès et chaque nouvelle technologie seraient partagés également avec tous les projets, ce qui entraînerait presque certainement un développement et une innovation accrus à tous les niveaux.

31 Deloitte. Blockchain to blockchains: Broad adoption and integration enter the realm of the possible. 2018

### 2.7.1 L'interconnexion des blockchains

VERROU 12 : Des protocoles matures d'interconnexion des blockchains.

*Verrou scientifique dans la phase « design, develop, test »* (cf. Figure 5).

VERROU 13 : Des protocoles entre blockchains qui vont au-delà du paiement.

*Verrou scientifique entre la phase « explore, hypothesize, clarify »* (cf. Figure 5).

Les blockchains seront interconnectées à l'aide de deux types de protocoles. Il peut s'agir de protocoles spécifiques, définis par les applications et les utilisateurs, *via* des contrats intelligents créés par les utilisateurs ou bien de protocoles génériques de fonctionnement au niveau de l'infrastructure elle-même (voir Annexe B). Pour ces deux types de protocoles, il y a un manque de formalisation adéquate, ce qui empêche d'établir leurs propriétés en termes de sécurité et de performances, par exemple. De plus, pour les protocoles établis *via* des *smart contracts* créés par les utilisateurs, les utilisateurs interagissent non seulement *via* la blockchain mais aussi entre eux en suivant une logique complexe dont l'exécution n'est pas tracée dans la blockchain. Idéalement, les interactions hors chaîne entre les utilisateurs devraient être minimisées pour tirer parti des propriétés de vérifiabilité des chaînes de blocs. Dans le cas des *swaps* atomiques (voir Annexe B), par exemple, la phase de *trading* qui a lieu en amont de la constitution du *swap* devrait passer par la blockchain elle-même. Cela permettrait d'avoir des protocoles entre blockchains qui vont au-delà du paiement.

En conclusion, l'analyse de l'état de l'art permet de constater que les solutions pour l'interconnexion de blockchains émergent avec des principes de conception intéressants mais elles doivent encore être validées.

## 2.8 Souveraineté

VERROU 14 : Des moteurs de recherche et des outils de surveillance.

*Verrou technologique entre la phase « design, develop, test » et « implement, study efficacy, improve »* (cf. Figure 5).

*La souveraineté* est l'exercice du pouvoir d'un État à l'intérieur de ses frontières conformément à ses lois. L'avènement des technologies numériques et leur utilisation massive pose clairement la question de la régulation de leur utilisation et de s'assurer que l'exercice des fonctions régaliennes soit toujours une prérogative de l'État. Un exemple est l'identité des citoyens, dont la certification est clairement de la compétence de l'État. Pour toutes les questions liées à la souveraineté numérique, le récent rapport du Sénat[32] en fait une analyse très complète, qui débouche sur une

32 Rapport de la commission sénatoriale d'enquête sur la souveraineté numérique , 2019, http://www.senat.fr/fileadmin/Fichiers/Images/redaction_multimedia/2019/2019-Documents_pdf/20191004_Rapport_CE_SouvNum.pdf

série de recommandations intéressantes, parmi lesquelles on peut citer la protection de la vie privée (le citoyen contrôlant ses données et leurs usages), le *leadership* technologique et l'innovation (c'est-à-dire stimuler l'écosystème de l'innovation pour faciliter le développement de *start-up* à fort potentiel technologique) et enfin positionner la France sur deux technologies en particulier : la blockchain et le quantique.

Nos recommandations et l'analyse des verrous identifiés s'inscrivent complètement dans la ligne du rapport du sénat et proposent des étapes concrètes pour la protection de la souveraineté,

D'un point de vue plus formel, notre lettre de mission nous a demandé d'analyser les mécanismes de consensus des blockchains publiques et les phénomènes de centralisation du pouvoir que ces mécanismes génèrent, avec la question sous-jacente de la nécessité de maintenir des «nœuds d'État» dans les blockchains publiques, pour assurer une certaine résilience à une éventuelle prise de contrôle d'une autre entité, ou éventuellement l'intérêt même de lancer une « blockchain d'État » pour protéger nos infrastructures et services critiques.

Le monde de la blockchain est encore très fluide, et il est certainement encore trop tôt pour déterminer quelle est la blockchain idéale (et s'il y en aura effectivement une) et quelle technologie blockchain sera massivement utilisée (peut-être plusieurs). Aujourd'hui les blockchains se multiplient car elles se spécialisent à juste titre dans différents secteurs d'application. Lancer aujourd'hui (ou dans un avenir proche) un projet de « blockchain d'État » n'apparaît donc pas comme une priorité utile (et ce constat est partagé par une majorité des personnes que nous avons auditionnées). Aujourd'hui, le choix le plus sage serait de légiférer (établir des limites légales, dans la ligne du Visa de l'AMF pour les ICO, établi dans la Loi Pacte, par exemple) pour s'assurer que les blockchains soient utilisées correctement, en protégeant leurs utilisateurs (entreprises comme particuliers) tout en permettant aux entreprises de choisir et de construire les chaînes de blocs qui répondent le mieux à leurs besoins. Sur le plan technique, cette approche doit nécessairement s'appuyer sur des technologies d'exploration et d'analyse au sens large à l'instar de moteurs de recherche sur Internet. Et c'est précisément le verrou que nous voulons mettre en avant dans cette section outre le fait qu'il nous parait important de créer un service d'identité numérique basé sur une technologie blockchain, pour stimuler l'écosystème autour d'un service régalien et résoudre également des verrous sécuritaires (voir section 2.2).

### Outils d'exploration : vers des fonctionnalités plus sophistiquées

Souvent appelés *explorers* ou *scans*, les outils d'exploration des blockchains permettent typiquement de voir les blocs produits, les transactions à l'intérieur d'un bloc et le mineur qui l'a produit (*Etherscan* et *Ethereum blockchain explorer* pour Ethereum, *Bitcoin Blockchain Explorer* et *Block explorer* pour BitCoin). Il s'agit cependant d'outils très rudimentaires. En faisant un parallèle avec le Web ce serait comme obtenir l'ensemble des URL disponibles dans un domaine, par exemple, sans capacité de sélectionner un contenu *via* des requêtes ou sans capacité de surveillance (dans le cas d'une blockchain, par exemple des alertes en cas de censure de nos propres transactions, etc.). Les outils d'exploration devront nécessairement évoluer vers des outils beaucoup plus sophistiqués, à l'instar des moteurs de recherche sur le Web, avec de vraies fonctionnalités de surveillance ou d'audit.

Ces outils pourront devoir obéir à des règles spécifiques de conception et répondre à des exigences de sécurité[33]. Nous imaginons qu'un marché pourrait se développer autour de ces outils assez rapidement. Nous pensons également que ces outils sont stratégiques dans la mesure où une blockchain sera vraiment « vue » au travers de ces outils. Un outil performant, répondant au niveau de sécurité établi sera la porte d'accès à la blockchain sous-jacente et en déterminera en

33 Un parallèle peut être fait avec Qwant dans le domaine des moteurs de recherche.

grande partie son adoption. Ces outils d'exploration seront les vrais garants de la transparence et des capacités d'audit des blockchains.

## 2.9 Aide à la conception

Comme constaté dans les sections précédentes, la conception, l'analyse et la validation d'un système de chaîne de blocs comportent un certain nombre de verrous à lever.

En premier lieu, un système de chaîne de blocs idéal combinant toutes les propriétés de sécurité souhaitées ne peut exister à cause du théorème CAP (voir Annexe A). Si des compromis doivent être trouvés entre sécurité, passage à l'échelle, consommation énergétiques, etc., nous manquons cruellement d'outils de conception et validation qui nous aideraient à trouver les bons compromis pour une application donnée. La capacité à trouver des compromis repose aujourd'hui sur des scientifiques et chercheurs ayant une expertise hors de portée d'un ingénieur. En outre, l'intégration de considérations économiques, liées par exemple aux incitations dans un système ouvert, à l'équité et la participation, à l'efficacité de contrats intelligents avancés, est un nouvel élément qui reste étranger aux méthodes de conception et de validation développés dans le monde de la recherche en informatique.

Un intérêt vif des groupes industriels les plus avancés sur le sujet s'est révélé au cours de nos entretiens pour pouvoir comparer différentes blockchains ou technologies de consensus non seulement au niveau de leur performance, de la mémoire nécessitée, de l'énergie consommée mais aussi sur des critères plus vaguement définis de niveau de fiabilité, de sécurité, de garantie de cohérence…

Sur tous ces sujets, la recherche et les entreprises françaises sont particulièrement bien placées, avec des compétences reconnues au niveau international. Cependant, les appliquer aux problèmes spécifiques de la blockchain est et reste un enjeu non trivial qu'il est important de relever car nous en avons les capacités d'une part, et d'autre part le moment est opportun au regard de l'état de l'art. Les besoins identifiés se situent à de multiples niveaux sur le cycle de vie d'une application blockchain. Ci-dessous une liste non exhaustive de besoins.

### 2.9.1 Vérification et certification

VERROU 15 : Des méthodes et outils formels pour la vérification et la certification des chaînes et des applications et services distribués.

*Verrou scientifique/technologique dans la phase « design, develop, test »* (cf. Figure 5).

La vérification du code des blockchains et des applications et services distribués qu'elles supportent est un verrou pour de nombreux acteurs du secteur. Au cours de nos auditions, plusieurs ont souhaité la mise en place d'un processus de certification. Pour les fournisseurs d'applications, il s'agit plutôt de la certification des *smart contracts*, pour les fournisseurs des blockchains, la certification s'adresserait à l'environnent d'exécution (chaîne de compilation, machine virtuelle et protocoles de consensus). Cette demande nécessite de lever le verrou 4 et mais également les verrous déjà rencontrés dans la section 2.2 sur les différentes couches (données, consensus, *smart contracts*) avec la considération supplémentaire des modèles économiques en jeu (Section 2.5). **Les problèmes techniques sont liés donc à la considération du système blockchain dans son ensemble** :

- exécution concurrente voire distribuée de *smart contracts* (bug de *réentrance* de *The DAO*, qui aurait coûté 50 millions de dollars ~~M$~~[34]) ;
- environnement hostile (modèle *byzantin*); *partitionnement* et *éclipses*[35] *;*
- caractéristiques des données: *provenance*, *autorité*, *secret ;*
- recours à des théories mathématiques : algèbre (cryptographie), théorie des jeux (économie).

### 2.9.2 Simulation et test

VERROU 16 : Des méthodes et des outils pour la simulation multi-niveaux et le test.

*Verrou scientifique/technologique dans la phase « design, develop, test »* (cf. Figure 5).

Lors de nos entretiens, il est apparu que quasiment tous nos interlocuteurs reconnaissaient les difficultés à simuler, tester et vérifier une application blockchain, que le manque de maturité des applications développées vient aussi des difficultés rencontrées sur le plan du passage à l'échelle, du manque d'interopérabilité avec d'autres applications et services, de l'hétérogénéité d'applications qui inévitablement évolueront dans le temps et devront s'adapter à de nouvelles versions de blockchains.

Un outil de simulation permettant de dimensionner une application et de comprendre ses limitations pourrait avec profit s'adosser entre autres aux outils classiques connus en simulation de réseaux tels que NS3 ou de simulation multi-agents pour la couche applicative par exemple. Le

34 https://en.wikipedia.org/wiki/The_DAO_(organization)

35 Type d'attaque d'un réseau *peer-to-peer* ciblant un nœud particulier (cf. https://eprint.iacr.org/2015/263.pdf)

verrou se situe en particulier au niveau de la définition des dimensions spécifiques d'une application blockchain que l'on désire contrôler. Ce simulateur sera d'autant plus utile qu'il ne serait pas lié à une plateforme particulière, ce qui représente une difficulté d'intégration additionnelle.

Le test est une méthode de validation de base. Toutefois, la reproductibilité d'une exécution d'une application décentralisée est extrêmement complexe car il faut prendre en compte l'état de la chaîne et de nombreux paramètres (nombre de nœuds, différents temps de latence sur le réseau, etc.) qu'il faut savoir synchroniser. Ceci constitue un verrou important. À cela, il s'ajoute la question de la couverture de suite de tests qui permet d'estimer quand raisonnablement s'arrêter de tester.

### 2.9.3 Outils de benchmarking

VERROU 17 : Des outils de benchmarking.

*Verrou scientifique/technologique dans la phase « design, develop, test »* (cf. Figure 5).

Comparer les solutions blockchain est une nécessité clairement identifiée dans nos auditions. Une difficulté majeure est similaire à celles exprimées pour la simulation : pouvoir être neutre vis-à-vis d'une technologie puisqu'il s'agit de pouvoir les comparer. Là aussi se pose la question de quoi comparer et mesurer, quels critères, quelles dimensions. À cet égard, la constitution d'une suite d'applications bien choisies (en termes de couverture et de pertinence) sera sans doute une clé du succès. Une autre clé du succès, non triviale, sera de savoir produire des comparaisons de critères « toutes choses égales par ailleurs », c'est-à-dire de savoir maîtriser et contrôler l'environnement réseaux, les questions de dimensionnements ou encore de synchronisation,

Un tel outil de *benchmarking* devra être ouvert et la suite de tests largement publiée et accessible.

### 2.9.4 Architecture et modularité

VERROU 18 : Des méthodes et outils pour l'architecture et la modularité.

*Verrou scientifique/technologique dans la phase « design, develop, test »* (cf. Figure 5).

Les questions d'architecture d'applications blockchain sont complexes. Elles intègrent entre autre des questions de méthodes, des décisions de dimensionnement (selon de multiples paramètres), de choix d'algorithmes ou de technologie. La question de la sécurité doit être vue dès la conception car elle va/doit influencer des décisions d'architecture sur lesquelles il sera difficile de revenir.

Les blockchains peuvent être modifiées afin de, par exemple, pouvoir passer à l'échelle, traiter des questions d'archivage, ou encore traiter des questions d'anonymat. Pour cela, tout au long de son existence, la blockchain pourrait devoir changer ses paramètres de fonctionnement. Par exemple, si une nouvelle politique d'archivage doit être mise en place, alors certains blocs pourraient devenir archivables car relatifs à des transactions trop anciennes. À ces fins, la modularité est fondamentale pour permettre une meilleure évolutivité et pour rendre plus aisée

la migration d'une application vers une nouvelle version de la même plateforme blockchain voire une autre plateforme.

## 2.10 Synthèse des verrous

Dans la Figure 6, les verrous identifiés dans les sections précédentes sont projetés sur le cycle de R & I. Nous remarquons que la majorité des verrous se positionnent dans la phase « *Design, Develop, Test* », cependant un certain nombre d'entre eux sont dans des phases plus proches de l'industrialisation.

Bien évidemment, cela signifie que pour ces verrous des solutions peuvent être d'ores et déjà développées et commercialisées (comme par exemple un outil de surveillance et analyse), mais cela n'empêche pas que des solutions plus sophistiquées demanderaient de déplacer les verrous vers des phases plus amont (si par exemple nous voulons nous munir d'outils d'analyse de données et visualisation très sophistiqués).

Nous avons également mis en exergue avec un astérisque les verrous interdisciplinaires : les verrous qui pour être levés auront besoin de la collaboration de différentes disciplines.

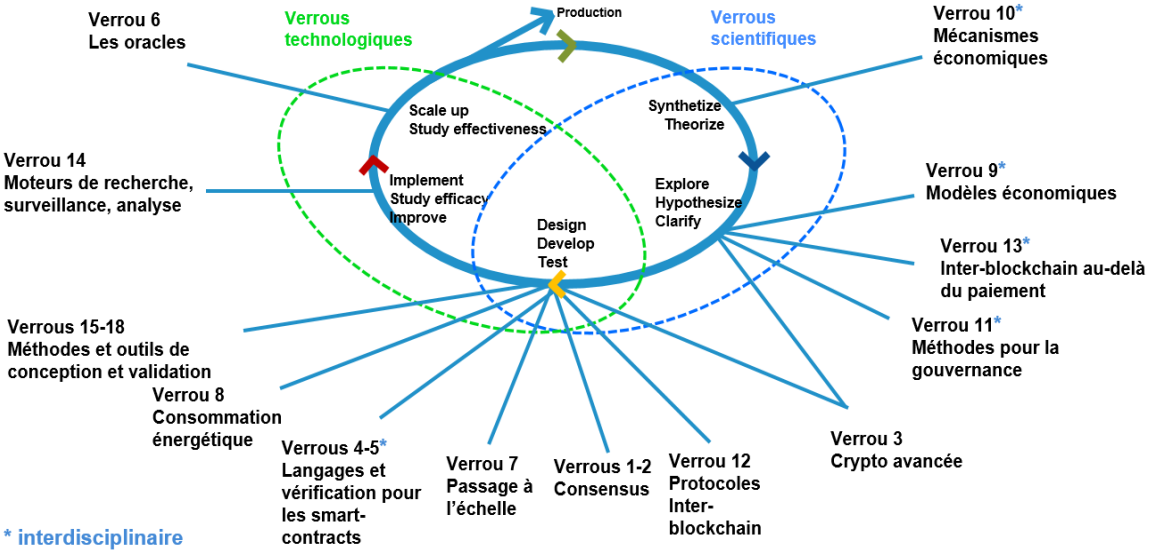



Figure 6 - Projection des verrous dans le cycle R & I

# 3 LES VERROUS ET L'INNOVATION

## 3.1 Les verrous dans la cartographie des usages

Dans la Figure 7, nous positionnons pour chaque niveau les verrous à lever.

Pour le niveau « Notaire » on peut affirmer que les applications, souvent pas très gourmandes en nombre de transactions et déployées sur un réseau à permissions ou privé, ont besoin de propriétés classiques : l'intégrité des enregistrements et leur disponibilité. On peut affirmer que les technologies « *enabling* », c'est-à-dire la réplication du registre et les primitives de cryptographie, sont matures. Une difficulté rencontrée souvent à ce niveau est la connexion à des oracles extérieurs (données provenant de capteurs, de services Web voire d'un utilisateur). Comme déjà discuté dans la Section 2.2.5 une consolidation de méthodes et pratiques pour la gestion des oracles est nécessaire (verrou 6). L'identification des oracles *via* un service d'identité numérique est également fondamentale pour développer des services et des règles d'accès. Même si pendant nos auditions nous avons également rencontré une difficulté reliée à la stabilité de codes des blockchains open source et aux environnements de développement, nous pensons que, au niveau « Notaire », une consolidation des méthodes et pratiques de conception, programmation et développement est suffisante. Des verrous de confidentialité sont également présents à ce niveau, mais des solutions de repli comme mettre la preuve d'existence d'une donnée plutôt que la donnée elle-même, ont été trouvé. À ce niveau des outils d'exploration des blockchains, de surveillance et analyse sont également des outils à développer (verrou 14).

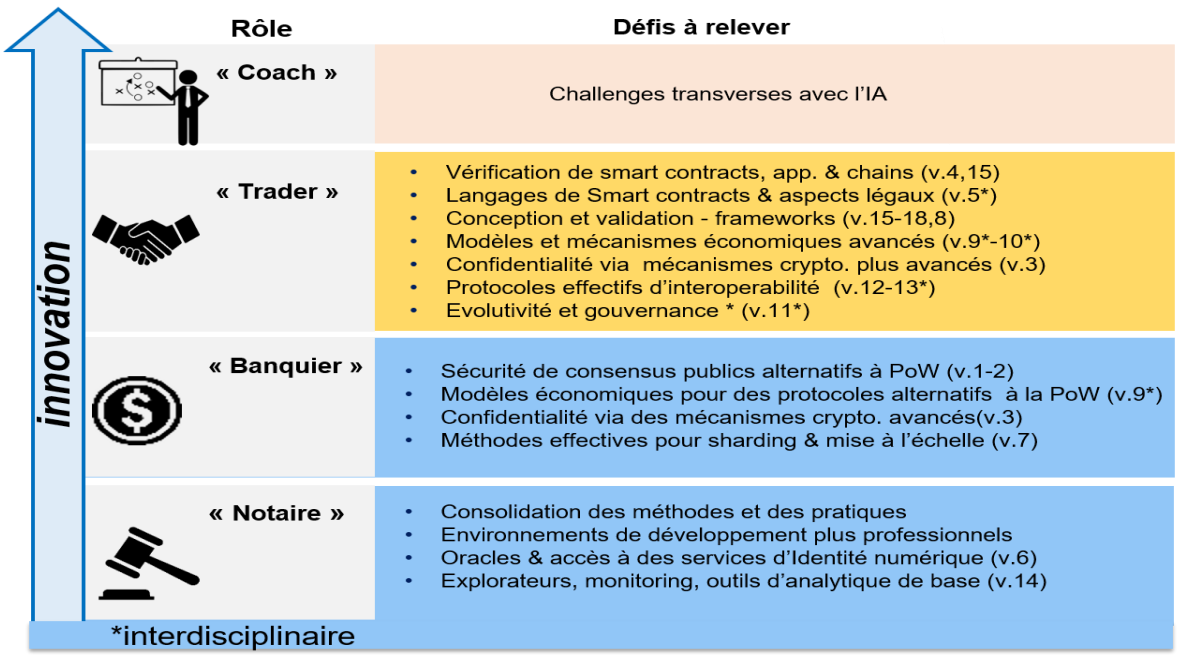



Figure 7 - Verrous et innovation

Pour le niveau « Banquier » le verrou majeur consiste à fournir des preuves de sécurité des alternatives à la preuve de travail (verrou 1) et à trouver les bons modèles d'incitation (verrou 9). De plus, il faut ici lever les verrous liés à la confidentialité de transactions exécutées en réseau public (verrou 3), à l'aide d'algorithmes cryptographiques avancés (verrou 3), et les verrous associés au passage à l'échelle au travers de méthodes efficaces de *sharding* (verrou 7).

Au niveau « *Trader* », nous trouvons tous les verrous reliés essentiellement aux contrats intelligents (verrous 4 et 5), aux gouvernances décentralisées (verrou 11) et à l'interopérabilité (verrous 12 et 13).

Nous remarquons que, à ce niveau, si s'assurer de la correction des contrats intelligents est un prérequis, il faudra également s'assurer de la sécurité de leur exécution : compilation et implémentation des mécanismes de consensus sous-jacents (le verrou 4 implique la résolution des verrous 1 et 2).

Les *smart contracts* à ce niveau ainsi que les protocoles d'interopérabilité et les méthodes de gouvernance décentralisée devront également être conçus et analysés en intégrant un point de vue légal, social et économique (verrous 5, 9 et 10).

Nous retrouvons encore le verrou lié aux mécanismes cryptographiques pour la préservation de la confidentialité, qui, à ce niveau, devra s'assurer de la confidentialité de l'exécution des *smart contracts* (verrou 3).

Ces verrous ne peuvent pas être levés sans des environnements de conception et de validation qui nous aideront à concevoir et valider les contrats intelligents mais également à concevoir et/ou sélectionner les mécanismes cryptographiques et de consensus sous-jacents les mieux adaptés (verrous 15, 16, 17, 18 et éventuellement 8).

Toutes les technologies *enabling* développées sur les premiers trois niveaux seront fondamentales pour développer des véritables gouvernances décentralisées auto-organisantes et de confiance dans quelques années, comme présenté au niveau *Coach*. Ces gouvernances décentralisées ont une dimension décisionnelle et d'optimisation globale forte, tout en laissant à l'être humain son rôle décisionnel dans le processus de décision globale. La dimension auto-organisant présente un lien naturel avec la recherche en intelligence artificielle distribuée ou multi-agents, qui devra considérer et intégrer les aspects de résilience à des comportements malveillants. De plus, si l'optimisation se fait à l'aide d'analyses de données, alors la question de la confiance que nous pouvons accorder à ces analyses trouve toute sa place à ce niveau, en rejoignant les verrous de l'IA classique.

## 3.2 Les solutions de repli aujourd'hui

À partir de l'analyse des problèmes ouverts, il est simple d'observer que les seules applications professionnelles qui peuvent être proposées sur le marché sont celles qui appartiennent à la première couche. Cela est confirmé par la cartographie start-up et par les auditions que nous avons menées pendant notre mission.

Pour les applications plus sophistiquées, il existe aujourd'hui des solutions de repli bien connues : comme exécuter des *smart contracts off-chain* en utilisant la blockchain à son niveau le plus élémentaire : *Notaire*. Cela se fait en mettant des preuves d'existence des calculs réalisés par ailleurs. Le même raisonnement se fait pour garantir la confidentialité des données.

Toutefois, il faut voir les solutions *off-chain* comme des solutions de repli dans le sens où elles n'offrent pas les propriétés de résilience promises par les blockchains, en particulier la disponibilité des données (ou des calculs faits par ailleurs) sera une problématique à résoudre. En outre l'architecture de ces systèmes est généralement plus complexe et difficile à mettre en œuvre.

## 3.3 Les verrous prioritaires et les acteurs français

Notre analyse nous amène à considérer comme prioritaires les verrous au niveau *Trader*, parce qu'accéder à ce niveau d'innovation signifie créer une vraie rupture technologique.

Grâce à nos cartographies, nous avons identifié que, parmi ces verrous :

- sur 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 sur ce sujet et des *start-up* actives dans le domaine, avec des compétences recherchées à l'étranger (Tweag, Origin Labs, Nomadic Labs) ;
- sur les verrous liés à la cryptographie appliquée à la blockchain, la recherche française est finalement peu impliquée, les réalisations plus importantes sur ce sujet se font aux États-Unis et en Israël. Néanmoins nous avons identifié Lambda Vision comme *start-up* active sur ce domaine ;
- sur les verrous sur les modèles et mécanismes économiques, l'interopérabilité et la gouvernance, nous ne sommes pas en retard, parce qu'il s'agit de verrous beaucoup plus prospectifs. Sur ces verrous, une recherche active se fait partout dans le monde, des actions interdisciplinaires de haut niveau sont en place en France sur les modèles et mécanismes économiques ;
- sur les verrous liés au génie logiciel, nous ne sommes pas en retard et c'est un vrai besoin industriel. Nous avons des compétences sur le sujet même s'il n'y a pas encore de recherche très active au-delà de la vérification des protocoles distribués (qui reste un sujet sur lequel la France est à la pointe). Le marché d'outils d'aide à la conception et validation est vierge avec une forte demande (à noter la *start-up* Xdev, essaimage de l'IRT SystemX) ;
- sur les verrous liés au consensus et à la mise à l'échelle (*enabling* pour le niveau *Trader*), nous ne sommes pas en avance, mais nous avons des compétences fortes en algorithmique distribuée avec des chercheurs bien impliqués sur ces sujets, et des chercheurs qui travaillent également avec des *start-up* qui ont un vrai besoin (Nomadic Labs et Transchain par exemple).

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 : elle permettrait une accélération de la productivité de solutions à ce niveau et contribuerait à l'adoption des blockchains.

## 3.4 Analyse Forces / Faiblesses / Opportunités / Menaces

Nous présentons dans cette section une analyse Forces/Faiblesses/Opportunités/Menaces (SWOT) de la blockchain en France, résumée dans la Figure 8.

La France a-t-elle les moyens d'être un *leader* technologique de la blockchain ? Son industrie (au sens large) et sa société pourront-elles profiter de ces technologies d'une manière qui « créera de la valeur » dans notre pays ? Dans le cadre de la stratégie nationale blockchain, ce rapport se concentre sur les aspects technologiques de ces questions.

Notre pays possède de réels atouts, avec en premier lieu la force de sa recherche dans des domaines très importants pour une technologie qui doit inspirer avant tout la confiance (vérification, preuves, langages…) ; et nous n'en voulons pour preuve que le fait que les compétences de nos chercheurs sont aujourd'hui activement recherchées par des sociétés étrangères. Mais nous avons aussi des *start-up* réellement innovantes dans le domaine et un « système entrepreneurial » très dynamique, de grandes entreprises et des organismes publics qui sont très attentifs à ces technologies et enfin un État qui soutient sans ambiguïté et de manière très volontaire « l'écosystème français de la blockchain ».

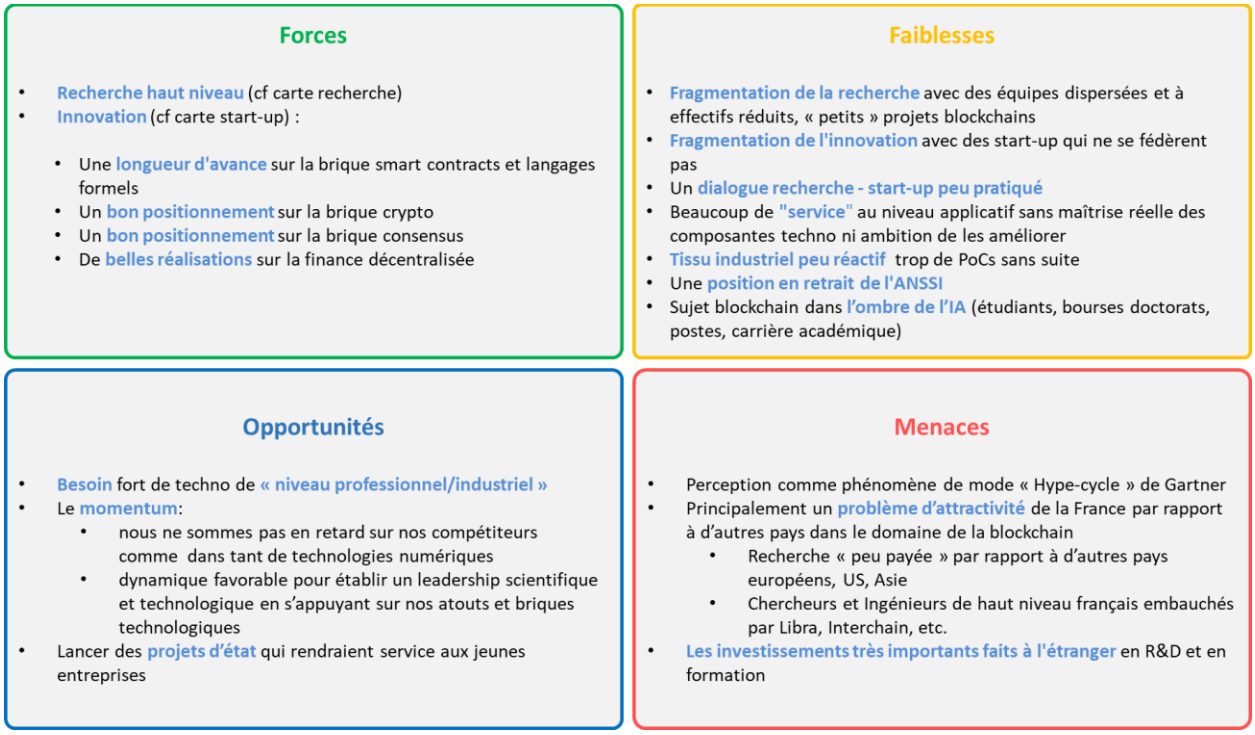


Figure 8 - Analyse SWOT

Nos faiblesses sont aussi réelles mais la plupart sont aussi bien connues et comprises, comme celles en lien avec la recherche publique (fragmentation, dialogue avec les *start-up*, rémunération des personnels, etc.). Certaines sont conjoncturelles (la « vague » blockchain a conduit les états-majors des grands groupes à lancer toutes sortes de preuves de concepts pour ne pas « rater le coche » et cela a créé un marché de services sans que les compétences ne soient vraiment présentes).

Les recommandations de ce rapport s'appuient sur les forces que nous avons identifiées et les opportunités perçues, en prenant en compte nos faiblesses et la durée pendant laquelle nous pouvons encore agir pour positionner la France le plus favorablement possible ; Gartner voit aujourd'hui un horizon 2023 pour les plateformes blockchain qui permettront la construction d'applications avec un impact fort en 2028.

Quelles seront ces plateformes, qui les « contrôlera » effectivement, comment la valeur se construira autour d'elles, sont des questions tout à fait naturelles et importantes pour comprendre comment notre pays peut se positionner sur ces technologiques. Comme pour d'autres types de logiciels ou d'infrastructures informatiques, le marché sera-t-il dominé par une poignée d'acteurs d'outre-Atlantique ? (le choix sera-t-il entre la blockchain de Microsoft, celle d'Amazon et celle de Google ?). Nous savons bien combien les prédictions sont difficiles dans nos domaines (ou tout au moins celles qui se révéleront justes), même à quatre ou cinq ans mais nous pouvons cependant nous risquer à prédire que les plateformes blockchain en 2028 seront toujours essentiellement basées sur des logiciels libres (le fort besoin de confiance et la complexité intrinsèque de ces plateformes devraient limiter l'apparition et la popularité de solutions « propriétaires »). La variété des applications possibles et la difficulté d'avoir certaines bonnes caractéristiques simultanément (cf. le théorème CAP, par exemple) devraient favoriser une certaine diversité dans ces plateformes et sans doute l'apparition de (quelques) plateformes modulaires. Sur ces plateformes, les développeurs pourront choisir les modules fournissant les caractéristiques nécessaires à leurs applications (un module de consensus adapté aux utilisateurs, un certain type de *smart contract*, un certain type de communication pair-à-pair, …) et en développer de nouveaux. Une telle situation (logiciels libres et plateformes modulaires) serait certainement la plus favorable pour l'écosystème français de la blockchain et pour maximiser l'efficacité de nos recommandations.

# 4 RECOMMANDATIONS

Cette section de notre rapport énonce un certain nombre de recommandations, issues de nos auditions et de nos réflexions, qui visent à lever les verrous que nous avons identifiés et plus généralement à favoriser, en France, le développement des technologies blockchains au bénéfice de la société et du monde économique.

Nous avons souhaité avant tout faire des recommandations pragmatiques, ambitieuses, mais réalistes, qui puissent avoir un réel effet de levier sur les avancées naturelles de la recherche et du développement dans ce domaine et qui s'appuient sur les atouts présents dans notre pays.

Le niveau de détail ou d'opérationnalité de nos recommandations diffère : entre encourager, promouvoir, lancer un projet ou mettre en place un comité… Il aurait été facile d'écrire que pour encourager la recherche sur un sujet comme le respect de la vie privée, il « suffit » que l'ANR lance un nouvel appel à projet. Nous sommes cependant bien conscients que la dynamique en la matière est plus complexe, avec de nombreux intervenants. Ainsi, lorsque nous recommandons « d'encourager » ou de « promouvoir » c'est bien un appel pour que chaque partie prenante intervienne avec ses moyens et toujours dans un dialogue avec la communauté des chercheurs. Nos recommandations les plus opérationnelles sont celles pour lesquelles nous voyons l'opportunité d'un réel effet de levier avec des bénéfices clairs à court ou moyen terme.

## 4.1 Sur la recherche

Les recommandations en matière de recherche sont bien entendu à articuler avec les différents appels à projet des programmes de R & D des différentes agences de financement, comme l'ANR ou la Commission européenne, dans le cadre d'Horizon Europe.

### 4.1.1 Actions interdisciplinaires

> Recommandation 1 : Encourager les collaborations et travaux communs entre spécialistes de différentes disciplines.

Même si dans notre mission nous nous sommes concentrés, avec une vision d'informaticien, sur les aspects technologiques de la blockchain, en tirer le meilleur parti, sociétal comme économique, nécessite une vision plus large. Il nous semble donc important d'encourager des actions de recherche interdisciplinaires, typiquement entre informaticiens et économistes, mais aussi juristes, voire sociologues, pour explorer tous les aspects de ces technologies.

Les technologies blockchain ont ceci de particulier qu'elles nécessitent d'agréger, en quelque sorte, des connaissances et des recherches dans des champs différents de l'informatique et des mathématiques : calcul distribué, cryptographie, langages, preuves formelles, et intelligence artificielle. Encourager les collaborations et travaux communs entre ces spécialistes est important, d'autant que ce n'est pas forcément naturel.

Des initiatives de création de groupes de réflexion et d'organisation de séminaires se développent (BART[36], divers séminaires sur Paris) et sont très utiles pour créer une communauté et susciter des

36 https://www.bart-blockchain.fr

échanges et des questionnements constructifs. Pour aller plus loin, il faudrait des moyens financiers (thèses en cotutelle, par exemple), mais aussi une reconnaissance par les pairs pour les chercheurs et pour les doctorants engagés dans ce type de d'actions interdisciplinaires. Une telle démarche est un pari risqué pour des doctorants et des jeunes chercheurs qui devront prendre plus de temps pour s'approprier les sujets et pour publier et auront plus de mal à trouver les bons contextes pour ce faire. Et les critères d'évaluation actuels de la recherche incitent à rester dans une discipline bien identifiée dans laquelle sa contribution pourra être plus facilement reconnue.

L'étude des comportements et interactions dans un environnement décentralisé et des propriétés de résilience vis-à-vis des approches de type théorie de jeux pour la composante consensus et *smart contracts* évolués est un exemple de thème où de telles collaborations interdisciplinaires seraient très fructueuses.

Cette recommandation vise à lever les verrous 5, 9, 10, 11 et 13.

### 4.1.2 Les compétences autour des aspects *langages*

> Recommandation 2 : Promouvoir l'intérêt et la valeur des compétences françaises en matière de langages.

Autour de ce que nous appelons les aspects « langages » pour la blockchain (langages de programmation pour l'infrastructure, langages de *smart contracts*, sémantique, vérifications, compilation optimisée en temps ou en énergie, etc.), la qualité de l'enseignement et de la recherche française sont très clairement reconnues. Nous en voulons pour preuve le fait que divers acteurs étrangers de la blockchain viennent chercher ces compétences dans notre pays (recrutement d'étudiants mais aussi de chercheurs en poste, par exemple).

Faire savoir cela, promouvoir l'intérêt et la valeur de ces compétences (notamment par rapport à des sujets plus à la mode comme l'intelligence artificielle) nous semble important pour continuer à maintenir notre position mondiale, maintenir un volume de recrutement de chercheurs suffisant et attirer de nouveaux étudiants et doctorants.

Cette recommandation vise la préservation de nos compétences pour lever les verrous 1, 4 et 15.

### 4.1.3 Le sujet *privacy*

> Recommandation 3 : Amplifier l'effort de recherche français dans le domaine *privacy*.

Par « le sujet *privacy* » nous entendons les recherches visant à prendre en compte le respect de la vie privée et contrôler l'accès à des données personnelles ou plus généralement à des données jugées sensibles (dans le cas de données d'entreprises ou d'organisations).

Notre constatation est qu'il existe relativement peu de travaux en France sur ce sujet, alors que, par exemple, sa composante cryptographie est beaucoup plus développée aux États-Unis et en Israël ; même si nous avons en France de très bons chercheurs qui s'y intéresse (sur des thèmes comme la vérification des algorithmes cryptographiques et la *privacy-by-design*).

Beaucoup d'applications intéressantes des blockchains pourraient faire usage d'avancées sur ce sujet. C'est un retour que nous avons eu de plusieurs de nos auditions.

Le contexte européen, avec le Règlement général sur la Protection des Données (RGPD), offre de belles opportunités, d'abord à cause des contraintes qu'il impose (et donc à la nécessité de trouver des solutions techniques pour les prendre en compte). Mais aussi (et surtout) il entraîne naturellement une nouvelle façon d'appréhender ces données : comme des biens immatériels et complexes dont un contrôle fin est nécessaire d'un point de vue sociétal mais aussi souhaitable d'un point de vue économique, pour développer de nouveaux services et potentiellement de nouvelles « chaînes de valeurs » qui les incorporent. Le RGPD pourrait permettre, de fait, de placer les entreprises européennes en avance dans l'hypothèse (assez probable) où de telles réglementations soient adoptées dans d'autres pays (à l'échelle d'un état américain c'est d'ailleurs déjà le cas en Californie depuis le 1er janvier 2020).

Il nous apparaît donc important d'amplifier l'effort de recherche national dans le domaine, par des recrutements ad-hoc et la création d'équipes de recherche spécialisées (et qui entendent évidemment appliquer leurs résultats au contexte blockchain).

Cette recommandation vise la levée du verrou 3.

### 4.1.4 Les aspects *génie logiciel*

> Recommandation 4 : Focaliser une partie de nos compétences en génie logiciel sur les problèmes spécifiques des infrastructures et des applications blockchain.

Développer la recherche sur ce que nous appelons les aspects génie logiciel nous semble indispensable pour le développement des technologies blockchain.

Par aspects « génie logiciel » nous entendons les méthodes et les outils de conception pour des applications utilisant la blockchain et pour les briques cœur comme les protocoles distribués d'infrastructure tels que le consensus, les protocoles d'interconnexion entre blockchains, les machines virtuelles, les *smart contracts*, les protocoles de communication P2P, les algorithmes cryptographiques, les mécanismes d'incitation.

Pour les méthodes et outils de conception, une attention particulière devrait être donnée aux sujets suivants :

- les méthodes formelles pour la conception et la validation ;
- la modularité ;
- l'interopérabilité ;
- l'évolutivité et la scalabilité ;
- l'architecture et l'exploration architecturale : choix de la technologie la mieux adaptée (la blockchain la mieux adaptée, avec les modules les mieux adaptés), dimensionnement, paramétrage ;
- les tests, avec la dimension particulière de reproductibilité (évidemment particulièrement délicate dans un tel environnement) ;
- le *benchmarking* et l'évaluation des performances ;
- la simulation (réseau, distribuée, multi-agents).

Si la plupart sinon tous ces sujets peuvent sembler tout à fait classiques, c'est le contexte particulier des applications blockchain qui introduit de nouvelles problématiques, avec le

caractère (potentiellement massivement) distribué, la durée de vie des données réparties et partagées et la nécessité d'une très grande sécurité de fonctionnement.

Sur tous ces sujets, la recherche française est particulièrement bien placée, avec des compétences reconnues mais très peu appliquées aux problèmes spécifiques de la blockchain aujourd'hui. C'est là qu'une action particulière pourrait avoir un impact à relativement court terme et c'est ce que nous proposons dans la section suivante.

Cette recommandation vise les verrous 14, 15, 16, 17 et 18.

### 4.1.5 Un Institut international interdisciplinaire de la Blockchain

> Recommandation 5 : Étudier la création d'un Institut international interdisciplinaire de la Blockchain.

Pour dynamiser la recherche française sur les blockchains et encourager l'interdisciplinarité, nous proposons d'étudier la création d'un Institut international interdisciplinaire de la Blockchain. Cet institut accueillerait des chercheurs (étrangers comme français), en résidence, sur des périodes de quelques mois à un an. Leurs travaux viendraient naturellement attaquer les verrous que nous avons identifiés (et renforcer ponctuellement les projets de la grande action d'innovation).

Le but est d'une part de construire (ou consolider) un réseau international de recherche sur la blockchain, de mettre l'accent sur l'interdisciplinarité du sujet et d'autre part, de nous assurer de l'obtention de résultats à hauts impacts scientifiques et technologiques.

Cet institut pourrait également financer des séjours de chercheurs français (et de doctorants) dans différents laboratoires internationaux. Il organiserait naturellement un ensemble d'événements de haute visibilité (master classes, workshops, conférences, séminaires, concours internationaux, ect.) afin de rassembler chercheurs d'envergure internationale, jeunes chercheurs et ingénieurs et de créer une dynamique vertueuse consolidant la notoriété de la France sur la thématique.

Nous sommes bien conscients des difficultés pratiques que pourrait poser la création d'un tel institut (outre son financement ; dans un paysage français de la recherche déjà bien complexe). Des modèles existent à l'étranger, comme par exemple l'Isaac Newton Institute en Grande-Bretagne (pour les mathématiques et leurs applications), dont nous pourrions nous inspirer.

Un tel institut pourrait héberger des recherches visant les verrous 3, 4, 9, 10, 11 et 13.

## 4.2 Une grande action d'innovation

> Recommandation 6 : Lancer une grande action d'innovation sur les sujets conception – validation – *benchmarking*.

Une grande action emblématique sur le sujet « *conception, validation et benchmarking* » pourrait avoir un rôle de catalyseur pour l'ensemble de l'écosystème français autour de la blockchain. Le but serait de porter à maturation les solutions existantes et surtout de développer un environnement d'aide à la conception et à la validation (un ensemble de nouveaux outils) qui

facilitera l'adoption des technologies blockchain par le développement plus facile de solutions fiables.

Un des objectifs est lié à l'évaluation formelle de certaines briques cœur ou applicatives, ce qui pourrait conduire à qualifier certaines d'entre elles ainsi qu'à en concevoir de nouvelles avec des approches formelles et à les mettre à disposition de nos jeunes entreprises. La question de la certification ou de la qualification nous semble primordiale pour rendre les technologies blockchain sûres et applicables dans un milieu industriel.

Un deuxième objectif est lié aux environnements de développement d'applications blockchain. Au cours de nos auditions, nous avons constaté que développer de telles applications requiert la connaissance de multiples environnements et technologies encore très fragmentées, difficilement intégrables et volatiles. La mise à disposition d'environnements de développement professionnels pour augmenter la qualité des codes applicatifs, leur stabilité et réduire les temps de développement nous semble donc essentiel et c'est donc un des objectifs.

Pour les verrous les plus difficiles à lever, pour lesquels des solutions sont encore à inventer, il nous semble essentiel de mettre à disposition de l'écosystème des méthodes et outils innovants d'aide à la conception : des outils et modèles de conception, simulation, validation et *benchmarking* par exemple. Cela permettra aux concepteurs de nouvelles solutions de les valider très tôt dans le cycle de développement. Certaines *start-up* se positionnent également sur ce créneau en termes d'offre technologique.

Enfin, la réalisation de nouvelles solutions (nouvelles méthodes cryptographiques pour la *privacy* ou méthodes de consensus pour le passage à l'échelle ou un moindre impact énergétique, par exemple) est également un objectif. Il s'agit bien évidemment de mettre en place des actions de recherche à plus long terme, cependant la mise à disposition d'outils et méthodes d'aide à la conception devrait faciliter l'émergence de solutions robustes et efficaces.

Pour garantir une efficacité maximale à cette grande action que nous proposons, un pilotage fort est nécessaire ainsi que la mobilisation et la coordination d'un certain nombre d'acteurs, publics comme privés. Nous proposons donc une structuration particulière : un consortium principal qui sera en charge des objectifs globaux et du pilotage d'un certain nombre de projets. Chaque projet sera réalisé par un consortium spécifique et visera la réalisation de deux types de briques technologiques :

- CF (composant fonctionnel) : pour développer et/ou valider un ou plusieurs modules d'un système blockchain (un compilateur de contrats intelligents, une implémentation modulaire d'un algorithme de consensus, une bibliothèque cryptographique, un protocole d'interconnexion, un oracle, des contrats intelligents particuliers et validés, etc.) ;
- MO (méthodes et outils) : pour les outils et méthodes pour le développement d'un système blockchain ; par exemple, une méthodologie basée sur la théorie de jeux pour la validation de mécanismes d'incitation, un simulateur multi-niveaux pour des applications basées sur des blockchains, des outils de vérification pour les *smart contracts*, des benchmarks, etc.

Les projets ont idéalement une courte durée (12 à 18 mois) avec des livrables bien définis sous forme de code, outil ou rapport technique. Ils seront sélectionnés par des appels spécifiques ouverts, au fil de l'eau, à tous les acteurs de la blockchain en France, sur la base d'un dossier et d'un entretien avec le consortium principal (qui pourra proposer des modifications au projet si nécessaire).

La durée de vie du consortium principal serait de 4 ans à 5 ans pour conserver une focalisation suffisante. Il aura à sa charge :

- les objectifs techniques globaux et des guides méthodologiques associés ;
- sélectionner les projets, en assurer le suivi avec des évaluations intermédiaires et une évaluation finale;
- créer et entretenir les interactions et synergies entre projets;
- intégrer les résultats des projets dans une plateforme technique facilement accessible;
- animer et faire grandir un écosystème blockchain en intégrant des PME fournisseurs de technologies ou utilisant la blockchain, des laboratoires de recherche et des industriels, *via* des ateliers ou autres événements.

Ce consortium principal devrait être composé d'organismes de recherche actifs dans le domaine et à même d'opérationnaliser les recommandations de recherche de ce rapport. Il associerait étroitement à son pilotage d'autres acteurs publics, comme les financeurs de cette grande action ou encore l'ANSSI (qui pourrait être associée au projet pour son expertise sur les questions de certification et/ou qualification).

Pour répondre le plus efficacement possible aux questions de recherche ouvertes et aux verrous à lever que nous avons identifiés, tout en accélérant l'innovation d'un grand écosystème, nous recommandons les critères d'évaluation suivants pour les projets :

- ouverture : une priorité serait donnée aux projets dont les résultats seront publics et, le cas échéant, open source ;
- *leadership* technologique : une priorité serait donnée aux projets réalisés par une jeune entreprise en partenariat avec des laboratoires de recherche sur un sujet en rupture;
- interdisciplinarité : une priorité serait donnée aux projets interdisciplinaires qui nécessitent la collaboration de différents laboratoires de recherche.

Le consortium principal organisera plusieurs appels à projets successifs, qui auront pour objectif de faire mûrir les différentes briques techniques par des projets de portée et d'ambition toujours plus grandes, en fédérant des projets et des consortiums qui ciblent par exemple le même sujet ou qui relèvent des mêmes compétences. Les sujets plus prospectifs pourraient être portés à maturation de manière incrémentale *via* une succession de projets. Concrètement, il pourrait être envisagé une première vague de projets de 18 mois (représentant un coût total de 8 millions d'euros), une deuxième vague de consolidation de projets de 18 mois (coût de 10 millions d'euros) et une dernière vague de projets plus courts (12 mois), qui permettraient en particulier de valider les résultats des projets précédents (pour un coût de 2 millions d'euros). Nous estimons à 2 millions d'euros le coût de la gouvernance du projet (pilotage, animation, etc.). Cette grande action d'innovation aurait ainsi un coût estimé de 25 millions d'euros.

Un événement de jumelage entre *start-up* et laboratoires de recherche pourrait être la première action concrète à lancer pour une phase d'avant-projet.

Cette recommandation s'attaque directement aux verrous 14, 15, 16, 17 et 18.

## 4.3 Sur la confiance numérique

La plupart des applications des technologies blockchain nécessitent une confiance forte dans le service. C'est donc un sujet sur lequel l'État peut avoir une influence notable.

### 4.3.1 La certification des produits, services et des acteurs de la blockchain

> Recommandation 7 : Le développement de nouvelles compétences de certification des produits et services utilisant la blockchain.

L'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI) est un acteur très reconnu avec une place unique en France. Il accompagne les candidats à la certification et collabore avec des centres d'évaluation agréés en charge des processus de certification des produits/services associés à des technologies. La capacité de ces centres à être capables d'émettre des recommandations sur des plateformes blockchain ou des applications données de cette technologie ne peut qu'avoir une influence positive sur la confiance en ces technologies et leur adoption. Nous sommes bien conscients que cela nécessite certainement de développer de nouvelles compétences au sein des centres d'évaluation partenaires de l'ANSSI et au sein de l'Agence.

### 4.3.2 La certification

> Recommandation 8 : Entamer une réflexion sur la certification.

Nous suggérons d'entamer une réflexion sur la certification des acteurs (développeurs de blockchain et d'applications, fournisseurs de services). Au-delà des normes existantes d'évaluation de la sécurité des systèmes et des logiciels (typiquement les critères communs, ISO 15408), une solution plus légère (en particulier plus adaptée au cas de *start-up* et plus généralement à des démarches d'innovation plus agiles) et adaptée aux technologies blockchain pourrait être développée.

### 4.3.3 Sur l'identité numérique

> Recommandation 9 : Lancer un projet visant à mettre en production un service d'identité numérique, évolutif, modulaire, pour les personnes physiques et morales.

L'identité numérique est la base de la confiance et la base des applications de la blockchain.

Créer un véritable service public de l'identité numérique, pour les personnes physiques comme pour les personnes morales, qui soit évolutif, utilisant des technologies cryptographiques avancées (en lien aussi avec les recherches mentionnées plus haut sur le sujet *privacy*), 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.

Concrètement, nous recommandons la mise en place d'une offre de service d'identité numérique accessible par les *smart contracts* des principales blockchains utilisées par les *start-up* françaises. Cette offre prendrait la forme d'oracles, c'est-à-dire de serveurs qui observent, enregistrent et répondent aux requêtes émises par les *smart contracts*, selon un protocole défini. *À minima*, cette offre pourrait être une simple adaptation des moyens d'identifications actuellement utilisés, comme France Connect, mais elle aurait naturellement vocation à être un volet du service d'identité numérique d'État en cours d'élaboration. Elle aurait aussi vocation à s'enrichir de services innovants issus de la recherche et développement d'acteurs français.

Cette action aurait trois objectifs :

- faciliter le développement de services sur blockchain en épargnant aux *start-up* l'implémentation de fonctions régaliennes ;
- promouvoir de bonnes pratiques en matière de lutte contre la fraude, et de protection des données et de la vie privée ;
- offrir une vitrine à la recherche et au développement de nouvelles technologies de protection de données.

La vérification d'identité est une fonctionnalité nécessaire pour pratiquement toutes les applications de la blockchain qui dépassent le niveau notarial ou strictement monétaire. C'est par exemple une composante du KYC (*Know Your Customer*) exigé pour l'agrément de services financiers par l'AMF. La plupart des acteurs que nous avons rencontrés ont donc dû implémenter pour leur usage propre cette fonctionnalité typiquement régalienne. Outre leur surcoût, la qualité de ces implémentations est variable. Comme elle impose à l'opérateur de retenir des données sensibles, ceci pose des problèmes réels de protection de ces données, qu'une adhésion de pure forme au RGPD ne résout pas vraiment.

Les protocoles utilisés pour ces services d'identité devront prendre un soin particulier à la protection des données échangées, compte tenu de la nature publique des données sur blockchain. Ceci limitera l'offre de service initiale. Il serait donc souhaitable que les opérateurs de ces services coopèrent avec les acteurs de la recherche et les *start-up* qui développeront des solutions cryptographiques innovantes en matière de protection des données, pour l'expérimentation et le déploiement de nouveaux services s'appuyant sur ces innovations. Ce serait à la fois une vitrine pour la recherche française, et en particulier pour la grande action d'innovation recommandée dans ce rapport.

Ce projet est lié au verrou 3 et à la recommandation 3, dont il pourrait utiliser à terme les résultats.

## 4.4 Sur l'appui aux politiques publiques et aux projets de l'état

Recommandation 10 : Créer un comité consultatif, issu de la recherche publique, pour soutenir l'état sur les questions technologiques liées à la blockchain.

La volonté de l'État, telle que nous la comprenons, est de favoriser le développement de la blockchain et les innovations autour de ces technologies. 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.

## 4.5 Sur les liens entre la recherche publique et les *start-up*

Recommandation 11 : Favoriser et promouvoir la collaboration entre recherche publique et start-up du domaine.

Nos entretiens ainsi que la cartographie des *start-up* montrent que le lien entre les laboratoires de recherche et les *start-up* est assez faible dans le domaine de la blockchain (à quelques exceptions près comme Nomadic Labs, IxxO, Transchain cf. cartographie start-up) alors que la maîtrise de la technologie blockchain requiert des compétences très avancées. Nous recommandons donc 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 distribué, cryptographie, vérification et certification de contrats intelligents, de finance et d'économie. Nous avons identifié des besoins concrets sur ces sujets mais il est souvent difficile pour les jeunes entrepreneurs de bénéficier des résultats du monde de la recherche.

Sur un plan plus opérationnel, nous recommandons (cf. 4.1) la mise en place d'un grand projet qui sera capable de mobiliser un écosystème autour de la blockchain et renforcer le lien entre recherche et *start-up* (recommandation 6).

## 4.6 Sur l'enseignement

Recommandation 12 : Mise en place par les organismes d'enseignement supérieur de formations spécialisées au niveau master, d'ingénieurs R & D spécialisés et d'ingénieurs d'application[37].

Recommandation 13 : Favoriser les formations en alternance, dans les laboratoires de recherche et développement du domaine.

Recommandation 14 : Développer une offre de MOOC et supporter les projets existants sur le sujet (offre hébergée par exemple sur par la plateforme FUN), créer des outils spécifiques permettant un haut niveau d'interactivité aux apprenants.

En premier lieu, il convient d'augmenter rapidement le nombre de formations de niveau master qui reste très insuffisant même si les écoles d'ingénieurs ont commencé à développer leur offre. Les entreprises (surtout *start-up*) du secteur sont déjà confrontées à une pénurie d'ingénieurs et le facteur limitant leur développement n'est plus leur financement mais leur capacité à recruter des ingénieurs maîtrisant la technologie blockchain.

37 Dans un premier temps, l'introduction de modules blockchain dans des enseignements existants pourra être encouragée.

De plus, il n'y a aucun répertoire centralisé des formations blockchain disponible. Ainsi, le site web de l'Onisep ne liste aucune formation actuellement. Nous recommandons la mise en place des informations nécessaires pour améliorer la situation et permettre aux étudiants et futurs étudiants de trouver ces formations simplement.

Le sondage confirme en outre les informations éparses que nous détenions déjà en démontrant que peu d'enseignements significatifs en volume sont délivrés en France. Plus précisément, nous n'avons identifié aucun parcours de niveau master dans un établissement public qui soit entièrement consacré à la blockchain. Hormis deux écoles qui proposent des parcours assez complets, seuls des modules d'initiation sont délivrés en particulier en école d'ingénieur (relativement peu en université jusqu'à cette année) comprenant très souvent une partie crypto-monnaie. Ces modules d'initiation, plus ou moins approfondis, sont délivrés dans différents parcours d'enseignement : en informatique distribuée, en systèmes d'information, en informatique théorique, en cybersécurité ou (moins souvent) en sciences économiques ou en droit, démontrant s'il le fallait la nature multidisciplinaire du sujet. Ceci pourrait et devrait changer dès l'année prochaine car nous avons relevé de nombreuses velléités de monter des enseignements de niveau M2 sur la blockchain ce qui est en phase avec notre recommandation qui se veut de nature incrémentale.

Il serait bon de créer au plus vite des gisements de personnels opérationnels sur la blockchain capables d'embrasser plusieurs des disciplines composant cette technologie afin de renforcer le potentiel industriel français.

Nous proposons à ce sujet de favoriser l'essor (déjà identifiable et significatif) des formations en alternance afin de développer les relations entre les industriels et le milieu académique (en particulier la recherche). Ainsi l'ouverture de nouvelles formations d'ingénieurs par apprentissage avec un profil blockchain doit être encouragée dans les établissements qui en ont les ressources. Une consigne dans ce sens donnée aux commissions d'accréditation (par exemple la CTI[38]) nous semble opportune.

De la même manière, il faudrait inciter la mise en place de contrats de professionnalisation à l'université ou en école d'ingénieur dans le cadre d'une année de spécialisation dans la blockchain.

À l'heure actuelle, seul le contrat d'apprentissage est applicable dans le secteur public. Y aurait-il un moyen d'ouvrir le contrat de professionnalisation aux laboratoires publics de recherche ? Cela pourrait être un bon moyen pour accélérer le passage des avancées technologiques des laboratoires aux entreprises, resserrant les liens entre formation et recherche dans le domaine de la blockchain.

Il sera bon également de développer plus de formations continues de bon niveau qui font encore cruellement défaut. Les compétences techniques à développer dans ce cadre seraient à priori les mêmes que dans les formations initiales en veillant à une progressivité pédagogique adaptée pour tenir compte des acquis en programmation. Ouvrir de telles formations assez courtes, s'appuyant sur de fortes compétences déjà présentes chez les apprenants ferait gagner du temps dans le processus d'apprentissage. Des formations continues privées existent ou sont à l'étude (par exemple par l'IRT SystemX) ; cependant, nous serions plus favorables au développement de formations continues certifiantes recensées dans les répertoires *ad-hoc* (type RNCP[39] et RSCH[40]).

38 Commission des Titres d'Ingénieurs.

39 Répertoire National des Certifications Professionnelles, cf. https://certificationprofessionnelle.fr/

40 Répertoire Spécifique des Certifications et des Habilitations.

Nous proposons enfin d'accélérer la mise en place de formations de niveau master de deux types de profils d'ingénieur ayant deux niveaux d'expertise différents. Ci-après nous détaillons les profils d'ingénieur que nous recommandons.

### Former des ingénieurs R & D spécialisés

Un diplômé de ce type de parcours devra être capable de concevoir et développer des éléments d'infrastructure d'une plateforme blockchain ; par exemple un algorithme particulier de consensus décentralisé, de savoir lier les éléments de la blockchain aux autres éléments d'une application complexe. Il devrait connaître et comprendre des notions avancées de calcul distribué, de cryptographie et être éventuellement capable de mener des travaux de recherche appliquée dans ces domaines le cas échéant.

### Former des ingénieurs d'application

Un diplômé de ce type d'enseignement devra être capable de programmer un *smart contract*, de développer les éléments essentiels d'une application blockchain, de la tester et de l'évaluer. Ce profil correspond à des ingénieurs *full stack* maîtrisant la chaîne applicative blockchain et ayant une bonne compréhension des mécanismes au cœur de la technologie blockchain.

Ces deux types de formations pourront bien évidemment avoir un tronc commun comprenant des notions de base de la blockchain.

Parallèlement au déploiement de ces formations pédagogiques académiques, serait également bienvenue toute initiative de l'État pour inciter, simplifier et soutenir la mise en place de formations visant la vulgarisation et la sensibilisation des utilisateurs. Ainsi, des structures telles que celles du Wagon[41] ou de Station F devraient être étendues à la province. L'État a son rôle à jouer dans ce déploiement en facilitant leur intégration dans le tissu économique sur l'ensemble du territoire.

Enfin, il nous paraît souhaitable de développer une offre de MOOC (ou d'autres outils d'*e-learning*) à la fois francophone et anglophone conséquente sur le sujet en s'appuyant, par exemple, sur la plateforme FUN. Plusieurs projets sont d'ailleurs en cours sur ce sujet et il faudra les prendre en compte afin éventuellement de les soutenir dans l'offre proposée.

## 4.7 Synthèse des recommandations

Pour le confort du lecteur, nous listons, dans cette dernière section, toutes nos recommandations.

Sur la recherche :

- Recommandation 1 : Encourager les collaborations et travaux communs entre spécialistes de différentes disciplines.
- Recommandation 2 : Promouvoir l'intérêt et la valeur des compétences françaises en matière de langages.
- Recommandation 3 : Amplifier l'effort de recherche français dans le domaine privacy.

41 https://www.lewagon.com/

- Recommandation 4 : Focaliser une partie de nos compétences en génie logiciel sur les problèmes spécifiques des infrastructures et des applications blockchain
- Recommandation 5 : Étudier la création d'un Institut international interdisciplinaire de la Blockchain ;

Sur l'innovation :

- Recommandation 6 : Lancer une grande action d'innovation sur les sujets conception – validation – benchmarking.

Sur la confiance numérique :

- Recommandation 7 : Le développement de nouvelles compétences de certification des produits et services utilisant la blockchain ;
- Recommandation 8 : Entamer une réflexion sur la certification ;
- Recommandation 9 : Lancer un projet visant à mettre en production un service d'identité numérique, évolutif, modulaire, pour les personnes physiques et morales ;

Sur l'appui aux politiques publiques :

- Recommandation 10 : Créer un comité consultatif, issu de la recherche publique, pour soutenir l'état sur les questions technologiques liées à la blockchain ;

Sur les liens recherche – *start-up* :

- Recommandation 11 : Favoriser et promouvoir la collaboration entre recherche publique et start-up du domaine ;

Sur l'enseignement :

- Recommandation 12 : Mise en place par les organismes d'enseignement supérieur de formations spécialisées au niveau master, d'ingénieurs R & D spécialisés et d'ingénieurs d'application ;
- Recommandation 13 : Favoriser les formations en alternance, dans les laboratoires de recherche et développement du domaine ;
- Recommandation 14 : Développer une offre de MOOC et supporter les projets existants sur le sujet (offre hébergée par exemple sur par la plateforme FUN), créer des outils spécifiques permettant un haut niveau d'interactivité aux apprenants.

# 5 CARTOGRAPHIE DE LA RECHERCHE

Cette section a pour objectif d'identifier les équipes de recherche françaises impliquées dans le domaine des blockchains et qui contribuent activement à lever les principaux verrous identifiés dans les sections précédentes.

Après une caractérisation de leurs activités par rapport à ces verrous, nous présentons quelques éléments permettant de les situer dans le contexte de la recherche internationale et leur contribution à son écosystème.

L'étude porte sur les acteurs français en premier lieu, mais nous présentons aussi rapidement les principaux laboratoires étrangers moteurs dans le domaine.

## 5.1 Méthodologie adoptée

Établir une cartographie des activités de recherche sur la blockchain se heurte à deux difficultés majeures :

- la technologie blockchain se caractérise par l'intégration de technologies et de services rendant transparente la gestion décentralisée et sécurisée d'interactions entre acteurs. Elle fait appel à de nombreuses spécialités pour proposer une solution intégrée de confiance. Recenser les équipes contribuant aux technologies utilisées, mais non directement investies dans le domaine de la blockchain, peut conduire à un ciblage beaucoup trop large pour l'étude et peu informatif quant à l'objectif recherché;
- cette technologie peut être impliquée dans de très nombreux domaines scientifiques, industriels, économiques, sociétaux, ce qui se traduit par une abondance de publications sortant du champ de l'étude.

Il est donc difficile de cerner les acteurs directement impliqués dans les fondamentaux de la technologie blockchain en tant que telle. Pour l'étude, nous avons restreint le cercle des laboratoires à considérer en nous concentrant sur les chercheurs qui s'identifient comme travaillant sur la blockchain car nous souhaitons identifier les acteurs de recherche positionnés sur les verrous identifiés. Nous avons donc écarté ceux qui proposent, dans leur domaine, des approches « à base de blockchain » ; ce qui relève plutôt d'applications métier.

Afin d'identifier les laboratoires actifs au sens où nous l'entendons ci-dessus, nous avons pris pour point de départ l'analyse de l'activité au sein de conférences et séminaires spécialisés organisés en France : les séminaires *Blocksem* à l'École Polytechnique 2017-2019, *Tokenomics* 2019[42], Collège de France 2019, séminaires BART[43] 2018-2019.

Cette première étude a conduit à l'identification des personnalités des institutions ou laboratoires de recherche suivants :

- Emmanuelle Anceaume, CNRS, IRISA (algorithmes distribués - passage à l'échelle des blockchains)
- Daniel Augot, Inria (cryptographie - gestion d'identité dans Bitcoin )
- Bruno Biais, HEC (économie - stabilité du consensus Bitcoin)

42 http://tokenomics2019.org/

43 https://www.bart-blockchain.fr/

- François Bobot, CEA LIST (vérification de programmes - vérification de *smart contracts*)
- Quentin Bramas, Université de Strasbourg (algorithmes distribués - passage à l'échelle des blockchains)
- Vincent Danos, ENS (informatique théorique - protocoles de blockchains)
- Cezara Dragoi, Inria, ENS (méthodes formelles - vérification de consensus de blockchains)
- Georg Fuchsbauer, Inria, ENS (cryptographie - protection de la vie privée dans les blockchains)
- Joaquín García-Alfaro, IMT Télécom SudParis (sécurité – sécurité et protection de la vie privée dans les blockchains)
- Georges Gonthier, Inria (méthodes formelles - vérification de *smart contracts*)
- Petr Kuznetsov, IMT Télécom Paris (algorithmes distribués - passage à l'échelle de la crypto-monnaie)
- Matthieu Latapy, Sorbonne Université (systèmes complexes - analyse de blockchains)
- Romaric Ludinard, IMT Atlantique (algorithmes distribués - passage à l'échelle de blockchains)
- Gérard Memmi, IMT Télécom Paris (réseaux - instrumentation et passage à l'échelle de blockchains)
- Julien Prat, CNRS, École Polytechnique (économie - bitcoin sustainability)
- Maria Potop-Butucaru, Sorbonne Université (algorithmes distribués - protocoles de blockchains, modèles d'incitations - interopérabilité des blockchains)
- Michel Raynal, Université Rennes 1, IRISA (algorithmes distribués - blockchains à consortium)
- Pierre-Yves Strub, École polytechnique (vérification de *smart contracts*)
- Yannick Seurin, ANSSI (cryptographie – multi-signatures pour Bitcoin)
- Sara Tucci-Piergiovanni, CEA LIST (formalisation des blockchains)

Nous avons ensuite exploré chacun de ces laboratoires et effectué des entretiens avec la plupart des chercheurs listés ci-dessus. Sur cette base, nous avons d'abord cerné leurs spécialités afin, dans un second temps, de les relier aux compétences nécessaires pour adresser les verrous identifiés dans ce rapport.

Les disciplines impliquées dans le développement de blockchains sont en effet nombreuses :

- Informatique
    - Systèmes distribués
    - Protocoles et réseaux
    - Bases de données et systèmes transactionnels
    - Langages de programmation et de modélisation (compilation)
    - Méthodes formelles (vérification, preuve, sémantique des langages de programmation)

- Mathématiques
  - Cryptographie
  - Optimisation (recherche de compromis, performances, sécurité, ressources)
  - Théorie des jeux
- Économie
  - Finance et nouveaux services financiers
  - Modèles et mécanismes : définition, étude et propriétés
  - Étude d'équilibres, évaluation de stratégies
- Droit
  - Droit des données personnelles
  - Droit des contrats électroniques
  - Droit international

Il n'était évidemment pas possible de recenser tous les laboratoires contribuant à ces différentes disciplines. Nous nous sommes donc focalisés sur les laboratoires directement impliqués dans les thématiques de recherche en support aux mécanismes fondamentaux des blockchains, que nous avons identifiés au sein d'unités relevant des disciplines classiques des référentiels de l'enseignement supérieur et de recherche. Il faut souligner pour autant une forte présence académique française dans des disciplines non directement ciblées dans cette étude, mais qui pourraient venir appuyer des développements futurs pour créer une ingénierie autour de la blockchain (c'est notamment le cas du génie logiciel).

Nous présentons, dans les sections suivantes, une cartographie synthétique des laboratoires français fortement impliqués dans les activités de recherche autour des blockchains, ainsi qu'une projection sur les domaines et thématiques de recherche permettant d'adresser les verrous identifiés en section 2.10.

## 5.2 Les laboratoires français au cœur des technologies de blockchain.

Notre démarche a permis de dégager les principaux laboratoires de recherche travaillant explicitement dans le domaine des blockchains et tout particulièrement sur les verrous identifiés précédemment dans ce rapport. Ils sont présentés dans la carte de la Figure 9. La cartographie distingue les champs liés à l'informatique et à la cryptographie de ceux liés à l'économie et au droit.

### 5.2.1 Cartographie des laboratoires

Les laboratoires cités dans la carte en Figure 9 ont tous publié dans des conférences de haut niveau et sont associés à des comités de programme de conférences du domaine. Pour la plupart, des travaux de thèse sont en cours. Leurs recherches s'articulent autour de trois grands axes :

1. contribution à la conception et à l'analyse de mécanismes internes et de programmation pour une blockchain de confiance ;

2. proposition et évaluation de modèles d'incitation pour des systèmes de blockchains équitables et durables ;
3. analyse économique des modèles de blockchain.

Concernant le premier axe, le plus important car il concentre les spécialités de différents métiers de l'informatique et de la cryptographie (en orange sur la carte), on constate une forte présence des laboratoires sur les points critiques concernant :

- les protocoles et algorithmes distribués pour les blockchains (analyse, vérification, conception) ;
- la cryptographie (algorithmes, vérification) et la cybersécurité des blockchains avec une évolution pour prendre en compte les aspects privacy ;
- la modélisation et les méthodes formelles (langages et vérification de *smart contracts*).

Concernant le second axe, on remarque quelques travaux sur les modèles de blockchains en liaison avec les principes d'incitation dans le cadre d'études transdisciplinaires (systèmes distribués, modèles de théorie des jeux) regroupant des informaticiens et des économistes. Cette tendance est nouvelle et encore peu développée. Elle nécessite des efforts en raison de différences culturelles entre ces domaines. L'organisation de la conférence *Tokenomics*[44] a été lancée précisément pour permettre des échanges et rapprocher les communautés.

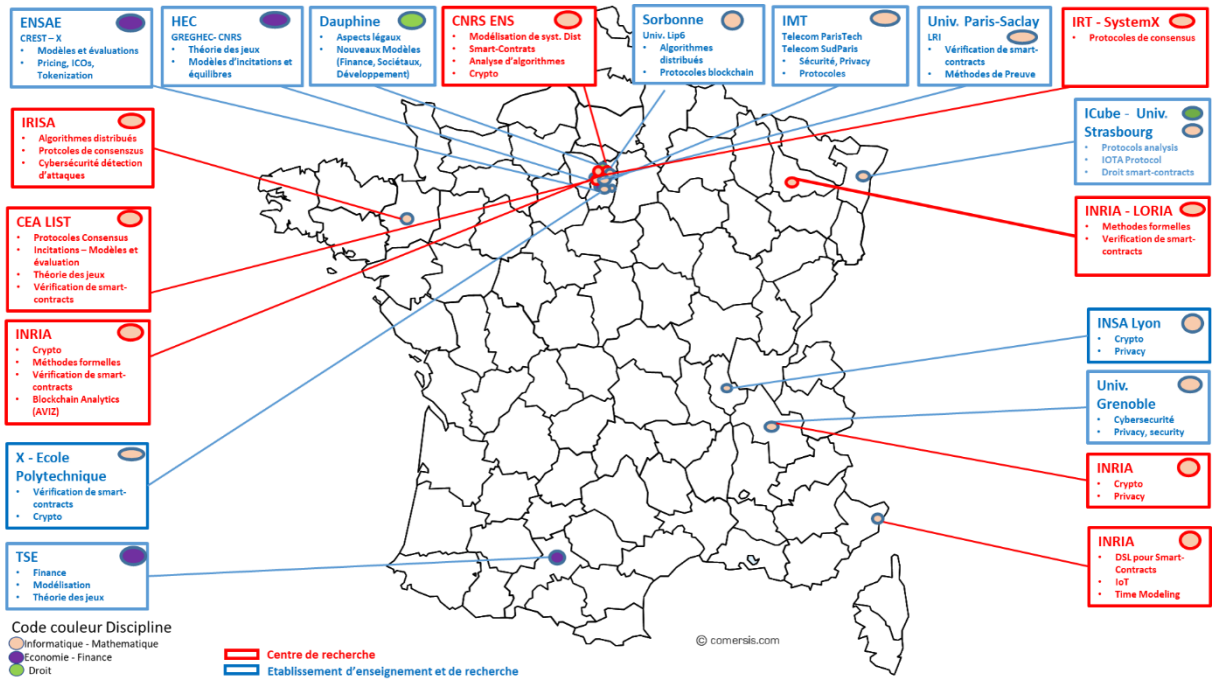



Figure 9 - Laboratoires français moteurs dans la recherche sur les blockchains

Concernant le troisième axe, plusieurs laboratoires s'intéressent à la modélisation et à des études d'équilibre ou d'impact des modèles de blockchain d'un point de vue économique (en violet sur la carte).

Enfin, quelques universités (en vert) conduisent des études sur les aspects juridiques liés à 1) l'utilisation de blockchains et 2) de *smart contracts*. Le premier point constitue un enjeu important pour la généralisation de services à base de blockchains en France, le second est encore

44 http://tokenomics2019.org/

grandement en discussion dans la mesure où le terme *smart contract* utilisé dans le monde des blockchains ne peut à ce jour nullement être apparenté à des contrats au sens juridique. Dans la plupart des cas, un *smart contract* est aujourd'hui un code informatique qui permet d'automatiser des actions relativement élémentaires au sein d'une blockchain.

À ce jour, la communauté est encore peu structurée même si des initiatives multiples se sont mises en place au cours des trois dernières années (séminaires, conférence Tokenomics, participation à des événements). La collaboration ou les échanges s'effectuent souvent sur la base d'initiatives individuelles ponctuelles.

### 5.2.2 Champs thématiques liés aux verrous et laboratoires

Pour aller plus loin et inventorier des opportunités de synergies pour adresser les verrous identifiés précédemment, nous proposons une cartographie par champs thématiques. Nous décrivons dans la Figure 10, la répartition des différentes dimensions nécessaires à la conception, la mise en œuvre et à la maîtrise des blockchains. Nous indiquons sur la carte ainsi obtenue, le positionnement des laboratoires français contribuant explicitement aux différentes thématiques identifiées. Enfin, nous projetons les verrous mis en évidence dans le chapitre 2 sur ces différents champs disciplinaires.

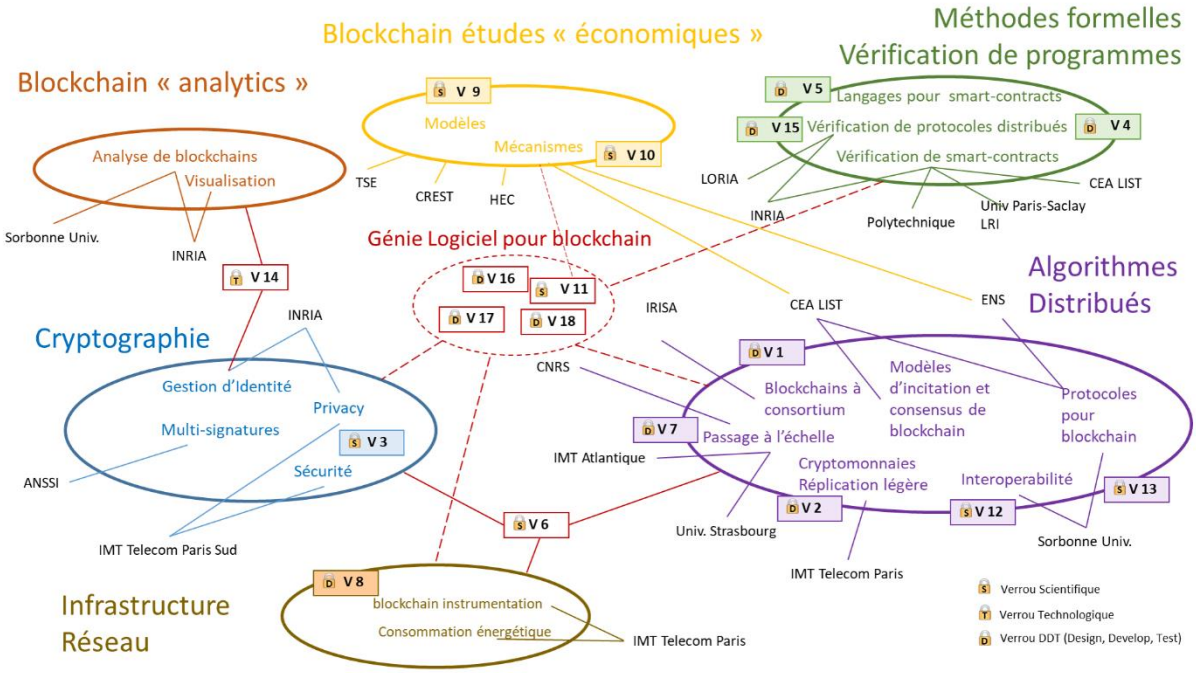



Figure 10 - Répartition des activités des laboratoires sur les verrous

Les verrous présentant un fond coloré sont identifiés et des travaux sont engagés à divers niveaux de maturité comme indiqué en section 2.10 (Figure 6). Les verrous transverses encadrés en rouge correspondent à une communauté et des activités à construire.

Cette figure appelle quelques remarques :

- le socle de base est constitué de compétences en : algorithmes distribués, cryptographie et réseaux. A cela s'ajoutent naturellement les compétences logicielles qui permettent de construire des solutions sûres et vérifiables ainsi que les moyens de programmation pour leur utilisation. En effet, s'il est possible de construire un système de blockchain à partir

de ces briques principales, la manière dont leur intégration doit être faite est en soi un axe de R & D qui nécessite des études amont si l'on veut garantir les propriétés qui permettront de justifier la confiance placée dans cette blockchain. Rappelons qu'il s'agit de substituer ces mécanismes à des tiers de confiance et que les enjeux sont critiques ;

- si les blockchains relèvent du champ des technologies de l'information, une de leurs spécificités est de nécessiter également un lien fort avec les sciences économiques et sociales pour prendre en compte le comportement des acteurs (utilisateurs, mineurs, voteurs) et étudier l'impact de différents choix (de politiques d'incitations par exemple). Réciproquement, les outils d'analyse et de simulation peuvent aider à mieux observer le comportement de modèles issus des sciences économiques. Cela ouvre la voie à de nouvelles transversalités entre informaticiens et économistes qui commencent tout juste à se concrétiser et qu'il est impératif de renforcer ;
- enfin, il est évident que de telles solutions ne peuvent être maîtrisées et déployées sans des outils d'analyse et de développement (du domaine du génie logiciel) adaptés au contexte des blockchains. Cette dimension n'est encore qu'à l'état embryonnaire et nécessite la mise en place de transversalités, mais en revanche, la France est très bien dotée de ce type de compétences et peut devenir un acteur majeur si l'on arrive à les mobiliser autour d'une action nationale commune (cf. recommandation 6).

### 5.2.3 Périmètre et limitations

Les acteurs de la recherche dans ce domaine relèvent de différents types d'institutions :

- laboratoires universitaires et écoles d'ingénieurs ;
- laboratoires internes à des grands groupes ;
- centres de recherche publics ;
- pôles de compétitivité et IRT (sur certains aspects).

Dans la cartographie présentée, nous n'avons retenu que des laboratoires académiques (i.e. relevant d'établissement d'enseignement supérieur, universités ou grandes écoles encadrés en bleu) ou liés à des organismes de recherche (Inria, CEA).

Au cours de l'étude menée, nous avons également consulté l'ANSSI, notamment pour ce qui concerne les aspects cybersécurité. L'agence ne figure pas dans la cartographie car son expertise cybersécurité n'y est pas spécifiquement liée aux blockchains.

Nous n'avons pas retenu :

- de pôle de compétitivité ; Systematic est bien présent dans le domaine des blockchains mais le pôle intervient plus dans le cadre d'animation d'un écosystème. Ilco-pilote notamment le nouveau projet *B-hub for Europe*[45] d'accompagnement des start-ups de l'écosystème blockchain dans le cadre de l'appel ICT 33 d'Horizon 2020 ;
- les laboratoires travaillant dans le cadre de projets qui visent l'utilisation de blockchains pour des besoins applicatifs. C'est le cas de l'Université de Lille qui est très impliquée dans le cadre du Partenariat européen de la Blockchain (PEB). Ils sont impliqués dans l'évaluation des technologies blockchains dans le cadre de la transition numérique pour les institutions et notamment les universités, pour différentes problématiques sensibles

45 https://b-hub.eu/

(identité et certificats vérifiables, enregistrement et vérification de diplômes, notarisation de documents, partage de données certifiées) ;

- les fondations diverses qui constituent plutôt un moyen de financement du développement de plateformes, que des centres de recherche. Néanmoins, en France, par exemple, les travaux de Nomadic Labs autour du développement de la blockchain Tezos sont financés par la fondation Tezos. Nomadic Labs à son tour noue des partenariats ou sous-traite des développements ou des expertises à Inria, au CEA ou à d'autres laboratoires.

Nous n'avons pas évoqué dans le cadre de l'étude, le rôle des organismes de normalisation comme l'AFNOR, même si des représentants du comité technique (CT 307) relatif aux blockchains ont été entendus. L'AFNOR contribue activement à la diffusion de la technologie et à l'émergence de référentiels avec d'autres organismes internationaux (ISO/IEEE, CENELEC, etc.). En revanche, les verrous technologiques identifiés dans le cadre de ce rapport demeurent du domaine de la recherche.

En conclusion, nous pouvons affirmer que la France est bien représentée en acteurs de recherche sur les sujets identifiés. En revanche, les équipes que nous avons consultées, sont souvent, malgré un haut niveau de compétence, de taille très réduite. D'où l'importance de créer une communauté scientifique autour de ces sujets qui permette aux jeunes chercheurs d'échanger. La création de projets fédérateurs peut être un moyen de stimuler ces échanges et de créer des synergies. C'est d'ailleurs une des recommandations de la mission.

## 5.3 Acteurs en Europe et dans le monde

Une cartographie des principaux laboratoires en Europe et dans le monde est présentée dans la Figure 11. Elle reflète une très grande activité à travers les trois pôles majeurs que sont : l'Amérique du nord, l'Europe ainsi qu'Israël et l'Asie, mais aussi des transversalités à travers de grandes collaborations comme IC$^3$ par exemple. Notons également une activité de recherche importante en Australie. Nous rappelons que si certains continents ou pays sont mal ou peu représentés ici, c'est que nous n'avons pas pris en compte les activités d'application des blockchains, mais les technologies y sont néanmoins bien présentes en Afrique du Nord, en Asie et en Inde et l'explosion des usages des blockchains est particulièrement significative en Chine. Enfin, la Russie est également très active et on la retrouve dans les instances de certification des blockchains tout comme la Chine.

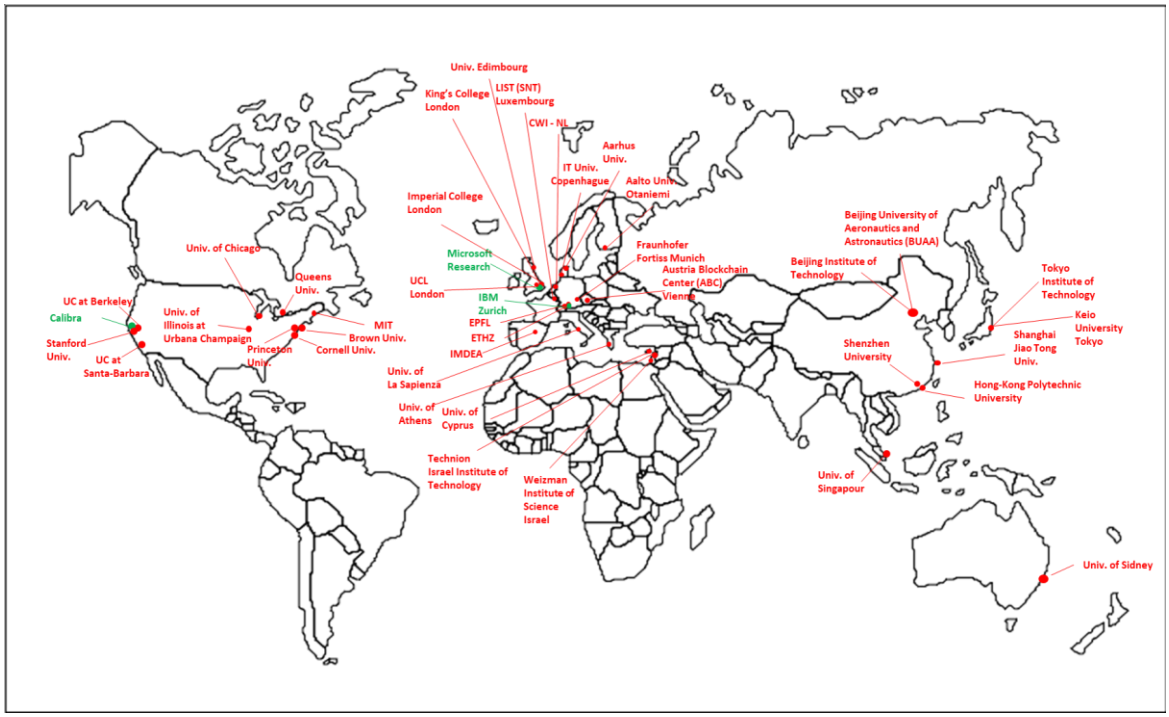



Figure 11 - Laboratoires de recherche dans le monde

## 5.3.1 La situation en Europe

***L'Europe*** est très active dans le domaine des blockchains, tant au plan de la recherche que du développement de plateformes.

***Au plan académique***, de nombreux pays s'impliquent dans le domaine.

Au Royaume-Uni (Londres et Édimbourg), en Suisse (EPFL et ETHZ), dans les pays scandinaves, notamment au Danemark (Aarhus et Copenhague) et en Finlande.

En Allemagne (Fraunhofer Fortiss), Autriche (TUV), Luxembourg (LIST et laboratoire SnT), l'activité des laboratoires est également dynamisée par la présence du centre de recherche IBM autour de Hyperledger, de la fondation IOTA, à Berlin ; ainsi que la création récente à Vienne de ABC (Austrian Blockchain Center) qui regroupe plusieurs laboratoires viennois.

En Espagne, l'IMDEA est un laboratoire mondialement reconnu dans le domaine ; l'activité de recherche autour des blockchains est aussi consolidée du fait de l'initiative Alastria qui permet de fédérer des expérimentations et de rapprocher les acteurs.

En Italie, l'université de Rome La Sapienza, est un acteur majeur notamment dans le domaine de la cryptographie et de la cybersécurité dans le contexte des blockchains.

En Israël, se concentrent les laboratoires majeurs pour tous les aspects cryptographie, cybersécurité et protocoles ; avec en tout premier lieu, Le Technion (aussi implanté à New York), l'Institut Weizmann, l'université de Tel Aviv et également très impliqués au sein de la collaboration IC[3]

À noter aussi la présence dynamique de la Grèce et Chypre et leur implication dans *IOHK*.

***Au plan des initiatives associant industriels et académiques :***

Dans ce contexte, quelques consortiums industriels ou fondations s'appuient directement sur des équipes universitaires pour les développements ou l'intégration de briques innovantes, de nouveaux algorithmes ou pour valider les choix techniques. Par exemple, *IOHK*, s'appuie sur l'université d'Édimbourg, King's College de Londres, l'université d'Athènes[46] et également l'Institut de Technologie de Tokyo[47] au Japon. La fondation Tezos finance des développements associant *start-up* et académiques dans le monde entier (dont en France Nomadic Labs par exemple qui développe des partenariats de recherche, Univ, INRIA, CEA). Des initiatives autour d'une plateforme, comme par exemple l'alliance Ethereum (Ethereum Enterprise Alliance – EEA), la fondation IOTA, Hyperledger recherchent la collaboration avec des académiques pour consolider leurs propositions.

***Au plan des initiatives fédératrices,*** il faut remarquer une accélération récente des créations d'organisations de différentes natures. Parfois, plutôt orientées vers le partage de connaissances, la sensibilisation, le conseil, ce sont plutôt des « Hubs » ou centres de compétences ; mais on remarque aussi la création de consortium ayant pour but la réalisation d'une blockchain. Ces initiatives se sont multipliées au cours des deux dernières années :

- The European Blockchain Center à Copenhague (ITU) ;
- ABC (Austrian Blockchain Center) à Vienne ;
- COBRA (Blockchain Research Center Aarhus) à Aarhus, qui développe la plateforme Concordium, et s'appuie sur des académiques nationaux et internationaux en coordination avec ETHZ en Suisse ;
- (EU blockchain Hub) au Luxembourg ,un centre d'excellence de la blockchain , créé en décembre 2019 ;
- le projet BOND en Finlande (Blockchain Boosting Finnish Industry).

Ces centres répondent en général à plusieurs objectifs : 1) mobiliser les acteurs du domaine et capitaliser sur leurs compétences pour assurer l'excellence de la recherche, l'innovation et le développement des nouvelles technologies de la blockchain ; 2) installer une culture et une communauté de compétences autour des blockchains, permettant notamment de proposer un support à la formation pour faciliter la diffusion de la technologie dans le monde industriel ; 3) contribuer aux standards.

Ces initiatives paraissent indispensables pour dynamiser et démultiplier l'impact des travaux sur les blockchains dans la perspective de la transition numérique qu'elles pourraient engendrer et son accompagnement. Leur financement peut être, selon les cas : national, le fruit d'un partenariat public privé, cofinancé par l'Europe.

Nous ne revenons pas ici sur les laboratoires français que nous venons de présenter dans la section précédente, mais nous pouvons signaler que des relations de collaboration et d'échanges nombreuses existent entre nos laboratoires et ceux que nous venons de citer en Europe et au-delà.

Il faut signaler ici une initiative intitulée Bsafe.network[48] qui regroupe des acteurs mondiaux de la recherche autour des blockchains sur les aspects technologiques mais aussi sociétaux et

46 National and Kapodistrian University of Athens

47 Tokyo Institute of Technology

48 http://www.bsafe.network/

économiques et dont l'un des animateurs est Joaquin Garcia-Alfarol, professeur à l'IMT - Télécom SudParis.

### 5.3.2 La situation en Amérique du Nord

***Aux États-Unis***, les laboratoires moteurs dans les blockchains sont en général aussi impliqués dans de grandes collaborations souvent soutenues par des fondations ou des entreprises. Certaines de ces collaborations font également appel à des collaborateurs européens :

- IC3[49] : une initiative regroupant Carnegie Mellon University, Cornell University, Cornell Tech, EPFL, ETHZ, UC Berkeley, University College London, University of Illinois Urbana-Champaign et The Technion (implantation de New York) ;
- CORDA/R3[50] : initialement un consortium de banques, l'ampleur prise par l'initiative nécessite des renforts venant du monde académique. Il est également très fortement représenté en Europe. Parmi leurs adhérents des banques françaises s'investissent fortement. Toutefois, la taille très importante du consortium peut poser des problèmes de gouvernance ;
- Calibra : en Californie, récemment l'équipe de Dahlia Malkhi (anciennement VMWare et Microsoft Research) a rallié cette l'initiative et y dirige une équipe.

Les recherches s'organisent au sein d'IC3 et de nombreux échanges s'effectuent au sein de séminaires. Par exemple la session d'automne 2019 au Simons Institute de Berkeley intitulée « *Proofs, Consensus, and Decentralizing Society* » rassemblait les plus grands experts du domaine, avec la participation de chercheurs français : Vincent Danos de l'ENS, Julien Prat du CNRS, Georg Fuchsbauer d'Inria, Linda Shilling de l'École Polytechnique.

L'adoption de technologies blockchains pour des besoins plus régaliens est également explorée à des échelles locales. Par exemple, l'État de l'Illinois s'implique très fortement dans l'utilisation des blockchains et conduit des expérimentations autour de l'identité numérique, la santé etc. Il a notamment rejoint R3 et l'alliance Ethereum (EEA).

Ainsi, à Chicago, le *Chicago Blockchain Center* (CBC), créé en 2017, rassemble, des expertises académiques, technologiques, mais aussi des économistes et dirigeants ainsi que des officiels gouvernementaux.

Dans le domaine de la sécurité, le NIST conduit des actions de veille et de standardisation sur les blockchains et tout particulièrement sur le sujet de l'identité numérique.

### 5.3.3 La situation en Asie

***En Asie***, les activités de R & D sont très intenses dans le domaine, les places fortes de la recherche sur les blockchains sont Singapour (Y-NUS), Hong Kong (Hong-Kong Polytechnic University), Shanghai (Shangai Jiao Tong University). Dans le domaine, Singapour University et des universités chinoises spécialisées notamment en télécommunications et cybersécurité (BUAA, Beijing Institute of Technology, Shentzen University)sont particulièrement renommées.

En Chine, sa présence est remarquable, sur le terrain du développement d'applications à base de blockchains notamment autour d'applications commerciales et financières. Une récente étude

49 https://www.initc3.org/about.html

50 https://www.corda.net/history/

de PwC[51] montre la part grandissante de l'Asie dans le domaine qui pourrait la porter au premier rang mondial. Malgré quelques excellentes universités, la majeure partie des implications dans ces technologies est orientée vers les applications. Il faut aussi souligner une forte implication dans les actions de normalisation, secteur pour lequel ils vont très vite et déposent beaucoup de brevets.

Au Japon, plusieurs centres d'excellence sont à la pointe de la recherche dans le domaine. Nous avons déjà mentionné l'institut de technologie de Tokyo qui contribue à IOHK, il faut citer aussi Keio University.

***En Océanie***, des équipes de recherche sont présentes en Australie et en Nouvelle Zélande. En Australie, une équipe de l'université de Sydney, sous la direction de Vincent Gramoli, professeur associé et chercheur formé en France[52], a développé la blockchain Red Belly. L'État australien soutient activement les initiatives autour des blockchains et a identifié récemment un besoin en experts dans les domaines des blockchains et de la cybersécurité.

## 5.4 Conclusion

Il faut souligner que cette cartographie de la recherche en France dans le domaine de la blockchain n'est pas exhaustive d'une part parce qu'elle ne couvre que des travaux portant sur les fondamentaux de la blockchain et non leur utilisation, et d'autre part parce qu'il s'agit d'un domaine très dynamique en cours de constitution donc encore non stabilisé.

En conclusion, la France dispose d'un noyau d'expertise se plaçant au plus haut niveau scientifique sur les technologies au cœur de la blockchain et en particulier sur les compétences couvrant les aspects consensus, sécurité/confidentialité ainsi que vérification et preuve. Elle est aussi bien reconnue dans la communauté scientifique internationale. Pour tirer parti plus amplement de ces compétences qui sont encore développées de manière relativement isolées, il serait bon de trouver des modalités pour favoriser les synergies entre les équipes et renforcer leur pouvoir catalyseur vis-à-vis d'actions d'innovation. Au plan de l'animation scientifique nationale, plusieurs réseaux de séminaires commencent à faciliter les échanges entre chercheurs des différentes disciplines impliquées. Mais il faut pouvoir aller au-delà et mobiliser également des chercheurs dont les disciplines ne sont pas directement ou pas assez impliquées à ce jour dans le domaine (comme par exemple le génie logiciel, les compétences en matière de méthodes formelles et de preuve) mais aussi des compétences en cybersécurité et en protection/confidentialité qui sont développées au plus haut niveau mais encore peu appliquées aux technologies blockchain. Les recommandations 5, 6 et 9 vont directement dans ce sens.

Soulignons aussi la forte implication de certains chercheurs de disciplines comme l'économie, le droit, les sciences sociales, encore peu nombreux mais qui peuvent enrichir notablement les angles d'analyse. Des transversalités avec les équipes de recherche en informatique peuvent conduire à des solutions originales et équilibrées en permettant l'expression d'une vision système globale, prenant en compte notamment impacts sociétaux et environnementaux dans la perspective de la transformation digitale dont la blockchain sera un élément majeur.

51 https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html

52 Vincent Gramoli a préparé sa thèse à Inria sous la direction du Professeur Michel Raynal.

# 6 CARTOGRAPHIE DES FORMATIONS

## 6.1 Démarche et limitations

### 6.1.1 Démarche

Pour répertorier les formations blockchain dans l'enseignement supérieur en France, les universités et les grandes écoles ont été invitées à répondre à un questionnaire (Annexe D). Elles ont reçu par courriel un message relayé par le MESRI, basé sur la liste des vice-présidents formation et vice-présidents numérique des établissements universitaires. Les grandes écoles ont reçu l'invitation à remplir le questionnaire par le truchement de la Confédération des Grandes Écoles.

Les membres de la mission ont également interrogé directement les enseignants-chercheurs du domaine avec lesquels ils étaient en contact afin d'identifier les cours qu'ils pouvaient donner. Les principaux chercheurs dans le domaine ont ainsi été sollicités.

Une étude des formations à la blockchain à l'étranger (Europe et reste du monde) a également été menée. Nous avons d'abord sélectionné les universités les plus importantes puis examiné leurs sites Web à la recherche de cours donnés sur la blockchain, pour extraire les informations nécessaires, en nous limitant au niveau master.

### 6.1.2 Limitations et choix

Nous avons volontairement écarté les formations de moins de 12 heures dans notre collecte. Nous estimons qu'en dessous de cette durée, il est difficile de construire une compétence solide dans le domaine des technologies blockchains, qui est à l'intersection de plusieurs disciplines fondamentales.

Nous avons également et naturellement concentré notre étude sur les formations diplômantes de l'enseignement supérieur. Et nous n'avons pas inventorié les séminaires ou les « *summer schools* », souvent difficiles à identifier, avec un contenu changeant et elles ne sont pas toujours adossées à une structure de l'enseignement supérieur. Dans certains cas, ce sont des formations d'introduction à la blockchain, à la limite de la vulgarisation ou de la culture générale.

Cependant, ces formations que nous n'avons pas cartographiées sont assez nombreuses et forment un tissu éducatif important pour l'éveil à la technologie blockchain et dans certains cas, préfigurent les syllabus des formations diplômantes.

À travers les réponses obtenues au questionnaire, nous n'écartons pas la possibilité de quelques manques (peut-être que certaines universités n'auraient pas répondu alors qu'elles dispensent une formation blockchain significative), mais cela reste limité. De plus, cette cartographie est une photographie à un temps « *t* »qui ne saurait refléter ou prédire l'évolution des formations dans le domaine de la blockchain.

Les programmes d'enseignement des établissements du supérieur évoluent au rythme des vagues d'accréditation. De nouvelles formations portant sur la blockchain sont en préparation dans plusieurs universités ou écoles mais ne seront identifiables que dans un an ou deux. Ceci constitue la principale limitation de notre travail de cartographie sur la France. En revanche, ce recensement permet d'avoir une image fidèle de l'état des lieux actuel des formations académiques sur la

technologie blockchain. Et, même si le biome des formations du supérieur dans ce domaine évolue constamment, cette cartographie est une bonne base pour cibler les éventuelles mesures à prendre pour améliorer l'offre des formations et déterminer la position de la France dans ce domaine vis à vis des autres pays.

La détermination du périmètre des formations à la blockchain est une autre difficulté qu'il convient de souligner. Une particularité importante de la technologie blockchain est qu'elle est au confluent de plusieurs disciplines. Elle se base sur la cryptographie, l'algorithmique distribuée, la sécurité informatique ou encore la vérification des logiciels qu'elle mêle intimement de manière originale et subtile. Nous avons donc identifié les formations à la pointe dans ces disciplines qui font le lien avec la technologie blockchain (bien qu'être à la pointe dans l'une de ces disciplines ne signifie pas que l'on maîtrise la technologie blockchain dans son ensemble).

### 6.1.3 Structuration de la cartographie des formations

Nos objectifs lors de l'élaboration de cette cartographie étaient au nombre de 4 :

1. dénombrer les formations sur la blockchain ;
2 positionner géographiquement et thématiquement les formations ;
3 identifier les établissements leaders dans les formations à la blockchain et repérer les lacunes et axes de progression dans l'offre globale de formation ;.
4 pouvoir comparer avec ce qui se fait ailleurs.

Les données collectées sont en nombre insuffisant pour qu'un traitement statistique significatif puisse être déployé. Nous avons donc mené une analyse majoritairement qualitative. Cependant, lorsque cela était possible une analyse quantitative a été réalisée afin de mettre en place des jalons pour mesurer les évolutions ultérieures de l'offre de formations.

## 6.2 Présentation des résultats

### 6.2.1 Localisation des formations en France

Les formations sont principalement situées dans le bassin parisien, avec près de 56 % de l'offre nationale en terme de nombre de formations et 81 % en terme d'heures de formation. On y trouve à la fois des formations sur le cœur de la technologie blockchain et des formations techniques sur l'intégration d'une blockchain dans un système (correspondant à un profil type *fullstack*). En parallèle, on y trouve des formations en économie, finance et droit traitant de la problématique blockchain dans ces domaines.

En termes d'offre de formation, la forte concentration en région parisienne n'est donc pas écrasante puisque la part de la province est similaire. Par contre, si l'on considère le nombre d'heures de formation, elle est en revanche bien plus imposante. Cela démontre que les formations à Paris et dans sa région sont globalement plus poussées que celles données en province puisqu'elles contiennent plus d'heures.

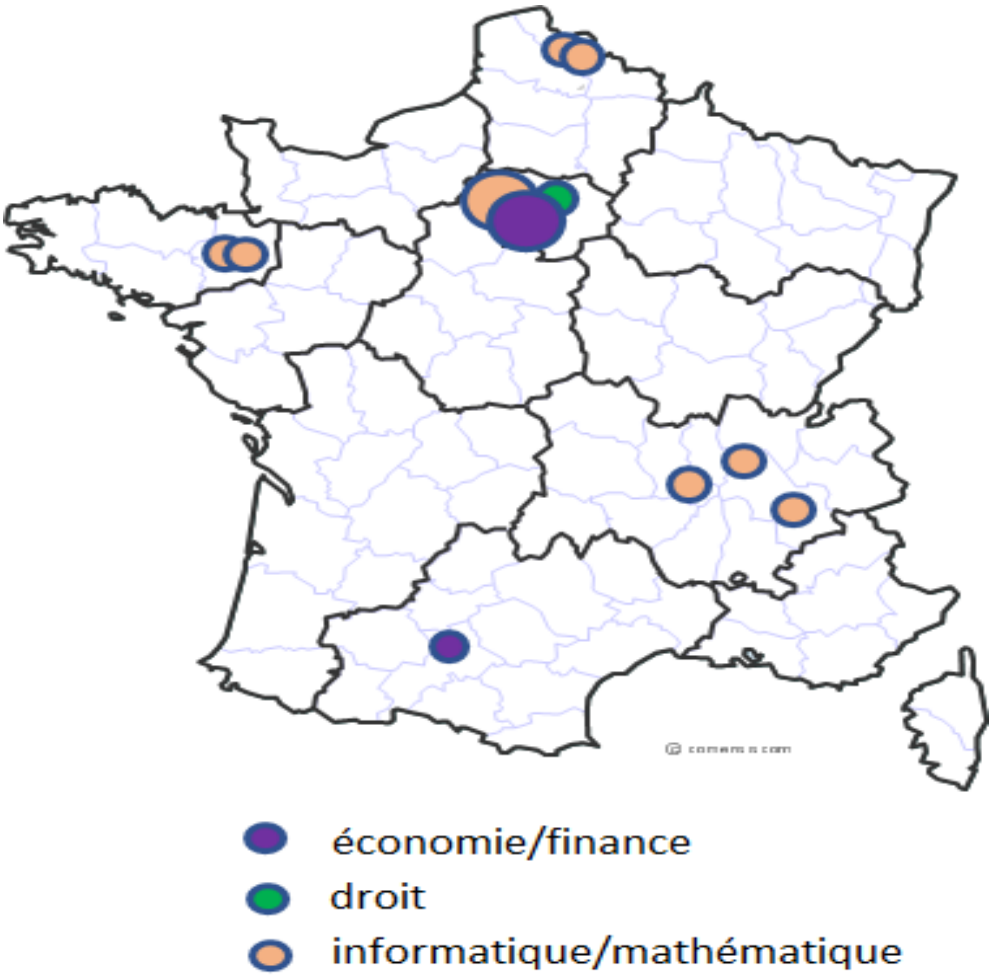



Figure 12 - Formations blockchain en France

De plus, hors Paris, l'offre de formation n'est localisée que dans quelques villes. Nous n'en avons pas répertorié en Corse ni outre-mer.

Près de 80 % des formations identifiées se font dans des grandes écoles qui possèdent un laboratoire dont les équipes (au moins un chercheur) travaillent sur les problématiques liées à la blockchain. Selon notre étude, la part des formations proposées par les universités demeure encore en retrait.

### 6.2.2 Cartographies thématiques

#### Les établissements

Nous listons ci-après les principales formations académiques à la blockchain que nous avons identifiées ainsi que leurs contenus disciplinaires.

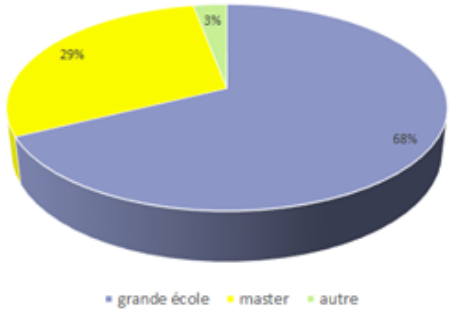
| Etablissement | Domaine disciplinaire abordé | | | | | | | | | Vol (h) | Effectif |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Info théorique | Systèmes distribués | Cyber sécurité | Systèmes d'Info | Cryptographie | Droit | Finance | Economie | Autre | | |
| Alyra | ■ | ■ | | | ■ | | | | | 350 | 16 |
| CentraleSupélec | ■ | ■ | | ■ | ■ | | | | | 24 | 35 |
| Ecole Polytechnique | | ■ | | | ■ | | | ■ | | 27 | 30 |
| Efrei Paris | | ■ | | ■ | | | ■ | ■ | | 35 | 40 |
| EISTI cyber | | | ■ | | | | | | | 42 | 26 |
| EISTI finance | | | | | ■ | | ■ | | | 45 | 18 |
| EISTI master IoT | | ■ | ■ | | ■ | | | | | 24 | 25 |
| ENSIIE | | | ■ | | ■ | | | | | 21 | 6 |
| EPF | ■ | ■ | ■ | ■ | | | | | | 30 | 50 |
| EPF école d'ing | | | | ■ | | ■ | ■ | ■ | Transfo digitale | 35 | 55 |
| ESGI | ■ | ■ | | ■ | ■ | ■ | | ■ | | 450 | 15 |
| ESGI (Paris 12) | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | 540 | 15 |
| ESIGELEC | | | | ■ | ■ | | | | | 60 | 30 |
| ESIGELEC | | | ■ | ■ | | | | | | 20 | 30 |
| HEC | | | | | | | ■ | ■ | | 12 | ? |
| Imag Grenoble | | | ■ | | ■ | | | | | 35 | 35 |
| IMT Atlantique | ■ | ■ | | | ■ | | | | | 21 | 20 |
| IMT Atlantique | ■ | ■ | | | ■ | | | | | 40 | - |
| INSA de Lyon | | ■ | ■ | | ■ | | | | | 32 | 20 |
| INSA de Lyon | | ■ | ■ | | ■ | | | | | 86 | 120 |
| ISEL | ■ | | | ■ | | ■ | | ■ | | 24 | 8 |
| ISEN - Yncréa H d F | ■ | | ■ | ■ | ■ | | | | | 30 | 35 |
| Paris-Diderot | ■ | ■ | | | ■ | | | ■ | | 24 | ? |
| Polytech Sorbonne | ■ | ■ | ■ | ■ | ■ | | | ■ | | 15 | 20 |
| Rennes 1 | ■ | ■ | ■ | | | | | | | 20 | ? |
| Telecom Paris | ■ | ■ | | | | | | | | 24 | 15 |
| Telecom Paris | | | ■ | | | | | | | 24 | 20 |
| Télécom St-Etienne | | ■ | ■ | ■ | | | | | | 12 | 20 |
| Université de Lille | | | | | ■ | | | ■ | | 192 | 25 |
| | | | | | | | | | | 2294 | 729 |

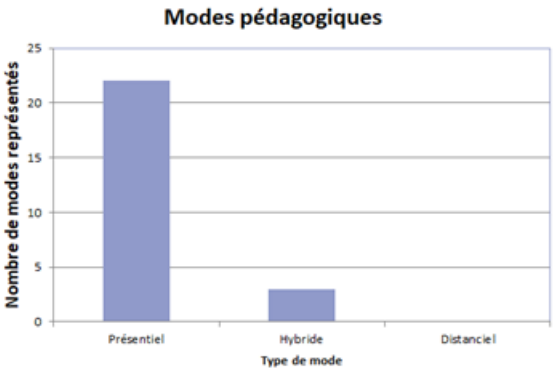
Remarques générales :

- le total annuel des heures enseignées est de près de 2 300 ;
- malgré les données incomplètes et variant d'une année à l'autre, on peut estimer le nombre d'élèves solidement formés à la blockchain à moins de mille par an ;
- l'ESGI et Alyra offrent des formations pointues entièrement dédiées à la blockchain ;
- l'Université de Lille propose un master de mathématique de plus de 900 heures dans lequel 192 heures sont exclusivement consacrées à la cryptographie et la finance en lien avec la technologie blockchain ;
- l'École d'ingénieur IMT Atlantique ouvre en février 2020 un enseignement de spécialité de 40 heures sur la blockchain. Le nombre d'élèves qui le suivront devrait être d'environ 25 ;
- l'Institut européen F2i, non présent dans le tableau, propose un Mastère Expert Digital Blockchain bénéficiant d'une certification professionnelle européenne enregistrée au RNCP.

## La pédagogie

Nous présentons ici quelques facettes de l'enseignement de la blockchain en France.

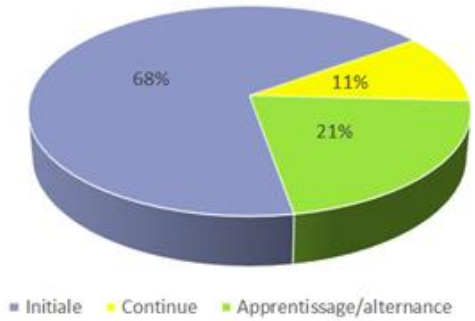


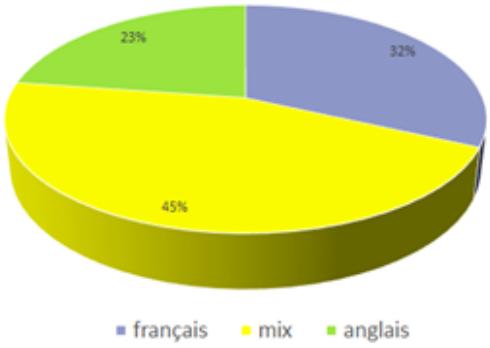




Tout d'abord, nous avons dénombré une grande majorité de formations provenant de grandes écoles. La proportion des masters est assez faible (29 %). Ces masters se jouent aussi bien à l'université qu'en école d'ingénieur ou de commerce. Cela signifie que peu de formations sur la blockchain se déroulent à l'université. Nous n'en avons relevées que 4. Certaines universités sont en train de construire de nouveaux masters et n'ont pas répondu à notre sondage.

Classiquement, la plupart des formations sont données en présentiel. Quelques cours se font en hybride c'est-à-dire avec une partie en présentiel et une partie à distance. Aucun enseignement académique ne se fait totalement à distance.

La grande majorité (68 %) des formations sont initiales (contre 11 % en formation continue) comme on pouvait s'y attendre. Mais il faut remarquer que plus d'un cinquième des formations se font en alternance. Cela est de bon augure pour les prochaines ouvertures de formation car par "mimétisme" la tendance devrait se poursuivre. Les formations d'ingénieurs ou techniciens en alternance impliquant les entreprises, cela montre les relations déjà établies entre les milieux académique et industriel dans le domaine de la blockchain.




De même, et c'est une bonne surprise, il faut noter que les formations en langue anglaise ou incluant de l'anglais sont majoritaires. Cette spécificité (qui est un atout) montre l'ouverture à l'international de ces formations qui se donnent ainsi le moyen d'attirer des étudiants non francophones et de préparer nos étudiants à l'internationalisation.

# 6.3 Comparaison avec l'international

## 6.3.1 Présentation

Pour chaque pays, nous avons recensé, dans le tableau suivant, les universités proposant des cours sur la technologie blockchain. Puis nous commentons ci-dessous les résultats de nos investigations. Ce travail se veut indicatif et non exhaustif. En effet, seulement une sélection des grandes universités a été considérée. En outre, au sein de cet échantillon, les pages web des programmes ne sont peut-être pas à jour et d'autre part il n'est pas facile d'être sûr des contenus d'un cours à partir des descriptions parfois très succinctes. Néanmoins cette cartographie a le mérite de fournir une première idée des forces en présence et d'aider à dégager des tendances marquées à l'étranger.

| Zone géographique | Pays | Université | Nombre de cours | Intitulés |
|---|---|---|---|---|
| **Asie/Océanie** | | | **25** | |
| | **Chine** | Peking Univ. | 1 | Blockchain Technology and Application (32 h) |
| | | Tsinghua Univ | 3 | iCenter Blockchain Technology Development Open Class ;Blockchain and cryptology ; Cyber intelligent Economy and Blockchain |
| | | Fudan Univ. | 1 | Blockchain Technology Lecture |
| | | Shanghai Jiao Ton Univ. | 1 | Blockchain Investment and Application Practice International Cours |
| | | Tonji Univ. | 5 | Blockchain technology and industry development, Ethereum, Hyperledger, PoC Practice, Top blockchain company business tour |
| | | Zhejiang | 1 | Blockchain and Digital Currency |
| | | Beihang | 2 | Blockchain Principles and Technologie ; Blockchain Experiments and Engineering Practices |
| | | Xidian | 1 | Blockchain technology Principle and development Practices and Digital Currency |
| | **Singapour** | Nanyang Univ. | 2 | CE7490 Distributed Systems ; CE7428 Computer and Network Security |
| | **Hongkong** | Hongkong Univ. | 5 | BC 202: Asset Tokenization & Digital Fiat ; BC 203: Governance & Compliance ; BC 204: Solutions Architecture ; BC 205: Fintech - Financial Technology ; BC 301: Blockchain Engineering - R3 Corda |
| | **Australie** | Sydney Univ. | 3 | Cryptocurrency Markets and Investments ; Distributed Systems ; Issues in Electronic Commerce |
| | **Inde** | IIT Madras | 1 | CS5666 - Foundations of Blockchain Technology |
| | | | | |
| **Europe** | | | **15** | |
| | **Italie** | Turin | 1 | Blockchain&Payments (module du master de cybersécurité) |
| | | Trento | 1 | Distributed system 2 |
| | | Pisa | 1 | Peer to Peer Systems and Blockchains |
| | **Suisse** | EPFL | 1 | CS451 Distributed Algorithms |
| | | Zürich | 1 | 227-0555-00L Distributed Systems |
| | **Danemark** | IT Univ. Copenhagen | 2 | Blockchain Economics ; Cryptographic Computation and Blockchain |
| | **GB** | Edinburgh | 1 | Blockchains and Distributed Ledgers |
| | **Chypre** | Nicosia | 1 | Master in Digital Currency |
| | **Malte** | Malte | 3 | Trois Masters of Science in Blockchain and Distributed Ledger Technologies dont deux en économie et droit |
| | **Espagne** | Barcelona | 1 | Global master in blockchain technology (en ligne) |
| | | Univ. Europea Madrid | 1 | Postgrado de Experto en Blockchain |
| | **Allemagne** | Frankfurt | 1 | Frankfurt School Blockchain Center (en ligne) |
| | | | | |

| | | | | |
|---|---|---|---|---|
| **Amériques** | | | **41** | |
| | **USA** | Stanford | 16 | CS251: Cryptocurrencies and blockchain technologies ; CS359B Designing Decentralized Applications on Blockchain ; CS02 Blockchain, Machine Learning, IoT and more ; LAW1044 Blockchain and Cryptocurrencies: technical Background ; ECON 152/ECON 252/PUBLPOL364/STAT238/LAW1038 The Future of Finance ; STRAMGT547 Riding the Next Wave in Developing Economies ; BUS35 The Business Basics of Blockchain, Crypto Currencies and token ; MGTECON515 Cryptocurrency ; LOW1031 Current Issues in Business Law |
| | | Austin | 2 | EE 382N-11: Distributed Systems |
| | | Cornell | 8 | CS 5094 - [Introduction to Blockchains, Cryptocurrencies, and Smart Contracts] ; CS 5433 - Blockchains, Cryptocurrencies, and Smart Contracts ; NBAY 5710 - Cryptocurrencies and Blockchains ; MGMT 5225 - Systems and Analytics ; LAW 6536 - Internet Transactions ; LAW 6459 - Law of FinTech ; CS 6432 - Distributed Consensus and Blockchains ; CS6466 Cryptocurrencies and smart contract |
| | | MIT | 1 | Blockchain Technologies : Business Innovation and Application (self-paced online) |
| | | Buffalo | 2 | CSE 4/526 Blockchain Application Develop |
| | | Berkeley | 2 | CS 198-077. Blockchain for Developers DeCal ; CS 198-078. Blockchain Fundamentals DeCal |
| | | UCLA | 1 | Law 561A/B - Bitcoin, Blockchain, and the Future of Transactional Practice |
| | | Columbia | 3 | Topics to signal processing — intro to blockchain tech ; Intro to blockchain, Cryptos and analytics ; Tech policy and culture in developing world |
| | | Princeton | 3 | COS435/ELE432 Information security ; COS597A/COS597J Advanced topics in computer science |
| | | Yale | 3 | F&ES1153 Blockchain-supplychainWKS ; CPSC367 Cryptography and security ; CPSC512 Designing the digital economy |
| | | | | |

### 6.3.2 Remarques générales

Comparativement à l'offre totale en informatique, nous n'avons identifié que peu de cours technologiques spécifiquement orientés blockchain parmi les grandes universités dans le monde (cette remarque s'applique un peu moins aux USA). Alors même que le blogue *Coinbase* relatait qu'en 2018 42 % des 50 premières universités mondiales proposaient au moins un cours sur la cryptographie ou la blockchain. De notre côté, n'ont été listés que les cours dont le syllabus est accessible ou, s'il est absent, pour lesquels le titre est assez précis. En règle générale, il y a peu de cours clairement fléchés blockchain.

Des cours en finance, économie et droit traitant de la blockchain sont également proposés par les universités. Ces cours sont nombreux, relativement aux cours purement technologiques. Nous en avons identifié au moins 26 significatifs. D'autres existent probablement mais nous nous sommes plutôt concentrés sur la recherche des cours en informatique puisque la mission est axée sur les verrous technologiques et scientifiques. **Il y a donc clairement une appropriation du sujet blockchain dans les enseignements en finance, en droit ou en sciences économiques de par le monde.**

Plusieurs universités étrangères proposent des programmes « *graduate* » (correspondant à master, niveau bac+4 et bac+5) en informatique, qui incluent des parcours traitant des principales avancées théoriques et technologiques qui constituent la blockchain (systèmes distribués, informatique théorique, cryptographie, sécurité…). Cependant, ces cours sont souvent répartis dans plusieurs spécialisations ou plusieurs modules « à la carte » parfois épars. Ainsi,des élèves peuvent se construire des parcours qui les forment de manière incomplète ou superficielle. Il n'y a, au final, qu'une petite proportion de programmes dans lesquels les élèves sont formés à l'ensemble des facettes de la technologie blockchain dans un cursus intégré et purement dédié blockchain. **Aussi, sur ce point, la France ne semble pas en retard.**

Enfin, il existe beaucoup de MOOC sur la blockchain dans plusieurs langues sur les grandes plateformes de MOOC (Coursera, edX, Udemy, FUN…). En règle générale, ces formations, ouvertes

à tous, ne sont pas du niveau d'un cours académique de master spécialisé en informatique mais plusieurs universités (en particulier américaines) ont développé des MOOC ou des cours en ligne sur la blockchain nécessitant des prérequis, qu'elles ont incorporés à leur cursus. Dans notre étude, nous avons fait le choix de ne pas nous concentrer sur l'offre MOOC ou de cours en ligne directement accessibles sur les sites des universités. Il pourrait cependant être judicieux d'initier un recensement exhaustif spécifique de ce type de formation à la blockchain dans le monde et d'en assurer le suivi. Cette collecte d'informations aurait un triple avantage :

1. en regroupant les liens recensés sur un portail officiel, elle fournirait un catalogue riche de formations à la blockchain utilisable dans le cadre de la formation continue et initiale ;
2. elle permettrait d'évaluer la position de la France sur le terrain des formations innovantes à la blockchain ;
3. elle constituerait un observatoire des tendances en matière de formations à la blockchain.

### 6.3.3 Le cas de l'Asie

Malgré nos recherches, pour nombre d'universités prestigieuses d'Asie, il ne nous a pas été possible de trouver des cours portant sur la blockchain. Cependant, si ni l'université de Kyoto ni celle de Tokyo n'affichent clairement de cours blockchain sur leur site Web, nous apprenons que cette dernière vient de recevoir une donation de 800 000 dollars pour monter un cours blockchain de trois ans destiné à former des « entrepreneurs blockchain ». Signalons également au passage que, principalement pour une bonne proportion des universités de Chine et du Japon que nous avons examinées, certaines pages de description de cours sont manquantes ou pas toujours remplies ou encore parfois non disponibles en anglais. Difficile dans ces conditions de se faire une idée claire des contenus pédagogiques proposés. Il est probable que les formations que nous avons identifiées ne soient que la partie émergée d'une offre plus vaste, d'autant plus que l'écosystème blockchain semble être développé dans cette région du monde (voir partie réflexions et recommandations).

### 6.3.4 Le cas des USA

Au niveau mondial, les États-Unis semblent avoir pris un certain *leadership* dans les formations académiques sur la blockchain, de par leur nombre, leur niveau et leur pénétration dans plusieurs disciplines (sciences, économie, juridique, commerce, finance…). Toutefois, les meilleures universités américaines ont aujourd'hui des offres très inégales en termes de quantité de cours donnés sur la blockchain. Certaines n'affichent pas de cours dédiés à cette technologie, d'autres en proposent plus d'une dizaine ! Notons enfin que les universités de Stanford et Cornell se démarquent avec un grand nombre de cours spécifiquement sur la blockchain et dont une bonne partie sont techniques et approfondis. De plus, de même qu'à Berkeley, la fréquentation de ces nouveaux cours s'avère très élevée et des candidatures sont refusées faute de places.

À cela s'ajoutent de nombreux cours en ligne sur la blockchain développés par les plus prestigieuses universités. Certains sont des cours inclus dans un programme d'enseignement auquel il faut être inscrit, d'autres sont des MOOC à l'accès totalement ouvert. Ces MOOC sont régulièrement suivis par des étudiants du monde entier. Dans la majorité des cas, ils sont payants et délivrent des certificats. La *Sloan School of Management* du MIT propose, par exemple, en plus du cours que nous avons relevé, plusieurs autres cours en ligne plus tournés vers les finances et la gestion.

Soulignons également des initiatives originales comme celle de l'association d'étudiants de Berkeley qui propose des cours[53] de tous niveaux sur la blockchain. L'université soutient totalement ce projet. C'est un modèle d'enseignement dont il pourrait être bon de s'inspirer.

Notons enfin une tendance générale (et très marquée aux USA) à décliner les sites internet des universités avec un nom de domaine commençant par « blockchain » ce qui offre une visibilité (et une lisibilité) intéressante.

### 6.3.5 Le cas de l'Europe

Nos voisins les plus proches proposent principalement des programmes sur la blockchain dans le cadre de masters. Hors France, le centre de gravité de l'offre est plutôt décalé vers l'Europe du Sud. Nous remarquons en effet, étonnamment, une offre académique qui semble actuellement encore peu développée (ou peu lisible) en Allemagne et Grande Bretagne, deux grands pays, tandis que les petites îles de Chypre et Malte ont dès à présent plusieurs offres de master en blockchain. La Suisse tire également très bien son épingle du jeu.

Là aussi, à ce stade, la France est bien positionnée. Il faut néanmoins s'assurer de la visibilité à l'étranger de nos offres de master en blockchain.

### 6.3.6 Réflexions et recommandations

Dans l'ensemble, l'offre de formation à la blockchain est en rapide développement. Notre système de formation académique n'est pas, pour le moment, en retard dans ce domaine par rapport aux autres pays où le manque d'offres pédagogiques diplômantes est patent dans de nombreux pays. Un rapport de Forkast[54] alerte ainsi sur le manque de formations en Chine mais signale dans le même temps que le problème est mondial. Néanmoins les choses bougent vite et vont changer dans les deux ans qui viennent : nous avons lu sur le Web que de nombreux financement affluent vers les universités étrangères pour monter des cours ambitieux sur le domaine. Dans le cas des technologies émergentes, des offres pédagogiques nouvelles apparaissent continuellement : les offres en termes de MOOC, séminaires ou ateliers sont nombreuses mais non systématiquement relevées dans cette étude.

Les étudiants forment aussi des associations dont le but est de diffuser les compétences dans ce domaine.

Sur le plan pédagogique, des universités américaines proposent parfois des « coding bootcamps »[55][56] dédiés à la blockchain. Une pratique qui pourrait être, avec profit, encouragée en France. L'État pourrait y contribuer de diverses manières : lancement de programmes dédiés, d'appels à projet, de valorisation des pratiques existantes, de financement d'associations pionnières, etc. Il pourrait s'assurer de leur visibilité en les faisant recenser sur les portails de recensement dédiés[57].

---

53 https://blockchain.berkeley.edu/

54 Forkast.Insights | China Blockchain Report 2019-2020 consultable à : https://forkast.news/wp-content/uploads/2019/12/Forkast.Insights-China-Blockchain-Report-2019-2020.pdf

55 Un « *coding bootcamp* » est un programme de formation court qui enseigne les compétences en programmation que les employeurs recherchent. Les « *coding bootcamps* » permettent aux étudiants ayant un manque de compétences en programmation de se concentrer sur ces aspects sur un laps de temps court et de pouvoir appliquer rapidement leurs nouvelles compétences dans leurs projets.

56 Voir par exemple https://www.coursereport.com/subjects/blockchain

57 Par exemple https://www.switchup.org/rankings/best-coding-bootcamps

Les concours internationaux de programmation sont un excellent moyen de détecter les meilleurs étudiants directement opérationnels sur un sujet donné. Par exemple plusieurs universités asiatiques organisent les Olympiades internationales de la blockchain[58]. Ce type d'action participe pleinement à la montée accélérée en compétence des étudiants sur la technologie blockchain directement utile pour les entreprises. Déjà, en France, quelques projets alternatifs aux formations classiques voient le jour, comme par exemple le projet « blockchain battle », kit d'animation librement téléchargeable par les enseignants souhaitant aborder cette thématique avec des lycéens. Ce projet est porté par l'association *Science Animation*[59] en partenariat avec la *start-up* PlayCurious[60].

Quel que soit sa forme (« hackathon » ou concours de programmation), il nous paraît important d'organiser ou de sponsoriser en France ce type d'évènement permettant à notre industrie de déceler tôt et simplement des futurs talents.

Enfin, nous recommandons de mettre en place une formation hybride qui profiterait de la création de nouveaux programmes académiques et pourrait s'appuyer simultanément sur un projet pédagogique spécifique.

Ce projet pédagogique serait construit autour de la blockchain en mettant à profit les pédagogies actives et les moyens d'enseignement en ligne tels que les MOOC interactifs intégrant des outils de codage ou de simulation ou de minage. L'idée est d'utiliser une palette complémentaire d'outils dans l'optique d'améliorer les formations pour répondre au besoin urgent de nos entreprises.

L'approche que nous suggérons pourrait prendre exemple sur ce qui a été créé dans la fabrication numérique[61] : il s'agirait de mettre en place un (ou des) parcours de formation mêlant un éventail de dispositifs pédagogiques modernes avec du coaching lors de sessions pratiques (par exemple lors de *coding bootcamp*) dédiées. Les professionnels doivent également être impliqués dans cette démarche. Au final, dans l'enseignement de la technologie blockchain, il s'agit de construire une approche pédagogique variée et agile dont la finalité est l'accélération de la formation pour pallier au manque actuel de diplômés et pour mettre rapidement sur le marché de jeunes recrutés opérationnels.

58 https://www.ibcol.org/2020/

59 https://www.science-animation.org/fr/actus-et-coulisses/blockcha1n-battle-un-projet-pour-tout-comprendre-la-blockchain

60 https://www.playcurious.games/fr/blockchainbattle

61 https://www.innovation-pedagogique.fr/article3209.html

# 7 CARTOGRAPHIE DES *START-UP*

## 7.1 Méthode

### 7.1.1 Le recensement des *start-up* françaises innovantes de la blockchain

L'approche initialement prévue pour entrer en relation avec les *start-up* françaises innovantes dans la blockchain, qualifiée classiquement de méthode « qualitative & quantitative », devait combiner des interviews et un questionnaire, destiné à élargir quantitativement la base des points de contacts[62].

Malgré la diffusion du questionnaire à plusieurs milliers de *start-up* françaises avec l'aide de *La Tribune* (partenaire de l'IMT dans de nombreuses initiatives liées à l'entrepreneuriat), le nombre de réponses est resté très faible et inexploitable vu les objectifs, ceci en dépit de plusieurs relances

Le recensement s'est finalement fondé sur l'exploitation de deux bases de données de *start-up*. La première, publique, est celle de Bpifrance[63]. La seconde, privée, émane de SIA Partners, cabinet français de conseil, doté d'une équipe dédiée à la blockchain qui évalue systématiquement les algorithmes de consensus.

L'accès à ces bases de données a permis de compléter le choix des *start-up* à interviewer dont le nombre s'est avéré restreint compte tenu de la durée de la mission.

*In fine*, la mission interministérielle a analysé les profils de 35 *start-up* innovantes dans la blockchain qui sont listées avec leurs descriptifs en Annexe E. Parmi les 35, 9 ont fait l'objet d'une interview. Ces dernières sont mentionnées explicitement dans la liste.

### 7.1.2 Le référentiel de la cartographie

Le référentiel utilisé pour la cartographie des *start-up* est celui utilisé dans l'ensemble de ce rapport, à savoir celui introduit dans l'article « Panorama des applications des blockchains à l'énergie, Gilles Deleuze & Sara Tucci-Piergiovanni. Revue de l'Électricité et de l'Électronique, Numéro 2, 2018 ».

Comme illustré dans la cartographie des 35 *start-up* recensées sur la figure ci-après, l'axe vertical du référentiel retenu repère les rôles de la blockchain, divisés en quatre niveaux d'innovation croissante en allant de bas en haut :

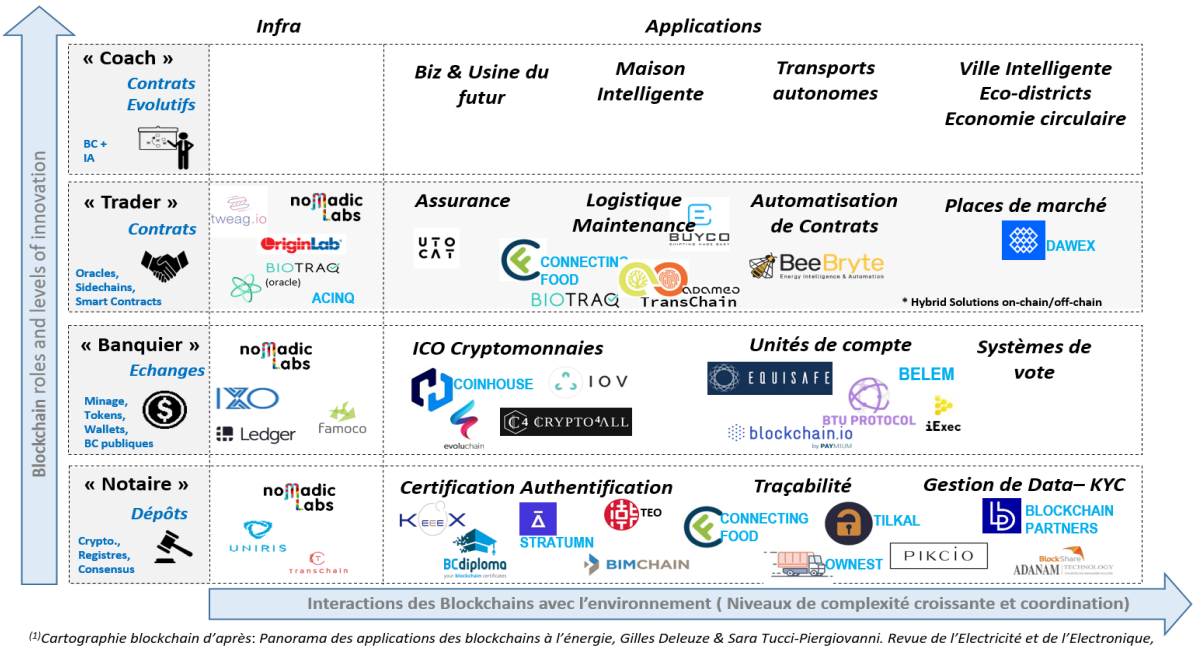
- enregistrement - notarisation (« Registry ») ;
- transfert de valeurs (« Value Transfer ») ;
- contractualisation Automatique (« Contracts ») ;
- « *coach* ».

L'axe horizontal, quant à lui, décrit pour chacun des quatre rôles de la blockchain, l'interaction avec l'environnement et le monde socio-économique.

62 https://www.imt.fr/mission-interministerielle-sur-les-verrous-de-la-blockchain/

63 https://lehub.web.bpifrance.fr/search?refinementList%5Btechnologies%5D%5B0%5D=Blockchain&page=1

La colonne « *infra* » (développement & fourniture d'infrastructures de blockchain) joue un rôle crucial dans la cartographie dans la mesure où elle liste des *start-up* qui développent, améliorent, voire inventent de nouvelles composantes structurelles des blockchains (algorithmes de consensus, crypto-monnaies, processus de tokenisation, etc.) en réponse à leurs verrous et limitations systémiques. Ces *start-up* vont, à cet égard, bien au-delà des cas d'usages peuplant les autres colonnes.




[1]*Cartographie blockchain d'après: Panorama des applications des blockchains à l'énergie, Gilles Deleuze & Sara Tucci-Piergiovanni. Revue de l'Electricité et de l'Electronique, N° 2, 2018*

Figure 13 - Positionnement des start-up sur le référentiel

# 7.2 Analyse

## 7.2.1 Cas d'usages versus infrastructure

Parmi les 35 *start-up* recensées, 26 (soit 74 %) sont plutôt focalisées sur la vente d'applications et de services dédiés à des cas d'usage de la blockchain (quatre colonnes de droite de la figure 1 ci-dessus), comme la traçabilité de chaînes de production d'aliments (Connecting Food) ou encore une place de marché de réservations touristiques (BTU Protocol).

Les 9 *start-up* restantes (soit 26 %) développent et fournissent à leurs clients des modules d'infrastructure blockchain (colonne « *infra* ») en s'appuyant sur une R & D avancée, internalisée et/ou en relation avec des laboratoires de recherche.

### 7.2.2 Répartition des cas d'usages

Sur les 26 *start-up* plutôt orientées usages, la répartition en fonction du rôle dévolu à la blockchain est la suivante :

- enregistrement – Notarisation (« Registry »), 42 % ;
- transfert de Valeurs (« Value Transfer »), 35 % ;
- contractualisation automatique (« Contracts »), 23 % ;
- *coach*, 0 %.

Les pourcentages reflètent directement les degrés de maturités associées : maturité élevée pour l'enregistrement et la notarisation, maturité de certaines solutions pour le transfert de valeurs, technologies en maturation pour la contractualisation automatique et solutions qui restent à inventer à ce jour pour la « machine de confiance intelligente » ou « augmentée » *via* l'intelligence artificielle.

### 7.2.3 Les *start-up* d'infrastructure

Parmi les 9 *start-up* proposant des infrastructures de blockchain, deux (Nomadic Labs et Lambda Vision) développent des solutions innovantes à trois niveaux, voir la figure ci-dessus, (Protocoles de confiance & Cryptographie, Tokenisation & Crypto-monnaies, *smart contracts* & Langages formels). Les 7 autres se répartissent de la manière suivante :

- protocoles de confiance & cryptographie, 28,5 % ;
- tokenisation & Crypto-monnaies, 28,5 % ;
- *smart-contracts* et langages formels, 43 %.

Aucune *start-up* recensée ne se positionne encore sur le niveau d'innovation le plus élevé, vers une « blockchain autonome ».

Parmi les 9 *start-up* « *infra* », trois, Nomadic Labs, Transchain et Lambda Vision, s'adossent à des laboratoires de recherche et à des écosystèmes marchés ou régaliens. Dans la suite, nous fournissons un descriptif de leur activité sur la base des entretiens que nous avons réalisés ainsi que des extraits d'entretien qui nous ont semblé importants pour notre mission (verrous à lever en priorité, sujets traités avec des laboratoire de recherche, besoins et craintes des clients, profils recherchés dans les recrutements… ). Il est important de souligner que ces extraits sont représentatifs de la grande majorité des entretiens que nous avons réalisés.

#### Nomadic Labs

Nomadic Labs abrite une équipe axée sur la recherche et le développement dans le secteur des systèmes distribués, décentralisés, formellement vérifiés. La technologie et le savoir-faire français en programmation et vérification forment le socle technologique de la société. Sa mission principale est de maintenir et faire évoluer la chaîne Tezos. Nomadic Labs développe une implémentation vérifiable du protocole économique de Tezos, ainsi que des langages pour les *smart contracts*. Nomadic Labs sert aussi d'incubateur pour de futures start-up (par exemple Marigold) qui développent des services/produits sur la chaîne Tezos.

À la question sur les verrous prioritaires : robustesse, sécurité et évolutivité des chaînes. Pour robustesse et sécurité, il s'agit de vérifier les codes qui implémentent la chaîne (y compris les compilateurs par exemple) et les *smart contracts*. Pour l'évolutivité, il s'agit de faire évoluer la

chaîne de manière démocratique et contrôlée en offrant des systèmes alternatifs aux *forks*. Une collaboration avec Inria est en cours sur ce sujet.

À la question sur les alternatives à la PoW : les dangers de la PoW sont la consommation énergétique, la centralisation des mineurs et le manque d'implication des mineurs (problème d'équité). La PoS (employée dans Tezos) répond à ces problèmes, il y a encore du travail sur le risque de censure, les incitations. Une collaboration avec le CEA est en cours sur ces thèmes.

À la question sur le passage à l'échelle : c'est un verrou mais pas une priorité.

À la question sur la *privacy* : c'est un verrou fondamental, la stratégie est de s'appuyer sur les résultats de la recherche.

À la question sur les obstacles à la diffusion des blockchains : le manque d'environnements de développement pour les utilisateurs, constitue un vrai problème pour l'accessibilité à la technologie.

À la question sur les pistes d'évolutions futures pour Nomadic Labs : compilateurs certifiés, gérer la cohabitation de plusieurs langages, interopérabilité avec d'autres chaînes et avec les environnements des systèmes d'information, langages de *smart contracts* de haut niveau. Le développement des langages de *smart contracts* se fait beaucoup en collaboration avec des start-up et chercheurs de l'écosystème autour de Tezos.

À la question sur les applications client : les premiers secteurs sont l'assurance, la finance et l'immobilier *via* des *start-up* comme EquiSafe. On observe un niveau de maturité des utilisateurs applicatifs encore faible et la taille des équipes souvent très réduite.

À la question sur les profils recherchés : besoin de profils hautement qualifiés difficiles à trouver. Il faut faire en sorte que la formation aux technologies sous-jacentes à la blockchain (algorithmique, systèmes distribués, cryptologie, langages de programmation, méthodes formelles) soit dispensée dans les formations post-baccalauréat.

### Transchain

La société Transchain a été créée à Strasbourg, en Alsace. Son cœur de métier est la recherche et le développement sur la technologie blockchain. Transchain a développé une blockchain publique pour des applications B2B. Il s'agit d'une chaîne de gestion de la preuve : dans la blockchain, ce qui est enregistré est l'empreinte des données, mais les données sont hébergées hors-chaîne. Ce choix répond directement à des besoins de confidentialité : en effet pour les clients la confidentialité est critique, donc les données sont gardées chez les clients. Quant à l'accessibilité de la chaîne, une problématique récurrente, Transchain a développé des interfaces et connecteurs pour accéder au service blockchain et l'intégrer dans les systèmes d'information des clients. Transchain a également une activité de service de développement d'applications sur une base ponctuelle dans la logistique, la pharmacie et l'automobile.

À la question sur les besoins de passage à l'échelle de la chaîne : le mécanisme de consensus actuel est en train d'être migré à une adaptation de Tendermint (cf. Section Consensus) pour passer à 1 000 transactions par seconde; à terme il faudra un support pour 10 000. Sur le sujet du passage à l'échelle, une thèse de doctorat est en cours avec le laboratoire I-cube, de l'Université de Strasbourg.

À la question sur une utilisation de *smart contracts* pour le développement d'applicatifs métiers : la confidentialité des données limite l'utilisation des *smart contracts* en réseau public. Cela implique que la disponibilité des données est gérée hors-chaîne.

À la question sur les verrous : outre le passage à l'échelle, les verrous à lever sont l'interopérabilité avec d'autres chaînes et interconnexion avec l'IoT.

À la question sur les besoins client : les clients viennent pour un besoin de digitalisation et d'automatisation de leurs processus.

À la question si Bitcoin représente une crainte et donc un frein pour l'adoption de la technologie blockchain : Bitcoin est encore une crainte pour certaines personnes mais la situation s'améliore ; la séparation entre blockchain et crypto-monnaie est de plus en plus claire et la blockchain vue comme un atout pour les applications.

À la question sur le recrutement et les profils recherchés : le recrutement reste difficile. Le profil recherché doit être pointu en algorithmique répartie, cryptographie et codage mais nous ne trouvons pas de formation adéquate (en tout cas à Strasbourg). Niveau recherché : M2 et puis formation interne ; souvent un stage aboutit à une thèse CIFRE.

Autre point : le PDG est actif à l'AFNOR. Il souligne l'importance de clarifier le cadre normatif/légal pour la « preuve fournie par une blockchain ».

### Lambda Vision - iXXo

La société Lambda Vision développe une solution de place de marché de biens et actifs financiers appelée iXXo. Le cœur de métier de Lambda Vision est la gestion de la confiance décentralisée combinant des techniques cryptographiques avancées avec un protocole de consensus de type « proof-of-authority » (MPOA pour *Mixed Proof of Authority*). Dans la solution iXXo, la consommation énergétique est fortement diminuée en optimisant le nombre de mineurs en fonction de la valeur ou des enjeux d'une transaction. Leur solution atteint une performance de 2 000 transactions par seconde et incorpore une notion de *nœud souverain* pour prendre en compte les aspects de souveraineté. Lamba Vision offre à ces clients une infrastructure blockchain *via* des interfaces et connecteurs pour l'intégration dans les systèmes d'information des clients. Lambda Vision a une collaboration active avec des équipes de recherche de l'IMT (Télécom SudParis) sur la gestion de la confidentialité *via* la cryptographie.

À la question sur les verrous prioritaires : le verrou prioritaire est la protection de la confidentialité et des droits d'accès. La blockchain ne représente qu'une petite partie du système de confiance à mettre en place pour gérer cette confidentialité sur des applications de type place de marché, par exemple.

À la question sur les obstacles à la diffusion des blockchains : Il y a aujourd'hui une difficulté reliée à la gestion projet des grandes plateformes open-source comme Ethereum ou Hyperledger qui reste peu professionnelle, ce qui nuit à la stabilité des codes.

À la question sur le recrutement et les profils recherchés : nous avons besoin des profils « hybrides » : des ingénieurs ou docteurs qui ont des connaissances fondamentales (cryptographie et algorithmes distribués) mais qu'ils sachent également développer. Il faudrait probablement un double cursus pour former ce type de profils.

## 7.3 Conclusion sur la cartographie *start-up*

En conclusion, il ressort que les véritables prises de risques et voies d'avancées de la blockchain proviennent potentiellement de start-up dotées de R & D avancée et suffisamment résilientes (par exemple *via* un adossement à des laboratoires de recherche) pour avoir, après plusieurs années, résolu un certain nombre de verrous et avoir en plus apporté des preuves de faisabilité et de revenus, en mode agile, autour des cas d'usages les plus prometteurs. Même si les Grands Comptes ont les moyens de tester de nombreuses preuves de concepts faisant appel aux registres distribués de confiance, notre perception est que ces expérimentations ne débouchent pas encore sur de véritables marchés, ni sur des confrontations aux différents verrous des registres distribués de confiance, comme la latence, la vitesse, la scalabilité, la souveraineté et la consommation d'énergie.

À cet égard, les avancées significatives dans la blockchain sont à attendre de la mise en œuvre opérationnelle d'écosystèmes pluridisciplinaires et multimétiers incluant nativement des *start-up*, des chercheurs et des grands comptes, capables de combiner des cycles longs de résolution de questions fondamentales, avec des cycles courts de mise sur le marché, autour de projets d'envergure régaliens centrés sur les usages et l'expérience utilisateur, comme par exemple dans la santé, sur la traçabilité du parcours patient.

# A. ANNEXE - LE CONSENSUS DANS LES REGISTRES DISTRIBUÉS

## Un peu de pédagogie

Le but d'une blockchain est de s'assurer que les transactions effectuées par les utilisateurs sont correctement traitées par un système réparti. Le cycle de vie d'une transaction correctement servie est décrit dans la Figure 14. On suppose ici que le système est centralisé avec un seul validateur pour expliquer plus facilement les différentes étapes. Le cycle de vie d'une transaction dans un système réparti doit rester le même du point de vue de l'observabilité par un utilisateur pour statuer que la transaction est exécutée correctement. Mais regardons de plus près les étapes de ce cycle de vie. Au début, la transaction est créée et signée par l'utilisateur (1), elle est ensuite envoyée au validateur qui la reçoit (2 et 3). Le validateur, une fois la transaction reçue, peut la vérifier (4). Si la transaction est valide, le validateur l'enregistre dans son registre. Une fois la transaction enregistrée, nous dirons que la transaction est acceptée par le validateur. Dans ce contexte, une fois la transaction acceptée par le validateur, elle est également confirmée. C'est seulement alors, la transaction étant confirmée, que l'utilisateur peut émettre une autre transaction à partir du même compte.

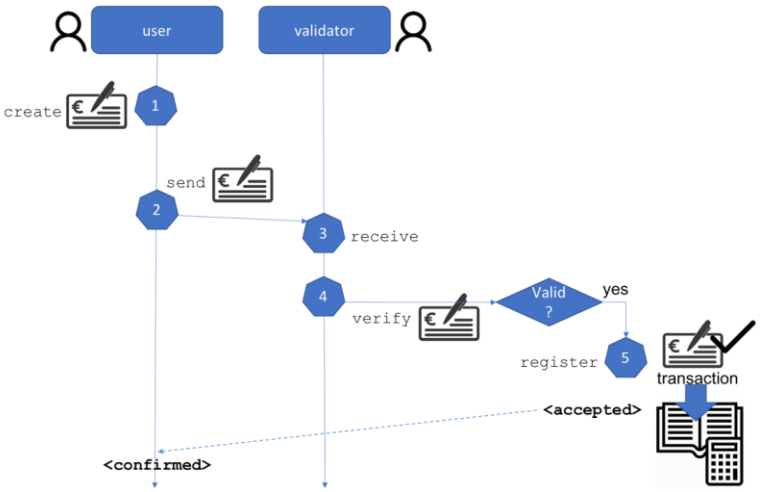



Figure 14 - Cycle de vie d'une transaction avec un validateur

La solution centralisée que nous venons de décrire n'est pas résiliente : en effet, le validateur peut se bloquer ou se comporter de manière malveillante. De plus, si le validateur tombe en panne, le système ne sera plus disponible et le contenu du registre sera perdu.

Une façon d'obtenir un système disponible consiste à répliquer les validateurs : si un validateur tombe en panne, un autre prendra la relève. Plus précisément, chaque validateur dispose d'une copie locale du registre, appelée réplique. La transaction émise sera envoyée à tous les validateurs (Figure 15), qui recevront et vérifieront la transaction. Dans ce cas, comment définissons-nous le moment où une transaction est confirmée ?

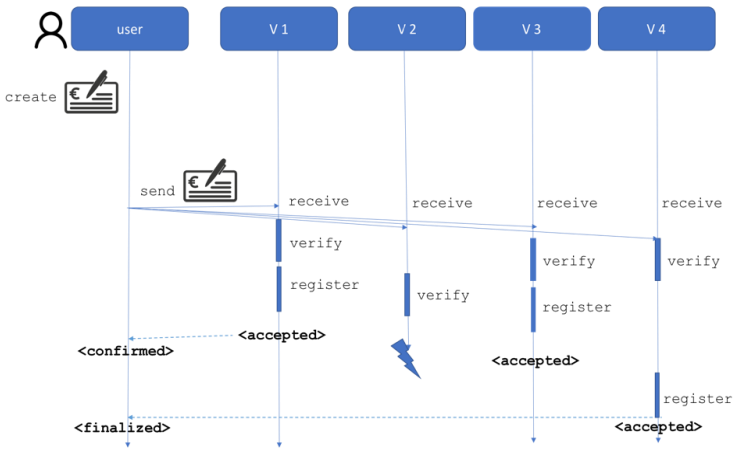



Figure 15 - Cycle de vie d'une transaction avec plusieurs validateurs

Ici, il convient de distinguer la *confirmation* de la *finalisation*. Le terme finalisation n'appartient pas au domaine informatique. La finalisation est un terme propre aux systèmes de paiement. Une transaction est finalisée lorsqu'elle n'est plus annulable, en sachant qu'entre son émission et sa finalisation des opérations sont généralement effectuées. En revenant à notre système informatique, nous disons qu'une transaction est confirmée dès qu'un validateur l'accepte. Une transaction confirmée est finalisée quand elle ne peut plus être annulée. Nous disons que le système est parvenu à un consensus sur la validité de la transaction à sa finalisation.

Le consensus sur la validité d'une transaction peut être trouvé de différentes manières, *via* des approches dites coordonnées ou à l'opposé, des approches non coordonnées.

Dans les approches dites *coordonnées*, les validateurs se coordonnent pour traiter une transaction *via* un algorithme distribué tolérant aux pannes avant d'accepter la transaction et de répondre à l'utilisateur. Cette coordination ne peut réussir que si un quorum de validateurs est disponible et connecté. Le principe est qu'une transaction, avant d'être acceptée, est envoyée entre les validateurs. Ce n'est que si un quorum majoritaire accepte la transaction que celle-ci est confirmée et finalisée. Dans ces approches, la finalisation arrive en même temps que la confirmation, on dit donc que les approches coordonnées donnent lieu à une finalisation instantanée.

Les approches coordonnées, cependant, exigent qu'un quorum soit connecté pour aboutir à une confirmation et donc à une finalisation. Cela signifie que si le réseau est partitionné (deux sous parties qui ne peuvent plus communiquer entre elles ; sur Internet, une partition peut durer de plusieurs minutes à plusieurs heures), aucune transaction ne sera confirmée pendant la partition et aucune nouvelle transaction ne pourra être émise par l'utilisateur. Le système ne sera plus disponible de point de vue de l'utilisateur.

Les approches *non coordonnées* trouvent leur raison d'être dans leur manière différente de réagir aux partitions. Dans ces approches, il n'y a pas de coordination entre les validateurs pour traiter une transaction. Chaque validateur traite la transaction localement, comme illustré à la figure 16. La transaction est confirmée dès son acceptation par un validateur. Cela signifie que le système sera disponible même si les validateurs ne sont pas connectés entre eux. Toutefois, la finalisation est plus compliquée. Sans coordination entre les validateurs, deux ou plusieurs transactions en

conflit peuvent être temporairement confirmées. C'est le cas, par exemple, d'un utilisateur malicieux qui fait une double dépense en créant simultanément deux transactions du même compte et en les envoyant à deux validateurs temporairement déconnectés l'un de l'autre. Les deux validateurs confirmeront chacun une transaction en créant une incohérence dans le système : une double dépense est acceptée. Dans ces approches, cependant, on s'attend à ce que les validateurs puissent finalement communiquer entre eux, détecter les conflits et les résoudre. La résolution des conflits peut amener à rejeter certaines transactions émises. Le moment de la finalisation, par contre, n'est pas connu a priori et, par conséquent, ces approches créent par construction une incertitude quant au moment où chaque transaction sera finalisée ou rejetée. Toutefois, étant donné que des transactions peuvent être créées et confirmées en permanence, une transaction peut accumuler un nombre important de confirmations au fil du temps, dès que les autres transactions qui y font référence sont également confirmées. C'est le principe des applications qui utilisent Bitcoin, par exemple, qui nécessitent souvent six confirmations, ce qui prend environ une heure.

Le tableau de la figure 16 résume les avantages et les inconvénients des deux types d'approches. Pour les approches non coordonnées, la latence de confirmation est meilleure car la progression (propriété de vivacité) est garantie même en présence de partitionnement du réseau. Cette meilleure résilience est payée par une perte potentielle de cohérence et une incertitude quant au temps nécessaire pour atteindre la finalisation. Les approches coordonnées garantissent la cohérence à tout moment, mais la latence de confirmation peut être importante car elle nécessite la réponse d'un quorum potentiellement grand sur un réseau étendu, disponible et connecté.

| | approches non coordonnées | approches coordonnées |
|---|---|---|
| Latence de la confirmation | + | - |
| Latence de la finalité | - | + |
| Résilience au partitionnement | + | - |
| Cohérence | - | + |

Figure 16 - Avantages et inconvénients des approches coordonnées ou non

Dans ces approches, la confirmation et la finalité coïncident, de sorte que la latence de la finalisation c'est-à-dire le temps écoulé entre la confirmation et la finalisation, est nul.

La tension entre cohérence, disponibilité et tolérance aux partitions, que nous avons présenté de manière pédagogique dans cette section est un dilemme bien connu dans la théorie du calcul distribué. Cela prend le nom de  théorème CAP (voir encadré).

***Zoom technique : le théorème CAP***

*Le théorème CAP dit qu'il est impossible sur un système informatique de calcul distribué de garantir en même temps les trois propriétés suivantes :*

1. *Cohérence (**C**onsistency en anglais) : les requêtes s'exécutent dans le système réparti comme si un seul nœud les servait en répondant aux requêtes une par une ;*
2. *Disponibilité (**A**vailability en anglais) : garantie que toutes les requêtes reçues reçoivent une réponse ;*
3. *Tolérance au partitionnement (**P**artition Tolerance en anglais) : aucune panne moins importante qu'une coupure totale du réseau ne doit empêcher le système de répondre : en cas de morcellement en sous-réseaux, chacun doit pouvoir fonctionner de manière autonome.*

*D'après ce théorème, un système de calcul/stockage distribué ne peut garantir à un instant t que deux de ces propriétés mais pas les trois.*

***Approches coordonnées:** CP (en cas de partition) or CA (pas de partition).*

***Approches non-coordonnées:** AP.*

# Situation actuelle

La situation actuelle peut se résumer très simplement en classant les solutions existantes en *coordonnées* et *non coordonnées*.

Qualitativement on peut d'ores et déjà observer que les solutions non coordonnées sont adaptées à des systèmes ouverts et à très large échelle, souvent sans permission. Le défi pour ces solutions est de trouver des mécanismes pour traiter, d'une façon empirique ou probabiliste, la question de la cohérence et le temps de latence pour la finalisation.

Les solutions coordonnées sont *a contrario* plus adaptées à des systèmes plus petits et clos, ou avec permissions, où l'on peut raisonnablement penser que le coût de la coordination reste raisonnable ou au moins contrôlé par un administrateur qui peut, par exemple, décider du nombre des validateurs. Cependant, comme les blockchains se veulent à large échelle et ouvertes, le défi pour les solutions coordonnées est de fournir des mécanismes décentralisés qui décident d'un petit nombre de validateurs.

## Bitcoin

Bitcoin est sans doute la solution la plus originale et la plus convaincante de par sa longévité, parmi les solutions non coordonnées. Le défi de la cohérence et de la finalisation est adressé par Bitcoin avec des mécanismes astucieux. En Bitcoin chaque transaction est traitée à l'aide d'un leader qui sera responsable pendant un temps limité de l'évolution de l'état du système. Pour des raisons d'efficacité, les transactions sont regroupées en blocs, chaque bloc est donc diffusé dans le réseau par le leader. *L'élection du leader se fait à l'aide de la preuve de travail* (Proof-of-Work) : un mécanisme cryptographique qui permet une sélection aléatoire d'un nœud du réseau. Ainsi le leader peut fournir la preuve qu'il est le leader légitime d'un bloc à d'autres participants, qui pourront vérifier sa légitimité sans connaître au préalable son identité. Chaque participant valide donc le bloc avant de l'accepter : il vérifie la légitimité du *leader* et la validité des transactions contenues. Mais comment le problème de la cohérence du registre est traité ?

Le problème est traité en garantissant que les *leaders* soient élus « lentement ». La difficulté pour générer une preuve de travail est ajustée pour s'assurer d'avoir un *leader* environ toutes les 10 minutes. Si aucun conflit n'est observé, le *leader* crée un bloc en étendant le dernier bloc observé. En cas de production de blocs concurrents, qui se traduit par l'extension d'un même bloc, nous aurons une fourche. Une fourche signifie une incohérence potentielle entre les copies du registre. Dans ce cas, un choix sera fait en sauvegardant localement les branches concurrentes et en ne conservant ultimement que les blocs qui appartiendront à la chaîne la plus longue. *Ce qui est garanti en Bitcoin n'est donc qu'une propriété de résolution des fourches dans le temps*, au travers d'un accord qui porte sur un préfixe croissant de la chaîne. En Bitcoin, nous considérons un bloc comme finalisé quand il sera suivi de 6 blocs. Plus un bloc est profond, plus nous pouvons raisonnablement penser qu'il ne sera plus abandonné car il fait partie du préfixe de la chaîne la plus longue. L'inconvénient de cette approche est que la latence de la finalisation peut être très importante. Dans Bitcoin, pour avoir une bonne garantie qu'une transaction soit finalisée car incluse dans un bloc finalisé, il est nécessaire d'attendre environ une heure. En réalité, ce système ne fonctionne que si les participants considèrent toujours plus utile d'étendre la chaîne la plus longue que d'accepter une chaîne alternative. À cette fin, un *mécanisme d'incitation* qui se traduit par accorder une récompense aux leaders qui ont créé les blocs de la chaîne la plus longue, est au cœur du système Bitcoin et plus généralement des blockchains sans permissions, qui ne sont pas administrées par une autorité extérieure.

Les plus grandes critiques à Bitcoin aujourd'hui sont, en premier lieu, la consommation énergétique engendrée par la preuve de travail mais aussi sa latence importante pour la confirmation d'une transaction (environ 10 minutes) et la finalisation (environ 1 heure).

Si le mécanisme d'incitation est très intéressant pour assurer la progression du système, les stratégies de récompenses doivent être étudiées avec soin pour ne pas risquer de privilégier des comportements déviants. Il est important d'observer qu'un validateur dans un système réparti a toute la latitude pour choisir les transactions à servir : le fait qu'il exclut intentionnellement une transaction est en principe non observable si le réseau peut perdre des messages. Une transaction peut donc être exclue et jamais traitée dans ce système. Nous disons dans ce cas que le système n'est pas *équitable*.

En termes de *résilience*, le système est résilient si la majorité de la puissance de calcul est dans les mains de participants honnêtes.

| | |
|---|---|
| **Avantages** | Résilience prouvée par la pratique |
| **Désavantages** | 1. importante consommation énergétique<br>2. finalisation incertaine (dépend du délai du réseau)<br>3. Importante latence de finalisation (1h en mode normal[64])<br>4. importante latence de confirmation (10mn en mode normal)<br>5. faible équité |
| **Technologies similaires** | Ethereum avec preuve de travail |

64 Le délai présenté représente une borne inférieure : pour avoir des bonnes propriétés de cohérence il faut attendre au moins ce délai, tout en respectant la borne de résilience.

## Les solutions à base de preuve d'enjeu (Proof of Stake)

Nous rappelons qu'en Bitcoin chaque *leader* est sélectionné à l'aide de la preuve de travail. Comme la preuve de travail consomme de l'énergie, d'autres mécanismes cryptographiques ont été mis au point. C'est le cas, par exemple, d'Ouroboros utilisant un algorithme appelé FTS qui sélectionne les leaders sur la base de leur « *stake* », une somme de crypto-monnaie mise de côté *via* des transactions incluses dans la blockchain. Sur la base de la conjecture que quelqu'un qui possède beaucoup de richesse investie dans la blockchain a intérêt à être un bon *leader*, la sélection privilégie les plus riches dans les systèmes à preuve de participation. Outre le fait que ces validateurs auront intérêt à ne pas créer de conflit *via* une fourche, ils seront également motivés pour résoudre les fourches observées. Toutefois cette conjecture n'a pas été prouvée et l*es systèmes d'incitations dans ce type d'approches sont encore un sujet de recherche très actif*. Une petite contre mesure souvent adoptée dans ce type de systèmes est de réduire la latence de la confirmation. Au lieu d'élire uniquement un *leader*, le mécanisme de sélection élit également un certain nombre d'endosseurs : le *leader* devra demander des endossements pour son bloc. Les endossements seront collectés par le *leader* qui suit et inclus dans son bloc. Dans ces systèmes un bloc sera confirmé dès qu'un bloc valide le suit. La finalisation dépendra du nombre d'endosseurs requis, mais ce nombre est souvent choisi empiriquement dans les systèmes actuels en cherchant un compromis entre latence et cohérence.

| | |
|---|---|
| **Avantages** | 1. non énergivore<br>2. latence de confirmation réduite (secondes en mode opérationnel normal)<br>3. latence de la finalisation réduite (minutes en mode opérationnel normal) |
| **Désavantages** | 1. mécanismes d'incitations et équité pas prouvés<br>2. finalisation souvent empirique |
| **Technologies** | Cardano, Ethereum Casper, Tezos Emmy |

## Solutions coordonnées

La plupart des approches coordonnées à l'heure actuelle reposent sur un algorithme de consensus qui tolère les fautes byzantines (comportement du système qui ne respecte pas ses spécifications, en donnant des résultats non conformes), consensus BFT dans la suite. Ces algorithmes sont tolérants à la présence d'un tiers de validateurs malveillants : un validateur malveillant est un nœud qui pourra dévier de son algorithme de manière arbitraire.

Le principal avantage de ces approches, à finalisation instantanée, est leur capacité à simuler une machine à états. Cela signifie que la validation de la transaction peut également impliquer l'exécution de tout programme informatique. C'est le principe des contrats intelligents génériques popularisés par la blockchain Ethereum. Un validateur conserve une copie d'un programme en local qui peut être appelée par l'utilisateur via des requêtes. Chaque requête comprend également une transaction par laquelle l'utilisateur paie l'exécution du programme appelé.

Toutefois l'implémentation d'une machine à états répliquée dans une blockchain est problématique. Étant donné que la complexité intrinsèque de la mise en œuvre d'un algorithme de consensus BFT en terme de trafic généré est au minimum quadratique comparée au nombre de validateurs, les comités doivent rester restreints. Nous rappelons également les problèmes liés

à l'absence de progression dans le cas d'un réseau peu fiable ou à la perte de cohérence si le seuil maximum d'un tiers des nœuds byzantins (déviant du comportement normal) n'est pas respecté.

Ces solutions s'attellent à ces problématiques en utilisant *un nombre raisonnable de validateurs*. En effet, au lieu d'élire un *leader*, le système choisit un comité de taille réduite qui sera responsable pendant un temps limité de l'évolution de l'état du système, généralement le temps de la création d'un bloc. Les validateurs du comité se coordonnent entre eux en utilisant un algorithme de consensus BFT, qui garantit que le bloc produit par le comité est finalisé.

Cependant, la question de *la sélection de tels comités dans ces solutions pose encore de grandes difficultés*. Premièrement, il faut s'assurer que pas plus d'un tiers de nœuds byzantins est sélectionné. De plus, la petite taille d'un comité peut créer des *problèmes de censure* si le comité n'est pas renouvelé de temps à autre. La censure est l'exclusion systématique des transactions qui proviennent du même acteur, par exemple. Ce problème est présent en particulier dans les systèmes avec permissions où l'identité de l'émetteur est connue.

Parmi les approches coordonnées basées sur un consensus BFT on peut mentionner Libra, Cosmos, Tendermint et Tezos TenderBake.

AlgoRAND fait également partie des approches coordonnées où pour chaque bloc le comité des validateurs est sélectionné sur la base de leur « stake » avec un mécanisme probabiliste appelé *cryptographic sortition*. Ce mécanisme conserve la propriété de ne pas pouvoir deviner au préalable l'identité des *leaders*. Cette mesure de sécurité protège les *leaders* contre d'éventuelles attaques (corruption ou déni de service). Une fois le comité élu, le bloc est produit *via* un algorithme spécifique appelé BA*. AlgoRAND fonctionne sans que les validateurs ne mettent de l'argent de côté : le « *stake* » est simplement la somme totale possédé par un participant. De par sa nature probabiliste, des fourches peuvent se manifester avec une probabilité inférieure à $10^{-7}$. Comme pour les autres approches coordonnées basés sur la preuve d'enjeu, *les mécanismes d'incitation ne sont pas définis*.

| | |
|---|---|
| **Avantages** | 1. non-énergivore<br>2. débit autour de 800 tx/s en conditions opérationnelles normales (sans fautes)<br>3. finalisation instantanée<br>support aux *smart contracts* génériques |
| **Désavantages** | 1. mécanismes d'incitation à trouver<br>2. temps de confirmation potentiellement important en cas de partition du réseau,<br>risque de censure dans les systèmes fermés. |
| **Technologies** | Libra, Cosmos, Tezos TenderBake, Algorand |

En synthèse, la mise en œuvre de la sélection et du renouvellement des comités est aujourd'hui le défi majeur de ces solutions pour ce qui concerne leur *sécurité*. À cela s'ajoute la difficulté de comprendre l'impact des mécanismes d'incitation sur le comportement des comités dans le temps. En attendant que la recherche avance sur ces points, nous pouvons affirmer qu'un mécanisme d'incitation convaincant reste encore à trouver (ce point est en lien avec les verrous 9 et 10 « les modèles et les mécanismes économiques »).

# B. ANNEXE - LES *SIDECHAINS* ET LES *SWAP* ATOMIQUES

Les *sidechains* ou chaînes latérales sont un moyen pour plusieurs chaînes de blocs de communiquer et d'interagir entre elles. La chaîne latérale est souvent une chaîne enfant (la chaine enfant hérite le bloc genèse de la chaîne parent) mais le terme est également utilisé pour désigner des chaînes autonomes qui communiquent entre elles. Dans ce cas, chaque chaîne est considérée comme la chaîne latérale de l'autre.

Un système de *sidechains* sert à réaliser certains types d'interactions entre les chaînes de blocs participantes. L'application la plus fondamentale est le transfert d'actifs d'une blockchain à l'autre ou *cross-chain payment*. Dans cette application, la nature de l'actif transféré est conservée. Lorsque l'actif transféré est transformé dans une classe d'actifs différente nous parlons de *swaps atomiques* ou *cross-chain atomic swaps*.

Les systèmes de *sidechains* pourraient être d'une grande valeur vis-à-vis des trois questions ouvertes suivantes :

**Interopérabilité** : il existe actuellement des centaines de crypto-monnaies déployées en production. Le transfert d'actifs entre différentes chaînes nécessite des transactions avec des intermédiaires. De plus, il n'y a aucun moyen de s'interfacer en toute sécurité avec une autre blockchain pour réagir aux événements qui s'y produisent. Les *sidechains* permettraient aux chaînes de blocs de nature différente de communiquer, et de fournir également un interfaçage avec le système bancaire existant.

**Passage à l'échelle** : bien que les *sidechains* n'aient pas été initialement proposées à des fins de passage à l'échelle, elles peuvent être utilisées pour décharger une chaîne de blocs en termes de transactions traitées. Une chaîne particulière peut offrir une spécialisation, par exemple pour un secteur industriel où une entreprise, afin d'éviter que la chaîne principale ne gère toutes les transactions. De plus, la blockchain spécialisée pourrait être de type consortium ou privée pour répondre à des exigences de confidentialité.

**Évolutivité** : une chaîne secondaire enfant peut être créée à partir d'une chaîne principale parent comme moyen d'explorer une nouvelle fonctionnalité dans le langage de *smart contracts* par exemple, ou un nouveau mécanisme de consensus, sans nécessiter de créer une nouvelle blockchain. La chaîne enfant n'a pas besoin de maintenir sa propre monnaie distincte car la valeur peut être déplacée entre la chaîne enfant et la chaîne principale à volonté. Si la nouvelle fonctionnalité de la chaîne enfant s'avère populaire, la chaîne principale peut éventuellement être abandonnée en déplaçant tous les actifs vers la chaîne enfant, qui peut devenir la nouvelle chaîne principale.

Compte tenu des avantages énumérés ci-dessus, il est important de traiter la question de la sécurité et de la faisabilité de ces solutions. Bien qu'il y ait eu plusieurs tentatives pour créer divers mécanismes de transfert entre chaînes, notamment Polkadot, Cosmos, Blockstream's Liquid et Interledger, jusqu'à présent et peut-être de manière surprenante, ces solutions n'ont pas reçu un traitement formel adéquat. À ce stade, en particulier, l'interaction de blockchains dotées des mécanismes de consensus différents reste une question ouverte. Cosmos, par exemple, offre un protocole d'interconnexion (appelé IBT) qui ne fonctionne aujourd'hui qu'entre blockchains avec une finalisation instantanée (cf. Section Consensus). La connexion entre Tendermint et Ethereum par exemple n'est pas possible aujourd'hui. Des travaux de recherche récents s'attaquent à l'interopérabilité des blockchains de type preuve d'enjeu (en ciblant en particulier la blockchain

Cardano), mais la résilience est prouvée sous l'hypothèse forte et peu réaliste d'un réseau de communication fiable et prédictible.

### *Cross-chain atomic swaps*

Les *swaps* atomiques sont des échanges sécurisés d'actifs numériques entre différentes chaînes de blocs effectués directement d'un utilisateur à un autre, sans intermédiaires. Le principe est le suivant : un ensemble d'utilisateurs décident de s'échanger des actifs appartenant à des blockchains différentes. Les utilisateurs se mettent d'accord sur une transaction, typiquement avec des mécanismes hors-chaîne. Considérons le scénario suivant :

- Carole veut vendre un actif sur la blockchain X en *greencoins ;*
- Alice est intéressée par l'actif de Carole, mais elle n'a pas le montant suffisant pour acheter l'actif de Carole sur la blockchain X; cependant elle possède la quantité suffisante sur une autre blockchain Y en *redcoins ;*
- Bob quant à lui, veut échanger des *greencoins* contre des *redcoins.*

La transaction est donc établie en terme de transfert d'actifs via des contrats intelligents, c'est-à-dire des scripts publiés sur la blockchain qui établissent et appliquent les conditions nécessaires pour transférer un actif d'un agent vers un autre. En particulier, chaque agent publie un contrat intelligent qui verrouille l'actif à transférer ainsi que les conditions pour exécuter le transfert. Ces conditions permettent d'encoder la synchronisation et la séquentialisation des transferts. Ainsi, Alice transférera ses *redcoins* à Bob qui les convertira en *greencoins* et les transférera à Carole, qui à son tour transférera son actif à Alice (Alice opère sur les deux blockchains X et Y mais elle n'a de crypto-monnaie que sur la blockchain X). Les protocoles *cross-chain swaps* sont munis d'un mécanisme de remboursement dans le cas où un ou plusieurs agents sortent du protocole de manière imprévue. De plus, si l'initiateur de la transaction (Alice dans notre scénario) se comporte de manière malveillante alors il sera le seul à perdre de l'argent, les autres agents seront remboursés.

Plusieurs projets sont en cours de développement. Les premières solutions visaient les échanges de Bitcoin avec d'autres crypto-monnaies (litecoin, vertcoin, decred, etc.). Dans ces solutions, cependant, pour que l'utilisateur effectue un échange atomique entre deux crypto-monnaies, il serait nécessaire que l'utilisateur télécharge les chaînes de blocs associées aux deux crypto-monnaies, ce qui n'est pas pratique. Le projet de Komodo, par exemple, s'attaque à ce problème.

Bien que les solutions pour les échanges atomiques soient en constante évolution, leur maturité n'est pas encore atteinte. Les problèmes de recherche ouverts relèvent de la formalisation et de l'analyse fine de ces protocoles en termes de résilience (comportements malveillants et communication peu fiable) et scalabilité, notamment dans les cas de transactions *multi-hop* qui nécessitent souvent un temps d'exécution long. En particulier, alors que les actifs sont verrouillés, l'initiateur de la transaction pourrait trouver de meilleures conditions ailleurs et vouloir annuler la transaction en cours. Dans ce cas, l'initiateur bénéficie d'un droit d'optionalité qui ne lui revient pas.

Une autre difficulté concerne la confidentialité des transactions sur des chaînes publiques. Dans Bitcoin, par exemple, les transactions associées à des transactions d'un *swap* sont facilement reconnaissables par rapport à des transactions natives.

Cependant, la problématique qui nous semble la plus importante concerne le fait que la mise en place d'une telle transaction se fait aujourd'hui hors-chaîne selon des méthodes à clarifier. Les utilisateurs doivent en effet trouver un accord entre eux (les actifs et les prix). Sur la base de cet accord les *smart contracts* ou les scripts associés sont configurés. De plus, ces protocoles

s'appuient souvent sur un coordinateur, élu parmi les participants, qui sera en charge d'interagir avec les blockchains pour mener à bien la transaction de chacun. L'élection de ce coordinateur se fait hors-chaîne ce qui peut conduire à des problèmes de résilience.

Pour surmonter les difficultés mentionnées, la collaboration de multiples spécialités comme la cryptographie, l'algorithmique distribuée et la vérification formelle est nécessaire. De plus, comme certaines problématiques relèvent de la sphère financière et économique (équité, inflation, optionalité, etc.), il serait important d'associer également des économistes aux travaux de recherche nécessaires.

# C. ANNEXE - LISTE DES PERSONNES AUDITIONNEES

Patrick Aknin, IRT-SystemX

Emmanuelle Anceaume, CNRS, IRISA

Daniel Augot, Inria

Alexandre Barrat, Autorité des Marchés Financiers

Thierry Bedoin, Banque de France

Frédéric Bertoia, Equisafe

Bruno Biais, HEC

Mathieu Boespflug, Tweag I/O

Louise Bonnel, Equisafe

Vincent Botbol, Nomadic Labs

Mathias Bourgouin, Nomadic Labs

Timothée Brugière, Transchain

Michel-Ange Camhi, Bureau Veritas

Laurent Camus, Autorité de contrôle prudentiel et de résolution

Sylvain Cariou, Crystalchain

Jérôme Chailloux, Nomadic Labs

Manuel Chakravarty, Tweag I/O

Louis Charpentier, Autorité des Marchés Financiers

Damien de Chillaz, Cap Gemini

Vidal Chriqui, BTU Protocol

Vincent Danos, CNRS, ENS

Caroline de Condé, AFNOR

Anatole de La Brosse, Sia Partners

Gilles Deleuze, EDF

Albert Dessaint, Blockchain Partner

Domitille Dessertine, Autorité des Marchés Financiers

Bilal El Alamy, Equisafe

Nadia Filali, CDC

Mickael Granval, Equisafe

Rachid Guerraoui, EPFL

Matthieu Hug, Tilkal

Sébastien Jéhan, Lambda Vision

Paul Jolie, Service de l'Information Stratégique et de la Sécurité Économique

Dominique Jourdan, Service l'Information Stratégique et de la Sécurité Économique

Alexandre Karako, Equisafe

Charles Kremer, Blockchain Xdev

Sébastien Kunz-Jacques, ANSSI

Fabrice Le Fessant, Origin Labs

Jean-François Legendre, AFNOR

David Leporini, Atos

Michel Mauny, Nomadic Labs

Édouard Morio de l'Isle, Cap Gemini

Rémy Ozcan, Crypto4All

Christophe Ozcan, Crypto4All

Maria Potop-Butucaru, Sorbonne Université

Julien Prat, CNRS, CREST, École Polytechnique

Michel Raynal, Université de Rennes 1

Yannick Seurin, ANSSI

# D. ANNEXE - QUESTIONNAIRE FORMATIONS

**NOM DE LA FORMATION AYANT TRAIT À LA BLOCKCHAIN***

**NOM DE L'ÉTABLISSEMENT PORTANT LA FORMATION**

**URL DE LA FORMATION***

**CATÉGORIE DE FORMATION***

- Inclue dans formation initiale
- Inclue dans formation continue
- Apprentissage/alternance

**LA FORMATION EST-ELLE DIPLÔMANTE ?***

- Oui
- Non

**TYPE DE FORMATION***

- DUT/BTS (Bac + 2)
- Licence/Bachelor (Bac + 3)
- Master (Bac + 5)
- Grande Ecole (Bac + 5)
- Master spécialisé (Bac + 6)
- MBA
- Autres

**CONTENU DE LA FORMATION***

- Informatique théorique
- Systèmes distribués
- Cybersécurité
- Systèmes d'Information
- Mathématique (cryptographie)
- Droit
- Finance
- Economie
- Autres

**DATE DE CRÉATION DE LA FORMATION***

**VOLUME DE LA FORMATION (EN HEURES OU EN HEURES/AN)***

**PRÉREQUIS (NIVEAU MINIMAL DANS UN DOMAINE, DIPLÔME, ETC.)**

**LANGUE DE LA FORMATION***

Français (100 %)

Anglais (100 %)

Mix Français/Anglais (proportions variables)

Autres

**FORMAT DE LA FORMATION**

Présentiel

En ligne (Type MOOC)

Hybride (une partie en présentiel, une autre en ligne)

Autres

**TARIF DE LA FORMATION (EN EUROS)**

**EFFECTIF MOYEN CONSTATÉ SUR LES DERNIÈRES SESSIONS***

**NOM ET PRÉNOM DU CONTACT POUR CETTE FORMATION***

**EMAIL PROFESSIONNEL DU CONTACT**

# E. ANNEXE - LES 35 *START-UP* FRANÇAISES RECENSÉES

**ACINQ** est l'une des trois sociétés au monde à développer Lightning, un réseau de paiement qui s'appuie sur Bitcoin tout en baissant les frais et le délai de transaction.

**ADANAM TECHNOLOGY** développe des solutions destinées aux entreprises, pour la traçabilité de bout en bout des flux de documents via la blockchain.

**ADAMEO** est un cabinet de conseil spécialisé en supply chain management. Un partenariat avec Transchain (cf. plus bas) est en cours pour l'utilisation de la blockchain comme outil de traçabilité.

**BCdiploma** développe une application de dématérialisation et automatisation de la délivrance d'attestations certifiées dédiée aux établissements d'enseignement supérieur et aux entreprises.

**BEEBRYTE** développe des solutions dédiées à la gestion énergétique des bâtiments. BEEBRYTE développe des outils de transaction pair-à-pair basés sur des *smart contracts*.

**BELEM** est une société de service spécialiste du développement de solutions blockchain et crypto-actifs dans des domaines comme la finance, l'assurance, ou le notariat.

**BIMCHAIN** développe une application autour de la traçabilité des données BIM (maquette numérique pour les projets dans le bâtiment) qui s'adresse aux maîtrises d'ouvrage.

**BIOTRAQ** propose des outils de suivi en temps-réel de la *supply chain* des denrées périssables en s'appuyant sur la collecte de données via des solutions IoT et l'exploitation intelligente de ces données à l'aide de *smart contracts* pour le suivi qualité.

**BLOCKCHAIN.IO**, société experte en développement à base de blockchains, iCOs, place de marchés,.Création hébergement et exploitation de services informatiques et de logiciels prestations de conseils. Paymium SAS est propriétaire et gestionnaire de deux plateformes d'échanges: - Paymium.com, l'unique place de marché Bitcoin/Euro régulée et auditée en France. - Blockchain.io, la place de marché dédiée exclusivement au trading de crypto-actifs.

**Blockchain Partner** (auditionnée) est une société de service qui aide les organisations à explorer et déployer les technologies blockchain

**BTU Protocol** (auditionnée) accompagne les entreprises dans leur développement digital afin de maximiser leur revenus et d'ouvrir de nouveaux canaux de distribution. Grâce à son modèle économique basé sur le crypto-actif "BTU", BTU Protocol prend 0 % de commission sur les réservations effectuées.

**BuyCo** simplifie les échanges entre les acteurs du transport maritime mondial.

**Connecting Food** propose des solutions de suivi de la qualité dans la filière alimentaire grâce à des services de traçabilité de bout en bout et d'audit exploitant les technologies blockchain et *smart contracts*.

**Coinhouse** propose une offre de service d'investissement dans des crypto-actifs (Bitcoin, ETH, ...) ainsi qu'un service de conservation. Ancienne filiale de Ledger, Coinhouse (ex "La Maison du Bitcoin") a pris son indépendance en novembre 2017.

**Crypto4all** (auditionnée) est spécialisée dans l'accompagnement des entreprises souhaitant développer des solutions basées sur la Technologie Blockchain : de l'étude préalable à la réalisation de la solution en passant par l'audit et la gestion de projet.

**Dawex** développe une plateforme d'échange de données et opère une grande place de marché de données. Elle permet aux entreprises et organisations d'orchestrer la circulation des données en les sourçant, monétisant et échangeant directement entre elles, en toute sécurité et dans le respect des réglementations en vigueur. La certification des échanges via un contrat de licence est archivée dans une blockchain Ethereum.

**Equisafe** (auditionnée) est une plateforme d'investissement basée sur la blockchain. Equisafe veut simplifier la gestion et les opérations d'un fonds d'investissement, tout en démocratisant l'investissement dans des titres financiers.

**Evoluchain** accompagne les entreprises avec une plateforme développeurs dédiée aux *smart contracts* et tokens, permettant la gestion en masse et la mise à jour de ceux-ci. Evoluchain propose également son expertise pour accompagner les ICO françaises et internationales sur le plan technologique.

**Famoco** propose une gamme de terminaux mobiles sécurisés basés sur Android, administrables à distance au moyen d'une plateforme MDM proposée en mode SaaS. Cette solution permet aux de configurer instantanément leurs appareils et un déploiement facile et rapide de leurs solutions métier.

**iExec** est une start-up française (issue d'Inria) qui vise à « décentraliser le cloud », en créant une place de marché mondiale du cloud computing où chacun peut louer contre RLC sa puissance de traitement

**IOV** fournit une blockchain annuaire de noms pour les portefeuilles de crypto-monnaies et les app décentralisées

**Lambda Vision** (auditionnée) développe des infrastructures de blockchain pour la gestion/monétisation décentralisée d'actifs intangibles et le trading de tokens. iXXo développe un nouveau protocole de confiance, MPOA (Mixed Proof of Authority).

**KeeeX** propose des solutions permettant de certifier et tracer documents, actifs numériques et processus via un procédé breveté combiné à la Blockchain. Ses solutions sont notamment utilisées dans la logistique, l'industrie, la banque/assurance et l'agroalimentaire.

**LEDGER** développe des solutions de sécurité et d'infrastructure pour les crypto-monnaies et applications blockchain, destinées à une clientèle de particuliers, d'entreprises, et de fonds d'investissement, en tirant parti d'un système d'exploitation propriétaire et exclusif : BOLOS, "Blockchain Open Ledger Operating System".

**Nomadic Labs** (auditionnée) développe la technologie Tezos en s'appuyant sur une équipe axée sur la recherche et le développement. Les principales compétences sont la théorie et la pratique du langage de programmation, les systèmes distribués et la vérification formelle.

**Origin Labs** (auditionnée) est une société qui crée une infrastructure et des applications décentralisées au niveau de l'entreprise. Origin Labs a développé Dune, un nouveau protocole Blockchain doublé d'une nouvelle crypto-monnaie.

**Ownest** sécurise le transfert de responsabilité grâce à la Blockchain, en ciblant les biens en transit sur les supply chains.

**PikcioChain** est une plateforme de données sécurisée, conforme et basée sur la blockchain qui permet automatiser n'importe quel processus qui nécessite la collecte, la certification et l'échange de données personnelles.

**Stratumn** développe une technologie « Proof of Process » qui sécurise chaque étape d'un processus industriel par un rail d'audit cryptographique pour garantir confidentialité, sécurité et traçabilité.

**TEO** pour "The Energy Origin", est une solution innovante basée sur l'utilisation de la Blockchain et des objets connectés qui permet de garantir l'origine verte de l'énergie utilisée.

**Tilkal** propose une infrastructure logicielle en production pour la traçabilité sécurisée et auditable de la supply chain. La plateforme permet de collecter et analyser les données du cycle de vie des produits de bout-en-bout et en temps réel, pour tous les intervenants d'une filière.

**TransChain** (auditionnée) s'adresse au monde du B2B en créant la confiance digitale entre les acteurs. Une interface pour que tous les acteurs puissent se connecter à la blockchain et ainsi garantir à leurs clients traçabilité et transparence.

**Tweag** (auditionnée) est une communauté d'experts en informatique, blockchain, science des données, IA, infrastructure cloud, traitement du signal, IoT, bio-informatique, physique et autres domaines.

**UNIRIS** développe un dispositif biométrique GDPR & Blockchain développé avec des chercheurs X/CNRS adressant le verrou du passage à l'échelle et de la consommation énergétique.

**UTOCAT** est un éditeur de logiciel blockchain pour le domaine bancaire et assurantiel.


cea
Institut Mines-Télécom
Inria