FINANCES PUBLIQUES

CONCOURS EXTERNE
POUR L'ACCÈS AU GRADE D'INSPECTEUR DES FINANCES PUBLIQUES AFFECTÉ AU TRAITEMENT DE L'INFORMATION EN QUALITÉ D'ANALYSTE

ANNÉE 2022

ÉPREUVE ÉCRITE D'ADMISSIBILITÉ N° 1

Durée : 4 heures – Coefficient : 4

Rédaction d'une note de synthèse à partir d'un dossier relatif aux questions économiques et financières

---

Toute note inférieure à 5/20 est éliminatoire.

Recommandations importantes

Le candidat trouvera au verso la manière de servir la copie dédiée.

Sous peine d'annulation, en dehors du volet rabattable d'en-tête, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tels que nom, prénom, signature, paraphe, localisation, initiale, numéro ou toute autre indication, même fictive, étrangère au traitement du sujet.

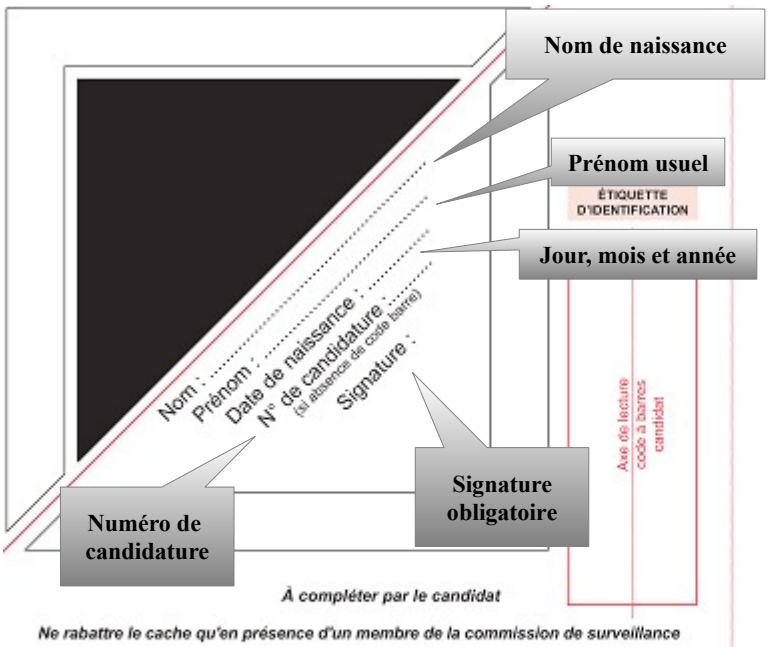
Sur les copies, les candidats devront écrire et souligner si nécessaire au stylo bille, plume ou feutre de couleur noire ou bleue uniquement. De même, l'utilisation de crayon surligneur est interdite.

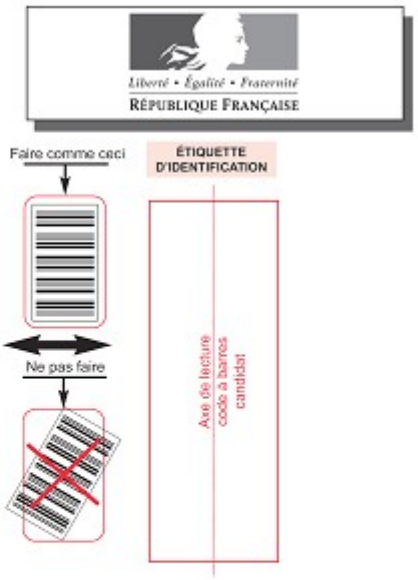
Il devra obligatoirement se conformer aux directives données.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Tournez la page S.V.P.

Le candidat complétera l'intérieur du volet rabattable des informations demandées et se conformera aux instructions données





Concours externe - interne - professionnel - ou examen professionnel (1)
(1) Rayer les mentions inutiles

Externe

Pour l'emploi de : **Inspecteur des Finances Publiques affecté au traitement de l'information en qualité d'analyste**

Épreuve n° : **1**

Matière : **006 – Rédaction d'une note de synthèse**

Date : **16/11/2021**

Préciser éventuellement le nombre d'intercalaires supplémentaires

Nombre d'intercalaires supplémentaires :

À L'ATTENTION DU CANDIDAT

En dehors de la zone d'identification rabattable, les copies doivent être totalement anonymes et ne comporter aucun élément d'identification tel que nom, prénom, signature, paraphe, localisation, initiale, numéro, ou toute autre indication même fictive étrangère au traitement du sujet.

Il est demandé aux candidats d'écrire et de souligner si nécessaire au stylo bille, plume ou feutre, de couleur noire ou bleue uniquement. Une autre couleur pourrait être considérée comme un signe distinctif par le jury, auquel cas la note de zéro serait attribuée. De même, l'utilisation de crayon surligneur est interdite.

Les étiquettes d'identification codes à barres, destinées à permettre à l'administration d'identifier votre copie, ne doivent être détachées et collées dans les deux cadres prévus à cet effet qu'en présence d'un membre de la commission de surveillance.

Suivre les instructions données pour les étiquettes d'identification

NOTE / 20 ,

RÉSERVÉ À L'ADMINISTRATION

À L'ATTENTION DU CORRECTEUR

Pour remplir ce document :
Utilisez un stylo ou une pointe feutre de couleur NOIRE ou BLEUE.

EXEMPLE DE MARQUAGE : Faire comme ceci — Ne pas faire

Pour porter votre note, cochez les gélules correspondantes.

Reportez la note dans les zones **NOTE / 20** et dans le cadre **A**

En cas d'erreur de codification dans le report des notes cochez la case **erreur** et reportez la note dans le cadre **B**.

Cadre A réservé à la notation		
20	19	18
17	16	15
14	13	12
11	10	09
08	07	06
05	04	03
02	01	00
Décimales		
,00	,25	,50 ,75

Cadre B réservé à la notation rectificative		
20	19	18
17	16	15
14	13	12
11	10	09
08	07	06
05	04	03
02	01	00
Décimales		
,00	,25	,50 ,75
Erreur		

NOTE / 20 ,

EN AUCUN CAS, LE CANDIDAT NE FERMERA LE VOLET RABATTABLE AVANT D'Y AVOIR ÉTÉ AUTORISÉ PAR LA COMMISSION DE SURVEILLANCE

FINANCES PUBLIQUES

SUJET

RÉDACTION D'UNE NOTE DE SYNTHÈSE À PARTIR D'UN DOSSIER RELATIF AUX QUESTIONS ÉCONOMIQUES ET FINANCIÈRES

Code matière : 006

Les candidates et les candidats peuvent avoir à leur disposition sur la table de concours le matériel d'écriture, une règle, un correcteur, des surligneurs.

À l'aide des seuls documents joints, vous rédigerez une note de synthèse dans laquelle vous présenterez la technologie *blockchain*. Vous montrerez également les perspectives pour développer les usages de cette technologie, ainsi que ses limites.

Vous rédigerez ensuite une note de propositions (deux pages au maximum), en vous appuyant sur vos connaissances personnelles, présentant des actions concrètes pour accompagner et réguler le développement des *blockchains*.

Tournez la page S.V.P.

Liste des documents

Le fonds documentaire comporte 22 pages.

Qu'est-ce que la *blockchain* ?

Source : Bercy Infos, site www.economie.gouv.fr – 20 septembre 2019

Saviez-vous que la *blockchain* est une technologie qui permet de garder la trace d'un ensemble de transactions, de manière décentralisée, sécurisée et transparente, sous forme d'une chaîne de blocs ? Vous n'y comprenez toujours rien ? Pas de panique, on vous explique tout !

La *blockchain* : c'est quoi ?

Développée à partir de 2008, la *blockchain* est en premier lieu une technologie de stockage et de transmission d'informations. Cette technologie offre de hauts standards de transparence et de sécurité car elle fonctionne sans organe central de contrôle.

Plus concrètement, la *blockchain* permet à ses utilisateurs – connectés en réseau – de partager des données sans intermédiaire.

***Blockchain* : définition**

Dans son rapport publié en décembre 2018, la mission d'information commune de l'Assemblée nationale sur les usages des chaînes de blocs et autres technologies de certification de registre donne la définition suivante de la *blockchain* :

Une blockchain *est un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie.*

La *blockchain* : comment ça marche ?

En pratique, une *blockchain* est une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. La Banque de France en explique les principales caractéristiques :

- l'**identification** de chaque partie s'effectue par un procédé cryptographique
- la **transaction** est envoyée à un réseau (ou « nœud » de stockage) d'ordinateurs situés dans le monde entier
- chaque « **nœud** » héberge une copie de la base de données dans lequel est inscrit l'historique des transactions effectuées. Toutes les parties prenantes peuvent y accéder simultanément
- le **système de sécurisation** repose sur un mécanisme de consensus de tous les « nœuds » à chaque ajout d'informations. Les données sont déchiffrées et authentifiées par des « centres de données » ou « mineurs ». La transaction ainsi validée est ajoutée dans la base sous forme d'un bloc de données chiffrées (c'est le « *block* » dans « *blockchain* »)
- la **décentralisation de la gestion** de la sécurité empêche la falsification des transactions. Chaque nouveau bloc ajouté à la *blockchain* est lié au précédent et une copie est transmise à tous les « nœuds » du réseau. L'intégration est chronologique, indélébile et infalsifiable.

Tournez la page S.V.P.

La *blockchain* : quels avantages ?

L'utilisation de la *blockchain* comporte de nombreux avantages, parmi lesquels :

- la **rapidité des transactions** grâce au fait que la validation d'un bloc ne prend que quelques secondes à quelques minutes
- la **sécurité du système**, qui est assuré par le fait que la validation est effectuée par un ensemble d'utilisateurs différents, qui ne se connaissent pas. Cela permet de se prémunir du risque de malveillance ou de détournement, puisque les nœuds surveillent le système et se contrôlent mutuellement
- les **gains de productivité et d'efficacité** générés grâce au fait que la *blockchain* confie l'organisation des échanges à un protocole informatique, ce qui réduit mécaniquement les coûts de transaction ou de centralisation existant dans les systèmes traditionnels (frais financiers, frais de contrôle ou de certification, recours à des intermédiaires qui se rémunèrent pour leur service ; automatisation de certaines prestations, etc.).

La *blockchain* : quelles applications ?

La *blockchain* représente une innovation majeure qui est notamment utilisée dans le secteur bancaire. En effet, historiquement, la technologie *blockchain* s'est développée pour soutenir des transactions réalisées via les crypto-monnaies/crypto-actifs (dont les *bitcoins* qui sont la forme la plus connue) et qui ont comme caractéristique principale de ne pas dépendre d'un organisme centralisateur (comme une banque centrale) et d'être internationales.

Mais son usage ne se limite pas aux crypto-monnaies. De nombreux domaines et secteurs d'activités, marchands ou non marchands, publics ou privés, utilisent déjà la *blockchain* ou prévoient de le faire dans les années à venir. Le rapport de la mission d'information commune de l'Assemblée nationale sur les usages des chaînes de blocs et autres technologies de certification de registre, détaille quelques-uns des champs d'utilisation de la *blockchain* :

- dans le secteur **banque**, la technologie ouvre la possibilité de valider des transactions sans l'intermédiaire d'une chambre de compensation, ce qui devrait permettre de certifier des opérations dans des délais beaucoup plus courts ; la *blockchain* peut aussi favoriser le partage d'informations entre acteurs concurrents d'une place financière dans le respect du secret de leurs données commerciales et, ce faisant, faciliter la gestion de structures ou d'instruments communs en réduisant les coûts de contact et les frais d'administration
- dans le secteur de l'**assurance**, l'apport de la *blockchain* tient par exemple à l'automatisation des procédures de remboursement et à l'allégement de certaines formalités à la charge des sociétés comme de leurs clients, sous réserve que les hypothèses et les conditions d'indemnisation et de préjudice soient clairement établies
- dans le secteur de la **logistique**, la *blockchain* présente deux intérêts : assurer une traçabilité des produits, ainsi que la mémoire des différentes interventions sur une chaîne de production et de distribution ; alléger les formalités et créer les conditions d'une coopération entre les acteurs d'une filière, notamment en matière d'échange d'informations ; cet usage pourrait trouver aussi une application dans le secteur **agro-alimentaire** pour la traçabilité des aliments, particulièrement intéressante en cas de crise sanitaire

- dans le secteur **énergétique**, en autorisant l'échange de services et de valeurs en dehors d'une instance de gestion centrale, la *blockchain* crée potentiellement les conditions de la mise en place – à une plus ou moins grande échelle suivant les capacités techniques – de réseaux locaux de production, d'échange et de revente d'énergie pour équilibrer l'offre et la demande à tout moment, ce qui est une contrainte forte des réseaux d'électricité en particulier.

Mais de nombreux autres secteurs sont potentiellement concernés par l'utilisation de la technologie *blockchain* : **santé, immobilier, luxe, aéronautique**, etc.

La *blockchain* : et si on résumait ?

La *blockchain* :

1. c'est une technologie de stockage et de transmission d'informations, prenant la forme d'une base de données
2. qui a la particularité d'être partagée simultanément avec tous ses utilisateurs et qui ne dépend d'aucun organe central
3. a pour avantage d'être rapide et sécurisée
4. et dont le champ d'application est bien plus large que celui des crypto-monnaies/crypto-actifs (assurance, logistique, énergie, industrie, santé, etc.).

Comprendre les *blockchains* (chaînes de blocs) – Extrait de la note scientifique n° 4 de l'Office

Source : Office parlementaire d'évaluation des choix scientifiques et technologiques

Avril 2018

Résumé

- *Apparues il y a 10 ans comme combinaison de technologies plus anciennes formant le protocole sous-jacent au bitcoin, les* blockchains *permettent des échanges décentralisés et sécurisés sans qu'il soit besoin d'un tiers de confiance.*
- *Leurs applications dépassent le cadre strict des crypto-monnaies et sont potentiellement nombreuses mais peu conjuguent, à ce jour, maturité technologique suffisante et pertinence de l'usage.*
- *La recherche doit relever le défi de la capacité des* blockchains *à monter en charge, ainsi que celui de leur consommation énergétique.*

Contexte de la note

La présente note répond à une demande de la mission d'information commune sur « les usages des *blockchains* et autres technologies de certification de registres » créée à l'Assemblée nationale. Elle sera suivie d'une note plus développée. Ce qu'on appelle, par métonymie, chaînes de blocs ou *blockchains* sont des t**echnologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers.**

Pour comprendre le fonctionnement de ces registres informatiques, qui utilisent des réseaux décentralisés pair à pair (*peer to peer*), et forment les technologies sous-jacentes aux crypto-monnaies, type particulier de monnaies virtuelles, il est nécessaire de revenir à leurs origines.

Aux origines des *blockchains*

L'émergence des crypto-monnaies a partie liée avec le **mouvement pour le logiciel libre**, initié dans les années 1980 par Richard Stallman, ainsi qu'avec la communauté « ***cypherpunk*** », désireuse d'utiliser les technologies de chiffrement pour créer une monnaie électronique et garantir des transactions anonymes.

Les premières tentatives – David Chaum en 1983 avec *e-cash* puis en 1990 avec *digicash*, Wei Dai en 1998 avec *b-money* et, Nick Szabo avec *bit-gold* – sont des échecs. L'invention de *hashcash* par Adam Back en 1997, avait pourtant marqué un progrès avec l'idée de valider les transactions en utilisant les fonctions de hachage cryptographiques, appelées « preuve de travail ». L'objectif de ces technologies est de rendre inutile l'existence d'un « tiers de confiance », en recourant à un système de confiance distribuée permettant de constituer une sorte de « grand livre comptable » infalsifiable.

L'obstacle à lever résidait dans le problème de la double dépense (risque qu'une même somme soit dépensée deux fois) et, plus généralement, dans celui de la tolérance aux pannes, qu'elles soient accidentelles ou malveillantes.

La réponse à ces difficultés est apportée en 2008 dans un **article de Satoshi Nakamoto.** Ce dernier y décrit le fonctionnement d'un protocole infalsifiable utilisant un réseau pair à pair – la *blockchain* – comme couche technologique d'une nouvelle crypto-monnaie – le *bitcoin*.

Le fonctionnement de la *blockchain*

Le *bitcoin* repose sur un protocole sous-jacent appelé *blockchain*. On parle de chaînes de blocs, ou *blockchains*, car les transactions effectuées entre les utilisateurs du réseau sont **regroupées par bloc « horodaté »**.

Une fois le bloc validé, en moyenne toutes les dix minutes, la transaction devient visible pour l'ensemble des détenteurs du registre, potentiellement tous les utilisateurs, qui vont alors l'ajouter à leur chaîne de blocs.

Chaque transaction a recours à la cryptographie asymétrique, apparue avec le protocole Diffie-Hellman de 1976, qui fonctionne avec une paire de clés, l'une privée et l'autre publique, liées entre elles par un algorithme à courbes elliptiques (ECDSA). La clé publique est diffusable et permet de recevoir des transactions, la clé privée est quant à elle gardée secrète. Protéger ses clés privées est le seul moyen de conserver ses *bitcoins* en sécurité. Dans la mesure où il est possible de retracer toutes les transactions du propriétaire d'une clé publique, il s'agit plus d'un système pseudonyme qu'anonyme. La datation des blocs ainsi constitués est appelée « **horodatage** ».

Chaque bloc, outre les transactions et l'horodatage, possède un identifiant (…) qui prend la forme d'un « ***hash*** » permettant de relier les blocs les uns aux autres. En informatique, le « **hachage** » permet de convertir n'importe quel ensemble de données numériques en un *hash*, c'est-à-dire en une courte suite binaire qui lui est propre. L'algorithme de chiffrement utilisé à cet effet est appelé « fonction de hachage cryptographique ». Le *hash* d'un ensemble de données peut ainsi être comparé à une empreinte digitale, bien moins complexe que l'individu entier, mais l'identifiant de manière précise et unique. Une fonction de hachage est dite « à sens unique » : elle est conçue de telle sorte que le *hash* produit, à savoir une image ou empreinte de taille fixe créée à partir d'une donnée de taille variable, fournie en entrée, est impossible à inverser. Celle utilisée pour le *bitcoin* est parmi les plus répandues : il s'agit de la fonction *Secure Hash Algorithm-256* (SHA 256), ainsi dénommée car elle produit des *hashs* d'une taille de 256 bits.

Nœuds du réseau, « mineurs » et consensus

Chaque bloc est validé par certains utilisateurs baptisés « **mineurs** » (en référence aux chercheurs d'or), et sont transmis aux « nœuds » du réseau, c'est-à-dire aux détenteurs du registre, qui l'actualisent en permanence. La validation des blocs permet de se prémunir du risque d'attaques malveillantes. Aucune autorité centrale ne s'en occupe, puisque les utilisateurs s'en chargent en surveillant le système et en se contrôlant mutuellement. Cette sécurité, source de confiance, est l'un des aspects essentiels de la *blockchain*. Le fait que des centaines de copies du registre soient mises à jour simultanément et régulièrement, au terme d'une compétition cryptographique, rend les *blockchains* quasiment indestructibles. Une « **méthode de consensus** » permet de décider qui validera le prochain bloc à ajouter à la chaîne. Dans le cas du *bitcoin*, elle est appelée « **preuve de travail** » (*proof of work*) car elle suppose la réussite à une épreuve cryptographique dénommée « **minage** », qui se répète en moyenne toutes les dix minutes. Elle consiste en la résolution par les mineurs de problèmes cryptographiques complexes. Ils consistent à obtenir un *hash*, commençant par un certain nombre de zéros, du bloc que le mineur souhaite intégrer. Cette opération, très coûteuse en puissance de calcul informatique, est motivée par l'obtention d'une récompense en *bitcoins* par le mineur gagnant. Le bloc validé par ce dernier est transmis de pair à pair à chaque nœud qui ajoute à sa propre *blockchain* le bloc ainsi validé. Si deux blocs sont validés au même moment, les mineurs utilisent l'un ou l'autre et **deux chaînes parallèles se développent**. Le protocole prévoit alors que, rapidement, seule **la plus longue subsiste**, c'est-à-dire en pratique celle que la majorité des nœuds aura adoptée

La **rémunération des mineurs** est complétée par des **frais** prélevés sur les transactions qu'ils intègrent à chaque nouveau bloc. Leur montant est en théorie déterminé librement par les utilisateurs, mais les mineurs sélectionnant en priorité les plus élevés, ces frais varient de fait en fonction du nombre de transactions en attente. L'**organisation des mineurs en groupements** ou « *pools* » induit le risque qu'une majorité organisée oriente la validation des blocs. La confiance des

utilisateurs dans le système étant en théorie un objectif partagé par les mineurs, celui-ci est censé suffire à garantir le respect des règles, dans une logique de « main invisible » protégeant les intérêts privés. Il faut cependant souligner que quatre pools dont trois chinois, appuyés sur des « fermes de minage », assurent aujourd'hui plus de 60 % de la puissance de calcul nécessaire à la *blockchain* du *bitcoin* et pourraient utiliser cette position dominante contre l'intérêt des autres utilisateurs.

D'autres méthodes de consensus que la « preuve de travail » (*proof of work*) existent et sont souvent plus centralisées : la principale alternative, qui présenterait un risque plus grand d'utilisation malveillante, est la « **preuve d'enjeu** », appelée aussi « preuve de participation » *(proof of stake)*, basée sur la possession de crypto-monnaies mises en gage, qui se décline à son tour en « preuve de possession » *(proof of hold)*, fondée sur la durée de possession, « preuve d'utilisation » *(proof of use)*, fonction du volume de transactions, ou encore « preuve d'importance » *(proof of importance)*, reposant sur la « réputation ». Deux autres méthodes moins usitées peuvent aussi être évoquées : la « preuve de capacité » *(proof of space)* qui consiste à mettre en gage de l'espace disque disponible, ou encore la « preuve de destruction » *(proof of burn)* qui revient à détruire des crypto-actifs, pour obtenir la confiance du réseau.

Réformer la *blockchain* : *hard* et *soft forks*

Il est possible de modifier les règles régissant une *blockchain*, on parle alors d'embranchement *(fork)*. Cela suppose toutefois qu'une modification du code soit intégrée par l'ensemble du réseau. Toute personne peut proposer des modifications mais elles émanent le plus souvent de quelques développeurs (un noyau d'une quarantaine dans le cas du *bitcoin*). On distingue deux types d'évolutions : les « *soft forks* », lorsque les blocs produits sous la nouvelle version peuvent être ajoutés par des nœuds fonctionnant encore sous l'ancienne version, et les « *hard forks* », lorsqu'une telle rétrocompatibilité est impossible. Lorsqu'ils ne sont pas adoptés à l'unanimité, les *hard forks* peuvent donner naissance à des *blockchains* alternatives de la version originelle. En 2017, *bitcoin* cash et *bitcoin* gold sont ainsi nés de *hardforks* du *bitcoin* d'origine. Ils peuvent aussi permettre de revenir à un état antérieur de la *blockchain* lorsque celle-ci a été altérée, ce qui pourrait supposer d'annuler les transactions ultérieures.

Le défi de la montée en charge (« scalabilité »)

La **capacité à faire face à une augmentation du nombre de transactions** constitue l'un des principaux défis pour les *blockchains*, à commencer par celle du *bitcoin*. Cette dernière ne permettait jusqu'en 2017 la validation que de quatre transactions par seconde en moyenne (autour de 20 en 2018). Ce défi de la montée en charge (scalabilité) reste entier. Il a conduit à accélérer la naissance d'autres crypto-monnaies, plus de 1 500 à ce jour, souvent dites alternatives (« *altcoins* »). Il a également mené à des innovations encore peu matures d'un point de vue technologique comme la parallélisation de *blockchains* collatérales, aux fonctions différentes et complémentaires (« *sidechains* » pour le *bitcoin* , « *sharding* » ou « *plasma chains* » sur Ethereum), le recours à des bases de données liées à la *blockchain* (« *side databases* ») ou encore la création d'une nouvelle couche de protocole allégé et rapide « au-dessus » de la *blockchain* mais bénéficiant de sa sécurité (« *lightning networks* » pour le *bitcoin*, « *state channels* » sur Ethereum).

D'autres applications pour la *blockchain* ?

Le rôle de la *blockchain* en tant que **technologie sous-jacente des nombreuses crypto-monnaies** est aujourd'hui dominant. Cependant, ses protocoles **se déclinent dans de nombreux secteurs** et pourront donner naissance à des applications nouvelles variées, dépassant le cadre strict de la finance : par exemple des services d'attestation et de certification pouvant concerner l'état civil, le cadastre, des contrats de type notarié ou encore des mécanismes de protection de la propriété intellectuelle. Mais peu d'applications conjuguent, à ce jour, pertinence de l'usage et maturité technologique suffisante. La *blockchain* Ethereum offre une infrastructure adaptée à des outils tels

que des codes informatiques qui pourraient s'exécuter après avoir été écrits dans une *blockchain* : *smart contracts,* applications décentralisées dites « *Dapps* » et organisations autonomes décentralisées ou « DAO ».

Programmer la *blockchain* : les *smart contracts*

Les « contrats intelligents » ou *smart contracts* sont des programmes informatiques inscrits dans la *blockchain*. En effet, il est possible d'échanger en son sein des lignes de script, au même titre que des transactions. Ce ne sont pas des contrats au sens juridique, mais des codes informatiques qui facilitent, vérifient ou exécutent un contrat au stade de sa négociation ou de sa mise en œuvre. Par rapport à des programmes classiques, les *smart contracts* présentent l'avantage de bénéficier des caractéristiques particulières de la *blockchain*. Ainsi, leur exécution est irrémédiable et leur code est vérifiable librement par les nœuds du réseau. Ils permettent notamment de placer des fonds sous séquestre de manière vérifiable. Leur mise en œuvre suppose toutefois plusieurs préalables, notamment des mécanismes de vérification approfondis, utiles en raison de l'immuabilité du registre, ainsi que le développement d'un langage de programmation adapté aux contraintes de volume de données propres à un réseau distribué. Par ailleurs, l'exécution de la plupart des cas d'usage annoncés, est conditionnée par l'apport et l'export d'informations. Que ce soit pour relever une température, livrer un colis, prouver la réalisation d'un travail, ou donner l'heure d'arrivée d'un avion, un tiers, qualifié d'oracle dans l'écosystème Ethereum, doit faire le lien entre la *blockchain* et le reste du monde, ce qui s'apparente au retour d'un « tiers de confiance ».

La distinction entre *blockchains* ouvertes ou publiques et *blockchains* fermées ou privées

La distinction *blockchains* publiques/*blockchains* privées **ne repose pas sur une distinction entre *blockchains* de personnes publiques** (États, collectivités…) **et *blockchains* de personnes privées** (entreprises, ONG…), **mais sur le caractère ouvert ou fermé de la *blockchain***, les protocoles de chaînes de blocs pouvant être distingués selon qu'ils sont ouverts à l'écriture et à la lecture sans restriction ou que l'une ou l'autre de ces opérations est soumise à l'acceptation d'un tiers. On parlera de *blockchains* ouvertes (« *permissionless* ») ou fermées (« *permissioned* ») ou encore de *blockchains* publiques ou privées.

Les protocoles de *blockchains* sans restriction d'accès sont les plus connus. Ils soutiennent le *bitcoin* ou l'ether. Comme il a été vu, n'importe qui peut en devenir un nœud, et ces protocoles nécessitent une méthode de consensus.

Il existe aussi un grand nombre de **protocoles à restriction d'accès,** pour certains particulièrement aboutis et déjà opérationnels. Parmi ces derniers, les *blockchains* « de consortium » résultent du regroupement de plusieurs organisations indépendantes, voire concurrentes, utilisant la *blockchain* pour archiver dans un registre décentralisé des transactions sécurisées, ou échanger des actes certifiés, sans avoir à faire intervenir un tiers de confiance. D'autres protocoles sont utilisés au sein d'une même organisation, pour simplifier et automatiser des échanges et des certifications. Dans une *blockchain* privée, une autorité régulatrice valide l'introduction de nouveaux membres, et accorde les droits en écriture et en lecture. Cette autorité peut être seule aux commandes, ou gouvernée collégialement par les différents participants. À la différence d'une *blockchain* publique, les *blockchains* privées peuvent exiger une majorité renforcée. De même, il suffit de trois participants pour faire fonctionner une *blockchain* privée, tandis que les *blockchains* publiques sont appelées à en compter plusieurs milliers.

Un débat existe pour qualifier les *blockchains* privées de « vraies » ou de « fausses » *blockchains*, sachant que créer un produit recourant à ces technologies est aussi un **enjeu de marketing**. Le recours de certaines applications aux *blockchains* ne semble pas toujours justifié, les fonctionnalités offertes par les bases de données partagées et sécurisées existantes apparaissant en effet suffisantes à leur réalisation, alors que des technologies alternatives de registres distribués sont en développement : *hashgraph, tangle* ou *directed acyclic graph* (DAG).

Le succès de certaines levées de fonds spécifiques à l'écosystème des crypto monnaies (*Initial Coin Offering*, ou ICO) interroge également. Ces émissions d'actifs numériques (appelés jetons ou *tokens*) échangeables contre des crypto-monnaies ont représenté plus de 3 milliards de dollars en 2017, ce qui peut sembler peu rationnel puisqu'elles n'offrent aucune garantie aux investisseurs.

Un regard plus distancié paraît nécessaire, en raison des **effets de mode propres aux écosystèmes entrepreneuriaux.** Ces effets de mode, visibles dans le recours à certains concepts, tels que les technologies disruptives, l'intelligence artificielle, les données massives *(big data)*, le *cloud*, l'internet des objets (IoT, pour « *internet of things* ») ou, encore, la *blockchain*, sont parfois le reflet de stratégies marketing séduisantes, mais sans toujours s'accompagner d'innovations aussi majeures que celles annoncées.

Les enjeux énergétiques et environnementaux

Outre les questions de montée en charge, de sécurité, de régime fiscal, ou de cadre juridique, les *blockchains* posent aussi celle, essentielle, de leurs impacts énergétiques et environnementaux. Les besoins en électricité des *blockchains* fondées sur la preuve de travail sont considérables.

Leur estimation fait l'objet de débats mais la consommation pour le seul *bitcoin* est d'au moins **24 TWh/an**. La dépense énergétique étant corrélée à l'intéressement des mineurs, sa croissance est quasi exponentielle. Face à l'explosion des cours, la réduction par deux tous les quatre ans des récompenses de minage (phénomène appelé « *halving* ») apparaît insuffisante pour jouer son rôle de régulation de la compétition. De meilleures capacités de calcul ou l'utilisation de surplus électrique ne permettront pas de diminuer la consommation énergétique. En effet, la compétition se jouant sur les coûts, les économies offertes aux mineurs le sont aussi aux attaquants potentiels.

L'impact en termes d'émissions de gaz à effet de serre est d'autant plus important que les groupements de mineurs sont surtout établis en Chine, pays qui présente l'intensité carbone la plus élevée au monde. La recherche doit donc **relever ce défi de la consommation énergétique** des *blockchains*, à l'image de l'initiative française BART (« *Blockchain Advanced Research & Technologies* »), qui doit permettre de valider la *blockchain* en consommant moins d'énergie, par des méthodes de consensus robustes aux moyens cryptographiques avancés, tout en développant de nouvelles architectures facilitant la fiabilité et la montée en charge du réseau.

Rapport « Les enjeux des *blockchains* » – Synthèse

Source : Rapport France Stratégie – 21 juin 2018

SORTIR LA *BLOCKCHAIN* DU BAC À SABLE

Pour mettre pleinement à profit une innovation, il faut penser neuf. La technologie de la *blockchain* nous y invite, à moins qu'elle ne nous y contraigne. En un mot, il s'agit d'une nouvelle façon de stocker de l'information, de la préserver sans modification, d'y accéder et d'intégrer de nouvelles informations qui deviennent infalsifiables. Ces nouvelles données peuvent résulter de l'exécution d'une opération, d'une transaction ou de l'exécution « automatique » d'un programme informatique. Elles sont inscrites sur l'équivalent d'un vaste registre « distribué », c'est-à-dire partagé sur les ordinateurs de tous les membres du réseau, un système qui permet transparence et auditabilité. Dans une telle architecture, les questions de contrôle et de sécurité se trouvent radicalement modifiées.

On conçoit l'ampleur des mutations que promet une telle innovation. Techniquement, elle pourrait offrir une solution aux fragilités des systèmes centralisés. Économiquement, elle devrait permettre d'augmenter la productivité en limitant les intermédiaires et en automatisant les transactions. Institutionnellement, elle est une réponse à la défiance dont souffrent les institutions politiques et économiques, avec à la clé une fluidification des relations économiques et sociales.

La *blockchain* est donc une technologie promise à un bel avenir. Dans la grande variété des usages envisagés, deux grandes catégories se dégagent.

- *Les applications de type « notarial » liées à la tenue d'un registre* qui a vocation à être partagé. La *blockchain* pourrait modifier les modalités de contrôle des transactions, de transfert de biens et d'échanges entre personnes, et au-delà la certification des processus industriels ou financiers. On attend en particulier son utilisation dans la traçabilité des médicaments ou des produits alimentaires ; elle pourrait aussi donner jour à des systèmes sécurisés de vote en ligne ou d'identification numérique des personnes.
- *Les applications couplant la dimension transactionnelle au monde physique*, ce qu'on appelle « l'internet de la valeur ». Une transaction peut être déclenchée par une intervention directe ou par l'exécution d'un programme informatique susceptible de comporter des conditions ou des vérifications particulières, par exemple sur la date ou à partir d'informations venant du monde physique. Avec de tels « smart contracts », les *blockchains* ouvrent l'ère des transactions programmables, sans intervention d'un tiers de confiance. Ces applications visent à créer de la confiance là où elle fait défaut ou à se substituer à des mécanismes de confiance centralisés. En supprimant les intermédiaires et en décentralisant les processus de validation, elles doivent permettre des gains de productivité substantiels.

À ce jour, cependant, les cas d'usage réellement opérationnels sont rares. De fait, si on veut rendre effectives les potentialités de la *blockchain*, il faudra surmonter de nombreuses difficultés de nature diverse.

Tournez la page S.V.P.

Les enjeux sont techniques

Scalabilité. Les protocoles *blockchain*, qui pour l'heure gèrent des données restreintes, supporteront-ils le changement d'échelle en cas de diffusion massive ? Le réseau *Bitcoin* par exemple traite une poignée de transactions par seconde, contre plusieurs milliers pour un opérateur de carte bancaire. Le mécanisme de validation historique de la *blockchain*, avec ses nœuds multiples et ses procédés cryptographiques, est source de lenteur. Les solutions techniques passent par des mécanismes de validation moins lourds, mais par conséquent moins fiables.

Protocole de consensus. Qui a accès à la *blockchain*, qui définit les modalités d'un ajout sur la chaîne, comment décider d'une évolution du protocole ? Le choix du « protocole de consensus distribué » est une question éminemment stratégique. La *blockchain* peut être publique, avec une architecture ouverte, ou privée, avec un nombre volontairement limité de participants et la réintroduction d'une forme d'autorité centralisée. L'enjeu technique se fait ici enjeu de gouvernance.

Identité électronique. Les applications requièrent que soit traitée au préalable la question de la vérification de l'identité électronique des biens ou des personnes, puisque la *blockchain* sert de support d'enregistrement sécurisé des transactions. Les questions des modalités – et de l'éventuelle fragilité – de l'interfaçage entre le monde numérique et le monde « réel » sont au cœur de la nouvelle technologie.

Consommation électrique. Les opérations de vérification, de validation et de cryptographie sont très consommatrices en électricité. Même si les chiffres sont contestés, une large diffusion des *blockchains* pourrait entraîner une externalité environnementale fortement négative. L'enjeu technique se fait ici enjeu environnemental.

Les enjeux sont monétaires et financiers

Volatilité et spéculation. Bâties sur la technologie *blockchain*, les crypto-monnaies se sont multipliées ces dernières années : il en existe aujourd'hui plus de 1 500, avec une capitalisation totale supérieure à 300 milliards d'euros. Mais la grande volatilité de leur cours empêche de construire des modèles économiques pérennes. La trajectoire récente du *bitcoin* – avec une envolée de son cours suivie d'une correction massive fin 2017 – a mis en évidence la dimension spéculative de ces crypto-actifs. Pour lutter contre ce phénomène, il faudrait imposer des réglementations comparables à celles qui sont appliquées aux marchés financiers, notamment concernant la manipulation de cours.

Dissociation entre blockchain et crypto-monnaies. On a voulu instaurer une sorte de cordon sanitaire entre les crypto-monnaies, considérées avec une certaine suspicion, et la *blockchain*, considérée comme très prometteuse. Utile dans un premier temps pour laisser se déployer l'innovation malgré les problèmes de fraude que posent certains usages des crypto-monnaies, cette séparation commence à poser problème. De fait, les protocoles de consensus qui sont au cœur des *blockchains* publiques reposent tous sur des mécanismes d'incitation économique qui requièrent l'émission d'un actif numérique. Cet actif permet d'inciter les différents acteurs à participer à la sécurisation du réseau – le protocole attribuant automatiquement un certain nombre de « jetons » aux validateurs des nouveaux blocs. Ce fonctionnement fait des actifs numériques une des pierres angulaires des *blockchains* publiques. Pour séparer le bon grain de l'ivraie et bénéficier des seuls effets souhaités des *blockchains*, il ne suffira donc pas d'essayer d'interdire ou de contrôler le *bitcoin*.

Vers une monnaie digitale de banque centrale ? Cette solution permettrait un couplage effectif entre monnaie et univers de la *blockchain*. Ce moyen de règlement émis par la banque centrale de nature crypto-monétaire donnerait le soutien matériel (existence d'un bilan) et institutionnel (légal et budgétaire) dont manquent aujourd'hui les crypto-monnaies. L'idée serait à l'étude au Royaume-Uni, au Canada, en Inde, en Suède, en Chine, à Singapour et en Russie. Le débat est bel et bien lancé. Un nouvel acronyme a même vu le jour, CBDC, pour *Central Bank Digital Currency*.

Une économie qui pourrait être transformée. La spéculation et les « arnaques » autour des crypto-monnaies ne doivent pas masquer l'essentiel. Ce qui explique le succès de ces crypto-actifs, c'est la promesse d'un ou plusieurs réseaux de transactions automatiques et de notarisation. Nombreux sont ceux qui parient sur l'avenir de la *blockchain* comme hier ils pariaient sur Google et Facebook. Une fois passée la phase de mise au point, cette technologie est susceptible de bouleverser l'économie. Les échanges devenus par ailleurs totalement numérisés pourraient être certifiés. Les opérations entourant les échanges – appels d'offres, validations partielles par des tiers, règlements conditionnés, etc. – pourraient être gérés automatiquement et en confiance grâce aux *smart contracts*. En somme, l'économie deviendrait en partie programmable. En France, depuis quelques années, plusieurs acteurs institutionnels majeurs – Assemblée nationale, Consortium LabChain autour de la Caisse des dépôts, Banque de France, AMF, Trésor, MEDEF – ont porté des initiatives montrant leur volonté de favoriser le développement des *blockchains* en France. Un écosystème dynamique se développe progressivement, avec des startups, des cabinets de conseil et l'implication de grandes entreprises qui étudient le sujet et y dédient des ressources.

Les enjeux sont sécuritaires

Défaillances et piratages. Encore largement expérimentale, la *blockchain* a fait l'objet de nombreux piratages ou bogues qui mettent à mal la promesse de confiance et d'infaillibilité – même si le protocole numérique du *bitcoin* apparaît aujourd'hui peu susceptible d'être pris en défaut. Une tension se fait jour entre l'allègement nécessaire des mécanismes de certification et la fragilisation des *blockchains*.

Lutte contre les activités illicites. Les crypto-monnaies se signalent aussi par leur capacité – qui varie avec le degré d'anonymat et de traçabilité des transactions – à permettre les paiements frauduleux (drogue, armes, blanchiment) ou l'évasion fiscale. Les transactions frauduleuses seraient en baisse en proportion mais en croissance en valeur absolue. Les pouvoirs publics de nombreux pays appellent au renforcement des politiques de lutte contre le blanchiment et le financement du terrorisme (politiques AML et KYC), en adoptant les modalités de mise en œuvre aux spécificités des crypto-monnaies.

Anonymat et traçabilité. Tout l'enjeu consiste à concilier – comme avec l'argent liquide – les attentes légitimes d'anonymat, pour la protection de la vie privée ou le secret des affaires, et les objectifs de traçabilité pour lutter contre la fraude. Des outils d'analyse commencent à se développer qui permettent de tracer les opérations par-delà le pseudonymat des transactions.

Les enjeux sont économiques et commerciaux

Extension à tous les secteurs d'activité. La *blockchain* ne doit pas être considérée comme cantonnée au monde de la finance qui l'a vue naître. Cette technologie qui fait l'impasse sur le tiers de confiance a vocation à se diffuser dans tous les secteurs économiques. Cette extension est déjà perceptible dans l'orientation des financements : alors que les ressources levées par ICO (*Initial*

Coin Offering) étaient majoritairement destinées à des projets concernant l'amélioration des infrastructures et la finance, on assiste depuis 2017 à une diversification de plus en plus grande, en direction notamment des secteurs des médias, des jeux et de l'internet des objets.

Une technologie disruptive ? Dans la banque, l'assurance, mais aussi la logistique ou la santé, la technologie de la *blockchain* pourrait provoquer une véritable mutation dans la chaîne de valeur. Les plateformes numériques, qui sont des systèmes centralisés, ne sont pas à l'abri : championne de la désintermédiation, la *blockchain* a pu être décrite comme un moyen d' « ubériser Uber ». Les acteurs historiques doivent se préparer, mais l'histoire du numérique nous a appris qu'ils sont rarement les acteurs de la disruption, même quand ils en sont les inventeurs (à l'instar de Kodak). De fait, il est difficile pour une entreprise de développer des services concurrents à son cœur de métier et qui mettent en péril ses profits immédiats.

La logistique, premier candidat ? En tant que registre mémorisant sans possibilité de falsification toutes les opérations effectuées, la *blockchain* pourrait se révéler un outil révolutionnaire en matière de logistique. C'est tout le cycle de vie d'un produit qui peut être ainsi certifié. L'objectif est double : il s'agit non seulement de permettre la transparence des filières vis-à-vis des consommateurs, mais aussi de sécuriser ces filières contre les dysfonctionnements opérationnels ou contre diverses formes de commerce illicite. Plusieurs pilotes sont en cours de déploiement. Cette traçabilité des chaînes d'approvisionnement, du fabricant au consommateur, intéresse en premier lieu l'industrie agro-alimentaire (origine contrôlée, respect de la chaîne du froid, etc.), mais aussi l'industrie du luxe ou du médicament (lutte contre la contrefaçon).

Transparence et confidentialité. Les *blockchains* publiques permettent la traçabilité de l'ensemble des opérations effectuées, de manière transparente. Cette caractéristique va à l'encontre du secret des affaires. Parce que le registre est distribué, les informations qu'il contient en clair sont accessibles aux parties prenantes. C'est un avantage pour assurer la traçabilité des transactions mais un défaut rédhibitoire si des informations relevant du secret des affaires sont ainsi livrées, par exemple en finance ou en matière de santé. La confidentialité de l'information doit pouvoir être préservée pour respecter le secret commercial.

Les enjeux sont juridiques

Le droit de la preuve. Les certifications diverses (transferts de fonds, transactions, livraison de marchandises, création d'une oeuvre originale, etc.) enregistrées sur la *blockchain* doivent avoir une portée probatoire avérée, sinon il faudra recourir aux tiers de confiance traditionnels. Aujourd'hui prédomine une insécurité juridique qui freine l'attrait de cette technologie auprès des opérateurs. Il faut donc conférer à la preuve de type « *blockchain* » une portée juridique reflétant la fiabilité revendiquée par la technologie. Après une phase où il était nécessaire de laisser se déployer les initiatives pour faciliter l'innovation, les inconvénients de l'insécurité juridique prennent le pas sur les avantages.

Fiscalité. L'imprécision qui pèse aujourd'hui sur le traitement fiscal des opérations apparaît également comme un frein au développement des *blockchains* en France. La nature juridique des actifs numériques reste imprécise, donc difficilement prise en compte par la réglementation. Une politique fiscale claire et adaptée aux crypto-monnaies (régime des opérations d'achat, de vente et d'échange) serait de nature à attirer des acteurs sérieux sur le territoire.

Droit au compte. Les émetteurs ou vendeurs professionnels de cyber-monnaies ont la plus grande difficulté à ouvrir et à maintenir ouvert un compte bancaire classique auprès d'un établissement de crédit en France dans le cadre de leur activité. Ces difficultés s'étendent à l'ensemble des entreprises gérant des cyber-monnaies dans le cadre de leur activité générale, soit parce qu'elles les acceptent comme moyen de paiement, soit parce que ces actifs numériques sont intégrés à leur offre de produit. La méconnaissance des cyber-monnaies et autres actifs numériques conduit les établissements bancaires – qui ont eux-mêmes des obligations en matière d'identification précise de l'origine des fonds – à refuser automatiquement de gérer les comptes des entreprises ayant des cyber-monnaies à leur patrimoine. Cela tient au caractère insuffisant des données que les plateformes d'échange exigent ou fournissent aujourd'hui à leurs clients. Un tel blocage est préjudiciable au développement du marché français et à l'attractivité de la place de Paris.

Un besoin de régulation

La plupart de ces nombreux enjeux fonctionnent comme des freins au développement de la nouvelle technologie. De fait, la révolution annoncée ne s'est pas encore produite, malgré les milliers de projets en cours. Il faut pourtant s'engager résolument, sans attendre l'arrivée à maturité de la *blockchain*. Certains des défis évoqués ci-dessus ne concernent pas les *blockchains* privées ; quant aux *blockchains* publiques, c'est en les testant qu'on en améliorera la performance. On le sait, dans l'économie numérique, les effets de réseaux sont tels que les entreprises arc-boutées sur la préservation de leurs situations acquises risquent de se trouver marginalisées.

Déjà, les pays développés se mobilisent. Ils expriment d'abord une volonté accrue de contrôler les pratiques frauduleuses liées à l'usage des *blockchains* – en témoigne la mise à l'ordre du jour du G20 du sujet, à la demande de la France. Ils affichent ensuite un intérêt marqué pour la technologie, et des stratégies nationales spécifiques se font jour ici et là. Du côté des industriels, quelques acteurs comme IBM cherchent à se positionner dans le développement de solutions. Pour l'instant les grands acteurs des plateformes numériques sont plutôt restés en retrait.

Après une période où la régulation semblait l'ennemi juré de l'innovation, l'heure semble venue de trouver un moyen de tenir la chaîne par les deux bouts : réglementer de façon coordonnée sur un certain nombre de sujets permettra à la fois de contrôler les usages délictueux et de favoriser les développements souhaités.

Les recommandations formulées par le groupe de travail doivent être considérées comme de premières orientations au niveau national. En réalité, en matière de *blockchains*, c'est une réponse à l'échelle européenne voire mondiale qu'il conviendrait de viser. Les « protocoles de registres distribués » ou protocoles *blockchain* revêtent des enjeux stratégiques sur lesquels la réflexion et l'action s'imposent. D'autant que nous sommes parvenus à un moment décisif pour cette nouvelle technologie. Après une période d'expérimentation sans contrainte, il est temps de « sortir du bac à sable », selon l'expression usuelle dans l'économie numérique. Par une sorte de convergence naturelle, la plupart des acteurs sont aujourd'hui disposés à entrer dans une nouvelle phase, celle d'une intervention des pouvoirs publics pour fixer un cadre juridique et réglementaire qui permette le plein essor de cette nouvelle technologie.

Tournez la page S.V.P.

Sept grandes orientations

Le rapport propose les grands axes d'une stratégie visant à réglementer de façon coordonnée sur un certain nombre de sujets critiques de façon à contrôler les usages délictueux et à favoriser l'innovation et les développements souhaités. À ce stade du développement des usages, l'insécurité juridique sur des sujets de base comme la comptabilité, la fiscalité, la relation avec les banques et le manque d'expertise des pouvoirs publics sur le sujet devient néfaste, tant du point de vue du contrôle des usages délictuels que de l'accompagnement du développement industriel d'un secteur prometteur.

1. Promouvoir des travaux de recherche et développement, en veillant à favoriser l'interdisciplinarité.

2. Inciter au développement de formations approfondies et aider à l'appropriation du sujet.

3. Établir les régulations de base permettant de contrôler les usages frauduleux des crypto-monnaies et développer les usages des *blockchains* en s'appuyant sur un groupe à compétences transversales, à l'intérieur de l'État. Sur un certain nombre de sujets, il y a urgence à ce que l'État apporte des réponses coordonnées et équilibrés au regard des objectifs concomitants de soutien à l'innovation et de préservation de l'ordre public. Il faut disposer de l'appui technique nécessaire à la définition de solutions efficaces et rapidement apporter des réponses aux différentes questions réglementaires soulevées en matière de fiscalité, de droit au compte, de lutte anti-blanchiment et de traitement comptable.

4. Contribuer au financement des projets « d'infrastructure logicielle ». il est nécessaire de construire les infrastructures *blockchains* publiques de demain. Deux scénarios sont envisageables : ou bien encadrer suffisamment les *blockchains* existantes ; ou bien favoriser le développement de nouvelles infrastructures plus sécurisées. À ce jour, il est difficile de trancher le dilemme : le rapport recommande donc de mener de front les deux stratégies de « maîtrise » des *blockchains* existantes et d'accompagnement de l'émergence de nouvelles solutions.

5. Soutenir des secteurs correspondant à des domaines d'excellence ou d'intérêt stratégique en France : logistique, lutte contre la contrefaçon, traçabilité, banque et assurance et santé, en rendant possible la sortie du bac à sable.

6. Tester, expertiser, former et s'équiper au sein des pouvoirs publics ; analyser l'évolution des *blockchains* publiques ; diffuser l'information, développer et utiliser des applications non critiques.

7. Répondre aux défis auxquels se heurte l'internet de la valeur, ce qui suppose une monnaie numérique suffisamment stable pour servir de contrepartie de transactions.

Blockchain : une technologie de stockage et de transmission d'informations à améliorer

Source : Site www.vie-publique.fr – 27 avril 2021

La stratégie nationale *blockchain* a été lancée le 15 avril 2019. Elle vise à faire de la France un pays à la pointe de cette technologie. De juin 2019 à janvier 2020, une mission a travaillé à identifier les verrous technologiques autour de la *blockchain*. De ces travaux sont issues des recommandations sur les évolutions à mettre en place.

Souveraineté, sécurité (cryptographie, protocoles...), interopérabilité et évolutivité, consommation d'énergie, modèles économiques : dans son rapport sur les *blockchains* présenté le 15 avril 2021, la Direction générale des entreprises (DGE) identifie les différents verrous liés à la technologie *blockchain*. Après avoir analysé ces multiples problématiques, la DGE présente ses recommandations afin de permettre à la France d'être une « *nation de la blockchain* » au bénéfice de la société et du monde économique.

Blockchain : de quoi s'agit-il ?

Les applications de ces chaînes de blocs sont multiples : transactions dans le domaine bancaire (les crypto-monnaies reposent sur cette technologie), allégement des formalités et automatisation des remboursements dans le secteur de l'assurance, traçabilité des produits et mémoire des interventions en logistique... Les enjeux, en termes tant économiques que technologiques, sont donc majeurs.

La technologie *blockchain* permet de stocker et de transmettre des informations de manière hautement sécurisée. Les vérifications sont effectuées non par un organe central de contrôle, mais par des « nœuds » d'utilisateurs connectés en réseau, qui possèdent chacun une copie des données. Les modifications sont effectuées par l'ajout de blocs de données transmis à chaque nœud. Chaque bloc est lié au précédent et intégré dans un historique. La falsification est donc impossible.

La sécurité de cette technologie repose sur le mécanisme de consensus des nœuds à chaque ajout d'informations et sur la décentralisation de la gestion. Le rapport appelle confiance décentralisée la possibilité de faire coopérer des acteurs qui ne se font pas confiance sans passer par une tierce partie.

Quelles pistes d'avenir ?

Le rapport identifie les verrous de la *blockchain*, en France, sous trois aspects distincts :

- maturité de la recherche sur ces sujets : le cadre théorique existe mais les solutions n'ont pas encore été mises en application ;
- innovation : seule une vraie rupture technologique permettra des avancées dans les domaines les plus pointus de la technologie *blockchain* (contrats intelligents avancés ou autonomes, protocoles inter-*blockchain*...) ;
- acteurs français : la France est en avance dans certains domaines (contrats intelligents, algorithmique distribuée) mais ne met pas suffisamment en avant son expertise dans d'autres (cryptographie). Pour le reste, aucun retard n'est à déplorer mais la concurrence internationale est active (modèles et mécanismes économiques, génie logiciel...). Cela implique une collaboration entre recherche et *start-up*.

Tournez la page S.V.P.

Face à ce constat, le rapport fait une série de recommandations réparties en six domaines :

- recherche : favoriser les actions interdisciplinaires et se concentrer sur la confidentialité et la gestion des données personnelles ou sensibles, le génie logiciel, les applications et les infrastructures *blockchain* ;
- innovation : créer les outils qui favoriseront l'adoption de la technologie *blockchain* via des projets qui réuniront laboratoires et start-up ;
- confiance numérique : l'identité numérique étant à la base de la confiance qui permet la technologie *blockchain*, le rapport préconise la création d'un véritable service public de l'identité numérique ;
- appui aux politiques publiques : mise en place d'un comité consultatif issu de la recherche publique afin d'appuyer les projets de l'État ;
- liens entre recherche publique et *start-up* : consolider et promouvoir la collaboration entre ces deux « mondes » ;
- enseignement : augmenter le nombre de formations spécialisées et favoriser la formation en alternance dans les laboratoires de recherche et développement du domaine *blockchain*.

La stratégie nationale *blockchain*

Source : Site www.entreprise.gouv.fr – 08 octobre 2020

Présentée le 15 avril 2019, à l'occasion de la Paris Blockchain Conference, la stratégie nationale *blockchain* est le fruit d'un travail intensif mené par la DGE (Direction générale des entreprises) avec l'ensemble de l'écosystème de la *blockchain*. Cette stratégie vise à faire de la France une nation de la *blockchain*.

La première étape de la stratégie nationale *blockchain* a consisté à établir un cadre juridique, comptable et fiscal clair, permettant l'utilisation de la *blockchain* pour le transfert d'instruments financiers et l'émission d'actifs numériques dans un cadre sécurisé. Ces travaux se sont concrétisés avec la loi de finance 2019 et le 11 avril 2019 avec l'adoption définitive par l'Assemblée du projet de loi PACTE (Plan d'action pour la croissance et la compétitivité des entreprises).

Afin de définir les nouveaux enjeux du développement de la *blockchain* en France sur les usages non financiers, une concertation a été conduite auprès des acteurs de l'écosystème afin de leur permettre de communiquer sur leurs difficultés et leurs attentes pour l'État. À l'issue de ces travaux, le Gouvernement a lancé **4 axes de travail principaux** pour faire de la France une nation de la *blockchain*.

Axe 1 : Renforcer l'excellence et la structuration des filières industrielles françaises pour déployer des projets basés sur les technologies de registres distribués

Conscients du potentiel que représente pour eux la technologie de chaîne de blocs, les grands groupes sont actifs dans la mise en œuvre d'expérimentations au sein de leur entreprise, en France ou à l'international. Le Conseil National de l'Industrie (CNI) permet depuis 2013 une structuration forte de l'écosystème industriel. Les Comités Stratégiques de Filière (CSF), qui réunissent les industriels français autour de projets de filière ambitieux, sont un levier particulièrement puissant pour que l'industrie française accélère le passage à l'échelle des projets *blockchain*.

Axe 2 : Être à la pointe des enjeux technologiques

Pour être leader dans la résolution des défis techniques et technologiques posés par la *blockchain*, il est primordial d'identifier les verrous scientifiques et techniques actuels de la technologie.

Une mission prospective a ainsi été confiée au CEA-LIST, à l'IMT et à l'INRIA en mai 2019 en vue d'identifier ces verrous, et de proposer de **véritables effets de levier** permettant à la France de devenir leader dans la résolution de ces défis technologiques. Les chercheurs missionnés ont également dressé un panorama des formations initiales et continues existant en France, ainsi qu'une cartographie des forces de recherche françaises dans le domaine et une autre de l'écosystème startup *blockchain* national, selon le degré de complexité de la technologie utilisée.

Les conclusions de cette mission ont été présentées en avant-première le 10 février 2020 à l'occasion de la seconde réunion de la task force *blockchain*. Parmi les différents éléments clés, citons tout d'abord les forces de la France en la matière, que sont l'**excellence de sa recherche dans les domaines de la cryptographie et des langages** ainsi que le **dynamisme et la structuration de son écosystème de *startups***. Ces atouts pourraient permettre à la France de faire

Tournez la page S.V.P.

émerger de futurs champions de la *blockchain*. Pour se faire, il est nécessaire de mettre en place des environnements de développement professionnels facilitant le développement d'applications de qualité. Il s'agira de concilier les caractéristiques de performance, de sécurité et de consommation énergétique des réseaux *blockchain*. La conformité au RGPD et aux règles de protection des données commerciales sensibles représente également un défi clé. Les enjeux associés à la gouvernance, la souveraineté, l'interopérabilité, les modèles économiques et l'accessibilité pour le grand public sont également étudiés dans le rapport de la mission.

Les travaux de la Direction générale des entreprises (DGE) se concentrent désormais sur le **renforcement des collaborations interdisciplinaires entre équipes de chercheurs** et sur le **développement de partenariats entre recherche et startups.**

Axe 3 : Encourager les projets innovants s'appuyant sur les technologies de registres distribués

Tous dispositifs confondus, l'État va investir 4,5 milliards d'euros dans le financement de l'innovation de rupture sur les cinq prochaines années, notamment via le plan *Deep Tech*. La technologie *blockchain* est éligible à ces financements.

L'appel à projets Concours d'Innovation i-Nov financé par le Programme d'Investissements d'Avenir (PIA), permet de financer des projets innovants, proches du marché et à fort potentiel pour l'économie française. La *blockchain* a été identifiée comme l'une des technologies de rupture clés pour le concours, en particulier dans sa thématique Numérique *Deep Tech*. Le but de cet appel à projet est de financer des projets proches du marché présentant une innovation de rupture, pour une assiette comprise entre 600 000 et 5 millions d'euros.

Depuis le lancement de la stratégie en avril 2019, le concours *i-Nov* a permis de financer 7 *startups blockchain* lauréates (Ownest, iExec, Infolegale, Libriciel Scop, Neurochain, Pikcio et Kleros) pour un montant total de plus de 4,5 millions d'euros. En parallèle, la *startup* Massa Lab s'est vue attribuée une bourse *French Tech Emergence* de 90 000 €. La *French Tech* a mis à l'honneur LGO dans sa sélection 2020 de 120 *startups* en phase d'hypercroissance : le *French Tech 120*. Ledger a été sélectionné pour rejoindre le *Next40* qui rassemble les 40 *startups* françaises les plus prometteuses et a obtenu le soutien de Bpifrance pour 2.5 millions d'euros en 2020.

Au total, les financements publics visant à soutenir les projets *blockchain* français s'élèvent à 5,5 millions d'euros distribués en 2019 et 5 millions d'euros de prêts pour faire face à la crise en 2020. Bpifrance a participé en outre, via ses fonds partenaires, à l'investissement de plus de 50 millions d'euros dans des *startups blockchain* telles que Stratumn, Ledger, Utocat, Tilkal ou encore Cosmian.

Axe 4 : Accompagner et sécuriser les porteurs de projets *blockchain* dans leurs questionnements, notamment juridiques et réglementaires

Avec le projet de loi PACTE et la loi de finances 2019, la France s'est dotée d'un cadre sécurisant pour les acteurs de l'écosystème. Pour permettre aux acteurs de sécuriser juridiquement leurs projets innovants quel que soit le domaine d'application, le guichet France Expérimentation assure un accompagnement renforcé des porteurs de projets *blockchain* dans les défis juridiques qu'ils rencontrent.

De plus, des ateliers gratuits sont organisés au sein de French Tech Central à Station F pour faciliter les échanges entre les administrations compétentes et les startups et entreprises de l'écosystème. La prochaine session d'ateliers est prévue sous format virtuel lors de l'édition 2020 de la Paris Blockchain Conference.

Une *task force* d'experts animée par la DGE

Afin de poursuivre le dialogue avec l'écosystème et mettre en œuvre cette stratégie d'ambition pour la France, une *task force* composée d'experts nationaux de tous horizons (entrepreneurs, régulateurs, industriels, associations et acteurs publics), coordonnée par la DGE, a été mise en place de manière pérenne.

Dans ce cadre, l'écosystème *blockchain* tout entier a été appelé à participer aux groupes de travail « Sensibilisation des acteurs privés à la *blockchain* » et « Attractivité de la France pour les entrepreneurs et investisseurs en *blockchain* ». La première consultation a permis de collecter les besoins de l'écosystème sur ces deux sujets. La seconde consultation permet de construire des guides sur-mesure d'information et d'orientation des acteurs privés, des entrepreneurs et des investisseurs.

Tournez la page S.V.P.

France : un des premiers pays européens à se doter d'un cadre réglementaire pour la *blockchain* – Communiqué de presse, Ministère de l'Économie et des Finances, Cabinet de Bruno LE MAIRE

Source : Site www.finyear.com – 22 novembre 2019

La France est l'un des premiers pays européens à se doter d'un cadre réglementaire pour la *blockchain*

La France a complété le cadre réglementaire régissant les applications de la *blockchain* aux services financiers en l'étendant aux prestataires de services sur actifs numériques (PSAN) et conforte ainsi sa position de pionnier européen en la matière.

Après avoir été l'un des premiers pays au monde à donner force de loi à l'utilisation de la technologie *blockchain* en matière d'inscription et de transfert de titres financiers, la France conforte sa position pionnière en complétant l'un des cadres les plus exhaustifs au monde en matière d'actifs numériques, qui couvre aussi bien les aspects réglementaires que fiscaux ou encore comptables.

Le décret n° 2019-1213 publié ce jour vient parachever le cadre juridique spécifique à ces actifs numériques créé par la loi Pacte. Sur le marché primaire, il était déjà possible pour les émetteurs de solliciter auprès de l'Autorité des marchés financiers un visa préalablement à leur émission d'actifs numériques (*Initial Coin Offering* - ICO), en application directe de la loi Pacte. En ce qui concerne le marché secondaire, le présent décret vient préciser les contours des statuts applicables aux prestataires sur actifs numériques, et leur ouvre désormais la possibilité de s'enregistrer et de solliciter un agrément auprès de l'Autorité des marchés financiers.

L'obtention de cet agrément est conditionnée au respect de dispositions prévues par la loi et précisées par le présent décret. Il s'agit par exemple d'obligations sur la sécurité des systèmes informatiques, en termes de fonds propres ou d'assurance, et d'obligations spécifiques à chaque service (par exemple pour un service de conservation, obligation de restitution de la maîtrise des actifs numériques conservés). Cet agrément optionnel est complété pour certains types de prestataires par un enregistrement au titre des exigences de lutte contre le blanchiment et le financement du terrorisme.

Le décret renforce par ailleurs l'accès aux services bancaires pour les émetteurs ayant reçu un visa de l'Autorité des marchés financiers sur leur émission ainsi que pour les prestataires de services sur actifs numériques enregistrés ou agréés. En cas de refus injustifié, même implicite, d'accès aux services de comptes et de dépôts, les émetteurs ou prestataires pourront exercer un recours auprès de l'Autorité de contrôle prudentiel et de résolution en vue de déclencher une procédure de droit au compte.

Bruno Le Maire a déclaré : « Le cadre issu de la loi PACTE va favoriser le développement d'un écosystème *blockchain* en France dynamique et robuste, qui allie capacité d'innovation, transparence et haut niveau de sécurité pour les épargnants et investisseurs. En étant l'un des premiers pays à se doter d'un tel cadre, Paris se donne les moyens de devenir la première place européenne de la *blockchain* et conforte son engagement en faveur de l'innovation financière ».

Actifs numériques : renforcement par ordonnance du cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) appliqué aux prestataires de services sur actifs numériques (PSAN)

Source : Site www.amf-france.org, Autorité des marchés financiers (AMF) – 12 février 2021

Une ordonnance publiée en décembre dernier modifie le régime des prestataires de services sur actifs numériques (PSAN) établi par la loi PACTE. Elle soumet à enregistrement obligatoire auprès de l'Autorité des marchés financiers (AMF) les PSAN fournissant les services d'échange d'actifs numériques contre d'autres actifs numériques et d'exploitation d'une plateforme de négociation d'actifs numériques. Elle recentre également sur les obligations clés en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) le contrôle préalable effectué par les autorités lors de l'enregistrement des PSAN fournissant les services de conservation et d'achat ou de vente d'actifs numériques en monnaie ayant cours légal.

Deux nouveaux services soumis à enregistrement obligatoire

L'ordonnance n° 2020-1544 du 9 décembre 2020 renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques a modifié le régime des PSAN en ajoutant deux nouveaux services sur actifs numériques soumis à l'enregistrement obligatoire :

- l'échange d'actifs numériques contre d'autres actifs numériques (dits « crypto contre crypto ») ;
- et l'exploitation d'une plateforme de négociation d'actifs numériques.

La fourniture en France de ces services définis aux 3° et 4° de l'article L. 54-10-2 du code monétaire et financier est désormais soumise à enregistrement obligatoire auprès de l'AMF, après avis conforme de l'Autorité de contrôle prudentiel et de résolution (ACPR). Les PSAN exerçant déjà ces activités avant l'entrée en vigueur de l'ordonnance bénéficient d'un délai de 6 mois à compter de sa publication pour être enregistrés auprès de l'AMF (soit avant le 11 juin 2021). Les acteurs concernés sont invités à se rapprocher rapidement de l'AMF pour entamer leur procédure d'enregistrement.

Recentrage du contrôle LCB-FT (lutte contre le blanchiment de capitaux et le financement du terrorisme)

Concernant les services sur actifs numériques déjà soumis à l'enregistrement obligatoire, à savoir la conservation d'actifs numériques pour compte de tiers et l'achat-vente d'actifs numériques en monnaie ayant cours légal (définis aux 1° et 2° de l'article L. 54-10-2 du code monétaire et financier), le contrôle du dispositif LCB-FT et de gel des avoirs dans le cadre de la procédure d'enregistrement est désormais recentré sur les points clés (classification des risques, identification et vérification d'identité, connaissance de la clientèle, examen renforcé, déclaration de soupçon, gel des avoirs).

Une fois enregistrés, ces PSAN doivent mettre en œuvre l'intégralité des obligations relatives à la LCB-FT et au gel des avoirs. Par ailleurs, pour les PSAN fournissant ces services 1° et 2° qui sont déjà enregistrés ou immatriculés dans l'Union européenne ou dans l'Espace économique européen, les autorités ne vérifieront pas l'honorabilité et la compétence des dirigeants et bénéficiaires effectifs, vérifications réputées avoir déjà été réalisées par l'autorité d'origine. L'ensemble de ces dispositions s'applique non seulement aux nouvelles demandes d'enregistrement mais également aux demandes déjà déposées ou en cours d'examen.

Conditions d'enregistrement des PSAN étrangers

L'ordonnance confirme que les PSAN établis en France doivent s'enregistrer auprès de l'AMF mais également les PSAN établis à l'étranger fournissant des services sur actifs numériques en France. Elle rappelle qu'il est nécessaire d'être établi en France, dans l'UE ou dans l'EEE pour être enregistré. Le règlement général de l'AMF précisera les conditions dans lesquelles un service sur actifs numériques est considéré comme fourni en France. Les PSAN établis dans des pays tiers devront donc justifier d'un enregistrement ou d'une immatriculation dans l'UE ou l'EEE pour pouvoir fournir des services sur actifs numériques en France et être enregistrés.

Renforcement des obligations LCB-FT des PSAN

L'ordonnance ouvre aux PSAN la possibilité de recourir à des tiers pour la mise en œuvre de leurs obligations de vigilance à l'entrée en relation d'affaires et de procéder eux-mêmes, pour des tiers, à ces mêmes obligations. Elle pose l'interdiction pour les PSAN de tenir des comptes anonymes. Elle impose enfin, sauf dans certains cas limités et sous certaines conditions, aux PSAN appartenant à des groupes d'informer les entités de ce groupe des déclarations de soupçon qu'ils ont réalisées et confirme la possibilité, sous certaines conditions, pour les entreprises-mères de bénéficier des échanges d'informations intragroupes relatifs aux déclarations de soupçon.