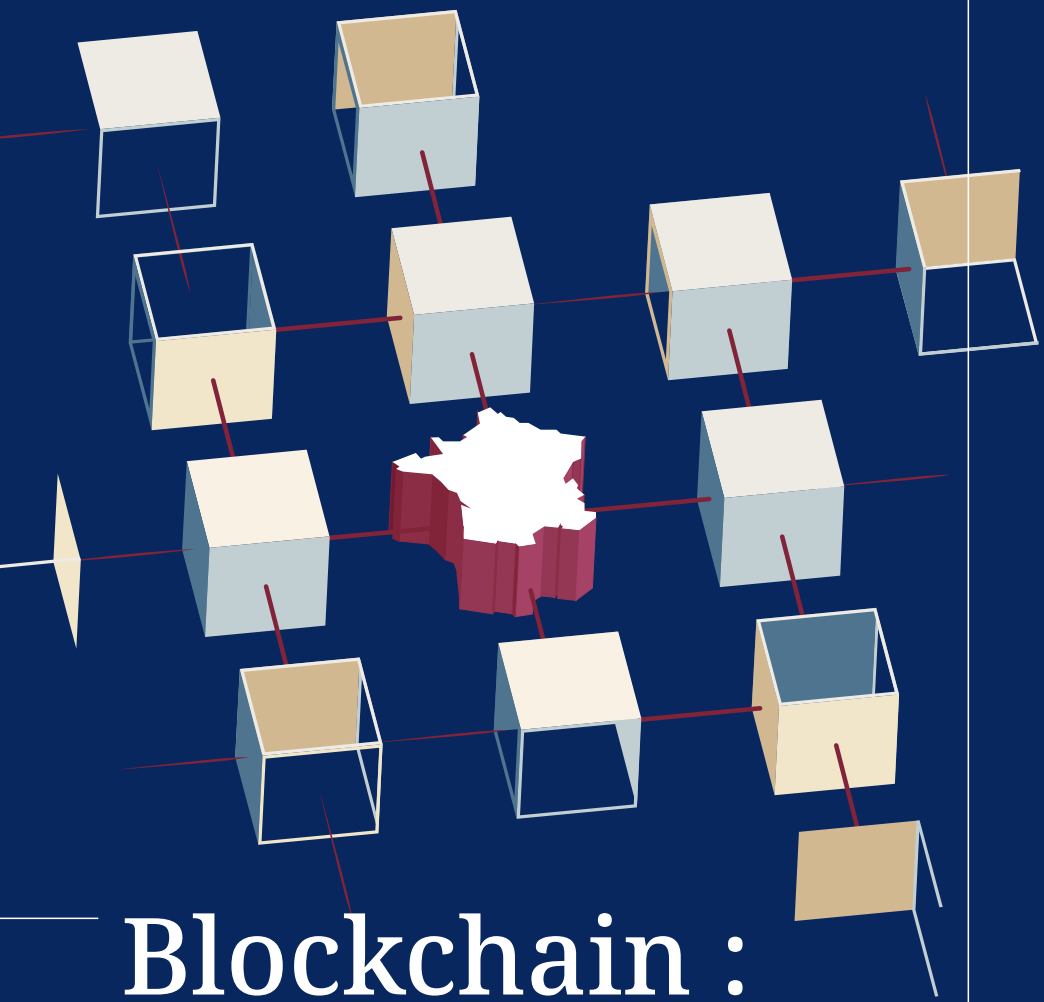
INSTITUT Montaigne



Blockchain :

Consolider nos atouts

JUIN 2023

Think tank de référence en France et en Europe, l'Institut Montaigne est un espace de réflexion indépendant au service de l'intérêt général. Ses travaux prennent en compte les grands déterminants économiques, sociétaux, technologiques, environnementaux et géopolitiques afin de proposer des études et des débats sur les politiques publiques françaises et européennes. Il se situe à la confluence de la réflexion et de l'action, des idées et de la décision.

RAPPORT - Juin 2023

Blockchain :

Consolider nos atouts

Les rapports de l'Institut Montaigne proposent des analyses exhaustives, issues d'une réflexion collégiale et ont vocation à identifier des solutions de long terme.

Table des matières

Synthèse

Les *blockchains* (chaîne de blocs) sont des infrastructures informatiques qui permettent d'**échanger librement et de manière sécurisée des actifs numériques** tels que des monnaies, des actes de propriété, des certificats ou des œuvres d'art, sans passer par les tiers de confiance usuels que peuvent être les banques ou les notaires. Le principe est simple : un utilisateur inscrit une donnée sur la base commune de données qu'est la *blockchain*, avec l'accord d'un réseau de validateurs internes propres à chaque chaîne. Une fois la donnée inscrite, elle est immuable car chaque membre de la *blockchain* détient une copie de la base de données partagée comprenant l'historique de chaque transaction - il est ainsi impossible de la modifier unilatéralement. Le support garantit l'origine et la nature de la donnée ; le contenant garantit le contenu.

Utilisées initialement pour **échanger des données en protégeant la confidentialité des opérateurs** ou échapper à des contrôles étatiques ou commerciaux jugés trop contraignants ou politiquement inacceptables, les *blockchains* se sont développées à grande échelle à partir de 2008 avec Bitcoin puis Ethereum et **représentent aujourd'hui, pour certains usages, des infrastructures alternatives aux grandes plateformes commerciales** car elles ont su incarner la confiance sans dépendance à des acteurs conventionnels spécifiques.

Ainsi, aujourd'hui, les *blockchains* servent quatre cas d'usage majeurs. Tout d'abord, le cas d'usage **des paiements** afin de renforcer l'accessibilité du système de paiement quels que soient le moment, le lieu et la personne et de réduire les coûts de transaction ; également le cas d'usage de la **programmabilité d'échanges financiers** (prêts, produits dérivés ou d'assurance) dans le cadre d'une finance décentralisée et désintermédiée ; ensuite, le cas d'usage de **l'identité numérique** afin de garantir l'identité et les références d'une personne inscrite sur une *blockchain* ; enfin, le cas d'usage de **la traçabilité** pour suivre et rendre transparents des processus faisant intervenir de nombreux acteurs et garantir ainsi l'origine, la composition d'un produit ou sa transformation tout au long de son cycle de vie.

Parmi ces cas d'usage, celui des **paiements constitue indéniablement un enjeu de souveraineté**. Sur ce secteur, l'Europe dépend d'acteurs privés non européens, que ce soient les acteurs historiques du paiement (duopole Visa-Mastercard) ou les géants mondiaux de la Tech qui investissent la finance et la banque. Cette situation de dépendance tend à se propager au secteur des actifs numériques dont certains (notamment les *stablecoins*) s'arriment à des monnaies fiduciaires au premier rang desquelles le dollar américain. La question des acteurs de ces infrastructures de confiance est donc stratégique et appelle une coopération étroite avec les banques et les acteurs publics afin de maîtriser nos dépendances. Or, **le développement de solutions opérationnelles est aujourd'hui freiné par un manque de coordination au niveau européen** et requiert une meilleure coopération entre les acteurs de la *blockchain*, les banques et les autorités publiques.

La France a été pionnière sur la technologie *blockchain* grâce à ses chercheurs et ses entrepreneurs et dispose aujourd'hui d'atouts techniques et réglementaires incontestables.

En effet, la recherche française bénéficie d'une **avance certaine en matière de briques technologiques fondamentales, de langages formels et de contrats autonomes** *(smart contracts)* qui permettent de construire et d'effectuer des opérations *blockchain*. L'enjeu est désormais de **multiplier notre expertise sur un spectre plus large de protocoles et de les rendre interopérables** entre eux pour **faire émerger de nouveaux produits et services**.

Plusieurs acteurs importants de l'écosystème international *blockchain*, tels que Ledger ou Sorare, sont nés en France, s'y sont développés et se démarquent de leurs pairs internationaux par une offre singulière et une croissance plus élevée que la moyenne. Riche d'acteurs comme Arianee, Morpho, Kiln ou encore Mangrove, **l'écosystème français possède tous les atouts techniques pour se hisser au niveau de pays *leaders* de la blockchain comme par exemple les États-Unis ou la Suisse**.

Cette avance doit être cultivée pour elle-même mais également dans le contexte du développement de technologies et d'usages tiers, en particulier les univers virtuels ou « métavers », dans lesquels la *blockchain* apporte de la valeur sur les plans de l'identification et du transactionnel.

La loi PACTE de 2019 a défini un cadre juridique précurseur : pour les consommateurs de services *blockchain*, elle offre de la protection ; pour les entreprises du secteur, elle sécurise et légitimise les usages auprès de tiers conventionnels tout en permettant la flexibilité nécessaire à l'innovation. L'adoption récente du règlement MiCA (Markets in Crypto-Assets) qui permet de généraliser et de compléter ce cadre à l'échelle européenne, rend d'autant plus attractif l'écosystème français qu'il confirme sa pertinence réglementaire à l'échelle mondiale.

La France doit désormais affirmer son leadership européen en capitalisant sur ses atouts et en continuant à professionnaliser le secteur.

Objectif 1

Capitaliser sur le cadre juridique français pour soutenir les acteurs nationaux et attirer des acteurs étrangers de la *blockchain*

Recommandation 1 : organiser une communication internationale portée par les autorités publiques afin de faire valoir l'intérêt du cadre juridique et fiscal français auprès des acteurs étrangers qui souhaitent opérer en Europe.

Recommandation 2 : assurer la mise en œuvre effective de la loi PACTE en matière d'accès des prestataires d'actifs numériques aux services

classiques de la banque et de l'assurance, en associant tous ces acteurs aux processus opérationnels et en encourageant l'ACPR, le régulateur du secteur financier, à formuler les lignes directrices appropriées.

Recommandation 3 : mettre en place un coordinateur national *blockchain* afin de définir une approche commune des autorités françaises et piloter les chantiers prioritaires qui auront été identifiés dans ce domaine.

Recommandation 4 : préparer les autorités publiques et les acteurs de l'écosystème à l'entrée en vigueur du cadre réglementaire européen MiCA.

Objectif 2

Consolider le cadre juridique dédié à la *blockchain* de manière à assurer un développement du secteur innovant et protecteur des utilisateurs

Recommandation 5 : clarifier les modalités de traitement des données personnelles des utilisateurs sur la *blockchain*. À cette fin, valider la conformité de la technique cryptographique du *Zero Knowledge Proof* (preuve à divulgation nulle de connaissance) comme moyen d'apporter des garanties de contenu tout en maintenant la confidentialité des émetteurs de ces contenus.

Recommandation 6 : clarifier le cadre fiscal applicable aux prises de participation en *tokens* (équivalents dématérialisés d'une action d'entreprise) dans des projets de *blockchain* pour les fonds d'investissement afin de leur permettre d'investir pour leurs clients et utilisateurs en toute conformité fiscale.

Recommandation 7 : engager les chantiers de suivi puis de réglementation des nouveaux usages et des nouvelles modalités de traitement, en particulier :

- traiter les *tokens* non fongibles (NFT - *Non-Fungible Tokens*), qui représentent des actifs dématérialisés, comme des véhicules juridiquement transparents permettant de traiter leurs sous-jacents matériels selon les réglementations existantes en vigueur ;
- étudier l'opportunité de reconnaître juridiquement les communautés et processus de collaboration au sein d'une *blockchain*, dits organisations autonomes décentralisées (DAO – *Decentralized Autonomous Organizations*), en s'appuyant sur l'exemple du DAO Model Law qui prône une harmonisation internationale pour une meilleure sécurité juridique ;
- mettre en place un observatoire dédié à la finance décentralisée (*DeFi – Decentralized Finance*) pour pouvoir réguler à terme ces activités aujourd'hui non suivies.

Recommandation 8 : investir dans des travaux sur la reconnaissance de la *blockchain* comme moyen de preuve et de support pour une identité numérique, la France étant absente des discussions européennes sur ce thème. Pour cela :

- mobiliser la France pour qu'elle participe à l'adaptation du régime applicable en matière de preuve électronique (règlement européen eIDAS) afin de le rendre compatible avec l'utilisation de la *blockchain* ;
- impliquer l'ANSSI dans les travaux en cours autour d'une identité numérique européenne.

1 La *blockchain*, pourquoi ?

L'intérêt croissant suscité par la technologie *blockchain*, que ce soit pour les particuliers, les entreprises ou les pouvoirs publics, s'accompagne de plusieurs interrogations et incompréhensions sur sa nature technologique, ses usages et ses apports concrets pour la société.

La technologie *blockchain* est apparue dans les années 1990 sous la forme de registres partagés par une communauté d'utilisateurs dans lesquels il était possible d'échanger et de stocker de manière anonyme une information, sans qu'un utilisateur ne puisse avoir une influence prépondérante sur les autres.

Imprégnée d'un idéal de partage et de collaboration de manière anonyme, cette technologie a d'abord été développée pour protéger la vie privée des individus dans des environnements digitaux où les problèmes de la confidentialité des données personnelles devenaient un véritable enjeu.

Avec l'apparition de Bitcoin en 2008, la *blockchain* prend une ampleur nouvelle, en se présentant comme une solution d'échange de monnaie électronique à grande échelle sans intermédiaire centralisé, tel qu'un gouvernement ou une banque centrale. En résolvant le problème informatique de la double dépense dans un environnement pleinement décentralisé, c'est-à-dire éviter qu'un même actif numérique soit dépensé plusieurs fois sans s'appuyer sur un superviseur unique, elle permet à tous les acteurs de participer à ces échanges sans risquer d'altérer le système.

C'est ensuite avec la mise en place d'Ethereum en 2013 et des contrats autonomes *(smart contacts)* que les usages de la *blockchain* se sont diversifiés et propagés dans de nombreux secteurs (bancaire, artistique, légal, etc.).

Différents usages pour les entreprises et les pouvoirs publics peuvent être cités. Certains sont désormais établis, d'autres sont émergents et doivent encore faire leurs preuves.

1. Sécuriser l'enregistrement des données ou la preuve de leur existence :
- en produisant des documents certifiés et infalsifiables ;
- en contribuant à la transparence et la traçabilité des informations et activités ;
- en conciliant la protection des données sensibles et leur partage à grande échelle pour faire progresser la science et l'innovation.

2. Exécuter des logiciels ou des applications décentralisées :
- en faisant interagir des dispositifs entre eux sans tiers de confiance ;
- en automatisant des conditions de déclenchement d'un contrat (réduction du risque d'erreur, de collusion, etc.).

3. Produire des ressources numériques dans des environnements virtuels :
- en décentralisant les applications du Web pour permettre à chacun d'en posséder une partie des ressources ;
- en permettant d'échanger des actifs numériques dans des environnements virtuels ;
- en créant de nouvelles formes de rémunérations pour la création de contenu.

4. Apporter plus de transparence et d'inclusivité au système financier :
- en facilitant les échanges de valeur transfrontaliers, en renforçant l'accessibilité du système bancaire et en réduisant les coûts d'accès à certains produits financiers ;
- en optimisant et en automatisant le fonctionnement du système financier ;
- en le rendant plus ouvert ;
- en se prémunissant contre la dévaluation de certaines monnaies nationales.

5. Simplifier et automatiser des processus existants ;
- en standardisant les méthodologies et les produits ;
- en participant à la digitalisation des processus ;
- en améliorant la relation client, en particulier pour les acteurs en B2B2C[1].

6. Faire émerger de nouvelles formes d'organisations plus participatives :
- en créant de nouvelles méthodes de gouvernance plus efficaces ;
- en faisant émerger des modèles décisionnels *« bottom up »* plus inclusifs ;
- en ouvrant d'autres possibilités de financement des entreprises (*Initial Coin Offering* ou ICO).

7. Transformer les business models, au-delà des aspects technologiques :
- en incitant des acteurs avec des intérêts différents évoluant dans un univers concurrentiel à coopérer et partager leurs données entre eux, malgré le risque de concentration posé par les plateformes numériques, ce qui pourrait donner lieu à des avancées majeurs dans le secteur de la *supply chain*, de la santé ou de l'assurance ;
- en redonnant le pouvoir aux utilisateurs de se réapproprier leur propre patrimoine numérique ;
- en repensant la notion de création et de partage de la valeur avec le Web3.

8. Proposer de nouveaux modes d'usages et de gouvernance pour les citoyens dans une société plus numérique et connectée :
- en permettant à chacun de contrôler et de posséder ses données d'identité en ligne *via* l'identité numérique et de bénéficier de nouveaux usages et services en toute sécurité ;
- en permettant à chacun d'effectuer des paiements sur internet de manière sécurisée, plus rapide, et sans forcément posséder un compte bancaire ;

[1] Le B2B2C est un terme utilisé pour désigner une approche marketing qui consiste à devoir s'adresser aussi bien à une cible de professionnels (distributeurs ou prescripteurs) qu'au client final consommateur.

- en permettant d'expérimenter des formes de gouvernance alternatives plus horizontales et polycentriques, utiles notamment dans des pays avec des institutions défaillantes.

Ces cas d'usages font l'objet de développements approfondis tout au long du rapport, ainsi qu'en Annexe 1.

La capitalisation boursière des crypto-actifs témoigne de l'intérêt croissant qu'y portent de nombreux acteurs de l'économie : environ 1 trillion d'euros fin mars 2023 pour plus de 23 000 crypto-monnaies et plus de 570 plateformes d'échange, soit l'équivalent du PIB de pays comme l'Arabie Saoudite ou les Pays Bas ou de la capitalisation boursière d'Amazon. Les investissements dans les NFT, avec l'emblématique vente de l'œuvre de l'artiste Beeple pour un montant de plus de 69 millions de dollars, confirment l'intérêt de la *blockchain* et de ses évolutions sur le plan financier.

Malgré cet engouement, et bien que l'évolution de la *blockchain* et de ses cas d'usages s'inscrivent dans une volonté de liberté et d'émancipation, sa rigidité peut néanmoins poser de réels défis.

Que ce soit dans notre système financier, économique, juridique ou social, l'ambiguïté est à la fois une faiblesse et une force. Si elle peut parfois nuire à l'efficacité de procédures ou de services rendus, elle permet souvent une approche au cas par cas mieux adaptée aux situations individuelles de chacun et conforme à nos valeurs démocratiques. Or, les applications les plus abouties de la *blockchain* s'opposent structurellement à ce type d'approche puisqu'elles vont jusqu'à automatiser des processus de gouvernance dans un code informatique.

Par ailleurs, dans un environnement structurellement concurrentiel où la transparence n'est pas dans l'intérêt de tous, il semble difficile de tenir la promesse initiale de la *blockchain*. Cette promesse était d'offrir un environnement à grande échelle dans lequel il est structurellement plus avantageux de coopérer et de partager des données que de cloisonner

l'information, pour faire émerger des projets que des acteurs isolés ou en silo ne pourraient jamais construire. Si l'apport est déterminant sur le plan théorique, et notamment pour la théorie des incitations économiques, sa concrétisation n'est pas réaliste dans un univers concurrentiel où le cloisonnement de l'information permet de faire valoir son intérêt.

Pourtant, à l'ère du Big Data, de l'intelligence artificielle et des écosystèmes connectés, le partage d'information entre différents acteurs est devenu une réalité. C'est le premier facteur de succès du développement d'un algorithme de *machine learning* performant. Aujourd'hui, ce partage est l'apanage de quelques plateformes très performantes, qui construisent des algorithmes qui régissent nos comportements sur internet avec leurs propres méthodes.

Avec la *blockchain*, ce partage pourrait être étendu à d'autres acteurs, potentiellement plus représentatifs de la société, mais dont la compétence et la légitimité restent à démontrer. Or c'est ici que la *blockchain* est confrontée à un défi d'ampleur : pour faire ses preuves, la technologie doit se diffuser car sa valeur et sa sécurisation repose sur l'ampleur de sa communauté d'utilisateurs[2], mais pour se diffuser la technologie doit convaincre les utilisateurs et faire ses preuves.

Cela pose des questions complexes : qui est compétent aujourd'hui pour construire les algorithmes *blockchain*, les faire évoluer et sanctionner leurs éventuelles défaillances ? Quels pans de notre économie et de notre société gagneraient à automatiser la confiance ? Est-ce techniquement faisable et philosophiquement souhaitable ?

Face à ces questions, l'objectif de ce rapport est de poser une explication claire des mécanismes et des limites de la *blockchain*, de présenter le positionnement de la France en matière de réalisations économiques et de réglementation, et de formuler des recommandations aux pouvoirs

[2] Spécifiquement, ce sont les nœuds validateurs qui assurent sa sécurisation.

publics pour permettre à l'écosystème *blockchain* français de se déployer dans des conditions équilibrées et respectueuses de nos valeurs démocratiques.

2 La *blockchain*, c'est quoi ?

Les *blockchains* permettent d'échanger librement et de manière sécurisée des actifs numériques, sans passer par un tiers de confiance. Ces actifs numériques peuvent être fongibles (monnaie, titres, lesquels sont interchangeables) ou non fongibles (actes de propriété, certificats, œuvres d'art).

Concrètement, les *blockchains* sont des bases de données électroniques uniques faisant office de référence commune aux détenteurs d'actifs numériques, tel un livre de compte partagé. En retraçant l'intégralité des transactions ayant été effectuées, tout en s'assurant de leur provenance et de leur faisabilité (par exemple que l'actif numérique n'a pas déjà été dépensé, aussi nommé « double-dépense »), elles permettent à ses utilisateurs d'interagir en toute confiance directement entre eux en réseau, sans passer par un tiers.

Si les données retracées dans les *blockchains* sont souvent qualifiées d'actifs, c'est en raison de la notion d'unicité d'une donnée numérique[3] permise par la technologie *blockchain* : pour dupliquer, modifier, supprimer une donnée sur une *blockchain*, il faudrait qu'une majorité des validateurs adaptent leur copie de *blockchain* en conséquence, de manière indépendante et parallèle. Cette notion d'unicité empêche aussi bien la double dépense que les actes malveillants.

[3] Chohan, Usman W., The Double Spending Problem and Cryptocurrencies (January 6, 2021). Available at SSRN: https://ssrn.com/abstract=3090174

À l'image d'internet, la technologie *blockchain* constitue une infrastructure numérique régie par un ensemble de règles appelées « protocoles ». Ces protocoles s'organisent selon un système en couches. Chaque couche utilise les services des couches inférieures et fournit des services aux couches supérieures. En particulier, la couche infrastructure assure les services sous-jacents, à l'image du TCP/IP pour internet, et la couche applicative comprend les services plus spécifiques qui s'y adossent, à l'image de services internet comme les réseaux sociaux.

2.1. LA COUCHE INFRASTRUCTURE : LES SIX PRINCIPES DE LA *BLOCKCHAIN*

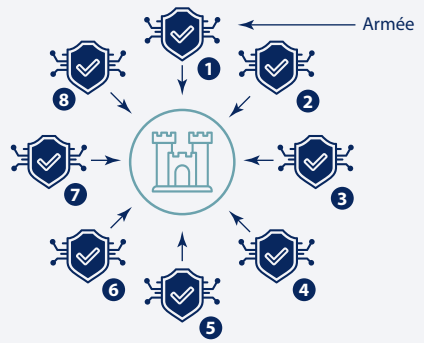
La couche infrastructure propose une base pour le développement de solutions diverses. Il existe différentes infrastructures *blockchains*, et chacune compose son propre réseau. Il existe aussi des infrastructures *blockchain* privées, c'est-à-dire non ouvertes à tout public. C'est ce que peut développer par exemple une entreprise voulant restreindre le réseau d'utilisateurs à ses collaborateurs. Dans cette couche, des ressources numériques dénommées « coin » sont présentes (Bitcoin, Ether, Tez) pour récompenser les validateurs. En tant qu'unités de compte natives du réseau, elles constituent la seule ressource numérique d'une *blockchain* présente dans sa couche infrastructure.

Encadré : comprendre les 6 principes qui sous-tendent le fonctionnement de la *blockchain*

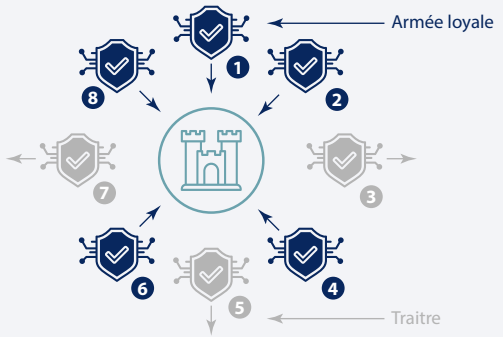
D'un point de vue scientifique, la technologie *blockchain* propose une alternative au problème dit des « généraux byzantins », mis en lumière par Leslie Lamport et al. en 1982. Cette étude traite, par la métaphore, de la difficulté pour un réseau d'ordinateurs à s'organiser dans un contexte où la fiabilité de transmission d'informations n'est pas certaine.

Dans leur métaphore, Lamport et al. représentent le réseau d'ordinateurs par un réseau de cités belligérantes, dont le but est de piller Byzance de concert. Des cités traîtresses peuvent toutefois se trouver parmi elles, aller à l'encontre du plan défini, et potentiellement causer la perte des cités fiables. Comment pourraient-elles se coordonner efficacement, de sorte à faire face à d'éventuels éléments malveillants dans leurs rangs ?

Attaque coordonnée – victoire



Attaque non coordonnée – défaite



La *blockchain* est dite **« tolérante à la faute byzantine »** puisque même si une partie des membres du réseau ne sont pas fiables, le réseau dans son ensemble l'est.

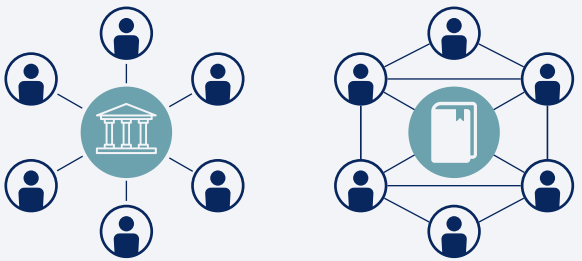
Les six principes fondamentaux suivants sous-tendent cette tolérance à la défaillance interne :

- **Principe numéro 1 :** les ordinateurs du réseau communiquent de manière directe, et se passent d'intermédiaires centralisés.
- **Principe numéro 2 :** une donnée gravée dans la *blockchain* l'est définitivement, il n'est ensuite possible ni de la retirer, ni de la modifier.
- **Principe numéro 3 :** toute donnée gravée dans la *blockchain* est accompagnée d'une signature, qui identifie son émetteur initial de manière pseudonymisée[4].
- **Principe numéro 4 :** les données sont gravées dans la *blockchain* suivant une règle de consensus préalablement définie et qui peut être amenée à évoluer.
- **Principe numéro 5 :** les validateurs peuvent vérifier rapidement et simplement la bonne synchronisation des registres distribués dans le réseau *blockchain*.
- **Principe numéro 6 :** les principaux réseaux *blockchain* incitent les utilisateurs à devenir validateurs

Principe numéro 1 : les ordinateurs du réseau communiquent de manière directe, et se passent d'intermédiaires centralisés.
Un réseau pair à pair est un modèle d'architecture informatique, dans lequel les utilisateurs (aussi appelés « nœuds ») jouent à la fois les rôles de client et de serveur. Cette architecture permet aux réseaux *blockchain* d'exister sans la présence d'une autorité, d'une hiérarchie ou d'un serveur central.

[4] La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. Contrairement à l'anonymisation, la pseudonymisation est une opération réversible : il est possible de retrouver l'identité d'une personne si l'on dispose d'informations supplémentaires.

- Dans un réseau d'échange centralisé, le livre de comptes est tenu par l'acteur central, et c'est par son biais que les utilisateurs du réseau s'y réfèrent.
- Dans un réseau *blockchain* (décentralisé), il y a autant de livres de comptes que de validateurs (les nœuds des réseaux *blockchain*). Pour synchroniser l'ensemble des livres de compte, les validateurs communiquent directement entre eux. Il est possible d'être utilisateur d'un réseau *blockchain* sans en être un validateur, et c'est alors par le biais de n'importe quel validateur qu'il pourra se référer au livre de comptes, c'est-à-dire la *blockchain*.



Réseau centralisé — Réseau pair à pair

Principe numéro 2 : une donnée gravée dans la *blockchain* l'est définitivement, il n'est ensuite possible ni de la retirer, ni de la modifier.
Le second principe d'une *blockchain* réside dans son caractère inaltérable. De fait, quand une information est ajoutée à la chaîne de blocs, elle ne peut théoriquement plus être retirée ou modifiée. En effet, la possibilité pour un ou plusieurs utilisateurs de retirer ou de modifier des données sur la *blockchain* irait à l'encontre d'un des objectifs de cette technologie qui est de créer un registre ouvert et transparent, dans lequel il est facile de retracer toutes les transactions ayant été effectuées. La tenue de la *blockchain* s'effectue alors uniquement par l'ajout concerté de nouvelles données.

Ce principe trouve son fondement dans le terme « *blockchain* » lui-même, soit « chaîne de blocs » en français, puisqu'il fait référence à des blocs de données (des données regroupées) qui vont être ajoutés successivement aux blocs précédemment ajoutés.

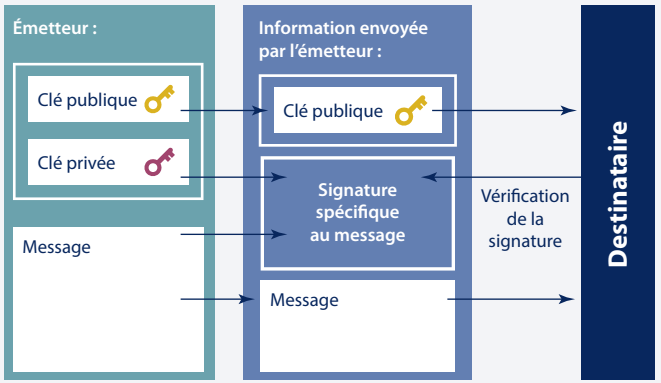
Une donnée enregistrée dans la *blockchain* peut ainsi être considérée comme un engagement pris par un utilisateur puisqu'une fois émise, elle finira par être ajoutée à la « chaîne de blocs » préexistante, et sera immuable. Il n'est ainsi en théorie plus possible de se rétracter après l'envoi d'une donnée, même si celle-ci n'est pas encore ajoutée à la *blockchain*. Cette forme de communication est dite « engageante » car elle contribue à créer des réseaux *blockchain* « inarrêtables » : les utilisateurs formulent des engagements que les validateurs exécutent ensuite.

En théorie, seuls des événements limités, comme une coupure totale du réseau et de ses validateurs, peuvent empêcher l'exécution des engagements qui ont été pris. En pratique, il est possible de procéder à une réécriture de la *blockchain*, mais cela se fait de manière publique et transparente. On appelle cela un *fork*, c'est-à-dire la coexistence de la *blockchain* principale (non modifiée) et de la *blockchain* réécrite. Cela conduit donc à deux *blockchains* distinctes, mais avec une part commune de leur historique.

Principe numéro 3 : toute donnée gravée dans la *blockchain* est accompagnée d'une signature, qui identifie son émetteur initial de manière pseudonymisée.

La cryptographie consiste à chiffrer une donnée pour permettre à un destinataire de la déchiffrer uniquement s'il en possède la clé. Quiconque possède la bonne clé et l'information chiffrée pourra la déchiffrer. Les méthodes de cryptographie existent depuis l'Antiquité, et l'utilisation première est d'assurer la confidentialité d'un

message. Les réseaux *blockchain* utilisent la cryptographie avec un objectif différent : assurer la provenance d'un message. À l'entrée dans le réseau, un membre génère une paire de clés de chiffrement : une clé privée et une clé publique. Cela va lui permettre de générer une signature unique à chaque message qu'il transmet au réseau avec sa clé privée, et les autres membres pourront vérifier l'authenticité de sa signature, grâce à sa clé publique[5]. La clé publique d'un utilisateur est en pratique son pseudonyme dans un réseau *blockchain*, et c'est par son biais que les autres utilisateurs identifient ses engagements.



Principe numéro 4 : les données sont gravées dans la *blockchain* suivant une règle de consensus préalablement définie et qui peut être amenée à évoluer.

Une parfaite synchronisation dans le temps de la *blockchain* est indispensable pour qu'il s'agisse d'un document qui soit une

[5] *La clé privée est essentielle pour dépenser ses crypto-actifs, et elle ne doit donc pas être partagée. Les clés publiques doivent être partagées pour permettre la vérification de l'authenticité des signatures générées par les clés privées associées. En pratique, les clés publiques génèrent des « adresses » qui servent d'identifiants publics, au même titre que les IBAN pour les comptes bancaires. Ce sont ces adresses qui sont partagées.*

référence commune pour l'ensemble du réseau. Cette synchronisation fonctionne avec des blocs de données, ajoutés successivement à la *blockchain*, et de manière uniforme dans le réseau.

Illustration : le cheminement d'une transaction

Toute transaction dans le réseau suit un chemin unique pour être inscrite dans la *blockchain* :

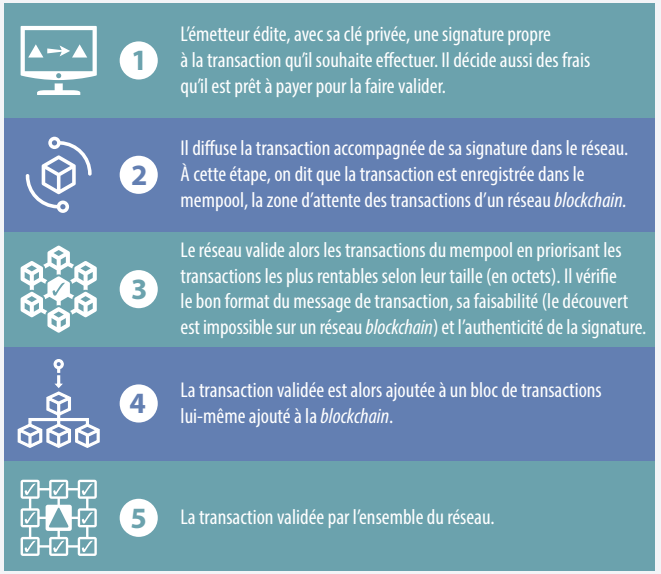
1. L'émetteur édite, avec sa clef privée[6], une signature propre à la transaction qu'il souhaite effectuer. Il décide aussi des frais qu'il est prêt à payer pour la faire valider.

2. Il diffuse la transaction accompagnée de sa signature dans le réseau, une validation sera accordée selon le protocole de consensus en vigueur. À cette étape, on dit que la transaction est enregistrée dans le mempool, la zone d'attente des transactions d'un réseau *blockchain*.

3. Le réseau valide alors une par une les transactions du mempool, en choisissant en priorité les transactions les plus rentables selon leur complexité. Il vérifie le bon format du message de transaction, sa faisabilité (le découvert est impossible sur un réseau *blockchain*) et l'authenticité de la signature.

4. La transaction est alors inscrite et validée dans le réseau lorsqu'un bloc contenant cette transaction est ajouté à la *blockchain* par n'importe quel validateur et validé par l'ensemble des nœuds du réseau.

[6] *Certains portefeuilles sont multi-signatures (wallet multi sig), et exigent les signatures d'un groupe déterminé d'utilisateurs pour que la transaction soit approuvée.*



Chaque utilisateur peut constituer son propre bloc de données à ajouter à la *blockchain*, et devenir ainsi validateur du réseau. Il s'agit d'un rôle complémentaire à celui de simple utilisateur de la technologie, cela consiste à proposer de nouveaux blocs de données au réseau, et de vérifier constamment l'intégrité de toute donnée avant de l'inscrire dans la *blockchain*. Selon le protocole en vigueur, à intervalle de temps fixe ou à espérance fixe, un unique bloc de données est sélectionné parmi ceux proposés par les validateurs du réseau. Cette sélection s'effectue suivant une méthode objective et stricte : il s'agit des protocoles de consensus. Ils peuvent différer d'un réseau *blockchain* à un autre, mais dans un réseau donné, ils définissent de manière exhaustive et non libre à l'interprétation les règles qui s'appliquent aux membres, sans distinction. Quand tout utilisateur peut rejoindre le réseau, consulter les transactions passées et participer au processus de

validation, on parle de *blockchain* publique. Dans le cas où, au contraire, la possibilité de faire ou de consulter des transactions est restreinte à des acteurs présélectionnés par une autorité dite de confiance, on parle de *blockchain* privée.

Il y a principalement deux protocoles de consensus distincts existants à l'heure actuelle : La preuve de travail, (*Proof of Work* en Anglais), et la preuve d'enjeu (ou *Proof of Stake*)[7].

Preuve de travail *(Proof of Work)*

La preuve de travail consiste à prouver qu'une certaine quantité de ressources a bien été dépensée pour la formation d'un bloc, et d'ainsi s'assurer que les mineurs aient intérêt à proposer des blocs valides plutôt que des blocs malhonnêtes. En effet, afin de déterminer quel validateur du réseau ajoutera son bloc à la *blockchain*, les protocoles dits de preuve de travail requièrent que les validateurs réalisent simultanément une tâche supplémentaire à la validation et au regroupement d'informations dans un bloc. Cette tâche, que l'on appelle minage, consiste à déterminer une certaine valeur numérique, qui ne peut être trouvée que par une succession d'essais aléatoires[8]. Le premier qui la détermine voit son bloc être accepté par le réseau ; il s'agit en fait d'une course à la vitesse de génération et de test de nombres aléatoires. L'efficacité est fondée sur l'énergie dépensée et tout validateur peut y allouer autant de ressources énergétiques qu'il le souhaite.

Preuve d'enjeu *(Proof of Stake)*

[7] Il est possible pour un réseau blockchain de changer de protocole de consensus. C'est par exemple le cas du réseau Ethereum (une des blockchains les plus importantes en termes de transactions, de valeur échangée, de nombre de nœuds validateurs, et de développeurs). Ethereum a opéré un passage de "preuve de travail" à "preuve d'enjeu" au courant du mois de septembre 2022.

[8] Ce qu'on appelle communément la "force brute".

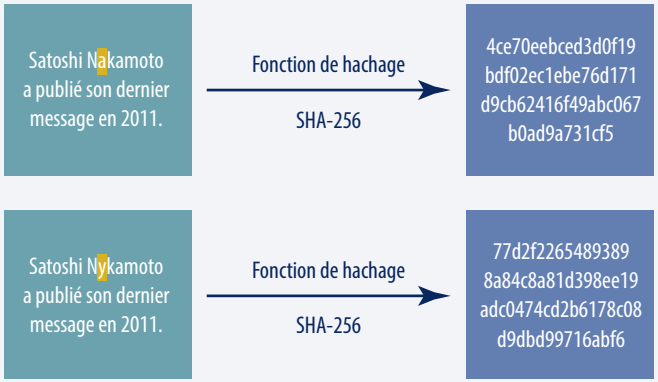
Le protocole par preuve d'enjeu, quant à lui, demande aux validateurs de mettre en séquestre une partie de leur capital pour participer à l'ajout d'un bloc. La probabilité d'être sélectionné dans le réseau pour voir son bloc être accepté dépend ici du capital. Par exemple, dans le cas de la *blockchain* Ethereum, il s'agirait des Ether, bloquées par les validateurs. Il s'agit d'un protocole discriminatoire au capital, mais bien moins énergivore.

Principe numéro 5 : les validateurs peuvent vérifier rapidement et simplement l'intégrité des données des registres distribués dans le réseau *blockchain*.

Le hachage est une fonction déterministe (non aléatoire) qui, à partir d'une donnée quelconque fournie en entrée, calcule un résultat de taille fixe que l'on appelle le hash. Cette fonction permet de vérifier l'intégrité des données au sein des réseaux *blockchain*. Si le hash de la donnée est modifié, cela signifie que la donnée hachée a été modifiée. Il s'agit d'une fonction cryptographique particulière (SHA-256, dans le cas de Bitcoin[9]) qui a la propriété d'être à sens unique, c'est à dire qu'il est pratiquement impossible de retrouver une donnée à partir de son hash. En hachant les données de transaction de la *blockchain*, les validateurs peuvent comparer les résultats obtenus, et ainsi s'assurer de sa parfaite synchronisation dans le réseau. La principale méthode utilisée pour vérifier l'intégrité des données dans les réseaux *blockchain* est une technique de répétition de hachage, appelée arbre de hachage (ou arbre de Merkle[10]).

[9] SHA-2 est un ensemble de fonctions de hachage cryptographique (SHA-224, SHA-256, etc.) conçu par l'Agence Nationale de Sécurité Américaine (NSA). https://medium.com/swlh/the-mathematics-of-Bitcoin

[10] Merkle, Ralph C. "A digital signature based on a conventional encryption function."Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1987. Il existe une version de ce papier plus accessible : Mykletun, Einar, Maithili Narasimha, and Gene Tsudik. "Providing authentication and integrity in outsourced databases using Merkle hash trees." UCI-SCONCE Technical Report (2003).



En modifiant une lettre d'un mot, la fonction de hachage est complètement différente.

Principe numéro 6 : les principaux réseaux *blockchain* incitent les utilisateurs à devenir validateurs.

Sans autorité centrale pour coordonner le réseau, le maintien de sa sécurité et de son intégrité ne va pas de soi, et requiert une participation active des membres du réseau. Ainsi, pour garantir l'intégrité d'un réseau *blockchain*, son protocole doit encourager ses membres à être validateurs. Cela passe par un système de récompenses, de deux types :

- L'émission de nouveaux jetons, actifs numériques fongibles propres à chaque *blockchain*. Lorsqu'un validateur ajoute un bloc, celui-ci est récompensé par un nombre fixé de nouveaux jetons.
- Des frais de transaction (appelés transaction fees), payés directement par les utilisateurs pour la validation et l'ajout des données à inscrire dans la *blockchain*[11].

[11] *Le gas est l'unité qui mesure la complexité des calculs requis pour exécuter des opérations spécifiques. Le coût du gas varie au cours du temps et est fixé par un mécanisme de marché. Le principe de gas est apparu sur le réseau Ethereum et a été repris depuis, par d'autres blockchains permettant l'usage de smart contracts.*

Un système de « congestion » se met en place naturellement dans les réseaux *blockchains*. Les blocs de données sont limités en taille (par exemple en octets pour Bitcoin ou en gas, c'est-à-dire en unités de calculs, pour Ethereum), et donc en volume de données échangées. Lorsque le nombre de données émises devient supérieur à cette limite, les frais de transaction des utilisateurs augmentent puisque les validateurs peuvent effectuer un choix parmi les données à valider dans le réseau. Le critère de choix est le gain à valider la donnée ou le calcul par rapport à sa complexité.

Être validateur est donc rémunérateur, et l'est plus encore dans un réseau congestionné.

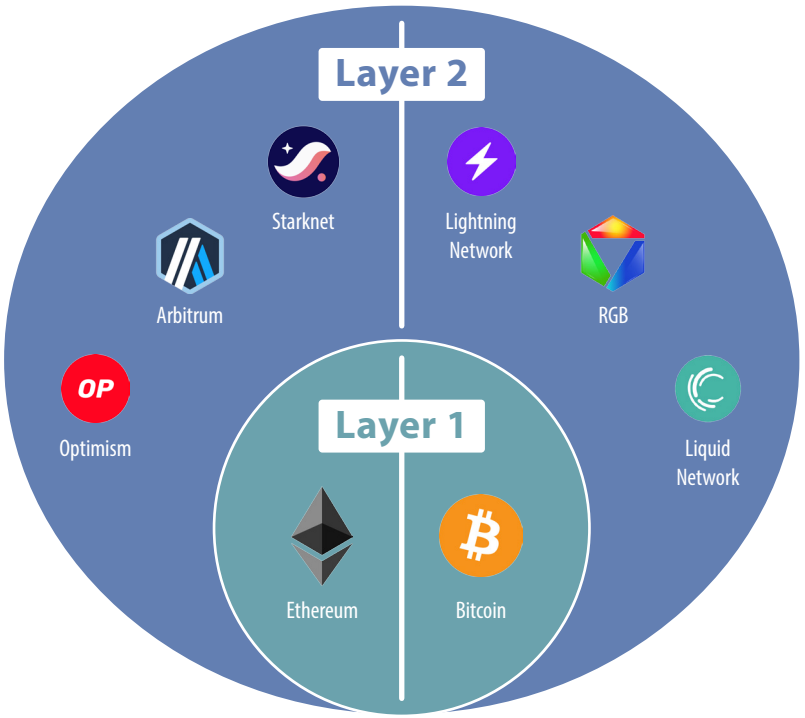
2.2. LA COUCHE APPLICATIVE DES *BLOCKCHAINS*

La couche applicative regroupe toutes les solutions génériques s'appuyant sur la couche infrastructure du réseau, proposant ainsi de nouvelles fonctionnalités pour les échanges. Voici trois types d'applications importantes :

- Les **contrats autonomes** (ou ***smart contracts*** en anglais), qui permettent aux utilisateurs de programmer leurs propres engagements, selon des conditions prédéfinies.
- Les **oracles**, qui permettent d'intégrer automatiquement dans la *blockchain* des données et variables initialement hors *blockchain*, notamment provenant du « monde réel ». Il s'agit d'une source d'informations qui peut être précieuse pour les *smart contracts* et les conditions requises pour leur exécution. Par exemple : injecter des données météo pour déclencher des assurances sécheresse sur la *blockchain* ; ou injecter des cours de bourse pour déclencher certains contrats sur la *blockchain*.
- Les ***layer 2***, qui permettent d'agréger les données dans la *blockchain*, et d'en augmenter leur débit. Le principe d'un *layer 2* est de traiter des

ensembles de transactions du réseau de la couche infrastructure de la *blockchain (layer 1)* sur un réseau parallèle *(layer 2)*. À tout moment, les parties prenantes peuvent récupérer un gain acquis sur le *layer 2*, et le transférer directement sur le *layer 1*.

Schéma représentant différents layers sur les *blockchains* Ethereum et Bitcoin



Les cas d'usages s'appuient donc sur la couche application – les *smart contracts* notamment – et ses nouvelles fonctionnalités proposées dans un but précis, industriel ou non.

Diverses ressources numériques sont présentes dans la couche application, se stockent dans des portefeuilles (appelés wallets) et se développent de plus en plus vite à mesure de leur adoption à travers le monde :

- Les ***stablecoins*** ont pour objectif et intérêt de répliquer le cours d'un actif (monnaie ayant cours légal, crypto-monnaie ou tout autre type d'actif) *via* plusieurs mécanismes possibles de stabilisation – souvent un adossement à des réserves de l'actif en question. Ils conservent l'intérêt fonctionnel des crypto-actifs, sans l'inconvénient de leur volatilité.

- Les **utility *tokens*** ont une fonction applicative car ils permettent d'utiliser une application présente sur la *blockchain* (par exemple un service de stockage de *cloud* décentralisé). On peut subdiviser les *utility tokens* suivant leur fonction, on peut retrouver notamment :
  - les *tokens* avec fonction réputationnelle permettent de déterminer la fidélité ou la fiabilité d'un utilisateur du réseau ;
  - les *tokens* avec fonction participative, soit « *token* de gouvernance », permettent de prendre part à la gouvernance d'un projet et de voter sur les modalités « *on chain* » et « *off chain* » de son évolution (cf. organisation autonome décentralisée, ou DAO, plus bas).

- Les ***security tokens*** ont une fonction d'investissement car ils procurent des droits financiers et décisionnaires (droits à un dividende et droit de vote en Assemblée Générale par exemple), leur valeur étant directement connectée à celle des produits et services auxquels ils sont associés. Ils présentent les caractéristiques juridiques d'instruments financiers.

- Les **NFT** (ou jetons non fongibles) sont des *tokens* associés à un sous-jacent numérique ou physique qui, selon leurs objectifs, peuvent représenter un certificat d'authenticité d'un bien physique, ou une preuve de provenance d'œuvre d'art par exemple.

D'autres applications sont apparues pour permettre le transfert sécurisé d'informations sur le réseau avec des cas d'usages pour la traçabilité de chaîne d'approvisionnement d'un produit, pour garantir son authenticité et son auditabilité. L'innovation et la recherche sur ces nouvelles applications et les langages informatiques associés sont dynamiques, ce qui laisse augurer la création future de nouvelles applications.

2.3. L'ÉVOLUTION DE LA *BLOCKCHAIN* DANS LE TEMPS

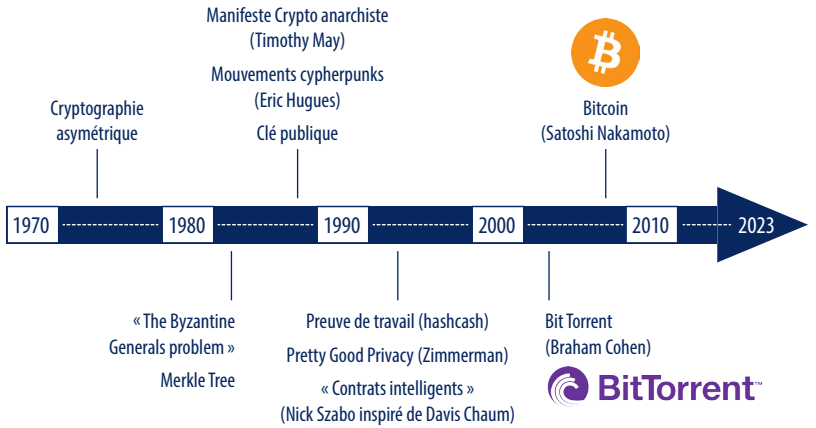
Avant le Bitcoin

Bien que Bitcoin soit la première *blockchain* décentralisée, elle s'appuie sur des composants qui existaient depuis longtemps. Plus largement, elle s'inscrit dans un mouvement politique et philosophique connu sous le nom de cypherpunks et dans une tradition scientifique dans le domaine de la cryptographie et plus précisément des monnaies numériques.

Le mouvement cypherpunk part du constat que le développement du numérique dans le cadre d'entités centralisées (des États ou des entités privées notamment) pourrait représenter une menace pour le contrôle d'utilisateurs sur leurs données personnelles. Il repose sur la croyance que la cryptographie peut être au service de la protection de la vie privée et de la confidentialité des données. Dans ce cadre, Bitcoin se présente comme une solution d'échange de monnaie électronique fondée sur de la cryptographie. Ce système permet aux utilisateurs de se passer d'un intermédiaire de confiance, qui, dans les modèles traditionnels, est chargé de la tenue des comptes. Se passer de cet intermédiaire donne une forme d'autonomie monétaire et d'indépendance financière à ses utilisateurs.

Les *blockchains* trouvent donc leur origine dans une tradition de nature scientifique et politique.

La frise chronologique suivante résume les grandes innovations techniques sur lesquelles repose la *blockchain* telle qu'on la connaît aujourd'hui, en parallèle des grandes étapes de l'évolution du mouvement cypherpunk.



De Bitcoin aux diverses blockchains

Première levée de fonds par ICO pour le projet Mastercoin en 2013

Dès 2013 commencent les premières levées de fonds pour des projets de crypto-actifs avec Mastercoin, qui leva l'équivalent de $ 500 000 en Bitcoins. Ces levées de fonds se font par « *Initial Coin Offering* » (ICO), techniques proches du crowdfunding dans leur fonctionnement. Les créateurs du projet proposent aux intéressés d'acheter des *tokens* de leur projet. Ces *tokens* donnent aux investisseurs des droits d'accès prédéfinis à des produits ou services, des droits de vote et/ou des droits financiers sur le projet.

Création de la blockchain Ethereum en 2015 permettant l'utilisation de smart contracts

La *blockchain* Ethereum a été développée pour pallier les limites de la *blockchain* Bitcoin, qui est difficile à utiliser pour des applications impliquant une complexité algorithmique et logique. Elle se présente comme un système d'exploitation universel pouvant héberger tout type d'application. Son langage de programmation avancé permet d'incorporer des instructions dans un code informatique qui sont ensuite interprétées par la machine virtuelle d'Ethereum *(Ethereum Virtual Machine)*. La machine virtuelle d'Ethereum garantit que les instructions seront exécutées par tous les membres du réseau. Pour éviter les comportements malveillants liés à l'ouverture du réseau, un coût (le gas) est associé à chaque instruction. Le coût de déploiement est d'abord payé par l'utilisateur qui enregistre le *smart contract* sur la *blockchain*, puis par tous les utilisateurs qui interagissent avec ce *smart contract* ensuite : il s'agit du coût d'exécution.

Les *smart contracts* sont des outils qui permettent de vérifier automatiquement si une transaction remplit les conditions nécessaires pour pouvoir être effectuée selon des critères incorporés directement *« on chain »*. Ils sont ainsi *« trustless »* (sans confiance) puisqu'ils ne nécessitent pas de relations de confiance pour être acceptés par les utilisateurs.

Les initiateurs du projet Ethereum ont réalisé en 2014 une ICO qui a permis de lever 18 millions de dollars. La *blockchain* Ethereum est vite devenue la deuxième plus importante après Bitcoin en termes de capitalisation boursière.

Des blockchains au Web3/métavers/DeFi/DAOs

Grâce à sa capacité de désintermédiation et de sécurisation, la *blockchain* a permis de faire évoluer de nombreux domaines comme le web ou l'échange de valeurs, notamment dans le métavers.

Le Web3

Le Web1 (1990-2000) était un réseau internet de diffusion de contenu (« Content Delivery Network ») où l'utilisateur avait uniquement la possibilité de lire des pages web statiques adaptées à un seul support (ordinateur et/ou minitel). On y retrouvait des applications comme Hotmail, AOL ou des applications de recherche comme Lycos ou AltaVista.

Le Web2 (2000-2020), quant à lui, est un réseau internet plus intéractif où l'utilisateur a la possibilité d'écrire, de lire et de modifier du contenu en ligne. Avec une rapidité accrue par rapport au Web 1.0, le commerce en ligne se développe. De nombreuses applications ont vu le jour (Wikipedia, Airbnb, etc.).

C'est Jeffrey Zeldman qui est des premiers à faire émerger la notion de Web3 en 2006[12], notion reprise par Gavin Wood, co-fondateur d'Ethereum en 2014 selon les principes suivants.

- C'est un réseau internet décentralisé, c'est-à-dire pair-à-pair, où l'information est répartie entre les membres du réseau, et non plus entre serveurs centralisés.
- Les utilisateurs peuvent sélectionner avec plus de précision les données qu'ils souhaitent partager : c'est l'auto gouvernance des données.
- Les données des utilisateurs peuvent être garanties en fournissant une preuve de leur détention, sans obligatoirement en dévoiler le contenu[13].

La *blockchain* joue un rôle clé dans la mise en œuvre du Web3 en fournissant une infrastructure décentralisée, sécurisée et transparente. Elle permet de redonner la possibilité aux utilisateurs d'être en contrôle de leurs données.

[12] *Jeffrey Zeldman. (2006). Web 3.0. UbiKann. https://alistapart.com/article/web3point0/*

[13] *Certaines utilisations alternatives du hash d'un document peuvent tout à fait fournir la preuve d'obtention de ce dit document, tout en masquant son contenu. Cela est rendu possible puisque le hash du document seul ne suffit pas pour retrouver le document.*

Le métavers

Si le terme « Métavers » n'a jamais autant été usité que cette dernière année, le concept est né il y a plus de 30 ans dans Snow Crash, un livre qui évoque la vie d'un entrepreneur fou décidant de créer un monde virtuel où il pourrait contrôler l'esprit des individus.

Le métavers n'a eu que très peu d'essor, car peu de réalité, jusqu'à l'arrivée des nouvelles technologies, et notamment de la réalité augmentée.

Chacun aura sa propre définition du métavers, mais on peut s'accorder sur le fait qu'il est un réseau de mondes et de simulations numériques, persistants, interactifs et rendus en temps réel qui assurent la continuité de l'identité, des objets, des données et des droits, et peuvent être vécus de manière synchrone par un nombre illimité d'utilisateurs. C'est un terme très utilisé dans un contexte vidéoludique. Les technologies de réalité augmentée et de réalité virtuelle y sont souvent associées.

Encadré : qu'est-ce que le métavers ?

L'écosystème autour du métavers se regroupe en deux grandes catégories : d'une part les publics professionnels autour de la réalité virtuelle (offre de Meta) ou augmentée (offre de Niantic, Snapchat ou Apple), d'autre part, des projets Web3 utilisant des technologies de registre distribué de type *blockchain* ou NFT (Sandbox, Decentraland).

Le métavers permet aux utilisateurs de revendiquer la propriété des ressources numériques avec lesquelles ils interagissent, et, a fortiori, devenir producteurs de ressources numériques. Ainsi, il apporte de la "territorialisation" en créant des mondes virtuels distincts les uns des autres, situés dans des espaces délimités. Le métavers fait apparaître la notion de territoire sur le plan géographique, avec la possibilité de se déplacer d'un point à un autre en son sein. Néanmoins, la détention d'un NFT ne peut s'assimiler à un droit de propriété car si les serveurs des opérateurs sont déconnectés du jour au lendemain, la parcelle de terrain achetée par le biais d'un *token* et certifiée par le biais d'un NFT n'existe plus. Derrière le métavers se cache de nombreuses technologies comme la *blockchain*, ou les plateformes virtuelles en 3D ou en réalité virtuelle, mais surtout des communautés. Ces mondes virtuels ont en effet chacun leurs codes, leurs esthétismes et leurs communautés.

Le métavers ne se cantonne pas aux projets de Meta, mais englobe des technologies sociales d'immersion très disparates, qui se développent rapidement, et esquissent un horizon commun. Dans la mission d'information d'octobre 2022 sur le métavers (Basdevant, François & Ronfard), le métavers relève plutôt d'un concept général de l'immersion, tandis que les métavers renvoient à des outils comme les mondes virtuels, la technologie 3D ou encore le temps réel pour opérationnaliser ce concept général.

Aujourd'hui, les métavers sont davantage poussés par l'offre industrielle que par la demande des utilisateurs.

La mission d'information précitée déplore un manque de communication entre les acteurs qui portent ces deux catégories, et préconise à cet égard de capitaliser sur l'opportunité des Jeux Olympiques et Paralympiques de 2024 pour mobiliser ces deux écosystèmes autour de projets d'expériences immersives concrets.

Un rapport de Global Counsel de novembre 2022 estime l'impact économique du métavers entre 4 trilliards et 5 trilliards de dollars à horizon 2030 au niveau mondial, alors que nous sommes entre 200 et 300 milliards de dollars fin 2022, sachant que les marques de luxe et de mode ont été les premières à adopter cette approche, afin de resserrer le lien avec leurs clients et leurs communautés.

Quel rapport avec la *blockchain* ?

Les *blockchains* peuvent être considérées comme des vecteurs de développement des métavers du fait de leur capacité à faciliter l'échange d'actifs numériques.

De fait, un élément clé manquait pour totalement conceptualiser le métavers. Dans ces espaces immersifs virtuels où les objets numériques ont une valeur financière, la *blockchain* et plus particulièrement les *tokens* non fongibles (NFT) permettent d'échanger des actifs numériques en s'assurant de la sécurisation et de la transparence de leur stockage.

Des plateformes telles que Decentraland, The Sandbox, Cryptovoxels, Somnium Space, et Bloktopia (sur Ethereum) proposent des expériences de métavers dans lesquelles les utilisateurs peuvent créer, acheter, échanger et vendre des actifs numériques.

L'échange de valeur entre les utilisateurs dans les métavers soulève des questions d'interopérabilité, qui peuvent être résolues par l'utilisation de *layers 2* tels que Starkware ou Arbitrum. L'initiative « Open Metaverse Alliance » regroupe des plateformes de métavers telles que Decentraland et The Sandbox pour rendre les métavers plus interopérables.

Trois grands enjeux peuvent être mis en avant concernant la technologie *blockchain* et le métavers :
- la demande croissante d'interopérabilité entre les différents métavers de la part des utilisateurs: l'interopérabilité désigne des réalités variées (connectivité, règles, gestion de l'identité des utilisateurs) et conditionne l'adoption de la technologie à terme ;
- la persistance d'une image négative des métavers combinant casques de réalité virtuelle / augmentée et détention de crypto-actifs, qui pâtissent d'une double image négative (respectivement isolement et spéculation). Cette mauvaise image est particulièrement forte au Royaume-Uni et en France, moins aux États-Unis, selon un rapport de Global Counsel de novembre 2022 ;
- l'apparition de nouveaux modes de gouvernance portés par des organisations autonomes décentralisées (DAO) souvent plus adaptés aux modalités de création artistique, dans un contexte où les contenus sont encore trop souvent dépendants de la politique de l'éditeur de ces mondes virtuels. De manière générale, le métavers est une opportunité unique pour rassembler industriels, chercheurs et artistes autour d'œuvres immersives innovantes et à impact sociétal positif.

La DeFi (Finance Décentralisée)

Le terme *DeFi*, diminutif de l'anglais *Decentralized Finance* (Finance Décentralisée en français), désigne un ensemble de services financiers s'appuyant sur la technologie *blockchain* qui remplace sur certains champs le recours à des intermédiaires centralisés. Les engagements financiers pris par les différentes parties sont enregistrés dans la *blockchain* et exécutés *via smart contracts*.

La *DeFi* se distingue de la finance traditionnelle de quatre manières :
- Un accès davantage ouvert : aucune entité ou institution n'a le pouvoir d'empêcher l'entrée d'un participant, public ou privé, individuel ou collectif. Cependant, des mécanismes de *whitelisting* permettant d'interagir avec des *smart contracts* peuvent être mis en place.
- Des règles déterministes faisant autorité : les contrats et les infrastructures soutenant les solutions *DeFi* sont codés dans des scripts publics et autonomes, assurant ainsi que les conditions du contrat financier ne pourront pas changer suite à une décision d'un tiers, comme cela peut exister dans la finance traditionnelle.

- Des services sans garde d'actifs : comme la *DeFi* permet à des actifs de vivre intégralement dans le protocole par le biais de contrats autonomes *(smart contracts)*, il est possible d'automatiser à l'infini tout un ensemble de leurs propriétés.
- Des protocoles composables et à accès public : les protocoles *DeFi* peuvent être combinés à volonté pour générer de nouvelles solutions, et plusieurs interfaces utilisateur distinctes pour un même protocole peuvent coexister sans problème.

La *DeFi* reprend les principes de base du Bitcoin pour créer une alternative numérique aux places boursières. Sa promesse est de faire naître des marchés financiers plus ouverts, plus libres et plus équitables, accessibles à l'aide d'une simple connexion Internet. Leur intégrité se veut garantie au niveau protocolaire, dans le code, et non par des institutions financières ou des intermédiaires physiques.

En pratique, la *DeFi* fonctionne à l'aide d'ordres programmables *via* l'utilisation de *smart contracts*. Le carnet d'ordres (d'achat et de vente), très difficile à coder en *DeFi*[14], est substitué par de nouveaux objets, en particulier les AMM *(Automated Market Makers)*, et ces ordres sont programmables directement par les utilisateurs *via* l'utilisation de *smart contracts*, ce qui permet d'ajouter certaines conditions à leur exécution. Les informations prises en compte dans le protocole *DeFi* peuvent provenir soit d'une source présente sur la *blockchain*, soit d'une source extérieure à la *blockchain*, c'est-à-dire qu'elle sont importées par le biais d'un oracle. Par exemple, si l'on a besoin du cours d'un crypto-actif ou d'un actif de la finance traditionnelle il faudra donc utiliser un oracle.

[14] *Mangrove, l'entreprise française, sort après plusieurs années de R&D en mars 2023 un carnet d'ordre programmable. Cela va simplifier le développement sur la DeFi.*

Les DAOs

Les organisations autonomes décentralisées (dites « DAO ») sont dotées d'une gouvernance programmable spécifiée sur une *blockchain* et reposent sur la technologie des *smart contracts* comme source primaire et souvent exclusive de gouvernance. Leur degré d'autonomie est variable : certaines DAO se basent sur des comités d'experts alors que d'autres se basent exclusivement sur le vote des détenteurs de *tokens*. La *blockchain* apporte une transparence sur les décisions prises et son accessibilité permet à quiconque ayant une connexion Internet de contribuer à ces projets. De plus, le fonctionnement par *smart contract* assure l'irrévocabilité et l'immuabilité des transactions effectuées et des évolutions du code du projet.

Leur émergence répond à un besoin réel dans un contexte où le taux moyen d'insatisfaction avec les organisations démocratiques traditionnelles approche les 55 % d'après le Center for the future of democracy. Les DAOs sont aujourd'hui des laboratoires d'expérimentation de nouvelles méthodes de gouvernance, à l'instar de la démocratie liquide et du vote quadratique utilisé par les sénateurs du Colorado en 2019 pour leurs lois de finance.

Les DAOs ont accumulé l'équivalent de 10 milliards d'actifs sous gestion selon le rapport 2022 de la société de capital risque américaine a16z. Leur apport principal est de faire émerger des modèles décisionnels par le bas, « *bottom-up* », en mobilisant des modalités de vote plus ou moins sophistiquées (quorum, majorité relative, « *rage quitting* »[15], quadratique[16], de conviction ou mobilisant le consensus holographique[17],

[15] *Le Rage-quit est le processus par lequel un membre d'une DAO se retire d'une partie ou de la totalité de sa participation dans la trésorerie de la DAO et abandonne sa participation. L'objectif principal est de donner aux membres la liberté de choisir le meilleur moment pour retirer leurs fonds sans aucune condition préalable supplémentaire.*

[16] *https://medium.com/metawoodstudios/quadratic-voting-why-we-use-it-6c1c27b4304*

[17] *https://medium.com/daostack/holographic-consensus-part-1-116a73ba1e1c*

fondé sur la réputation ou sur la connaissance). Morpho et Mangrove, *via* une association loi 1901, revendiquent être les premiers projets de DAO en droit français.

Les défis futurs pour les DAO sont essentiellement pratiques et juridiques. Sur le plan pratique, les DAOs restent vulnérables à des incidents de type TheDAO[18] et au manque d'engagement de la part des parties prenantes dans les mécanismes de vote, ce qui fait peser des risques de concentration de la prise de décision dans les systèmes. Sur le plan juridique, de nombreuses questions restent en suspens sur le plan de la gouvernance interne comme externe. Cela pose de nombreuses questions pragmatiques comme le fait de savoir contre qui faire des recours en cas de litige par exemple. Le recours de la CFTC, le régulateur américain des bourses de commerce, contre la DAO Ooki illustre d'ailleurs le risque de poursuites judiciaires dans le cas d'une DAO non incorporée, qui n'est associée à aucune entité légale. L'état américain du Wyoming a donné un statut juridique au concept de DAO, mais il devra rester vigilant à ce que celui-ci ne soit pas vu *in fine* comme un cadre contraignant dans un écosystème évoluant rapidement.

2.4. LES DÉFIS DE LA *BLOCKCHAIN*

Les défis techniques: le trilemme des blockchains

Aujourd'hui, malgré les avancées et les discussions en cours, les *blockchains* ne parviennent pas à traiter un grand nombre de transactions. Une éventuelle solution à ce problème pourrait se traduire par une fragmentation des *blockchains* publiques existantes. De fait, un nombre trop important de *blockchains* entraînerait un nouveau problème d'interopérabilité des *blockchains* entre elles.

[18] TheDAO a été la première DAO sur la blockchain Ethereum, mais le projet a été interrompu à la suite de l'exploitation d'une vulnérabilité du code ayant empêché le bon fonctionnement du projet.

Ce problème d'interopérabilité est toutefois activement étudié par la communauté scientifique, ce qui nécessite des compétences informatiques et économiques, car il est fortement lié à la théorie des incitations.

L'évolution des *blockchains* peut être catégorisée selon trois grands axes de développement : la sécurité, la scalabilité et la décentralisation.

Selon le trilemme des *blockchains* de Joseph Abadi Markus Brunnermeier, repris par Vitalik Buterin, il n'est pas possible de développer les trois axes simultanément puisqu'ils sont contradictoires, mais éventuellement deux axes au détriment du troisième.

Sécurité

Le système assure l'intégrité des données de façon pratiquement absolue *via* des prérogatives cryptographiques. Il doit protéger les membres fiables des membres défaillants et des attaques contre le réseau. En théorie, une *blockchain* ne peut pas être parfaitement sécurisée. Par exemple, une prise de contrôle de la *blockchain* Bitcoin (réputée pour sa sécurité) pourrait être envisageable pour un individu ou groupe concerté d'individus arrivant à regrouper durablement plus de 51 % de la puissance de calcul mise à disposition pour le réseau.

Scalabilité

Le système doit s'adapter au volume de transactions, et ainsi garantir la fluidité du réseau. L'infrastructure Bitcoin est par exemple peu scalable en soi, puisqu'une taille maximale est fixée pour un bloc de transaction, et que les blocs sont ajoutés à délai moyen quasiment fixe. On arrive donc à une situation d'engorgement dans le réseau lorsque de nombreuses transactions sont enregistrées dans le mempool, la zone d'attente des transactions d'un réseau *blockchain*. L'unique solution pour les membres est alors d'augmenter les frais de transaction et ainsi être prioritaire aux yeux des validateurs. Une piste de solution pourrait être dans l'augmentation

de la taille maximale d'un bloc, mais cela aurait des conséquences négatives sur le réseau de trois manières.

- Conséquence de latence : des blocs de données volumineux sont plus longs à se transmettre entre validateurs, et se diffuseraient donc plus lentement dans le réseau.

- Conséquence de coût : à intervalle égal entre deux blocs, une *blockchain* constituée de blocs plus volumineux serait elle-même plus volumineuse. Un nouveau nœud devrait consacrer bien plus de ressources énergétiques pour se synchroniser avec le reste du réseau, et ce problème s'applique aussi aux nœuds qui fournissent des informations aux nouveaux nœuds. Cela pourrait également amener la *blockchain* à reposer sur un nombre d'acteurs plus réduit, à rebours de sa logique de décentralisation.

- Multiplication des *forks* : la probabilité que deux mineurs produisent quasi simultanément un bloc valide est inversement proportionnelle à la durée de production des blocs. Réduire cette durée entraîne mécaniquement une multiplication des *forks* dans l'historique de la *blockchain*.

Encadré : les approches proposées pour augmenter la taille des blocs sur Bitcoin

Plusieurs augmentations des tailles de blocs ont été proposées pour Bitcoin, mais ont été refusées par la communauté puisque cela augmenterait les coûts pour les validateurs (nouveaux et anciens), créerait des problèmes de latence et remettrait en question son caractère entièrement décentralisé. Un Hard Fork, appelé Bitcoin Cash, a été initié permettant d'augmenter la taille des blocs, ce projet n'a pas connu un grand succès. Sur Bitcoin, les inscriptions Ordinals tirent profit des modifications de la taille des blocs post-segwit[19] pour permettre le stockage d'images ou d'autres fichiers directement on-chain. Les Ordinals divisent la communauté car Bitcoin car pour certains elles n'ont pas vocation à stocker des données de taille significative pour certains. Une autre solution actuellement étudiée (non mise en pratique encore) est le *sharding*, qui consiste à fragmenter une *blockchain* en plusieurs sous-*blockchains* coordonnées. Chaque sous-*blockchain* (ou shard) aurait les capacités de la *blockchain* d'origine, et ensemble, elles se diviseraient équitablement la validation des données du réseau.

Décentralisation

L'innovation de rupture de la technologie *blockchain* est de tenir à jour un livre de compte sans recours à des tiers de confiance, ce qui n'était possible dans aucun autre système avant. Lorsque l'on parle de décentralisation d'un système informatique, on peut la percevoir sous trois sens :

- Au sens logique : si l'on scinde un réseau *blockchain* en plusieurs sous-réseaux (incluant utilisateurs et validateurs), chaque sous-réseau peut continuer à exister et fonctionner de manière indépendante et autonome. Les *forks* et le *sharding* sont deux exemples de cette décentralisation logique.
- Au sens architectural : les points de défaillance du système sont davantage éparpillés que dans un système centralisé où l'unique point de défaillance est son serveur central. Dans les réseaux *blockchain*, de nombreux validateurs autonomes participent à la tenue du réseau. Ainsi, chaque nouveau validateur déconcentre davantage la défaillance du système. L'attaque d'un réseau *blockchain* doit donc se faire en ciblant indépendamment un grand nombre de validateurs, et de manière

[19] *SegWit (Segregated Witness) est une mise à niveau du protocole qui modifie la structure des données de transaction Bitcoin. Il a été activé sur Bitcoin le 23 août 2017.*

simultanée. Les principaux réseaux *blockchains* incitent les utilisateurs à devenir validateurs, et donc à décentraliser le système au sens architectural.

- Au sens politique : la capacité d'un groupe restreint d'utilisateurs à modifier le consensus du réseau se trouve limitée dans les systèmes *blockchain*. C'est selon la part minimum d'utilisateurs que doit contenir ce groupe restreint pour modifier le consensus qu'un réseau se qualifie sur sa centralisation/décentralisation politique. Ainsi la *blockchain* Ethereum est considérée comme décentralisée puisqu'il faut l'approbation des nœuds[20] du réseau pour faire une modification sur le consensus et il est impossible d'obliger des nœuds à accepter une modification contre leur gré. Pour autant, il faut noter que Vitalik Buterin, cofondateur de Ethereum, garde une grande influence sur les décisions, étant à la tête de la Fondation Ethereum. Une illustration récente est par exemple la mise à jour d"Ethereum «The Merge» en Septembre 2022, annoncée et proposée par la fondation Ethereum, et acceptée des utilisateurs. Bitcoin peut davantage être considéré politiquement décentralisé notamment parce que son fondateur (Satoshi Nakamoto) n'a plus interagi avec les utilisateurs depuis 2011.

Encadré : zoom sur la *blockchain* MASSA, un exemple de projet français qui a pour objectif de résoudre le défi du passage à l'échelle

Encore en développement, la *blockchain* MASSA se fixe pour objectif de résoudre le trilemme précédemment décrit des *blockchains* (décentralisation, sécurité, efficacité), en se focalisant sur le volet décentralisation. Selon les porteurs de projet, la technologie multi-chaîne est susceptible de générer une adoption de masse.

MASSA se démarque dans l'écosystème grâce au développement de *smart contracts* autonomes dans leur solution, soit des contrats capables d'exécuter des transactions prédéfinies de manière totalement décentralisée. D'autres données que des informations sur les transactions peuvent être stockées dans ce type de *smart contracts* ce qui les rend uniques au sein de l'écosystème.

La solution a été développée par trois personnes issues de l'INRIA, ENS et Polytechnique, ce qui témoigne de l'excellence technologique française.

Les défis écologiques : bond en avant ou retour au charbon ?

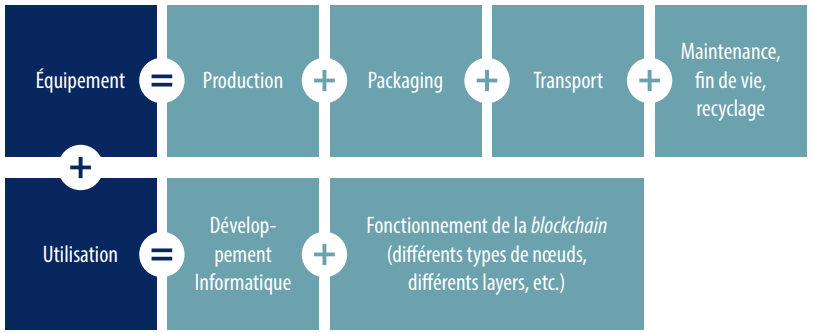
La *blockchain* a une mauvaise image à cause de son impact environnemental. Si cette image est justifiée pour certaines *blockchains* (*Proof of Work* notamment), dans certains contextes d'utilisation, elle ne s'applique pas dans tous les cas.

Déterminer l'impact d'une *blockchain* sur l'environnement, c'est considérer l'intégralité du cycle de vie des produits et/ou services qu'elle permet, ses effets directs et indirects.

Une analyse de cycle de vie comprend l'étude de l'impact des équipements utilisés pour le fonctionnement de cette *blockchain*, ainsi qu'un examen des conséquences environnementales de son *utilisation*.

[20] *Si des nœuds sont en désaccord avec le réseau, ils sont libres de se retirer du consensus.*

Analyse de cycle de vie d'une *blockchain*



En raison de leur différent niveau de garantie de sécurité, les *blockchain Proof of Work* sont beaucoup plus énergivores que les *blockchain Proof-of-Stake*.

Une *blockchain Proof of Work* (PoW) requiert de très grandes capacités de calcul pour sécuriser le réseau. L'impact environnemental concerne non seulement l'énergie requise pour effectuer les calculs nécessaires au fonctionnement de la *blockchain* PoW, mais aussi pour fabriquer les machines de minage – appelées rigs ou ASICs. Rapporté à une transaction unique, le Bitcoin (PoW) consomme 908 kWh. Selon l'étude « Bitcoin: Cryptopayments Energy Efficiency », la consommation actuelle de Bitcoin, une *blockchain* PoW, est de 80,69 TWh/an. À titre de comparaison, aux États-Unis la totalité des sèche-linges consomme 71,53 TWh/an[21] et la consommation électrique totale du Chili s'élève à 77,53 TWh/an[22] en 2021. La même étude relève que la *blockchain Proof of Stake* Tezos a consommé 997 886 MJ d'électricité en 2021, ce qui équivaut à 0,000277 TWh, soit près de 300 000 fois moins.

[21] (89 millions de sèche-linges aux USA, un sèche linge consomme 800 kWh/an) https://www.nrdc.org/sites/default/files/efficient-clothes-dryers-IB.pdf https://www.nrdc.org/sites/default/files/ene_14060901a.pdf

[22] Les données sur l'impact du Chili sont disponibles sur Digiconomist https://digiconomist.net/

Hormis le choix d'une *blockchain Proof of Stake* plutôt qu'une *blockchain Proof of Work*, et le mix énergétique du pays dans lequel la *blockchain* est opérée, il existe des innovations permettant de réduire l'impact environnemental de la *blockchain*. Par exemple, les mineurs des *blockchains* PoW privilégient au maximum les énergies recyclables, essentiellement pour des raisons financières, ou installent les serveurs dans des zones géographiques où la population ne consomme pas l'ensemble des énergies disponibles.

Les limites écologiques de la *blockchain* sont présentées en faits et chiffres de manière détaillée en Annexe 2.

Les défis liés à l'intégration de données externes dans la blockchain

Il est important de rappeler que la *blockchain* ne permet pas une désintermédiation généralisée. Elle permet seulement de remplacer les intermédiaires qui sont aujourd'hui responsables de l'interopérabilité et de la mise en cohérence de bases de données déjà existantes entre elles. Ainsi, la *blockchain* n'a pas de prise sur la relation entre le monde réel *(off-chain)* et le monde codifié *(on-chain)*. Elle ne peut se substituer à des intermédiaires qui assurent la mise en cohérence du monde réel avec le monde digital, par exemple les compagnies d'assurance.

Les oracles permettent d'intégrer automatiquement dans la *blockchain* des données et variables initialement hors *blockchain*. Ils peuvent être une source d'informations précieuse pour les *smart contracts* et les conditions requises pour leur exécution. Enfin, ils peuvent faciliter les solutions d'interopérabilité entre deux *blockchains* distinctes.

Deux types d'oracles émergent donc :

- Les oracles qui récoltent automatiquement des données disponibles en open source, et majoritairement en provenance de sites web (exemple : site spécialisé dans l'analyse financière pour importer les cours de bourse). Il y a cependant toujours un risque de *hack*, de manque de fiabilité de la source de données, ou de fermeture du site.

- Les oracles physiques, dont les données proviennent d'outils de mesure tels que des capteurs physiques (exemple : taux de précipitation déterminé *via* un capteur météorologique). Les données récoltées par un capteur peuvent toujours être corrompues lors de leur acheminement jusqu'à la *blockchain*, ou le capteur pourrait être défaillant.

La fiabilisation d'un oracle s'obtient soit par la multiplication du nombre de sources de provenance des données[23] (de nombreux sites web, de nombreux capteurs distincts…), soit par un acteur se portant garant des données importées et potentiellement des pertes dues aux défaillances de ces données. Dans ce second cas, il y a un risque introduit par la corruptibilité ou la défaillance de cet acteur.

Il est néanmoins à souligner que l'utilisation d'oracles, en tant qu'intermédiaires centralisés chargés de fournir des données fiables, peut introduire une forme de recentralisation dans les cas d'usage *blockchain.* Cette situation peut entraîner des problèmes de sécurité et de fiabilité concernant la collecte et l'utilisation des données.

Les défis liés aux arnaques et hack : un fléau en extinction ou en extension ?

Les *blockchains* sont, pour de bonnes raisons, réputées très sécurisées. Mais tout système comporte ses failles, et celles des *blockchains* se situent essentiellement au niveau des applications, des utilisateurs ou des plateformes. En fait, les *blockchains* sont des infrastructures sécurisées, mais les environnements au sein desquelles elles sont utilisées ne le sont pas forcément.

[23] *La multiplication des sources de données est l'approche favorisée par le réseau Chainlink d'oracles décentralisés (https://chain.link).*

On observe deux types de failles majeures :

- Les failles technologiques dues à des failles techniques notamment dans les *smart contracts*, alors exploitées par des *hackers*. Il existe d'autres types de failles technologiques qui ne sont pas forcément liées à la technologie *blockchain* en tant que telle, mais aux risques digitaux « traditionnels » comme les cyberattaques.
- Les fraudes, à l'image des rug-pull, où des équipes mal intentionnées vont fonder un projet dans le but de voler l'argent des investisseurs. En effet, un rug-pull définit une situation où l'équipe mère d'un projet disparaît subitement avec les fonds des investisseurs en abandonnant le projet initial.

L'Annexe 3 détaille les failles liées aux utilisateurs, aux développeurs, et aux plateformes.

Dans quelques débats publics sur les *blockchains*, on constate encore un manque de distinction entre la technologie sous-jacente et certains de ses usages. Cela se traduit par un nombre élevé de projets spéculatifs, mal gérés ou à but malveillant qui ont défrayé la chronique.

C'est essentiellement la mauvaise gestion des risques et les fraudes commises par certains acteurs centralisés qui ont contribué à la mauvaise image de la *blockchain.* Ces défaillances de gestion et fraudes auraient tout aussi bien pu survenir dans d'autres secteurs avec d'autres outils technologiques.

Encadré : le cas FTX

L'effondrement de la plateforme d'échange de crypto-actifs FTX en novembre 2022, jusqu'alors seconde mondiale en termes de part de marché, est emblématique du décalage entre performance de la technologie *blockchain* et qualité de la gouvernance :

- Le 2 novembre 2022, un rapport publié par CoinDesk révèle qu'Alameda Research, le fond d'investissement lié à la plateforme FTX, pourrait se retrouver en état d'insolvabilité si le cours du FTT venait à chuter.
- Suite à la publication de ce rapport, Binance, entreprise concurrente de FTX et 1re en termes de part de marché déclare publiquement mettre sur le marché ses *tokens* FTT, obtenus au lancement de FTX.
- Le cours du *token* chute[24] d'approximativement 25 dollars à moins de 2 dollars entre le 7 et le 13 novembre 2022. FTX est déclaré en faillite le 11 novembre.
- John J. Ray III, le liquidateur en chef, devenu de facto entre-temps le nouveau PDG de FTX, déclare le 18 novembre 2022 : « Jamais, au cours de ma carrière, je n'ai vu un échec aussi complet des contrôles d'entreprise et une absence aussi totale d'informations financières fiables qu'ici. Il avait notamment supervisé la procédure de faillite d'Enron, à hauteur de 23 milliards de dollars. De l'intégrité compromise des systèmes et de la surveillance réglementaire défectueuse à l'étranger, à la concentration du contrôle entre les mains d'un très petit groupe d'individus inexpérimentés, peu avertis et potentiellement compromis, cette situation est sans précédent ».

[24] https://coinmarketcap.com/fr/currencies/ftx-token/

Quelles répercussions sur l'écosystème ?

- Suite à la faillite, une baisse globale des cours de nombreuses crypto-actifs a eu lieu :
- le SOL, crypto-monnaie fortement soutenue par FTX, chute de 16 % en quelques heures, et perd 68 % entre le 5 et le 9 novembre 2022[25].
- Le Bitcoin chute de 28 %, entre le 5 et le 21 novembre 2022
- L'Ether chute de 36 % entre le 4 et le 9 novembre 2022.
- La dette de FTX s'élève à plus de 3 milliards de dollars pour ses 50 créanciers les plus importants fin novembre 2022[26], et son nombre total de créanciers se compte en millions.
- Une vague de peur s'est alors propagée sur les marchés de crypto-actifs et a atteint de nombreuses entreprises de l'écosystème, liées de près ou de loin à FTX, par un effet domino.

Par ailleurs, il existe une difficile distinction entre différents concepts (*blockchain*, crypto-monnaie, crypto-actifs), exportant la mauvaise image des uns sur les autres: la crypto-monnaie reste encore associée par beaucoup à du blanchiment d'argent.

La *blockchain* est ainsi perçue comme un secteur d'activité, et on peut constater un réel amalgame entre *blockchains* et crypto-actifs.

D'une part, la plupart des entreprises détenant des crypto-actifs ne détiennent pas ou très peu de crypto-monnaies mais bien d'autres catégories d'actifs cryptos. D'après l'édition 2022 de l'étude de PwC « Blockchain et crypto: comment les entreprises en tirent bénéfice ? »

[25] https://fr.tradingview.com/

[26] https://www.latribune.fr/entreprises-finance/banques-finance/industrie-financiere/3-1-milliards-d-euros-la-dette-colossale-de-ftx-a-ses-50-plus-gros-creanciers-941440.html

seulement 30 % des entreprises au niveau mondial détenant des crypto-actifs, possèdent des crypto-monnaies de type Bitcoin, Ether et Tezos, tandis que la plupart des entreprises détiennent plutôt des *stablecoins*, jetons numériques fongibles et non fongibles et NFT. Cette tendance se retrouve également sur le marché français.

D'autre part, et particulièrement sur le marché français, le type de crypto-actif détenu par les entreprises est encore largement dépendant de la stabilité du cadre réglementaire en vigueur. Ainsi, 22 % des entreprises françaises détiennent des *utility tokens*, et seulement 16 % des NFT qui sont encore trop flous juridiquement, et pour lesquels il n'y pas vraiment de dispositifs dédiés de type cadre fiscalo-comptable. En tout état de cause, pour les crypto-actifs, la multiplication de nouvelles marketplaces telles qu'OpenSea, Immutable, ou encore Rarible a permis d'élargir la diffusion de ces crypto-actifs à la sphère réelle, dans laquelle les grands groupes ont pris une large part.

Cet amalgame appelle à une meilleure compréhension du fonctionnement, des bénéfices et des limites, et des usages de la *blockchain* par les décideurs politiques et économiques. Comme tout écosystème naissant et peu mature, et comme l'était internet à ses débuts, bien que la *blockchain* apporte une réelle valeur ajoutée, elle attire également des projets spéculatifs ou tendancieux qui profitent de cette incompréhension des différentes parties prenantes. Pour espérer un passage à l'échelle, il faut éclaircir ce point dans les débats publics. Dans le cas du scandale FTX, il est important de préciser qu'il s'agit avant tout d'une fraude liée à une absence de gouvernance et de contre-pouvoir, facilitée par une réglementation défaillante et non d'un problème de technologie. De plus, il s'agit d'une plateforme centralisée, proposant la conservation des actifs de ses clients sans respecter les principes de ségrégation des actifs, ce qui déroge aux principes de la *blockchain* à savoir la décentralisation et la suppression des intermédiaires de confiance.

3 La France a été pionnière sur la technologie *blockchain* et ses applications crypto

3.1. L'ÉCOSYSTÈME FRANÇAIS EST RICHE ET BIEN POSITIONNÉ SUR LA NOUVELLE CHAÎNE DE VALEUR PERMISE PAR LA TECHNOLOGIE *BLOCKCHAIN*

Les entreprises françaises se sont rapidement saisies des opportunités de la technologie *blockchain* pour développer des cas d'usage tandis que les autorités ont construit un cadre réglementaire avec les acteurs très tôt.

Sur le plan technique, une recherche de haut niveau a permis de consolider une avance sur les briques technologiques les plus techniques, soit les contrats autonomes dits *« smarts contracts »* et langages formels. L'enjeu est désormais de développer des protocoles plus élaborés pour rattraper notre retard sur les autres pays et de les rendre interopérables entre eux pour faire émerger des cas d'usage plus sophistiqués. Des acteurs comme Morpho, Kiln, Mangrove et beaucoup d'autres permettent à l'écosystème français de démontrer mondialement les compétences techniques présentes en France et de se hisser au niveau de pays leaders comme les États-Unis.

Encadré : la recherche française, pionnière sur la brique *smart contracts* et langages formels

La recherche française se distingue par sa longueur d'avance sur la brique *smart contracts* et sur les langages formels associés. Le cœur de cette avancée en France est le protocole de Tezos développé avec Nomadic Labs (langages de programmation

Michelson bas niveau statiquement typé pour ses *smart contracts*, systèmes distribués et vérification formelle du protocole économique) et l'INRIA (langage de programmation OCaml). Tezos a développé un écosystème allant au-delà de l'univers académique puisque sa fondation associe des industriels, des startups et autres parties prenantes directement impliquées dans le développement et les applications du protocole.

Il repose sur un consensus tolérant aux fautes byzantines, le consensus BFT, ce qui permet la validation de transactions et l'exécution de programmes informatiques[27].

Tezos permet de voter toute modification de son protocole pour rendre possible son évolution.

Plus largement, l'initiative BART *(Blockchain Advanced Research & Technologies)* lancée en mars 2018 contribue au rayonnement de la recherche française sur cette brique, en ce qu'elle l'incorpore aux 6 axes de sa feuille de route dédiée à la levée des verrous technologiques et scientifiques de la technologie *blockchain* pour accélérer le passage à l'échelle de l'écosystème.

Cette avance doit être cultivée en tant que telle mais également dans le contexte du développement de technologies et d'usages tiers, en particulier les univers virtuels ou « métavers », dans lesquels la *blockchain* apporte de la valeur. Ainsi en parallèle du développement de technologies de pointe sur la composante réalité virtuelle et augmentée du métavers tels que les jumeaux numériques portés par Dassault Systèmes, la France doit aussi développer son excellence dans la composante *blockchain*, nécessaire notamment pour l'échange d'actifs numériques dans ces espaces virtuels.

[27] *Voir théorème des généraux byzantins plus haut.*

Sur le plan des usages, la *blockchain* infuse rapidement la société française.

- D'après une étude de PwC d'avril 2022, les pure players français sont non seulement de plus en plus matures, mais ils se démarquent de leurs pairs à l'international, puisque leur croissance dépasse en moyenne celles des pure players des autres pays.

- Les crypto-actifs se propagent de manière croissante à la sphère réelle comme moyen de diversification de trésorerie, d'optimisation de modèle d'affaires ou de relais de croissance.

- En matière de cas d'usage l'écosystème français est extrêmement riche et les applications se multiplient même en période de marché baissier. Malgré tout, on observe une fuite des cerveaux et des projets vers des localisations plus ouvertes à l'utilisation des actifs numériques au sein de l'activité économique, comme la Suisse par exemple à l'image de la « Crypto Valley »[28].

Sur le plan juridique, la loi PACTE de 2019 et ses travaux préparatoires ont permis de poser les bases d'un cadre stable et protecteur soucieux de concilier protection des consommateurs et encouragement de l'innovation par le biais d'une approche centrée sur les acteurs et services fournis.

La France se positionne donc comme un des pionniers sur le plan juridique et réglementaire. Afin de continuer dans cette dynamique, il convient de rester dans une démarche propice à l'innovation des acteurs du secteur Web3 afin de faire émerger et/ou conserver les leaders de demain.

La Suisse est l'un des pays les plus avancés dans ce domaine. Le Conseil fédéral entend continuer d'améliorer les conditions nécessaires pour que la Suisse puisse tirer parti au mieux des avantages associés à ces

[28] https://cryptovalley.swiss/

technologies. Dès le 1er août 2021, la Suisse a mis en vigueur des dispositions légales pour la technologie *blockchain*[29].

Sur le plan intellectuel, la France défend sa propre vision de l'internet ouvert, libre, sûr et patrimoine commun de l'humanité[30]. Cela transparaît dans les discussions en cours sur l'organisation de l'infrastructure du métavers et les standards technologiques associés (W3C, *Metaverse Standards Forum*). La France y défend la construction de briques technologiques ouvertes, de confiance et gratuites, dans une logique d'offre, plutôt que l'incorporation de services dans le métavers à proprement parler, dans un contexte où la demande n'est pas encore au rendez-vous.

La France peut se targuer d'un écosystème *blockchain* dynamique, qui a très tôt développé des cas d'usage, que ce soit au niveau de l'infrastructure, de l'intergiciel *(middleware)*, de l'applicatif ou des services *blockchain*.

Encadré : l'attractivité des différents écosystèmes Web3, à l'échelle internationale

La France est un des *leaders* de l'innovation dans le secteur crypto, grâce à l'esprit d'initiative de ses *start-ups* et de ses licornes comme Ledger ou Sorare. Des acteurs qui ont depuis longtemps pris conscience des enjeux stratégiques de cette révolution pour notre futur.

[29] https://www.efd.admin.ch/efd/fr/home/numerisation/blockchain.html#:~:text=Le%201er%20ao%C3%BBt%202021%2C%20la,la%20place%20financi%C3%A8re%20est%20essentielle.

[30] *D'après le rapport Basdevant & al., « Mission exploratoire sur les métavers », 2022.* https://www.economie.gouv.fr/files/files/2022/Rapport-interministeriel-métavers.pdf

Néanmoins, les pays, par l'intermédiaire de leurs métropoles, s'affrontent désormais pour attirer les cerveaux du monde entier entre leurs murs comme en témoigne l'illustration suivante :

Top 20 Crypto Hub Cities

Source : Recap[31]

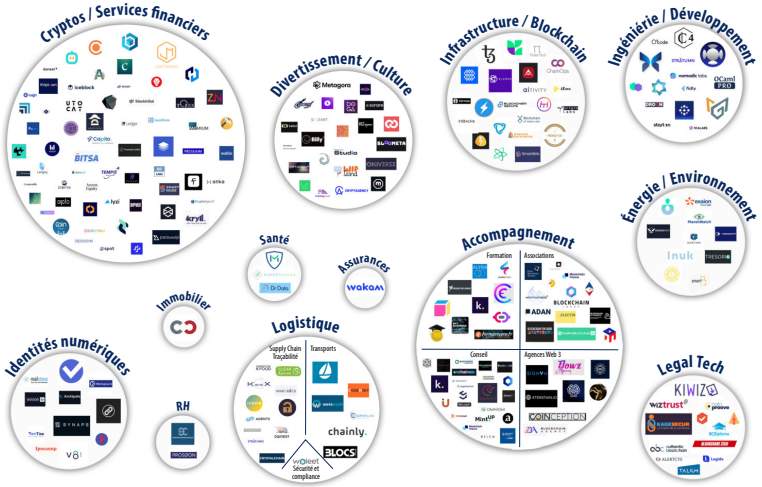
Ce classement a été établi par les experts de Recap[32] en Janvier 2023. Les chercheurs se sont basés sur 8 critères distincts pour établir leur classement :

- Qualité de vie
- Nombre d'évènements crypto par an dans la ville ;
- Pourcentage de travailleurs ayant un métier en lien avec le secteur crypto ;
- Nombre d'entreprises crypto installées ;
- Part du financement de la R&D dans le PIB ;
- Nombre d'ATM crypto ;
- Taxation sur les bénéfices crypto ;
- Pourcentage de personnes détenant des cryptos dans le pays.

[31] https://recap.io/blog/the-rise-of-crypto-hubs-which-cities-are-leading-the-way-in-cryptocurrency

[32] https://recap.io/blog/the-rise-of-crypto-hubs-which-cities-are-leading-the-way-in-cryptocurrency

Représentation visuelle et non exhaustive de l'écosystème *blockchain*, crypto et métavers français



Source : Une cartographie de l'écosystème blockchain français (non-exhaustive), établie en octobre 2022, par le portail collaboratif de ressources dédié à l'écosphère Web3 : 2140.fr.

En complément du schéma ci-dessus, certains projets ou initiatives récentes peuvent être cités :

- Legal Blockchain & Crypto Association[33], qui vise à réunir les juristes spécialisés dans les actifs numériques et les technologies *blockchain*. L'association accompagne la pratique, la recherche et les évolutions juridiques autour des crypto-actifs et des réseaux *blockchain* en France et à travers le monde.
- L'échange décentralisé Mangrove[34] est également un projet intéressant à suivre grâce à son optimisation de la liquidité dans la *DeFi*.

[33] https://lbca.io/

[34] https://www.mangrove.exchange/

- Enfin, les médias spécialisés jouent un rôle clé à l'image de The Big Whale[35], L'entonnoir du Bitcoin[36], Cointribune[37], Cryptoast[38], Le Crypto Daily, Wagmi Trends, ou encore N3w Society[39] notamment.

Finalement, il est intéressant d'observer que l'écosystème s'émancipe très rapidement. Il serait complexe de citer l'intégralité des parties prenantes en raison de la croissance des initiatives de la sphère Web3 en France. Les acteurs français continuent de construire et développer des cas d'usage malgré le *bear market* actuel. Malgré des ventes en berne sur la période 2022-2023, les NFT attirent toujours autant : la seconde édition du NFT Paris a attiré les 24 et 25 février 2023 plus de 10 000 visiteurs contre 600 l'année précédente.

Encadré : les entreprises françaises qui se sont développées très tôt

Les entreprises françaises se sont emparées très tôt de la technologie *blockchain* pour concevoir, développer et industrialiser des cas d'usage, dans un premier temps essentiellement financiers et liés aux *fintechs*, et tirer parti des opportunités de la technologie *blockchain* pour le soutien et l'optimisation des systèmes de paiement traditionnels. Cela s'est traduit par le lancement de nombreux projets pilotes par des institutions financières de renom, au premier rang desquelles Goldman Sachs, Santander, Deutsche Bank, CommonWealth Bank of Australia, etc. De nombreux

[35] https://www.thebigwhale.io

[36] https://podcasts.apple.com/fr/podcast/lentonnoir-du-Bitcoin/id1588897400

[37] https://www.cointribune.com/en/

[38] https://cryptoast.fr/

[39] https://www.instagram.com/n3wsociety/

consortiums internationaux ont aussi été mis en place au sein desquels la France a pris une part active comme le *consortium* R3 pour développer la plateforme open source CORDA destinée à faciliter les échanges interbancaires et les opérations de réconciliation de comptes pour une meilleure conformité aux obligations de KYC. En 2015, la Caisse des dépôts et consignations (CDC) a monté un consortium dédié avec des institutions bancaires françaises (BNP, BPCE, etc.) et des sociétés d'assurance françaises (AXA, CNP). Plusieurs participants ont néanmoins quitté le consortium comme Santander, Morgan Stanley et Goldman Sachs pour des raisons qui n'ont pas été précisées, mais qui pourraient s'apparenter à des problèmes de gouvernance et à des difficultés à s'entendre sur les objectifs de ces consortiums.

Enfin, l'écosystème français *blockchain* a construit des projets innovants, rassemblant acteurs privés, publics et semi-publics pour construire les briques nécessaires à la mise en place d'une identité numérique.

Encadré : une *blockchain* de consortium Archipels

Une *blockchain* de consortium Archipels a été lancée en 2021 par de grands acteurs français[40] et se présente comme une plateforme de services de confiance. Plaçant le concept d'identité numérique au cœur de son activité, il s'agit d'une solution prônant une navigation web plus libre, transparente, sécurisée et accessible par le biais de vérifications, de certifications et de simplifications d'accès aux services en ligne pour tous et permise par l'utilisation de

[40] Portée majoritairement par EDF, Engie, La Poste et la Caisse des Dépôts et Consignations.

la *blockchain*. La *blockchain* d'Archipels s'est construite autour de principes forts de confiance en ligne centrée sur l'utilisateur et dont le respect de la vie privée est prioritaire. Ayant pour ambition de développer le standard de l'identité décentralisée en conformité avec les normes européennes, Archipels vise à se conformer aux principes du RGPD et à la révision du règlement eIDAS[41] pour accroître la confiance dans les échanges de données et répondre à des besoins actuels avec une solution décentralisée, rapide et simple. La *blockchain* d'Archipels fait état de 7 millions de documents ancrés de manière mensuelle, avec plus de 60 millions de documents vérifiés, sécurisés et certifiés depuis son lancement.

La France a également pris toute sa part à l'exploration de la *blockchain* pour améliorer le fonctionnement des services publics. Sur le modèle d'Alastria, l'Alliance Blockchain France (ABF) a été construite en 2022. Il s'agit d'un consortium soutenu par de grands industriels, et qui aura pour mission de déployer une infrastructure *blockchain* commune qui s'ouvrira progressivement à tout type d'acteur (industriels, administrations françaises et plus petits acteurs) souhaitant bénéficier des avantages de la *blockchain*. Dans un communiqué de presse, l'ABF annonce soutenir la démocratisation de la technologie *blockchain* et commencer à se développer dans une perspective d'interopérabilité européenne, avec une trajectoire promouvant le développement durable et la compétitivité économique des entreprises françaises.

L'un des objectifs communs de ces consortiums est donc de participer à la création de standards européen transfrontaliers, notamment pour la vérification des informations administratives.

[41] Projet de règlement européen, electronic IDentification, Authentication and trust Services (eIDAS), visant à accroître la confiance dans les échanges de données en Europe.

Encadré : zoom sur le projet Alastria

Alastria, est un consortium *blockchain* lancé en Espagne en 2017. Avec plus de 200 nœuds validateurs hébergés par des entreprises et 600 participants, Alastria est le projet le plus avancé en la matière. Le gouvernement de la communauté autonome d'Aragon a annoncé qu'il avait rejoint le consortium Alastria afin d'utiliser la *blockchain* au sein de l'administration publique. L'objectif d'Alastria est de développer une infrastructure *blockchain* visant à promouvoir l'adoption de la technologie pour différents secteurs d'activité. Son modèle de fonctionnement est basé sur celui de Ethereum et vise à offrir une solution plus scalable et performante pour les entreprises. Les cas d'usages sont nombreux et variés, traitant de l'identité numérique, du secteur de l'énergie, de la finance, de la santé, des technologies, du sport, de l'agriculture, de l'art, etc.

Alastria est donc une *blockchain* privée, ouverte à toute entité légale, mais avec un droit d'entrée pour financer le développement du projet. Les adhérents d'Alastria peuvent donc bénéficier :

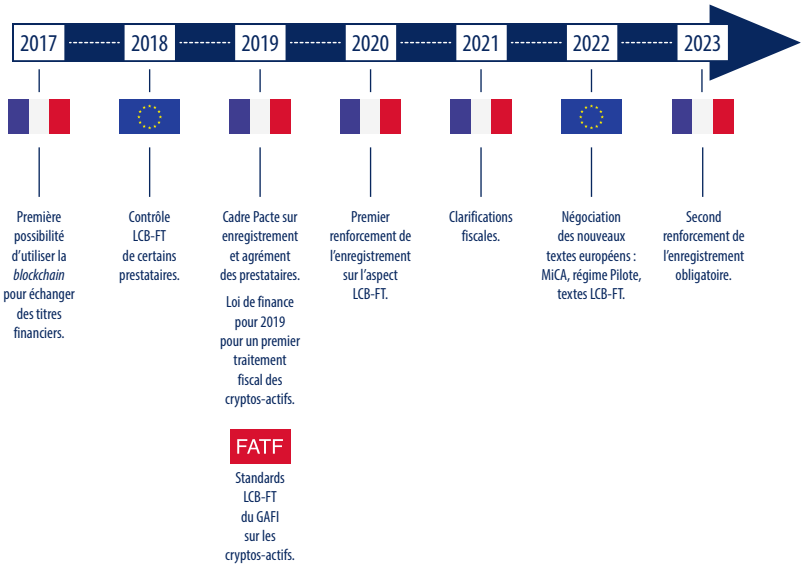
- D'une amélioration de la transparence et de l'efficacité de l'administration, en permettant d'attirer des initiatives commerciales ;
- D'un outil économique avec lequel les entités peuvent rester en contact et partager leurs informations ;
- D'une collaboration visant à promouvoir la modernisation technologique de l'administration publique et de l'offre de services ;
- De gains importants de productivité tout en renforçant la confiance et la sécurité des échanges entre adhérents ;
- D'un service qui permet une identification et une authentification claire des parties prenantes, ce qui est indispensable à l'appropriation industrielle de la technologie *blockchain*.

Alastria n'est donc pas la seule initiative européenne qui se développe et réunit des acteurs importants, on peut notamment citer Id Union en Allemagne, qui se concentre davantage sur le sujet de l'identité décentralisée.

3.2. LA FRANCE A TRÈS TÔT MIS EN PLACE UNE RÉGLEMENTATION DÉDIÉE À LA *BLOCKCHAIN* ET À SES APPLICATIONS, AVANT DE SOUTENIR UNE RÉGLEMENTATION EUROPÉENNE HARMONISÉE QUI ENTRERA PROCHAINEMENT EN APPLICATION

La France a été parmi les tout premiers pays à mettre en place une réglementation dédiée à la *blockchain* et à ses applications. Cet intérêt précoce des autorités françaises a permis d'ouvrir rapidement des discussions avec les différentes parties prenantes de l'écosystème et ainsi d'acquérir une avance en matière de compréhension et de réglementation des actifs numériques. La France est désormais un des pays les plus matures en matière de cadres juridique, réglementaire et fiscal.

Cette avance a par ailleurs permis aux autorités françaises de peser dans les discussions européennes qui ont abouti à l'adoption d'un règlement européen sur les marchés de crypto-actifs (règlement MiCA) et à l'adoption d'un règlement européen sur la possibilité d'expérimenter la technologie *blockchain* pour échanger des titres financiers (régime pilote). Ces corpus sont complétés par deux textes visant à renforcer les moyens de lutte contre le blanchiment et le financement du terrorisme (LCB-FT).



La réglementation des prestataires de services sur actifs numériques : de l'enregistrement obligatoire français à l'agrément obligatoire MiCA

En l'état, le droit applicable aux entités qui offrent des services en matière de crypto-actifs (une plateforme d'échange, un conservateur de crypto-actifs, etc.) découle de la loi PACTE de 2019, laquelle a créé le statut de prestataire de services sur actifs numériques (PSAN). La loi a prévu :

- Un enregistrement et une supervision obligatoire de la plupart des prestataires de services, par l'Autorité des marchés financiers (AMF) et l'Autorité de contrôle et de prudentiel et de résolution (ACPR) ;
- Une possibilité pour les prestataires qui le souhaitent d'aller plus loin et de solliciter un agrément facultatif qui comprend davantage de règles à respecter.

En date du 7 mars 2023, 67 sociétés ont été enregistrées et aucun agrément n'a été délivré.

Encadré : les éléments vérifiés dans le cadre de l'enregistrement obligatoire en France

Pour être enregistré, un prestataire doit respecter les obligations suivantes :

- être établi en France ou en UE ;
- les personnes en assurant la direction doivent posséder l'honorabilité et la compétence nécessaires ;
- mettre en place un dispositif de lutte contre le blanchiment et le financement du terrorisme.

Par ailleurs, conformément au renforcement de l'enregistrement prévu par la loi DDADUE du 9 mars 2023, des obligations supplémentaires sont imposées aux nouveaux entrants sur le marché à partir du 1er juillet 2023 :

- Avoir un système de sécurité adéquat ;
- Disposer d'une politique interne de gestion des conflits d'intérêts ;
- Assurer une communication claire et non trompeuse vis-à-vis des clients ;
- Donner des gages sur leur dispositif informatique et démontrer qu'il est sécurisé pour éviter les cyberattaques ;
- Pour les conservateurs de crypto-actifs : ségrégation des actifs conservés, obligation de restitution.

Le cadre français issu de la loi PACTE sera prochainement remplacé par le cadre harmonisé européen issu du règlement MiCA. S'agissant des prestataires de services sur actifs numériques (devenant prestataires de services sur crypto-actifs – PSCA en droit de l'UE), l'application du règlement reviendra essentiellement à ajouter des règles à respecter obligatoirement pour exercer dans l'UE. Les acteurs seront alors soumis à « agrément obligatoire », comportant toutes les règles présentées précédemment ainsi que de nombreuses règles « métier » spécifiques à chacune des

activités exercées. Pour les acteurs, il s'agira d'une marche importante à franchir pour pouvoir continuer d'exercer. En contrepartie, ils pourront offrir leurs services dans l'ensemble des 27 pays de l'UE.

S'agissant de la supervision, les prestataires resteront supervisés par les autorités nationales, seuls ceux comptant plus de 15 millions de clients étant soumis à la supervision de l'Autorité européenne des marchés financiers (AEMF).

Encadré : les risques pour les investisseurs

L'Autorité des marchés financiers (AMF) relève dans son rapport de 2021 une reconversion des escrocs du forex au Bitcoin : les dossiers de plainte contre les escroqueries ont explosé en proportion (25 % des dossiers d'investissement frauduleux en 2021 contre 6 % en 2020). D'après la médiatrice de l'AMF, début mai 2022, les actifs numériques représentent 20 % des litiges contre 6 % en 2020. Le montant moyen du préjudice par demandeur est de 4 200 € mais les pertes de certains investisseurs ont pu atteindre 200 000 €. Il s'agit principalement de porte-monnaies en crypto-actifs piratés, ou encore de plateformes d'échange dans l'incapacité de restituer des Bitcoins ou Eethers.

La réglementation fiscale et comptable en matière de crypto-actifs demeure une prérogative nationale

Cadre comptable

La France a été l'un des premiers pays au monde à se doter d' un cadre comptable, en favorisant le développement des activités liées aux actifs numériques en encadrant aussi bien les levées de fonds par émission de

jetons (ou ICO) (règlement comptable ANC 2018-07) que les prestataires de services sur actifs numériques au travers du règlement comptable ANC 2020-05.

Cadre fiscal

La loi de finances pour 2019 a apporté des précisions essentielles permettant aux particuliers investissant à titre occasionnel d'évoluer dans un cadre fiscal clair, à la suite d'un arrêt du 26 avril 2018 dans lequel le Conseil d'État avait jugé que les produits tirés par les particuliers de la cession de « Bitcoins » relevaient en principe de la catégorie des plus-values sur biens meubles.

Traitement des opérations d'échange entre actifs numériques	Pas d'imposition: elles sont considérées, en effet, comme neutres tant que les actifs numériques ne sont pas convertis en monnaie ayant cours légal, ou utilisés pour acquérir un bien ou un service. Lorsque cette conversion ou cette utilisation intervient, les plus-values réalisées sont imposées au taux de 30 % (12,8 % d'impôt sur le revenu et 17,2 % de prélèvements sociaux).
Traitement de la TVA	Le régime dépend de l'attribution, ou non, d'une contrepartie à un paiement en actifs numériques et de la nature de cette contrepartie (délivrance d'un bien ou fourniture d'un service). En revanche, les échanges de crypto-actifs sont assimilés à des opérations financières exonérées de TVA.
Imposition des plus-values	La loi de finances pour 2022 a permis d'apporter de nouvelles clarifications en matière d'imposition des plus-values. Il est désormais proposé aux particuliers cédants d'actifs numériques de pouvoir opter s'ils le souhaitent à une imposition au barème progressif. Par ailleurs, l'appréciation des opérations réalisées à titre occasionnel ou professionnel a été facilitée (en tenant compte de la part que représentent les revenus liés à la cession d'actifs numériques dans les revenus totaux).

Avec MiCA, la nouveauté de la réglementation des stablecoins

Le règlement MiCA a également réglementé des champs jusqu'à présent non traités spécifiquement en droit français et notamment les *stablecoins*. Les émetteurs de *stablecoins* ayant atteint une échelle dite systémique

seront soumis à la supervision de l'Autorité bancaire européenne (ABE) et les *stablecoins* devront respecter plusieurs règles : avoir un émetteur identifié, maintenir des réserves à hauteur de 1 pour 1 pour couvrir toutes les créances ; prévoir un droit de rachat permanent ; limites à l'utilisation des *stablecoins* assis sur des devises non européennes comme moyen de paiement. Par ailleurs, le texte demande aux émetteurs de *stablecoins* d'appliquer les mêmes règles que la monnaie électronique.

En revanche, les NFTs ne sont a priori pas couverts par la réglementation européenne, en dehors de certains cas particuliers de collection ou potentiellement d'unités fractionnaires de NFT. Les entités décentralisées (DEX, *DeFi* et protocoles de prêt) ne sont pas non plus couvertes par la réglementation européenne, mais ceci est à réévaluer dans le cadre d'une clause de révision (18 mois suivant l'entrée en vigueur de la réglementation).

Prochaines étapes découlant du règlement MiCA :
- Le règlement MiCA a été adopté le 20 avril 2023, en même temps que le règlement dit TFR (*Transfer of Funds Regulation* – voir infra).
- L'entrée en vigueur est prévue en 2024, soit 18 mois après la date de publication au Journal officiel de l'UE.
- Une période transitoire supplémentaire de 18 mois sera accordée aux acteurs bénéficiant d'un enregistrement ou d'un agrément de prestataire de services français (PSAN), qui pourront pendant cette période continuer à offrir leurs services au public français en attendant l'obtention de leur agrément MiCA en tant que prestataire de services européen (PSCA).

L'utilisation de la blockchain pour l'échange de titres financiers

S'agissant de l'utilisation de la *blockchain* pour l'échange de titres financiers, la France a ouvert cette possibilité pour les titres non cotés dès 2017. Grâce à l'adoption récente du règlement régime Pilote, il est désormais possible de tester cette technologie sur le champ des titres cotés.

Le régime pilote consiste en un cadre expérimental d'une durée initiale de trois ans, dédié à l'utilisation de la technologie *blockchain* en matière de marchés financiers. Il a été adopté en 2022, pour entrer en application le 23 mars 2023. Particulièrement soutenu par la France, il doit permettre de développer un marché secondaire de titres financiers « tokenisés » *(security tokens)* en levant certaines obligations bloquantes de la réglementation actuelle en matière d'échange de titres financiers. L'innovation de ce régime pilote repose dans le fait que pour la première fois un texte européen d'application directe autorise certains acteurs de marché à déroger à certaines exigences de la réglementation de droit commun. Un point important de ce régime pilote réside par ailleurs dans le fait qu'il sera désormais possible d'utiliser la *blockchain* pour échanger des titres financiers, à la fois en délivrant les titres par la *blockchain* (delivery) et en transférant la contrepartie de paiement (payment), ce qui nécessitera à terme l'utilisation d'une CBDC, et dans l'attente, ouvre la possibilité d'utiliser de la monnaie de banque commerciale « tokenisée » ou des e-money *tokens* au sens du règlement MiCA.

Encadré : l'intérêt des acteurs français pour la *blockchain* en matière financière

- Dès 2015, la Caisse des Dépôts a, conformément à ses missions de service public, développé une expertise dans le domaine de la technologie *blockchain* en lançant un programme Blockchain & Crypto-actifs afin d'explorer les opportunités du secteur financier français. Elle a participé à l'incubation de différents projets au sein de l'écosystème, a contribué à de nombreuses expérimentations de place (sous l'égide de La Banque de France notamment). En septembre 2021, elle obtient l'enregistrement en tant que Prestataire de Services sur Actifs Numériques (PSAN).

- Le groupe Société Générale a été précurseur dans les émissions d'obligations tokenisées dès avril 2019, *via* l'émission de 100 millions d'euros d'obligations sous forme de « *security tokens* » sur la *blockchain* publique Ethereum[42]. Depuis, SG Forge est la filiale dédiée pour expérimenter différentes solutions disruptives basées sur la *blockchain* et développer de nouvelles activités sur les marchés de capitaux : émission d'obligations tokenisées adossées à des prêts immobiliers[43] (juillet 2022), puis première transaction dans la *DeFi* en collatéralisant des obligations tokenisées pour réaliser un emprunt en stablecoin DAI sur la plateforme de prêt de MakerDAO (janvier 2023)[44].

- Dans la sphère publique, Bpifrance est l'établissement qui contribue le plus au secteur Web3 en France. Le groupe réalise des investissements dans des fonds spécialisés qui accompagnent les startups dont le modèle repose sur une *blockchain*[45]. Sur plus de 90 start-up Web3 financées dans l'Hexagone, Bpifrance a participé à 70 % des opérations. La banque publique d'investissement a distribué 30 millions de financements aux entreprises du secteur sous la forme de subventions et de prêts, investi 10 millions en direct dans six start-up (dont Ledger, Acinq, Arianee et Dogami), et près de 35 millions d'euros dans plusieurs fonds crypto[46].

[42] https://www.societegenerale.com/fr/actualites/newsroom/societe-generale-emet-la-premiere-obligation-securisee-sous-forme-de-security

[43] https://journalducoin.com/economie/societe-generale-pret-7-millions-dollars-dai-makerdao/

[44] https://www.sgforge.com/refinancing-dai-stablecoin-defi-makerdao/

[45] https://www.bpifrance.fr/nos-solutions/investissement/investissement-expertise/fonds-web3

[46] https://www.usine-digitale.fr/article/en-2023-bpifrance-continuera-a-soutenir-le-secteur-de-la-blockchain-et-des-cryptos.N2092391

	Traitement actuel en droit français	Traitement à venir en droit de l'UE
Crypto-actifs « classiques »	Enregistrement obligatoire des prestataires, notamment pour la LCB-FT, renforcé récemment pour les nouveaux entrants ; agrément facultatif pour la partie réglementation financière.	Régime obligatoire pour les deux volets.
Stablecoins	Pas de catégorie juridique dédiée en droit français, mais concept inclus dans la catégorie d'actifs numériques.	Catégorie juridique et réglementation dédiées.
NFT	Pas de catégorie juridique dédiée en droit français, inclusion incertaine dans la catégorie d'actifs numériques.	Essentiellement non couverts par le droit de l'UE.
Security tokens	Possibilité d'utiliser la *blockchain* pour des activités très limitées sur les titres financiers.	Le régime pilote permet de tester la *blockchain* y compris sur des activités liées aux titres financiers cotés.

Une approche commune en matière de LCB-FT

Les régimes français (PACTE) et européen (MiCA) sont complétés par des corpus traitant spécifiquement de la lutte contre le blanchiment et le financement du terrorisme (LCB-FT). Au niveau international, il s'agit de standards du Groupe d'action financière (GAFI), destinés à être repris par les textes de droit de l'UE ou de droit interne.

Encadré : les risques en matière de LCB-FT

Les crypto-actifs peuvent être détournés et utilisés pour des pratiques de blanchiment ou de financement du terrorisme.

En matière de blanchiment d'argent, les criminels peuvent utiliser des actifs numériques pour transférer des fonds ou acheter des

biens de manière anonyme. Cela peut être particulièrement vrai en ce qui concerne le blanchiment des produits de la drogue ou le blanchiment de fraude fiscale. Les activités qui convertissent des actifs numériques en monnaie fiduciaire sont donc particulièrement concernées.

En matière de financement du terrorisme, le risque est lié à l'envoi de fonds à des fins terroristes ou à l'acquisition de biens (par exemple des armes) de manière anonyme.

Pour autant, l'utilisation des crypto-actifs à des fins criminelles reste marginale, tant par rapport à l'utilisation totale des crypto-actifs (0,15 %en 2021) selon Chainanalysis, que par rapport à l'utilisation de devises à des fins criminelles.

Des éléments détaillés figurent en Annexe 4

Deux textes du droit de l'UE ont donc repris les standards du GAFI, en particulier sur les obligations en matière de transferts de crypto-actifs. Ils transposent en particulier les exigences en matière de LCB-FT liées aux transferts de fonds classiques aux crypto-actifs. Outre la levée du pseudonymat sur les échanges de pair à pair et l'obligation de déclarer aux autorités compétentes les transactions supérieures à 1 000 € sur les plateformes d'échange, les textes prévoient par ailleurs des dispositions contraignantes sur les « *unhosted wallets* » (portefeuille non hébergé) permettant de conserver en lieu sûr et de manière anonyme des crypto-actifs avec une clé publique déconnectée de la sphère réelle. Si un client envoie ou reçoit plus de 1 000 euros vers ou depuis son propre portefeuille, la plateforme d'échange devra vérifier si le portefeuille non hébergé est effectivement détenu ou contrôlé par ce client. Si l'écosystème déplore le risque pour les acteurs d'être incités à se tourner vers des solutions étrangères moins vertueuses, le manque de solutions

techniques en capacité de supporter un tel volume de transactions est également souligné.

À l'échelle mondiale, des approches différentes en matière de réglementation ont néanmoins été construites. Ci-dessous un panorama des approches les plus pertinentes dans le cadre de notre rapport.

Encadré : état des lieux de la réglementation *blockchain*[47] et actifs numériques à l'international

À l'international

Unidroit

L'Institut international pour l'unification du droit privé (UNIDROIT[48]) a mené en février 2023 une consultation publique concernant un ensemble de projets de principes et de commentaires sur les actifs numériques et le droit privé. Fruit de deux années de travail d'un groupe d'experts parmi lesquels deux français, qui représentaient la France *via* le Haut Comité Juridique de la Place Financière de Paris, ce projet vise notamment à mettre en place un nouveau régime de droit de propriété des actifs numériques, prévoir une règle de conflits de lois, déterminer les conséquences d'une faillite d'un conservateur d'actifs numériques et reconnaître l'efficacité d'une sûreté sur actifs numériques.

[47] *Voir le rapport Reuters de 2022 « Cryptocurrency regulations by country » https://drive.google.com/file/d/1DJnWelgscWQSsWTYgJEJHLKv1buaARrC/view ou pour une vue sur l'ensemble des crypto-actifs, voir le document « PwC Annual Global Crypto Tax Report » de 2022 : https://www.pwc.com/gx/en/financial-services/pdf/global-crypto-tax-report-2022.pdf*

[48] *https://www.unidroit.org/fr/travaux-en-cours/actifs-numeriques/actifs-numeriques-et-droit-prive-consultation-publique/*

Le projet traite du droit matériel, et non de la réglementation, comme MiCA (qui ne se prononce pas sur la nature juridique des actifs numériques).

Il s'agit d'un projet très ambitieux, assez proche du futur droit américain prévu à l'article 12 des UCC modifié en janvier 2022.

Une réponse à cette consultation a été préparée par plusieurs associations françaises.

G20

Par ailleurs, des réflexions ont été engagées pour mieux encadrer les activités liées aux actifs numériques. Tout récemment à l'occasion du G20, le FSB, le FMI et la BIS ont présenté le 25 Février 2023[49] des recommandations pour établir un cadre réglementaire mondial pour le secteur des crypto-actifs.

Le FSB[50] et la BIS[51] ont tous deux pris des positions en matière de traitement prudentiel pour les expositions en crypto-actifs.

Cependant, l'introduction des traitements prudentiels préconisés par ces deux organismes supra nationaux dans la réglementation européenne semble prématurée et soulève de nombreux problèmes en cours de discussion au Parlement européen :

- Les marchés des crypto-actifs sont des marchés mondiaux et il convient d'éviter les distorsions de concurrence au détriment des acteurs européens.

[49] https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/1st%20FMCBG%20Chair%20Summary.pdf

[50] *Financial Stability Board, 16 February 2022, « Assessment of Risks to Financial Stability from Crypto-assets », available: https://www.fsb.org/wp-content/uploads/P160222.pdf*

[51] *Basel Committee on Banking Supervision, December 2022, « Prudential treatment of cryptoasset exposures »: https://www.bis.org/bcbs/publ/d545.pdf*

- Le traitement prudentiel devrait être le même, quel que soit le type d'établissement exposé aux actifs numériques. Si le traitement des expositions aux crypto-actifs était introduit, seules les banques seraient soumises à un tel régime et les activités pourraient se développer dans le « *shadow banking* ».
- Le concept de crypto-actifs dans le cadre de la future législation devrait être conforme à la législation européenne existante. En effet, si les titres financiers tokenisés devaient être assimilés à des actifs numériques, cela aurait une incidence insurmontable pour l'application du régime pilote, les exigences prudentielles requises étant de 1 250 %.

FMI

Le 8 février 2023, le Conseil d'administration du Fonds monétaire international (FMI) a discuté d'un document de conseil intitulé *Elements of Effective Policies for Crypto Assets* qui fournit des orientations aux pays membres du FMI sur les éléments clés d'une réponse politique appropriée aux crypto-actifs. Les objectifs du document sont conformes au mandat du FMI, qui consiste à soutenir la stabilité économique et financière de ses membres. Le document répond aux questions soulevées par les pays membres du FMI sur les avantages et les risques des crypto-actifs et sur la manière de structurer des réponses politiques appropriées. Il rend opérationnels les principes énoncés dans le Bali Fintech Agenda (FMI et Banque mondiale 2018).

Le document présente un cadre de neuf grands principes[52] qui peuvent aider les membres à élaborer une réponse politique complète, cohérente et coordonnée.

[52] https://www.imf.org/en/News/Articles/2023/02/23/pr2351-imf-executive-board-discusses-elements-of-effective-policies-for-crypto-assets

États-Unis :

Après le scandale FTX et les nombreuses débâcles du marché des crypto-actifs en 2022, les régulateurs bancaires fédéraux américains (FED[53], OCC[54], FDIC[55]) ont eu pour objectif affiché d'éviter toute contagion entre le secteur bancaire traditionnel et l'écosystème des crypto-actifs.

- D'une part, ils ont publié dans un communiqué conjoint le 23 février 2023[56] des lignes directrices en matière de contrôle des risques et de liquidité à destination du secteur bancaire. À ce titre, deux risques majeurs sont mis en avant :
  - Les dépôts placés par une entreprise crypto pour le compte de ses clients, et donc susceptibles de faire l'objet de retraits massifs, en cas de panique, d'événement de marché ou d'incertitude.
  - Les dépôts constitués dans le cadre d'une réserve pour l'émission de stablecoin, également susceptibles d'induire un stress de liquidité en cas de mouvements de rachat massif ou de dislocation de marchés.

- D'autre part, ils ont engagé des procédures à l'encontre de certains acteurs en les sanctionnant lourdement financièrement du fait de la violation du droit fédéral. Plusieures décisions de sanction ont été prononcées en février 2023, en particulier :
  - Les services de *staking* proposés par Kraken ont été analysés par la SEC comme des opérations qui s'apparentent à des titres générant un rendement, et donc assimilés à des *security tokens* n'ayant pas été dûment enregistrés comme tels auprès de ses services : une amende de 30 millions de dollars[57] et une interdiction de proposer ses services de *staking* sur le sol américain jusqu'à nouvel ordre.
  - La société Paxos s'est vu reprocher une mauvaise appréciation des risques dans ses relations avec Binance en ayant laissé le BUSD[58] circuler sur d'autres *blockchain* que Ethereum, unique réseau autorisé par la NYDFS[59] : Interdiction d'émettre tout nouveau BUSD depuis le 21 février 2023, avec un remboursement des BUSD en circulation au plus tard avant Janvier 2024.

En Italie[60] :

- Formulation d'une définition des crypto-actifs dans le budget rectificatif de décembre 2022.
- Adoption d'une fiscalité plus avantageuse avec un taux d'IS de 26 % pour les bénéfices supérieurs à 2000 euros (en France les investisseurs sont soumis au PFU de 30 % si le total des cessions de l'année dépasse les 305 €).
- Adoption d'un système permettant aux investisseurs de reporter leurs pertes d'une année sur l'autre, ce qui n'est pas possible en France.

Au Royaume-Uni :

- Adoption d'une mesure favorable aux investisseurs étrangers en crypto-actifs qui seront exemptés d'impôt sur les plus-values, ce

[53] *Board of Governors of the Federal Reserve System.*

[54] *Office of the Comptroller of the Currency.*

[55] *Federal Deposit Insurance Corporation.*

[56] *https://www.occ.gov/news-issuances/news-releases/2023/nr-ia-2023-18.html*

[57] *https://www.sec.gov/news/press-release/2023-25*

[58] *Stablecoin de Binance.*

[59] *Département des services financiers de l'État de New York.*

[60] *Source: https://journalducoin.com/Bitcoin/taxation-cryptos-italie-augmente-26-imposition-plus-values/#:~:text=Selon%20les%20nouvelles%20r%C3%A8gles%20approuv%C3%A9es,euro%20(ou%20monnaie%20fiat).*

qui est susceptible de favoriser l'attractivité du territoire et d'attirer les investisseurs étrangers[61].

- Alors que l'Union Européenne a développé une réglementation spécifique pour les acteurs émergents de la crypto-monnaie, le Royaume-Uni a jusqu'à présent choisi de soumettre cette industrie aux règles existantes qui s'appliquent aux services financiers traditionnels. Cette approche réglementaire vise à créer des conditions de concurrence équitables entre les acteurs traditionnels de la finance et les acteurs de la crypto-monnaie. L'objectif est de garantir que toutes les parties respectent les mêmes normes de réglementation pour assurer la sécurité et la protection des consommateurs tout en favorisant l'innovation et la croissance de cette industrie[62].

Au Japon :

- Le Japon a créé le Japanese Virtual Currency Exchange Association et le Japan STO Association qui promeuvent la conformité réglementaire et cherchent à établir et étendre les meilleures pratiques et garantir la conformité réglementaire.

En Estonie :

- Il est obligatoire pour les entreprises proposant des services de crypto-monnaie d'avoir un bureau enregistré, une direction, et un bureau en Estonie. Cela inclut les entreprises proposant des wallets et des plateformes d'échanges.

Au Portugal :

- Le gouvernement portugais a publié un Digital Transition Action Plan avec 12 piliers, incluant notamment l'autonomisation numérique des personnes, la transformation numérique d'entreprises, et la numérisation de l'État.
- Le plan établit aussi un environnement réglementaire flexible pour tester et développer des technologies.
- Le régime de taxation inhabituel attire également beaucoup de traders. Les individus avec une « haute valeur culturelle ou économique » bénéficient d'exemptions et de réductions de taxe pendant 10 ans.

En Allemagne :

- Le gouvernement allemand a été un des premiers à proposer une certitude légale aux institutions financières, leur permettant de détenir des crypto-actifs. Les personnes physiques et morales peuvent acheter ou échanger des crypto-actifs tant que c'est fait par un *custodian* / une plateforme d'échange agréée.
- Vendre des cryptos détenus depuis plus d'un an est exempté de taxes, les gains de moins de 600 euros détenus moins d'un an par un individu sont également exemptés.

En Suisse :

- Le régulateur suisse des marchés financiers a défini les obligations d'enregistrement pour toutes les entreprises de crypto-actifs, dont les opérations kiosk de crypto-monnaies.
- La régulation des *tokens* est aussi très avancée avec la loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués qui donne un cadre et définit l'échange de droits par des registre électroniques distribués.
- La politique suisse d'exemption des gains par le capital de private wealth assets de l'impôt sur le revenu s'applique aussi aux crypto-actifs. Les gains venant de la vente de crypto-actifs ne

[61] https://www.coindesk.com/policy/2023/01/01/uk-enforces-crypto-tax-break-for-foreigners-using-local-brokers/

[62] https://www.lesechos.fr/finance-marches/marches-financiers/regulation-des-cryptos-londres-pret-a-faire-concurrence-a-lunion-europeenne-1904031

sont pas soumis aux taxes et les pertes venant de la vente de crypto-actifs ne sont pas déductibles d'impôts.

Au Salvador :

- Le Bitcoin a été adopté comme monnaie officielle, donc non taxée. La seule taxe crypto à payer est 10 % de taxe sur la valeur ajoutée pour financer la construction et les services de la ville crypto qu'ils essayent de construire.
- Pour encourager des investissements étrangers, le gouvernement a exempté les investisseurs étrangers dans les crypto-actifs de payer la taxe sur le revenu et sur les gains en capitaux sur Bitcoin. Un programme de Golden Visa existe également : un permis de résidence sera octroyé aux investisseurs crypto quand ils investissent suffisamment dans les cryptos.
- Le pays fait toutefois face à des critiques des établissements financiers comme le FMI.

Un positionnement particulier sur la mise en place d'une identité numérique

L'identité numérique peut être implémentée de deux manières aujourd'hui, l'une respectueuse du droit fondamental à la vie privée et du principe de séparation des pouvoirs, l'autre non souhaitable car donnant aux pouvoirs publics des prérogatives qui ne relèvent pas de leur compétence et pour lesquels ils n'ont pas de légitimité, soit la possibilité de contrôler la vie privée de sa population.

Pour mettre en œuvre l'identité numérique en respectant la première manière, des gardes-fous sont nécessaires.

C'est pourquoi, la France soutient globalement la proposition d'harmonisation de l'identification électronique en vue de faciliter les usages numériques pour l'ensemble des citoyens européens. Le Portefeuille Européen d'Identité Numérique (PEIN) est considéré comme une solution viable afin de renforcer la sécurité et la confiance pour les services en ligne.

Deux niveaux de sécurité sont tout de même requis quant à l'introduction du PEIN en France :

- Un niveau de sécurité substantiel et optionnel, garantissant une accessibilité simple au quotidien pour tous les citoyens européens ;
- Puis un niveau élevé pour l'accès aux services publics, pour les plus sensibles, et par le biais d'une infrastructure sécurisée et contrôlée par les États membres.

Pour faciliter l'adoption du PEIN, la France exige tout de même un certain niveau de flexibilité à l'introduction d'un identifiant unique et persistant obligatoire, avec la possibilité pour un citoyen européen de formuler une demande de nouvel identifiant.

Plusieures remarques ont tout de même été soulevées en vue d'une clarification de la proposition :

- La certification des attributs relevant du secteur public ;
- La certification de sécurité du PEIN, et le maintien d'un examen par les pairs ;
- La préservation du rôle central des autorités nationales de certification de cybersécurité, qui assureront le rôle à la fois de superviseur et de certificateur.

Le rapport de la commission européenne[63], daté de juillet 2022, pointe le retard de la France en termes d'infrastructure *blockchain* dans le cadre de la digitalisation de son administration.

[63] *https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_France_vFinal_0.pdf*

Encadré : avancées européennes en matière d'identité numérique

- Le Parlement européen ainsi que le Conseil de l'Union européenne ont adopté en 2014 le règlement eIDAS (electronic IDentification, Authentication and trust Services), visant à accroître la confiance dans les échanges de données en Europe. Ce règlement établit un socle commun de normes et standards à l'échelle européenne (certains standards ETSI à propos des profils de signature par exemple) pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.

- La Commission européenne souhaite généraliser l'EU digital ID Wallet, un portefeuille européen d'identité numérique. Ce portefeuille serait harmonisé, facultatif et accessible à l'ensemble des citoyens, résidents et entreprises de l'UE, avec une obligation de mise en place par les États membres d'ici à 2024. Son utilisation a vocation à être gratuite pour les personnes physiques, que ce soit pour leur authentification ou leur révocation. Le modèle d'architecture informatique permettant l'intégration de l'EU digital ID Wallet n'est pas encore déterminé et n'indique pas clairement l'utilisation ou non de la technologie *blockchain*, dont l'immuabilité des données reste un frein au regard des principes RGPD. Techniquement, il convient néanmoins de rappeler que la *blockchain* n'est pas incompatible *by design* aux principes RGPD, mais la définition des caractéristiques de ces portefeuilles numériques et leur utilisation permettra de déterminer la pertinence de retenir ou non la technologie *blockchain.*

- L'intégration des attributs d'identité sera contrainte par des normes techniques communes au sein de l'UE, de sorte à garantir un niveau de garantie « élevé ». En parallèle, la Commission européenne lance une boîte à outils réglementaire *(toolbox)* pour la *blockchain*, destinée à fournir un cadre d'expérimentation paneuropéen pour les solutions technologiques innovantes impliquant *blockchains* et registres distribués.

- En permettant une coopération étroite et structurée entre le secteur public et le secteur privé, en imposant des standards et des pratiques communes que les États membres devront respecter, cette initiative a vocation à renforcer la sécurité juridique du Web 3.

- L'introduction du PEIN se fera par la révision du règlement eIDAS. L'objectif principal est de pouvoir fournir un parcours utilisateur simple, efficace, et avec un haut niveau de confiance dans toute l'UE en utilisant une identité numérique unique. La révision de ce texte prône l'utilisation de *blockchains* privées ou de consortium conformes aux normes européennes, et dont l'une des clefs de l'interopérabilité entre celles-ci serait l'EU digital ID Wallet.

4 Les pouvoirs publics peuvent actionner plusieurs leviers pour capitaliser sur ces avancées techniques et réglementaires, pour continuer à sécuriser le cadre juridique et pour développer des services clés pour notre souveraineté

4.1. CAPITALISER SUR LE CADRE JURIDIQUE FRANÇAIS POUR SOUTENIR LES ACTEURS NATIONAUX ET ATTIRER DES ACTEURS ÉTRANGERS DE LA *BLOCKCHAIN*

Les pouvoirs publics ont pris la mesure du caractère stratégique de la technologie *blockchain* pour la compétitivité du pays. La France s'est ainsi positionnée pour être un acteur stratégique de cette technologie à la fois sur le plan interne – avec la loi PACTE notamment, et sur le plan européen – avec les négociations sur le règlement MiCA et le régime Pilote. Par ailleurs, les pouvoirs publics maintiennent une approche ouverte en matière de *blockchain*. Par exemple, le ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique ainsi que le ministre délégué au Numérique ont indiqué vouloir soutenir le développement de l'écosystème, à travers son financement par le plan d'investissement « France 2030 ». Ce plan vise notamment à soutenir la recherche et le développement sur des segments innovants (intelligence artificielle, 5G, *blockchain*). Le gouvernement continue à être force de proposition pour structurer et professionnaliser l'écosystème *blockchain* français : une mission a été confiée à l'inspection générale des finances pour appréhender de manière transverse le sujet des NFT – de manière à dépasser une approche souvent en silo des différents ministères concernés, ou encore une mission exploratoire sur le métavers a été réalisée sur demande du ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique et du ministre de la Culture. En outre, la première commission de normalisation du Métavers s'est tenue fin février 2022 en présence du ministre délégué au Numérique pour construire un métavers durable, éthique, responsable et accessible et amorcer une transition générale du Web 2 au Web 3.

Au-delà de ces sujets, plusieurs vecteurs de soutien pourraient permettre à la France de capitaliser sur ses avancées techniques et réglementaires.

- Faire davantage valoir l'intérêt du cadre français auprès des acteurs français et étrangers ;
- Assurer la mise en œuvre opérationnelle du cadre de la loi PACTE en matière d'accès des prestataires d'actifs numériques à la banque et à l'assurance ;
- Assurer une approche réglementaire coordonnée avec des interlocuteurs transverses dédiés ;
- Passer du régime PACTE au régime MiCA.

Faire davantage valoir l'intérêt du cadre français auprès des acteurs français et étrangers

La mise en avant de l'intérêt du cadre français apparaît essentielle, pour à la fois prévenir le risque de départ d'acteurs français et inciter des acteurs étrangers à s'établir en France. Si la France semble bénéficier d'atouts ce qui lui permet d'être attractive, comme en témoigne l'implantation en France de Binance, il reste que cet objectif doit être renforcé. Cela requiert la mobilisation d'acteurs privés ou de regroupements d'acteurs privés, tout comme la mobilisation des autorités françaises.

Ce serait notamment le rôle des acteurs français de la supervision, à savoir l'Autorité des marchés financiers et la Banque de France en ce qui concerne la réglementation des prestataires de services sur actifs numériques. À l'approche de l'entrée en vigueur du règlement MiCA, il serait notamment utile d'avoir une communication internationale pour attirer les acteurs qui voudraient préparer, *via* l'agrément de prestataire de services sur actifs numériques français, l'entrée dans l'agrément obligatoire MiCA.

Il reviendrait également au ministère de l'économie et des finances de mettre en avant l'ensemble des mesures réglementaires et fiscales (par exemple les régimes d'impatriés) favorables à l'écosystème, par rapport aux possibilités offertes dans les autres pays.

Recommandation n° 1

Organiser une communication internationale portée par les autorités publiques afin de faire valoir l'intérêt du cadre juridique et fiscal français auprès des acteurs étrangers qui souhaitent opérer en Europe.

Assurer la mise en œuvre opérationnelle du cadre de la loi PACTE en matière d'accès des prestataires d'actifs numériques à la banque et à l'assurance

L'accès effectif aux services bancaires reste difficile pour les acteurs. Des difficultés sont en effet à signaler tant du côté des usagers en actifs numériques que du côté des prestataires sur actifs numériques. Pour les premiers, sont notamment évoquées des cas de blocage d'opérations ; pour les seconds, la domiciliation bancaire, l'accès aux services de paiement ainsi que le maintien de la relation d'affaires sont des points souvent problématiques, les conduisant régulièrement à recourir à des établissements bancaires étrangers.

Ces difficultés ne sont pas nouvelles et avaient d'ailleurs été identifiées dès les discussions relatives à la loi PACTE, conduisant les parlementaires à envisager qu'en cas d'absence de solution bancaire, un établissement comme La Banque de France ou La Banque postale, soit désigné. C'est finalement un dispositif de recours devant l'ACPR qui a été retenu en cas de refus par un acteur bancaire, mais force est de constater que ce dispositif se borne à déclencher la procédure de droit au compte classique, très frustre au regard des besoins des entreprises de l'écosystème. Par ailleurs, du côté des établissements bancaires, de fortes réticences à entrer en relation d'affaires avec les prestataires sur actifs numériques persistent, malgré la supervision des prestataires par l'AMF et l'ACPR.

Encadré : les dispositifs de la loi PACTE concernant l'accès de l'écosystème aux services bancaires

La loi PACTE a prévu une exigence d'accès non discriminatoire aux services des établissements de crédit pour les prestataires enregistrés ou agréés et les émissions visées. Elle a prévu qu'un recours puisse s'exercer pour les acteurs enregistrés ou ayant obtenu un agrément, ou réalisant une émission de jetons ayant reçu un visa. Il prévoit en effet la possibilité de saisine de l'ACPR en cas de refus, le cas échéant implicite, des établissements de crédit d'accorder l'accès aux services bancaires. L'ACPR se prononce dans un délai de deux mois à compter de la saisine. Elle peut, le cas échéant, décider, dans ce délai, de mettre en œuvre à l'égard de l'établissement ses pouvoirs de contrôle et de sanction et proposer au demandeur de saisir en son nom et pour son compte la Banque de France d'une demande de désignation d'un établissement de crédit.

Il apparaît dès lors opportun pour les pouvoirs publics de rappeler au secteur bancaire la portée des enregistrements, visas et agréments, dans le cadre desquels les prestataires de services sur actifs numériques sont assujettis à l'ensemble des règles de LCB-FT. Par ailleurs, l'édiction de lignes directrices de l'ACPR, réclamée de longue date par les acteurs de l'écosystème, permettrait de clarifier le fait que le statut de prestataire de services sur actifs numériques suffit pour garantir la fiabilité de cet acteur du point de vue de la LCB-FT.

Par ailleurs, l'accès aux services de conservation reste limité pour les gestionnaires d'actifs qui souhaiteraient proposer des fonds en crypto-actifs ou des *security tokens*. En effet, la réglementation impose de faire appel à un dépositaire agréé par l'AMF pour la conservation de tous les actifs des Organismes de Placement Collectifs enregistrés en France. Cela implique donc de recourir à un établissement bancaire dûment agréé. À ce stade, un seul établissement dispose du statut de prestataire de services sur actifs numériques et peut donc offrir un service de conservation de crypto-actifs, et la plupart des établissements n'ont pas intégré les *tokens* (tant crypto-actifs que *security tokens*) dans leurs modèles opérationnels. Les fonds d'investissement (selon la catégorie Autres FIA de la directive

AIFM[64]) peuvent toutefois mettre en place des holdings dédiées pour détenir indirectement des jetons.

Enfin, l'écosystème a des difficultés d'accès à l'assurance. L'obligation pour un prestataire de disposer d'une assurance responsabilité civile professionnelle (ou de fonds propres suffisants) ne vaut à ce stade que pour les prestataires qui souhaitent disposer de l'agrément, mais dans le cadre du régime MiCA, le prestataire sera concerné par l'obligation de disposer de fonds propres suffisants ou d'une police d'assurance dans l'UE. Il serait utile que les pouvoirs publics prennent l'attache des représentants des assureurs pour préparer l'application du régime MiCA.

Recommandation n° 2

Assurer la mise en œuvre effective de la loi PACTE en matière d'accès des prestataires d'actifs numériques aux services classiques de la banque et de l'assurance, en associant tous ces acteurs aux processus opérationnels et en encourageant l'ACPR, le régulateur du secteur financier, à formuler les lignes directrices appropriées.

Assurer une approche réglementaire coordonnée avec des interlocuteurs transverses dédiés

Une difficulté que rencontrent les acteurs de l'écosystème est la diversité des interlocuteurs publics auxquels ils peuvent être confrontés et le manque de coordination entre eux. Au seul niveau des prestataires de services sur actifs numériques par exemple, la loi PACTE avait prévu la mise en place d'un guichet unique par l'Autorité des marchés financés, chargé d'internaliser les relations avec l'Autorité de contrôle prudentiel et

[64] https://www.amf-france.org/en/news-publications/news-releases/amf-news-releases/amf-position-regarding-alternative-investment-fund-managers-directive-aifmd-review

de régulation. En pratique, ce guichet unique apparaît artificiel, les prestataires devant régulièrement recourir à l'une ou l'autre des autorités selon le pan de leur dossier d'enregistrement. Cela tend à rendre les procédures longues et coûteuses, et requiert d'autant plus le recours à des conseils privés. Dans le cadre de cette procédure, il apparaît important que les acteurs sollicitant un enregistrement ou agrément puissent bénéficier de retours clairs de la part des autorités sur le niveau de conformité attendu.

Au-delà de ce cas particulier de l'enregistrement des prestataires de services sur actifs numériques, il n'existe en tout état de cause pas de coordinateur unique en matière de droit applicable dans d'autres domaines qui pourtant peuvent s'appliquer à un même cas d'usage : droit de la consommation, jeux d'argent, droit de la concurrence, etc. Pour les acteurs de l'écosystème, il est dès lors très difficile de pouvoir disposer de réponses claires des autorités publiques, source d'insécurité juridique.

Plusieurs autres éléments plaident en faveur de la mise en place d'un coordinateur unique dédié aux sujets *blockchain* :

- Ce coordinateur pourrait définir une approche commune en matière de *blockchain*, en particulier pour clarifier le positionnement des autorités françaises qui peine à trouver un équilibre et du sens pour les acteurs de l'écosystème, avec d'une part une ouverture favorable au moment de la loi PACTE et d'autres part une position relativement fermée à l'égard des projets de paiement sur *blockchain* ;
- Il pourrait apporter des réponses plus claires dans le cas des nombreux cas d'usage qui peuvent relever de plusieurs administrations différentes ;
- Il serait force de proposition pour ouvrir des chantiers juridiques (par exemple envisager des modifications sur plusieurs codes – code civil, code de commerce, code monétaire et financier, etc.) ;
- Alors que la majorité de l'écosystème déplore un manque de formation et d'expertise des pouvoirs publics sur les enjeux de la technologie *blockchain*, il serait possible d'associer à cette entité administrative un comité scientifique national, qui pourrait s'inspirer de l'expérience de la chamber of digital commerce aux États-Unis qui organise des sessions

régulières de formation à l'attention du législatif et de l'exécutif. Cela fait écho à une précédente recommandation de la mission « Verrous » conduite pour la DGE en 2019: « *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* ».

À l'image d'autres coordinateurs dédiés aux technologies de rupture (IA, quantique, cyber, etc.), le coordinateur national *blockchain* pourrait être rattaché au Secrétariat général pour l'investissement (SGPI) ou à la Direction générale des entreprises (DGE).

Une fois ce coordinateur désigné et établi dans ses fonctions, il pourrait également animer un réseau de conseillers par ministère, formés aux enjeux du Web 3, sur le même modèle que ce qui a été fait en matière de formation aux enjeux numériques de la sécurisation des infrastructures critiques de l'État.

Recommandation n° 3

Mettre en place un coordinateur national *blockchain* afin de définir une approche commune des autorités françaises et piloter les chantiers prioritaires qui auront été identifiés dans ce domaine.

Passer du régime PACTE au régime MiCA

Le régime issu de la loi PACTE en 2019, ainsi que de la loi de finances de la même année, avait pour ambition de fournir un cadre complet pour les crypto-actifs, de manière à donner de la visibilité aux acteurs, à fournir un cadre attractif, et à favoriser le développement de l'écosystème.

Le régime issu de la loi PACTE et complété par la suite a prévu un enregistrement de la plupart des prestataires de services sur actifs numériques. Malgré un délai raisonnable de mise en conformité, beaucoup de ces prestataires ont rencontré des difficultés à obtenir l'enregistrement, à la fois en raison de l'évolution des règles (élargissement des activités assujetties conduisant une même entité à devoir plusieurs fois soumettre un dossier), d'un manque de clarté des règles dont le corpus n'avait pas été éprouvé, du fort niveau d'exigence attendu, et des capacités limitées des superviseurs. Il apparaît dès lors opportun de tirer les leçons de la mise en place de la réglementation française pour prévenir de telles difficultés dans l'application de la réglementation européenne, à plus forte raison que cette dernière se fonde sur un régime entièrement obligatoire et non partiellement comme en droit français.

Il est tout d'abord impératif de donner le plus de visibilité possible aux acteurs et d'éviter de leur imposer des normes instables d'ici l'entrée en vigueur de l'agrément obligatoire européen. Aussi était-il préférable de ne pas revenir sur l'équilibre trouvé par la loi PACTE. Pour autant, à la suite de la faillite de la société FTX, une initiative du Sénat a consisté à rendre l'agrément français obligatoire, ce qui aurait alors imposé aux acteurs français de se mettre en conformité au corpus national avant même l'entrée en application du règlement MiCA. Après discussion avec l'Assemblée nationale, il a finalement été décidé de renforcer les exigences de l'enregistrement obligatoire (voir partie 2). Il reste que le renforcement de l'enregistrement obligatoire va déstabiliser l'écosystème, avec une application dès juillet 2023 de règles qui avaient vocation à ne s'appliquer qu'au moment de l'application du règlement MiCA, au cours de l'année

2024. En particulier, un renforcement des règles dans des délais si courts va rendre difficile pour les superviseurs de préparer les lignes directrices claires sur les obligations à respecter (notamment sur la sécurité des systèmes d'information), il va également se traduire par un surcoût substantiel de la procédure d'enregistrement et défavoriser les acteurs français par rapport aux autres acteurs européens.

Par ailleurs, il apparaît avant tout nécessaire de faire application du cadre existant plutôt que de chercher à le modifier à brève échéance. Le régime PACTE a en effet prévu d'importantes mesures de sanction en cas de non-respect des dispositions applicables aux prestataires de services sur actifs numériques. Par exemple, des acteurs étrangers qui en pratique offriraient des services en France (notamment par le biais d'une communication et d'une publicité dédiée à des ressortissants français) ont vocation à être enregistrés en France. S'ils ne le sont pas, l'Autorité des marchés financiers peut prononcer des sanctions, et par ailleurs demander au juge judiciaire de faire bloquer l'accès à leur site. Cette possibilité devrait être utilisée plus systématiquement, notamment dans un contexte dans lequel les défaillances de certaines plateformes ont affecté des utilisateurs dans l'ensemble des pays, y compris en France.

Jusqu'à présent, la réglementation française et européenne se fonde sur le principe selon lequel les acteurs régulés sont ceux qui offrent des services dans une zone géographique. Pour être régulé en France, un acteur étranger doit fournir des services en France (y compris comme évoqué plus haut par le biais d'une communication en français). En revanche, si un citoyen français s'adresse à une plateforme étrangère, il s'agit d'une « sollicitation inversée » ou *« reverse sollicitation »* ; la plateforme n'a alors pas à être régulée en France. La sollicitation inversée pourrait être un problème particulièrement prononcé dans la mesure où des fournisseurs de services en dehors de l'UE jouent un rôle dominant sur les marchés de crypto-actifs. Face à cette difficulté, il est important de veiller à ce que des juridictions hors de l'hors de l'UE mettent en place des régimes similaires au régime MiCA (logique du *« same rulebook »*).

Le passage d'une réglementation française à une réglementation européenne ne se traduit que partiellement par une intervention des superviseurs européens, l'essentiel de la supervision échéant aux superviseurs nationaux. Compte tenu des difficultés rencontrées dans l'examen des dossiers dans le cadre de l'application de la loi PACTE, il apparaît opportun de renforcer les équipes chargées du futur agrément obligatoire des prestataires. C'est notamment le cas pour l'Autorité des marchés financiers, et cela permettrait au superviseur de maintenir son avance et expertise dans ce domaine. Ainsi, la France pourrait être attractive en matière de délivrance d'agrément obligatoire. Elle pourrait également maintenir son avance dans les négociations et l'interprétation des textes découlant du règlement MiCA.

Recommandation n° 4

Préparer les autorités publiques et les acteurs de l'écosystème à l'entrée en vigueur du cadre réglementaire européen MiCA :

- **ne pas faire davantage évoluer le régime réglementaire français d'ici l'entrée en application du régime européen MiCA ;**
- **mieux faire usage des moyens de contrôle et de sanction donnés par le législateur vis-à-vis d'acteurs échappant à la réglementation (par exemple le blocage de site de prestataires non enregistrés en France) ;**
- **renforcer les équipes des autorités de supervision afin d'accompagner la mise en conformité des acteurs de l'écosystème ;**
- **plus largement, développer une position commune européenne en matière de réglementation des crypto-actifs à faire valoir face aux juridictions en dehors de l'UE (logique du *« same rulebook »*).**

4.2. LES AUTORITÉS PUBLIQUES DEVRAIENT POURSUIVRE LA CONSTRUCTION DU CADRE DÉDIÉ À LA *BLOCKCHAIN*, DE MANIÈRE À ASSURER UN DÉVELOPPEMENT DU SECTEUR À LA FOIS INNOVANT ET PROTECTEUR DES UTILISATEURS

Bien que la France ait été pionnière dans le développement d'un cadre juridique pour la *blockchain*, qui la place désormais dans une position favorable, elle doit continuer à faire évoluer le cadre existant. En ce sens, elle doit. En ce sens, elle doit l'adapter dans les différents domaines affectés par la *blockchain*, et suivre les évolutions de la technologie *blockchain* elle-même, dans la perspective de les réguler adéquatement.

Plusieurs axes d'évolution se dessinent, notamment pour :
- Clarifier les modalités de traitement des données personnelles sur *blockchain* ;
- Compléter les dispositions fiscales liées à l'utilisation de la *blockchain* en matière financière ;
- Engager les chantiers de suivi puis de réglementation des nouveaux usages ;
- Poursuivre les travaux sur la reconnaissance de la *blockchain* comme moyen de preuve.

Clarifier les modalités de traitement des données personnelles sur blockchain

La CNIL est venue préciser dans ses lignes directrices de 2018 les modalités d'application du RGPD à la technologie *blockchain.* Selon la CNIL, dès lors qu'un projet *blockchain* implique la manipulation de données personnelles, le RGPD s'applique.

Les projets *blockchain* soulèvent en général les enjeux suivants :
- Chaque participant a un identifiant composé d'une suite de caractères alphanumériques et qui constituent la clé publique du compte du participant. Il s'agit d'une identité « pseudonyme ». Cette clé publique se rapporte à une clé privée qui est censée rester confidentielle. Si néanmoins la clé privée est identifiée, l'identité des participants peut être dévoilée. L'ensemble constitue donc une donnée personnelle ;
- Les utilisateurs d'une *blockchain* sont libres d'inscrire toute donnée personnelle les concernant ou concernant des tiers sur la *blockchain*, sans possibilité de les retirer car elles sont immuables, c'est à dire non modifiables et non effaçables ;
- Des données personnelles « *off-chain* » peuvent être retrouvées en partant des données inscrites « *on-chain* », comme les résultats de tests KYC réalisés par des plateformes de trading de crypto-actifs, par le biais de la clé publique des participants.

S'il est clair que la technologie *blockchain* n'est pas en elle-même incompatible avec le RGPD, les analyses doivent être effectuées au cas par cas, ce qui rend difficile pour les acteurs d'avoir de la visibilité et de la sécurité pour leurs projets.

Ainsi, les points de tension suivants entre projets *blockchain* et respect du RGPD demeurent et doivent faire l'objet d'une attention accrue des porteurs de projets *blockchain* :
- Déterminer si les contraintes techniques de conservation et de traitement des données personnelles sur *blockchain* sont compatibles avec le traitement RGPD envisagé de ces données ;
- Ne pas aller à l'encontre du droit des personnes dont les données sont traitées, et qui doivent pouvoir être en mesure d'y accéder, de les rectifier et de demander leur suppression (articles 15-21 RGPD) ;
- Vérifier que l'inscription immuable de données sur une *blockchain* permet de respecter l'article 5 du RGPD selon lequel la conservation des données personnelles doit être limitée dans le temps :
  - À cet égard, la CNIL recommande i) de privilégier des solutions dans lesquelles la donnée est traité « *off-chain* » ou par ordre de préférence par i) un engagement cryptographique, ii) une empreinte de la donnée obtenue par une fonction de hachage à clé ou iii) un chiffré de la donnée ;

- Si aucune de ces fonctions ne peut être mise en œuvre, et que cela est justifié en terme de traitement et d'impact[65] la CNIL accepte que les données puissent être stockées avec une fonction de hachage ou en clair ;
- La CNIL précise aussi que la durée de conservation des identifiants des participants est « alignée avec celle de la *blockchain* ».

• Il est important de noter que seuls les participants actifs, soit les parties prenantes avec un droit d'écriture sur une *blockchain*, sont concernés par les lignes directrices de la CNIL. Les validateurs sont considérés comme des sous-traitants. Les rôles et obligations entre responsables de traitement et sous-traitants peuvent toutefois être difficiles à établir dans une organisation.

Au delà des précisions apportées par la CNIL dans sa communication de 2018, il est cependant possible de clarifier les points suivants :

• Pour respecter le droit à l'oubli, le *« Zero Knowledge Proof »* ou preuve à divulgation nulle pourrait être utilisé pour générer des preuves spécifiques sur les données personnelles tout en préservant l'anonymat du fournisseur de la preuve. Des clarifications pourraient être édictées par les autorités de supervision sur la conformité des dispositifs ZKP avec les lignes directrices RGPD de la CNIL de 2018.

[65] *À justifier par une analyse d'impact relative à la protection des données (AIPD).*

Encadré : le *zero-knowledge proof* (ZKP)

Le *zero-knowledge proof* (ZKP) est un procédé utilisé pour la première fois dans les années 80, afin de permettre à un tiers de prouver mathématiquement à un autre qu'une information est exacte sans toutefois révéler quelque autre information que sa véracité. Cela pourrait être utilisé pour prouver une identité numérique sans avoir à révéler cette dernière. Cela permet également de ne pas pouvoir associer l'historique des transactions sur la *blockchain* à chacune des entités intervenant dans chaque transaction.

• Plus largement, un travail d'actualisation des recommandations de la CNIL pourrait être entrepris, en s'appuyant sur des cas concrets de cas d'usage conformes au RGPD.

Recommandation n° 5

Clarifier les modalités de traitement des données personnelles des utilisateurs sur la *blockchain.* À cette fin, valider la conformité de la technique cryptographique du *Zero Knowledge Proof* (preuve à divulgation nulle de connaissance) comme moyen d'apporter des garanties de contenu tout en maintenant la confidentialité des émetteurs de ces contenus.

- **Sur la base d'un recueil concret de cas d'usage conformes au RGPD, enrichir les recommandations de la CNIL à l'attention des acteurs de l'écosystème.**

Clarifier les dispositions fiscales liées à l'utilisation de la blockchain en matière financière

De nombreuses propositions fiscales ont déjà pu être formulées par les représentants de l'écosystème[66] et discutées lors de l'examen de projets de loi de finances. À ce stade, peu de ces propositions ont été adoptées (en dehors des mesures sur les plus-values présentées plus haut).

Ces propositions reflètent le fait que le régime fiscal français des crypto-actifs pourrait être davantage approfondi. Il conviendrait en particulier de prévoir un cadre fiscal adapté aux nouveaux objets apparus avec la technologie *blockchain*. Par exemple, en matière de *tokens*, il conviendrait de lever l'incertitude sur le traitement fiscal associé. Cette incertitude a en particulier un impact sur les fonds, car elle porte atteinte à la transparence fiscale qu'ils fournissent à leurs clients. En outre, des questions importantes demeurent sans réponse comme la gestion de la plus-value du *staking*, et plus généralement des stratégies liquides en *DeFi* en intégrant le risque de contrepartie dans les obligations de KYC.

Recommandation n° 6

Clarifier le cadre fiscal applicable aux prises de participation en *tokens* (équivalents dématérialisés d'une valeur d'entreprise) dans des projets de *blockchain* pour les fonds d'investissement afin de leur permettre d'investir pour leurs clients et utilisateurs en toute conformité fiscale.

[66] *Voir par exemple : les propositions de l'Association pour le développement des actifs numériques (ADAN) à l'occasion du projet de loi de finances 2022.*

Engager les chantiers de suivi puis de réglementation des nouveaux usages

Plus fondamentalement, le cadre réglementaire reste incomplet du point de vue des nouveaux usages qui sont apparus avec la *blockchain*. C'est le cas dans le domaine financier, avec des pans non traités par la loi PACTE et le règlement MiCA, en matière de finance décentralisée notamment *(DeFi)*. C'est également le cas à la frontière entre domaine financier et non financier, notamment pour les *tokens* non fongibles (NFT).

S'agissant des NFT, en raison de leur récente apparition dans l'espace public, il n'existe peu, sinon pas, de réglementation dédiée aux NFT, ce qui entraîne pour les entités émettrices ou les utilisateurs une forte incertitude, préjudiciable au développement de leurs potentialités et à la protection des utilisateurs. À cet égard, le traitement réglementaire applicable peut fortement varier, de l'absence totale de réglementation du NFT en cause, à son assimilation – potentiellement à tort – à un actif financier. S'agissant d'un domaine récent, peu mature, il n'est pas illogique de ne pas avoir encore de cadre dédié et préférable de ne pas sur- ou mal réglementer, mais la réflexion devrait être ouverte dès maintenant. Elle pourrait notamment porter sur la définition des NFT et envisager de considérer le NFT comme un support transparent juridiquement, pour appliquer à appliquer à son sous-jacent un régime existant, s'il existe. Ainsi un NFT qui aurait pour sous-jacent un objet de type œuvre d'art pourrait se voir traiter juridiquement comme une œuvre d'art. De même avec d'autres sous-jacents possibles (un titre financier, un actif immobilier, etc.).

Pour les NFT, comme pour les autres cas d'usage en dehors du secteur financier, il ressort que la sécurité juridique est une composante essentielle du passage à l'échelle, quels que soient les secteurs d'activité. Les réflexions des pouvoirs publics devraient permettre d'assurer que les cas d'usage non financiers de la *blockchain* soient exclus de l'application du régime PACTE (comme du règlement MiCA) pour ne pas obérer les expérimentations dans ce domaine.

S'agissant de la *DeFi*, il est encore plus nécessaire de ne pas chercher à réglementer dès à présent un secteur aux risques encore très limités et méconnu. C'est la position retenue par les États membres lors de la négociation du règlement MiCA, consistant à suivre le développement de ces usages avant d'envisager une réglementation. Cette approche pourrait être étayée en France par la mise en place d'un observatoire dédié à la *DeFi*.

S'agissant des organisations autonomes décentralisées (DAO), il est nécessaire de clarifier et de rendre opérationnels les cadres de gouvernance que les professionnels développent et dans lesquels ils exercent.

Ces cadres sont définis « sur la chaîne » ce qui signifie qu'ils sont « automatisés » par le biais d'un protocole, permettant aux utilisateurs de s'entendre sur des propositions et évolutions du projet. Ils font référence aux « DAOs algorithmiques » qui par le biais d'un algorithme / protocole définissent a priori des modalités de vote dans le cadre d'un projet, qui sont ensuite exécutées automatiquement par le code. Ces modalités vont de systèmes simples de type « un jeton = un vote » à des systèmes beaucoup plus complexes et novateurs de type quadratiques ou holographiques pour hiérarchiser de la manière la plus fine possible les priorités et objectifs des communautés impliquées.

Encadré : exemples de cadre de gouvernance « sur la chaîne » pouvant être mis en place pour des systèmes de vote

- 1 vote = 1 *token* comme dans le cadre d'une élection classique ;
- Vote basé sur l'atteinte d'un quorum pour qu'une proposition soit actée ;
- Vote basé sur une majorité permissionnée : combien sont « pour » et combien sont « contre » sans nombre de vote minimum requis ;
- « *rage quitting* » avec période de grâce après l'approbation d'une proposition durant laquelle les votants peuvent reconsidérer leur position ;
- Vote quadratique où chaque votant peut voter autant qu'il veut mais avec un coût croissant de manière exponentielle (1V1T, 2V4T, 3V9T, etc.) ;
- Vote de conviction où le poids du vote augmente avec la durée durant laquelle il demeure inchangé pour valoriser les positions de long-terme au sein d'une communauté ;
- Consensus holographique pour gagner du temps et se concentrer sur les propositions qui ont le plus de chance d'être votées, les membres étant rémunérés sur la base de leurs prédictions ;
- Vote réputationnel où chaque membre gagne des jetons qui leur octroie davantage de poids de vote, les jetons n'étant pas transférables et ne pouvant pas être détruits ;
- « *Knowledge-extractable voting* » où chaque membre délègue son vote à des experts désignés au sein de la communauté (se rapproche de la démocratie représentative).

La réglementation en vigueur pourrait reconnaître ces cadres de gouvernance au même titre que les cadres de gouvernance qu'elle reconnaît déjà. Cela irait dans le sens d'une reconnaissance juridique des DAOs en droit français avec un double effet bénéfique: d'une part une sécurité juridique accrue pour les porteurs de projets DAO, et d'autre part des incitations renforcées à se conformer à la réglementation en vigueur pour ces mêmes porteurs de projet.

Une initiative notable en la matière est la « *DAO Model Law* » portée par le groupe de travail international Coalition of Automated Legal Applications (COALA) qui propose un cadre juridique souple pour permettre

la reconnaissance juridique des DAOs de manière harmonisée, afin de garantir leur légalité et leur sécurité juridique dans différents pays. Ce groupe a conduit une analyse comparative des différentes dispositions applicables au droit des sociétés dans le monde. Cette analyse a permis de dégager des grands principes réglementaires applicables à des entités juridiques remplissant des fonctions similaires à celles des DAOs. Le groupe de travail s'est ensuite attaché à identifier comment les garanties technologiques et les modalités de gouvernance mises en place par les DAOs pouvaient remplir certaines exigences réglementaires. Ainsi, cette loi-type énonce des principes d'équivalence réglementaire et fonctionnelle auxquels les DAOs doivent se conformer pour être considérées comme une société, au sens juridique du terme.

Conçue comme un guide de bonnes pratiques à destination des régulateurs, la « *DAO Model Law* » a pour objectif d'aider les pouvoirs publics à moderniser leur droit des sociétés pour tenir compte de l'apparition de nouveaux modèles d'organisations dites autonomes et décentralisées. La transposition de cette loi-type au cadre juridique national aurait pour effet de doter les DAOs d'une reconnaissance légale, ce qui en retour inciterait les porteurs de projets DAOs à se conformer aux dispositions réglementaires applicables en France afin de pouvoir bénéficier de cette reconnaissance juridique. Plus largement, cela leur permettrait également d'exercer dans un cadre juridique clair, dans un contexte où la plupart des DAOs sont aujourd'hui confrontées à des cadres réglementaires souvent inadaptés à leur caractère décentralisé, pseudonyme et transnational.

Recommandation n° 7

Engager les chantiers de suivi puis de réglementation des nouveaux usages et des nouvelles modalités de traitement, en particulier :

- traiter les *tokens* non fongibles (NFT – *Non-Fungible Tokens*), qui représentent des actifs dématérialisés, comme des véhicules juridiquement transparents permettant de traiter leurs sous-jacents matériels selon les réglementations existantes en vigueur ;
- étudier l'opportunité de reconnaître juridiquement les communautés et processus de collaboration au sein d'une *blockchain*, dits organisations autonomes décentralisées (DAO – *Decentralized Autonomous Organizations*), en s'appuyant sur l'exemple du DAO Model Law qui prône une harmonisation internationale pour une meilleure sécurité juridique ;
- mettre en place un observatoire dédié à la finance décentralisée (*DeFi – Decentralized Finance*) pour pouvoir réguler à terme ces activités aujourd'hui non suivies.

Poursuivre les travaux sur la reconnaissance de la blockchain comme moyen de preuve

La technologie *blockchain* constitue un moyen de preuve robuste du fait de ses caractéristiques présentées plus haut (notamment : infalsifiabilité, transparence, traçabilité, etc.). C'est pourquoi elle constitue déjà un moyen de preuve reconnu. En 2020 par exemple, les notaires de Paris ont lancé une *blockchain* notariale (privée). Par ailleurs, sur le plan juridique, la technologie est considérée comme un moyen de preuve opposable en justice, depuis la reconnaissance juridique de cette technologie sous le nom de « dispositif électronique d'enregistrement partagé » (DEEP).

Pour autant, en l'état du droit, il appartiendrait à un juge d'apprécier la valeur probatoire d'éléments inscrits sur *blockchain*, au vu des circonstances de l'espèce. En effet, ces éléments ne constituent pas une preuve irréfragable et ne sont pas équivalents à un « acte authentique » (par exemple un acte d'un notaire). En conséquence, il est difficile de déployer toutes les potentialités de la *blockchain* pour en faire un véritable instrument de sécurité juridique des transactions et des échanges.

Pour pouvoir développer des cas d'usage en matière de preuve, une principale difficulté doit être dépassée : en l'état, les seules preuves électroniques équivalentes à des preuves manuscrites sont celles qui répondent aux conditions de « signature électronique qualifiée » au sens du règlement eIDAS. Or, ce règlement impose d'identifier le signataire et de recourir à un prestataire de services de confiance qualifié qui assure l'enregistrement et l'horodatage, soient deux points sur lesquels les technologies *blockchain* ne sont pas adaptées. Le développement de cas d'usage en matière de preuve requiert donc une modification du règlement pour que celui-ci soit technologiquement neutre.

Un des principaux cas d'usage en matière de preuve concerne l'identité numérique, qui fait l'objet de nombreux travaux au niveau européen et mondial. Les apports d'une identité numérique européen seraient principalement les suivants :

- L'amélioration de l'efficacité et de la viabilité de certaines formalités administratives, comme par exemple le fait d'être majeur ou non, d'avoir obtenu tel ou tel diplôme ou qualifications, ou encore l'éligibilité à certaines prestations sociales ;
- L'automation de certaines procédures, à définir par les autorités compétentes et en lien avec la CNIL, en utilisant la technologie de *self-sovereign identity* (SSID) ;
- Le renforcement du contrôle des citoyens sur les données qu'ils souhaitent divulguer ou non aux autorités, par exemple en prouvant sa majorité sans avoir à divulguer son âge exact ou sa date de naissance.

Encadré : la gestion de l'identité numérique en Corée du Sud

La Corée du Sud a annoncé la mise en place de cartes d'identités numériques d'ici 2024.

- Ces cartes d'identité pourraient devenir des identifiants numériques, c'est-à-dire des documents édités sur une *blockchain* visiblement décentralisée.
- Le gouvernement coréen ne serait pas à même de voir à qui les citoyens coréens montrent leur carte d'identité numérique.
- Selon le directeur du Bureau numérique du gouvernement sud-coréen, cela pourrait permettre à tous les services qui ne sont pas encore entièrement numériques de sauter le pas de manière plus simplifiée et efficace.
- Le gouvernement s'attend à ce que 45 millions de citoyens de Corée du Sud adoptent ces cartes d'identité numérique dans les deux années qui suivront.

Le rapport de 2021[67] remis à la DGE sur les verrous restant à lever pour maximiser le potentiel de la technologie *blockchain* mentionnait déjà la nécessité de créer un service public de l'identité numérique, et soulignait la nécessité pour l'ANSSI de s'emparer du sujet. En outre, le sujet de l'identité numérique n'est aujourd'hui pas suivi par la France au niveau européen. Dans le cadre des travaux de l'*European Blockchain Partnership* (EBP), une initiative visant à élaborer une stratégie de l'UE sur la *blockchain* et à construire une infrastructure *blockchain* pour les services publics, la France est représentée par l'Université de Lille alors que ce sujet est suivi par des ministres ou secrétaires d'État dans les autres pays européens.

[67] *https://www.entreprises.gouv.fr/files/files/etudes-et-statistiques/synthese-blockchain.pdf*

Recommandation n° 8

Investir dans des travaux sur la reconnaissance de la *blockchain* comme moyen de preuve et de support pour une identité numérique, la France étant absente des discussions européennes sur ce thème. Pour cela :

- mobiliser la France pour qu'elle participe à l'adaptation du régime applicable en matière de preuve électronique (règlement européen eIDAS) afin de le rendre compatible avec l'utilisation de la *blockchain* ;
- impliquer l'ANSSI dans les travaux en cours autour d'une identité numérique européenne.

4.2. LA *BLOCKCHAIN* POURRAIT RAPIDEMENT DEVENIR DÉCISIVE POUR LA SOUVERAINETÉ NUMÉRIQUE DU SYSTÈME DE PAIEMENT EUROPÉEN

La technologie blockchain pourrait prendre une place importante dans les systèmes de paiement de demain

Compte tenu des caractéristiques de la *blockchain* et des crypto-actifs associés, cette technologie présente un attrait majeur pour établir un système de paiement.

C'est particulièrement le cas lorsque les dispositifs de paiement sont insuffisants, notamment dans certaines zones du monde : le faible niveau d'inclusion financière des populations, le coût élevé des paiements transfrontaliers (le plus souvent entre deux devises différentes), les longs délais liés à l'exécution des transactions, sont des faiblesses auxquelles l'utilisation de crypto-actifs et notamment de *stablecoins* pourrait répondre.

Dans les zones dans lesquelles les systèmes de paiement sont plus satisfaisants, la technologie *blockchain* est également susceptible d'être utilisée pour optimiser les moyens de paiement. Les paiements sont en effet opérés par des institutions financières (banques, assurances et autres institutions monétaires) qui communiquent entre elles pour financer l'économie, indépendamment des marchés financiers. L'action de ces institutions financières repose sur des infrastructures qui fournissent des supports techniques pour permettre le transfert de paiements et l'échange, la compensation et le règlement de titres financiers. Or, la technologie *blockchain* permet à plusieurs institutions d'utiliser une base de données unique, qui n'a plus besoin d'être mise en cohérence avec d'autres bases, car elle est cohérente par construction. Cette logique d'interopérabilité porte en elle de nombreuses opportunités pour optimiser les systèmes de paiement.

En outre, le besoin d'interopérabilité va très probablement s'accroître. Les clients vont avoir toujours plus de choix pour effectuer des paiements avec l'apparition des nouveaux acteurs. Ils vont vouloir de plus en plus de flexibilité et de moins en moins de frais pour réaliser leurs transactions. Pour répondre à ce besoin, les institutions financières vont devoir proposer des solutions de paiement plus rapides et flexibles. Par ailleurs, le marché va continuer de se transformer avec le big data et l'intelligence artificielle dans la mesure où la puissance des algorithmes dépend de la quantité des données disponibles. Cela va imposer aux acteurs financiers de coopérer et de partager davantage de données avec d'autres acteurs pour mettre au point des algorithmes fiables et performants. Cela nécessitera de se doter de bases de données partagées et fiables.

La maîtrise des infrastructures de paiement constitue par ailleurs un enjeu majeur de souveraineté. En matière d'infrastructures de paiement, force est de constater que l'Europe est en position de dépendance vis-à-vis d'acteurs privés non européens que sont les acteurs traditionnels du paiement (notamment le duopole Visa-Mastercard) et les géants mondiaux (GAFAM) qui cherchent désormais à conquérir le secteur bancaire et financier. Par exemple, au sein de la zone euro, 10 pays ont encore des réseaux qui n'acceptent pas les cartes des autres pays, ce qui rend

l'utilisation de cartes Visa ou Mastercard nécessaire. Si plusieurs grandes banques de l'UE ont envisagé avec le soutien de la Commission européenne et de la Banque centrale européen de mettre en place un nouveau système de paiement européen (dit « EPI »), il apparaît que beaucoup de banques se sont retirées du projet.

Le fait que ces acteurs du paiement soient essentiellement des infrastructures étrangères, rend potentiellement les pays européens dépendant de choix politiques externes (par exemple la politique d'extraterritorialité américaine), avec le risque d'interruption des services de paiement comme moyen de pression, ce qui pourrait considérablement affecter le fonctionnement de l'économie. Il faut également mentionner le fait que les données de paiement collectées sont stockées en dehors de l'UE.

Il existe un risque important de reproduire cette situation de dépendance dans le cadre de l'utilisation de la technologie *blockchain* à des fins de paiement. Par exemple, la très grande majorité des *stablecoins* sont développés par des entités non européennes et basés sur le dollar. C'est pourquoi il existe un enjeu stratégique de soutenir le développement d'initiatives européennes en la matière.

Encadré : la *DeFi*, un laboratoire de la désintermédiation et de l'automatisation du système financier

La finance décentralisée *(DeFi)* est aujourd'hui le principal laboratoire d'exploration de la désintermédiation et de l'automatisation de certains pans de notre système financier. Si les cas d'usage ne sont pas encore suffisamment matures pour être visibles du grand public, ils pourraient avoir sur nos systèmes de paiement un impact majeur. En effet, ils pourraient permettre de se passer de tiers de confiance dans certains cas pour automatiser et fiabiliser certaines transactions. En combinant des attributs informatiques et économiques, certains *smart contracts* proposent des solutions qui permettent de chaîner ensemble plusieurs opérations pour en faire une seule transaction régie au niveau protocolaire. Par exemple, les *flash loans* permettent d'emprunter sans collatéral. En effet, le *smart contract* du *flash loan* prévoit les trois étapes suivantes : d'abord l'emprunt est effectué auprès d'une entité quelconque, sans collatéral. Ensuite le montant de l'emprunt est utilisé pour effectuer différentes transactions sur les marchés financiers. Enfin, au bout d'une durée prédéterminée par le code, deux possibilités s'offrent à l'emprunteur : soit il restitue le montant au prêteur, soit il n'est pas en mesure de le faire, et la transaction est annulée dans son intégralité, l'emprunteur paye alors uniquement les coûts de calcul.

Des acteurs des paiements ont commencé à investir et à développer des cas d'usage dans cette logique

Les banques de détail

Dans les régions du monde où la majorité de la population est bancarisée, les banques de détail sont en concurrence avec les FinTechs qui proposent des solutions en ligne plus rapides, plus sécurisées et moins onéreuses. Dans ce cadre, la *blockchain* est un outil qui augmente la fiabilité des transactions réalisées en mettant en cohérence d'emblée les bases de données concernées. Banking Circle[68] a été nommé en 2022 par FXC Intelligence parmi les meilleures sociétés de paiements transfrontaliers au monde. Banking Circle a construit un réseau de compensation et de règlement en temps réel pour 25 devises, qui offre des paiements rapides et à faible coût – sans frais cachés pour le bénéficiaire.

[68] *https://www.corporatenews.lu/fr/archives-shortcut/archives/article/2022/03/banking-circle-nommee-parmi-les-meilleures-societes-de-paiements-transfrontaliers-au-monde*

Dans les régions du monde où la majorité de la population n'est pas bancarisée, les banques de détail sont en concurrence avec des solutions alternatives, pouvant reposer sur des *blockchains* et permettant d'effectuer des paiements sur mobile. La *blockchain* n'est pas toujours la solution adoptée, comme le démontre l'exemple du Unified Payment Service (UPI) en Inde qui draine des transactions équivalentes à plus de 100 Mds $ par mois et 150 M d'utilisateurs par mois. Cela traduit néanmoins une forte demande pour des solutions de paiement alternatives à des institutions bancaires, en particulier pour les paiements transfrontaliers.

Par ailleurs, la *blockchain* permet de démocratiser les transferts d'actifs internationaux en réduisant les coûts des virements entre particuliers qui avoisinent les 6 %[69] de la transaction dans le cadre du système SWIFT alors que l'objectif de l'ONU se situe autour des 3 %[70] tout comme le coût proposé par les prestataires en ligne.

Fin décembre 2022, BANK OF AFRICA a annoncé avoir franchi une nouvelle étape[71] dans l'accompagnement de ses clients dans la digitalisation des flux commerciaux internationaux à l'aide de la technologie *blockchain*.

Les banques d'investissement

Il existe également des opportunités dans le secteur de la banque d'investissement. En effet, la capitalisation boursière du marché des crypto-actifs et le soutien des institutionnels à ce marché a fortement augmenté ces dernières années pour atteindre environ 1 trillion de dollars début 2023[72].

[69] *https://www.worldremit.com/en/blog/french/frais-virement-international/#:~:text=Le%20co%C3%BBt%20d'un%20virement%20bancaire%20international%20repr%C3%A9sente%20en%20moyenne,%E2%82%AC%2C%20selon%20la%20Banque%20Mondiale*

[70] *https://www.un.org/fr/observances/remittances-day/background#:~:text=Parmi%20les%20objectifs%20mis%20en,co%C3%BBts%20sont%20sup%C3%A9rieurs%20%C3%A0%205%20%25*

[71] *https://www.prnewswire.com/news-releases/bank-of-africa-sassocie-a-dltledgers-afin-daccompagner-la-digitalisation-des-operations-de-commerce-international-au-travers-de-la-blockchain-301-706279.html*

[72] *https://coinmarketcap.com/fr/charts/*

La *blockchain* est prometteuse pour la banque d'investissement à plus d'un titre ; par exemple, la compensation de titres *(clearing)* n'est plus requise quand les titres sont échangés *via blockchain*.

Dans ce contexte, les banques ont déjà investi des montants importants pour permettre à leurs clients de transférer et de conserver des crypto-actifs et développer une infrastructure de services bancaires adaptée. Les plus à la pointe d'entre elles envisagent de se positionner comme des intermédiaires de confiance pour fournir des services de conservation de crypto-actifs sur des infrastructures adaptées à l'utilisation de plateformes d'échanges de crypto-actifs.

Les banques investissent surtout dans des solutions de stockage et de conservation de *tokens*, le plus souvent *off-chain*, qui combinent *trading* et *settlement*. Parmi les exemples les plus notables, la banque Morgan Stanley a par exemple mis un ticket de 1 Md$ dans la solution NYDIG qui propose des services de courtage, d'exécution et de conservation de crypto-actifs.

Elles soutiennent également l'écosystème crypto *via* leur activités de financement. Les banques investissent aussi de gros montants dans des infrastructures *blockchain* qui font tourner des nœuds et les mettent à la disposition d'autres utilisateurs, à l'instar des tickets mis par Morgan Stanley dans Figment qui propose une infrastructure de *staking*, d'intergiciel et d'applications Web 3 ou encore de BNY Mellon dans Talos une infrastructure de niveau institutionnel qui prend en charge l'ensemble du cycle de vie des actifs numériques. Les banques investissent également dans des services annexes de type fournisseurs de données sur les marchés de crypto-actifs ou sécurisation et audit des protocoles *blockchain* et des *smart contracts*. Goldman Sachs a ainsi investi 88 M$ récemment dans CertiK, une plateforme de vérification formelle des *smart contracts* et protocole *blockchain*.

Encadré : panorama des investissements réalisés par les banques de 2021 à 2022

Compagnie	Pays d'origine	Actifs sous gestion	Nombre d'investissements	La taille des cycles de financement comme indicateur de l'investissement	La taille des cycles de financement comme indicateur de l'investissement
Morgan Stanley	New York, USA	1 400 Md$	2	1 110 M$	Figment, NYDIG.
Glodman Sachs	New York, USA	2 000 Md$	5	698 M$	Certik, Coin Metrics, Elwood Technologies, Blockdaemon, Anchorage Digital.
BNY Mellon	New York, USA	2 300 Md$	3	690 M$	Talos, Coin Metrics, Fireblock.
Commonwealth Bank	New South Wales, Australie	785 M$	4	421 M$	Lygon, Xpansiv, Gemini.
CITI	New York, USA	2 291 Md$	6	215 M$	Talos, TRM, Contour, Blockdaemon, Amberdata.
UOB	Singapour	1 450 Md$	7	204 M$	Kyro, Play It Forward DAO, ADDX, Assembly, Evrynet, Yield Guild, Jambo.
HSBC	Londres, Royaume-Uni	3 021 Md$	1	200 M$	Consensys.
Wells Fargo	Californie, USA	1 948 Md$	2	165 M$	Talos, Elliptic.
KB Kookmin Bank	Séoul, Corée du Sud	970 Md$	8	143 M$	Streami, Buysell Strandards (PIECE), Xangle, Uprise, Kodebox, Lambda 256, Block Odyssey.

* Number of the « Group Company ».

Note : le nombre d'opérations et la taille des cycles de financement concernent les sociétés du groupe ainsi que leurs filiales.

Les banques centrales

Pour construire une infrastructure de paiement compatible avec les avancées technologiques permises par la technologie *blockchain* qui viennent d'être décrites, deux types de monnaie numérique banque centrale (MNBC en Français et CBDC en Anglais) sont en cours de construction. Elles s'appuient sur des technologies décentralisées qui reposent souvent sur des *blockchains*.

Les MNBC *retail* ont pour vocation à être accessibles au grand public en complément de la monnaie fiduciaire, en tant qu'équivalent numérique des billets et pièces, elle offre une nouvelle option pour la détention et l'échange monétaire.

Les MNBC *wholesale*, dite « de gros » ou « interbancaire », sont accessibles uniquement aux banques pour régler des transactions sur actifs financiers ou pour effectuer des paiements transfrontaliers. Leur développement pourrait accélérer l'intégration des technologies de registres distribués au sein des infrastructures actuelles de marché, et leur transformation au travers du régime Pilote. En effet, la possibilité de régler en MNBC des titres financiers tokenisés *(« on chain » Delivery-versus-Payment)* permettrait de résoudre une partie des problématiques d'interopérabilité entre les systèmes classiques et les technologies de registres distribués.

En novembre 2021, la Banque de France a annoncé l'achèvement des expériences lancées au printemps 2020. L'objectif était de tester le cas d'une MNBC *wholesale* dans plusieurs domaines, en soutenant les options technologiques et les implications macroéconomiques et de politique monétaire de l'émission d'une MNBC *wholesale* à un large ensemble de participants, y compris d'autres banques centrales.

Neuf expériences différentes ont permis de tester les risques, les avantages, et les implications techniques de la mise en œuvre d'une MNBC *wholesale*. Les tests ont couvert plusieurs cas d'utilisations de la MNBC,

de la souscription et du rachat de fonds monétaires jusqu'au règlement transfrontalier. Une émission réelle d'obligations d'une valeur de 100 millions d'euros a été réglée avec une MNBC *wholesale* conçue spécialement pour ces expériences.

Selon la Banque de France, les résultats soulignent que les MNBC basées sur la *blockchain* et les technologies de registres distribués peuvent être efficaces pour accélérer le règlement des transactions de sécurité entre différentes devises, tout en assurant la sécurité des échanges. La banque centrale a conservé le contrôle de l'émission et de la circulation de la monnaie grâce à l'utilisation de contrats autonomes *(smart contracts)*, tandis que l'interopérabilité avec les systèmes actuels de règlement de gros a également été testée. À titre d'exemple, en décembre 2021, la Banque de France, la Banque des Règlement Internationaux et la Banque nationale suisse ont expérimenté avec succès des CBDC pour des paiements internationaux (projet jura).

La Banque de France a par ailleurs annoncé le 11 octobre 2022, sa participation à une nouvelle expérimentation de monnaie numérique de banque centrale interbancaire avec SWIFT.

Encadré : les monnaies numériques banque centrale (CBDC) à l'étranger

Plus de 80 % des banques centrales envisagent de lancer une CBDC ou l'ont déjà fait. La CBDC est déjà utilisée aux Bahamas et au Nigeria, et la Jamaïque et les Caraïbes orientales devraient suivre. La Banque populaire de Chine procède à des essais publics à grande échelle dans certaines villes et l'e-CNY était l'un des trois seuls modes de paiement acceptés sur le site des Jeux olympiques d'hiver de 2022.

En février 2022, le ministre des Finances de l'Inde s'est engagé à mettre en place une version numérique de la roupie et, le mois suivant, les Philippines ont annoncé leur propre mise en œuvre pilote d'une CBDC. L'administration américaine a accordé « la plus grande urgence » aux efforts de recherche et de développement concernant la conception et le déploiement potentiels d'une CBDC américaine.

En outre, en Europe, la société finlandaise Membrane Finance à récemment créé l'EUROe, un *stablecoin* adossé à l'euro, selon le blog de la société daté du 2 février. La société est agréée par l'autorité finlandaise de surveillance financière (Fin-FSA), qui vise à réduire la complexité de la conversion et du paiement en crypto-actifs volatiles.

Le développement des MNBC se heurte toutefois à de nombreuses limites au premier rang desquelles la nécessité de construire des MNBC respectueuse de la protection des données de leurs utilisateurs, des risques cyber accrus dans un contexte de surveillance réglementaire encore réduite par rapport aux autres monnaies, des enjeux d'adoption car les paiements sont intrinsèquement culturels et un nouveau modèle de paiement entraîne des coûts additionnels de conformité et des défis techniques liés à leur capacité à traiter un très large volume de transactions.

Seules des coopérations réussies entre le secteur privé et le secteur public permettront de déployer le plein potentiel de la blockchain pour les systèmes de paiement

À rebours de la promesse initiale, et de la principale source de valeur de la technologie *blockchain* pour les systèmes de paiement européens, il existe encore trop d'initiatives industrielles qui se font concurrence et ne coopèrent pas assez.

Ce manque de coopération est dû à de nombreuses raisons :

- Les consortiums existants ne sont pas assez ouverts aux nouveaux acteurs désireux de les rejoindre.
- Les entreprises peuvent avoir des intérêts divergents selon leur positionnement sur la chaîne de valeur, et donc ne pas être favorable au partage des informations (notamment pour des questions d'intelligence économique).
- La communication est lente et peu efficace entre les acteurs privés et publics.
- Trop d'initiatives concurrentes coexistent, nuisant à la lisibilité par les industriels et réduisant l'intérêt que ceux-ci ont de rejoindre un consortium donné, ne sachant pas lequel « survivra ».
- En ouvrant la gouvernance aux consommateurs, les entreprises peuvent perdre le contrôle de la conception et la production des produits et services.
- Le ciblage de la communauté appropriée est clef pour le produit ou service proposé, or les codes, les cultures de ces communautés web3 peuvent être opaques pour les entreprises novices sur le web3.
- Le développement de nouveaux produits nécessite des expertises nouvelles pour les entreprises comme notamment des *« Engagement Leaders »* pour fédérer et stimuler ces communautés *via* des canaux dédiés (comme discord), des catalystes pour synchroniser et impulser l'ensemble des métiers, des designers 3D, des développeurs *blockchains* ou des Game Designers.

Par ailleurs, certains acteurs français ne travaillent pas suffisamment en écosystème national pour privilégier des partenariats avec d'autres acteurs français de la *blockchain* alors que les acteurs privés, au premier rang desquels les banques d'investissement, mettent les tickets les plus importants dans des solutions qui permettent d'envisager le déploiement d'une infrastructure *blockchain* avec un nombre important de nœuds et suivre le rythme du développement des transactions en crypto-actifs. Il est en effet critique d'accélérer le développement des nœuds en France,

en s'appuyant notamment sur des initiatives comme Exaion Node ou MASSA et d'une infrastructure haute performance pour rester compétitif et pertinents si l'adoption du Web 3 se généralise encore.

De nombreux consortiums ont ainsi été abandonnés alors que des solutions performantes sur le plan technique y étaient développées en raison d'une absence de coopération entre leurs membres, comme Tradelens qui avait pour objectif de recourir à la *blockchain* pour améliorer le fret maritime. Des acteurs comme Goldman Sachs, Morgan Stanley ou Santander ont quitté le consortium R3 qui avait pour objectif de faciliter les échanges interbancaires et les opérations de réconciliation de comptes pour une meilleure conformité aux obligations de KYC pour des difficultés de gouvernance.

C'est pourquoi, les pouvoirs publics ont un rôle à jouer pour fédérer les initiatives privées les plus prometteuses et augmenter la coopération autour des projets *blockchain*. La mission « Verrous » de la DGE avait déjà recommandé en 2019 une « grande action d'innovation » d'une durée de 4-5 ans autour de projets ciblés conduits par des petits consortiums associant startups et laboratoires de recherche sur des durées courtes (12 à 18 mois).

Il apparaît ainsi déterminant de soutenir une initiative pour faire émerger les solutions *blockchain* les plus pertinentes pour nos systèmes de paiement, et, compte tenu des enjeux stratégiques, que cette initiative soit menée au niveau européen. Cela permettrait d'afficher un soutien clair à la mise en œuvre de partenariats stratégiques entre les consortiums publics positionnés sur l'incorporation de la technologie *blockchain* aux systèmes de paiement, et les acteurs privés déjà bien avancés dans le domaine. Une gouvernance indépendante, composée d'experts issus du milieu réglementaire, du secteur privé et des communautés *blockchain* pourrait être mise en place sur base tournante tous les 2-3 ans. Les financements alloués seraient ciblés en fonction des besoins du marché, pour tenir compte de l'évolution rapide du secteur et des innovations portées

par les acteurs privés. L'important étant qu'une part substantielle des financements s'appuie sur la mise en commun des financements privés déjà existants, avec un soutien public en financement de fonctionnement.

Encadré : l'utilisation de véhicules de financement de projets transnationaux stratégiques

Conformément au principe de subsidiarité, il incombe à l'Union européenne d'assurer le développement de projets multinationaux transverses, multi-secteurs. Il existe pour ce faire certains véhicules, comme par exemple les EDIC. Ils ont vocation à financer des projets et nécessaires à la réalisation d'objectifs numériques. Ils complètent la politique industrielle européenne car ils permettent de dépasser le cadre de la recherche couvert par d'autres véhicules tels que les PIIEC ; l'exemple du PIIEC sur le *cloud* pourrait d'ailleurs inspirer un EDIC *blockchain* (Annexe 5). Pilotés par la Commission européenne, ils font intervenir les États-membres de l'UE et les acteurs privés. Trois sources de financement sont donc mobilisées : les budgets nationaux, le budget de l'UE et l'investissement privé.

Concrètement, l'EDIC, qui est doté de la personnalité juridique, répond à un appel à manifestation d'intérêt (AMI) lancé par la Commission européenne. Sa mise en œuvre est réalisée de manière coordonnée avec la Commission européenne et les représentants des États-membres parties prenantes. La Commission européenne a un rôle de conseil sur les mécanismes d'exécution, le choix des sources de financement, et leur combinaison avec les autres projets stratégiques multisectoriels en cours.

Il apparaît dès lors impératif de mettre à l'agenda européen la question stratégique du développement de la technologie *blockchain* en matière de paiement, en structurant une coopération entre les acteurs *blockchain*, les banques et le secteur public.

5 Dans le cadre d'ateliers de travail menés avec des industriels et des experts du secteur, des bonnes pratiques à destination des entreprises ont été identifiées

Plusieurs ateliers de travail ont été menés au cours de l'élaboration du rapport, avec l'objectif d'identifier les principaux points de blocage à l'industrialisation de projets *blockchain* dans différents cas d'usage. Ces blocages sont identifiés ci-dessous, et sont complétés d'éventuelles bonnes pratiques. Celles-ci ne sont aucunement des recommandations, mais ont l'objectif de proposer d'éventuelles pistes permettant de faire face aux blocages identifiés.

5.1. APPRÉCIER L'OPPORTUNITÉ DE RECOURIR À UNE *BLOCKCHAIN*

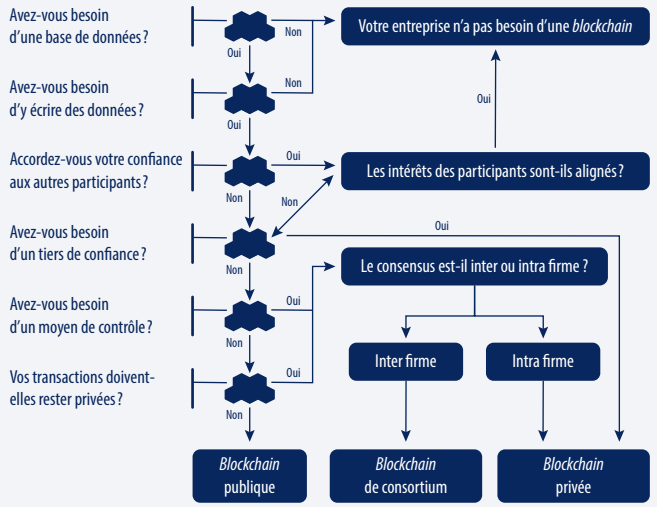
Certaines conditions doivent être réunies pour que la mise en place d'une *blockchain* soit réellement plus avantageuse que le recours à une autre technologie comme une base de données.

Encadré : l'intérêt du recours à la *blockchain* pour un cas d'usage, et le type de *blockchain* à envisager

Pour savoir si le recours à la *blockchain* est pertinent pour un cas d'usage, trois questions sont à se poser :

- Le cas d'usage nécessite-t-il une gouvernance décentralisée ? Si c'est le cas, le recours à la *blockchain* est pertinent.
- Le cas d'usage nécessite-t-il d'inscrire des données définitivement et d'être en mesure de les vérifier ? Si c'est le cas, le recours à la *blockchain* est pertinent.
- Le cas d'usage nécessite-t-il de communiquer, potentiellement entre plusieurs acteurs, des informations dynamiques, qui évoluent rapidement ? Si c'est le cas, le recours à la *blockchain* est pertinent.

Est ce que votre entreprise a besoin d'une *blockchain* ?



Source : Justin Case

La *blockchain* est une technologie qui permet de déterminer, de manière itérative, un état unique de référence, un point de vérité unique, c'est-à-dire une donnée qui fait consensus pour tout et qui est communément admise comme une donnée pouvant être prise comme référence par tous. En fonction de la nature des validateurs de cet état de référence, la *blockchain* utilisée sera publique, de consortium ou encore privée.

Encadré : avantages et inconvénients des différents types de *blockchain* pouvant être incorporées dans les entreprises

La *blockchain* publique

Les *blockchains* publiques ont plusieurs inconvénients :

- L'ensemble des données et transactions doivent être soumises à la vérification de tous les validateurs, ce qui crée des engorgements et donc des frais de transactions dans le réseau. Le *sharding*, ou partitionnement est une solution envisagée sur Ethereum pour remédier à ce problème. Cette technique déjà utilisée pour les bases de données consiste à partitionner les données de manière horizontale afin de répartir le stockage en mémoire. Pour Ethereum, dont l'ambition est d'être un ordinateur mondial, le *sharding* consisterait à paralléliser à la fois le stockage et l'exécution des smart contrats sans perdre en sécurité. Le *sharding* est envisagé par des développeurs d'autres protocoles qu'Ethereum.
- Les *layers 2* permettent de réduire l'engorgement mais demandent aujourd'hui un investissement financier non négligeable pour le déploiement et une certaine maîtrise de processus techniques pour un usage par un particulier, ou de confier la responsabilité de gestion à un dépositaire de clés privées. Enfin, dans le cas où l'on a besoin de faire appel à des opérations imbriquées dans des *layer 2* différents, alors leur exécution sera très lente (problème dit de « composabilité »).

Toutefois, elles sont prometteuses à plusieurs égards:

- Elles sont neutres technologiquement et fortement résilientes. De ce fait, dans un cadre transactionnel notamment, la *blockchain* publique devient intéressante en permettant un gain de souveraineté par rapport à ce qui est possible *via* internet.
- Concernant les *layers 2*, des protocoles sont aujourd'hui en cours de développement car contrairement aux coûts des *blockchains* qui sont proportionnels par rapport un nombre de transactions, les *layer 2* ont une structure de coût inversement proportionnelle : plus on regroupe les transactions, plus le coût par transaction est bas.

Les entreprises qui ont besoin de distribuer la confiance au sein de leur organisation devraient systématiquement recourir à ce type de *blockchain*. Contrairement aux *blockchains* de consortium, les informations inscrites sur une *blockchain* publique sont visibles par tous. Cette transparence est utile pour transférer de la valeur entre des départements / services différents où automatiser la gestion de l'identité à l'échelle d'une organisation.

La *blockchain* de consortium

Dans une *blockchain* de consortium, les validateurs sont définis à l'avance par les nœuds validateurs. Il s'agit d'organisations connues du grand public, qui garantissent la bonne et rapide exécution des transactions, en mettant leur image en jeu. On peut noter que des consortiums émergent dans différentes industries, avec R3, Vertrax ou Komgo.

Les utilisateurs peuvent tout de même vérifier que la validation a été effectuée sans manipulation ou falsification, puisqu'être validateur ne permet pas d'éditer des transactions valides au nom d'un utilisateur du réseau.

Aussi, avec la gouvernance plus restreinte d'une *blockchain* de consortium, il peut être plus facile de revenir à un état précédent, lorsqu'un problème survient, comme par exemple une cyberattaque, qui pourrait provoquer un consensus de la part de la gouvernance pour revenir à l'état précédent et restituer les fonds aux utilisateurs concernés (exemple du *hack* de The Dao en 2016).

Sachant cela, les *hackers* visent donc en priorité les *blockchains* publiques, dont la résolution d'une cyberattaque est plus complexe et donc avec une probabilité de conservation des gains pour le *hacker* plus élevée.

Les *blockchains* de consortium valident les transactions plus rapidement, et ne sont pas sujettes aux engorgements, avec des frais de transaction nuls ou faibles.

Cependant, étant donné que le maintien et la gestion de la *blockchain* de consortium sont effectués par un groupement d'institutions ou entreprises ayant des objectifs et intérêts communs, elles sont de ce fait moins neutres et résilientes. Une option toutefois envisageable est celle de connecter la *blockchain* de consortium à une *blockchain* publique, permettant ainsi de bénéficier de la neutralité et de la résilience élevée de cette dernière. Cela permet également de réduire les risques d'obsolescence du projet par « l'externalisation des mises à jour ». C'est ce que tentent de faire des acteurs comme JP Morgan *via* Quorum ou ce que fait déjà un acteur comme Kalima. À ce jour, on ne voit pas encore beaucoup d'initiatives allant dans ce sens.

L'adoption d'une *blockchain* de consortium peut offrir une alternative à la *blockchain* publique, offrant une sécurité et une scalabilité accrues tout en préservant un certain niveau de décentralisation. Les cas d'usage réussis concernent des situations où plusieurs acteurs différents doivent collaborer, tels que la gestion de la chaîne d'approvisionnement par exemple.

La *blockchain* privée

La *blockchain* à validateur unique (c'est à dire tenue par une seule institution ou entreprise) reste une option finalement assez proche d'une base de données centralisée.

Elles offrent un contrôle total sur l'infrastructure *blockchain*, avec des niveaux de sécurité et de confidentialité élevés.

Certains projets, comme le consortium Aura dans le secteur du luxe, ont d'abord utilisé une *blockchain* privée pour garder le contrôle sur leurs nœuds. L'objectif est de créer des passeports digitaux avec une *blockchain* privée pour améliorer la traçabilité des produits tout au long de la chaîne de valeur.

Mais ces *blockchains* recréent de la centralisation.

Toutefois, l'intérêt de la *blockchain* reste de définir un consensus, un état de référence qui satisfasse les parties prenantes, sans faire intervenir un tiers de confiance.

Dans ce cas, le recours à des processus de traitement de données sans l'utilisation de la *blockchain* sont plus pertinents :
- Ils demandent moins d'efforts opérationnels, de déploiement et de gestion ;
- Ils sont plus rapides et efficaces.

Sur le plan technique, la mise en place d'une *blockchain* demande un investissement initial élevé pour sécuriser et adapter les processus en interne, lesquels peuvent être incompatibles avec le modèle de traitement des données et les enjeux de sécurité sur les *blockchains*. Par ailleurs, la *blockchain* doit être maîtrisée sur l'ensemble des maillons de la chaîne de production pour être incorporée efficacement dans une organisation. Le recours aux *smart contracts* n'est souvent pas circonscrit par les industriels aux cas d'usages qui le nécessitent strictement comme par exemple la tokenisation, entraînant des lenteurs techniques et des surconsommations énergétiques et financières inutiles, et une perception erronée de l'efficacité technique de la *blockchain*.

À l'inverse, développer et exécuter « off chain » des programmes, accessibles de façon transparente en open-source, puis inscrire uniquement la preuve d'exécution sur la *blockchain*, est une alternative bien plus efficace que le recours aux *smart contracts* sur *blockchain* publique dans de nombreux cas. Avec l'utilisation des technologies de zero knowledge proof (ZKP),

aucune perte de transparence ou de confiance n'est à déplorer par rapport à l'utilisation d'un *smart contract* puisqu'à partir des procédés en open source, il reste possible de vérifier que la preuve inscrite sur la *blockchain* correspond bien à leur bonne exécution. Des solutions de Zk-SNARKS peuvent notamment être envisagées. Le Zk-SNARKs est une forme particulière de zero knowledge proof , qui a été développé pour les *blockchains*, afin de sécuriser les transactions et protéger la vie privée des utilisateurs. Il permet de prouver qu'une information est véridique sans avoir à la révéler, tout en cherchant à optimiser les ressources informatiques alloués à ce processus. En revanche, un gain en termes d'efficacité en découle puisque l'exécution des protocoles se fait de manière centralisée, rapide, et les preuves sont souvent moins volumineuses pour le réseau que les données elles-mêmes. Le respect des principes de protection des données personnelles (RGPD, PIPL, CCPA...) reste à la charge des entreprises et du secteur public, que l'immuabilité des *blockchains* n'impacte pas.

Encadré : avis d'experts sur les orientations techniques des *blockchains*

Arguments en faveur des *smart contracts*

Les *smart contracts* permettent une certaine forme de neutralité d'exécution, *via* des protocoles entièrement décentralisés et autosuffisants (l'exécution du protocole ne repose pas sur un acteur en particulier).

Lorsqu'il s'agit d'un protocole ayant vocation à être neutre vis-à-vis d'intermédiaires, les *smart contracts* et l'exécution « on chain » peuvent effectivement prendre sens, et l'entièreté du cadre est alors définie par le code.

Ainsi, dans le cas de la *DeFi* notamment, l'utilisation de *smart contracts* permet de s'assurer que le financement est présent et que si les conditions sont réunies, l'utilisateur recevra effectivement les fonds attendus.

Dans des cas de faillite d'un tiers, les *smart contracts* ont aussi un intérêt évident pour sécuriser techniquement le paiement des créanciers (caractère « inévitable du *smart contract* »).

Arguments en dévafeur des *smart contracts*

Certains acteurs et ingénieurs interrogés ont toutefois une position plus nuancée sur les *smart contracts*. Deux défauts majeurs sont systématiquement mis en avant:

- L'immuabilité des traitements, y compris en cas de bug (par exemple une défaillance d'un oracle), même si cela peut être résolu dans certains cas *via* un recours à la gouvernance pour traiter le bug de façon transparente (en exigeant par exemple qu'un quorum de membres a bien été atteint pour qu'un processus correctif soit déclenché et par qui)
- La lenteur d'exécution due au fait que le code est exécuté par autant de CPU que de validateurs, impliquant aussi un questionnement vis à vis de l'efficacité

Dans ce cas, ces acteurs considèrent qu'il conviendrait d'effectuer le traitement des données de manière transparente « off chain », et inscrire uniquement les preuves de traitement sur une *blockchain*. Cela amènerait le même niveau de transparence d'exécution, mais d'une manière plus optimale.

Ces limites posent la question de l'intérêt de décentraliser les processus sur la *blockchain* lorsque l'on peut simplement les rendre vérifiables plus simplement et tout aussi efficacement.

De plus, un traitement des données « off-chain » permettrait d'assurer qu'aucune donnée personnelle n'est enregistrée sur la *blockchain*, mais seulement leurs empreintes. Cette méthode respecte les objectifs fixés par la CNIL sur les données personnelles et le RGPD car les données n'ont pas besoin d'être partagées tant qu'elles sont vérifiables.

À noter que l'intérêt de la décentralisation réside en fait plus dans le partage et le contrôle de la base de données que dans son immuabilité.

Pour qu'un *smart contract* soit utile, il ne doit pas dépendre de la validation d'un acteur privé, et être parfaitement audité et sécurisé afin de limiter les risques de bug ou de censure. Par exemple, un *smart contract* qui sous-tend un flash loan est utile car son exécution est conditionnée par le comportement de plusieurs parties prenantes en fonction de conditions définies a priori entre ces parties prenantes ; elle est dynamique. En revanche, un *smart contract* pour certifier l'authenticité d'un diplôme n'est pas toujours la solution la plus efficace car l'authenticité de ce diplôme ne va pas varier en fonction du comportement de plusieurs parties prenantes selon des conditions prédéfinies ; elle reste statique.

Sur le plan économique, le modèle des *blockchains* n'est pas encore assez mature et il est difficile d'estimer correctement les gains que génère l'utilisation d'une *blockchain*, et donc de se projeter facilement

sur le long-terme, même si le cas d'usage est bien choisi. Par ailleurs, de nombreux industriels ont pu se lancer sur la mise en place de projets *blockchains* pour traiter de cas d'usages pour lesquels la *blockchain* n'était en fait pas la technologie la plus pertinente, et donc avec le meilleur retour sur investissement. Pour rappel, les cas d'usages appropriés sont ceux pour lesquels il fait sens d'avoir une gouvernance décentralisée, d'inscrire des données ad vitam æternam/définitivement et d'être en mesure de les vérifier et de communiquer des informations dynamiques, qui évoluent rapidement.

Encadré : l'exemple de Filecoin, une initiative de stockage *cloud* en open source et faisant appel à la tokenisation

Filecoin est une solution développée par Protocol Labs, un laboratoire de recherche basé à San Francisco qui crée des systèmes logiciels dédiés à la promotion d'une expérience utilisateur de qualité et avec une approche open-source.

L'objectif de Filecoin est de décentraliser le stockage des données, en encourageant les utilisateurs à participer à la marche du réseau, de trois manières :

- Mettre en location son propre espace de stockage sur le réseau,
- Stocker des données sur le réseau et en conditionner l'accès à sa guise,
- Consulter, acheter des données selon les conditions définies par leur propriétaire.

Le projet repose sur le protocole IPFS (InterPlanetary File System), aussi développé par Protocol Labs, et y ajoute une logique de marché avec son *token* FIL. Ce *token* permet aux utilisateurs de stocker ou acheter des données sur le réseau, et récompense les utilisateurs qui mettent leur espace de stockage à disposition du réseau. Aussi, le réseau Filecoin permet une grande interopérabilité, il est par exemple d'ores et déjà possible de stocker un *smart contract* publié sur Ethereum sur la *blockchain* de Filecoin, et aussi d'en assurer la confidentialité des transactions.

Il s'agit d'une solution de *cloud* décentralisé qui apporte aux utilisateurs :

- Une transparence d'exécution, tout en permettant de stocker des données confidentielles de manière cryptée
- Une réduction des coûts de stockage, l'espace disponible devient la ressource d'un nouveau marché ouvert et compétitif
- Un plus grand contrôle sur les données stockées.

Les communautés *blockchain* fonctionnent beaucoup en « peer production » par le biais de communs numériques de type organisation autonome décentralisée (DAO), avec des nombreux projets développés en « *no code* » pour générer des *smart contracts* selon le mode de gouvernance le plus adapté à l'organisation souhaitée (governance as a service). Une cellule pourrait être mise en place au sein des entreprises, afin d'analyser ces ressources en accès libre, et capitaliser sur l'expertise de ces communautés, que ce soit pour limiter l'investissement technique ou pour évaluer plus finement l'intérêt économique de la *blockchain* sur des cas d'usages spécifiques.

Bonne pratique n° 1

Pour l'opportunité du recours à la *blockchain* :

- diffuser largement un guide de bonnes pratiques avec des critères pour dire s'il est pertinent de mettre en place une *blockchain* ou non dans une organisation en fonction de sa maturité et des cas d'usages à traiter ;
- analyser et capitaliser sur les communs numériques en open source, notamment de type DAO avant de développer des projets *blockchains* ;
- identifier si le recours au *smart contract* est nécessaire ou si l'inscription de la preuve d'accomplissement sur la *blockchain* d'un programme développé et exécuté par l'entreprise, accessible en open source, est suffisante.

5.2. LEVER LA DIFFICULTÉ LIÉE AU VOLUME DE DONNÉES

En matière d'échange de données cependant, une première difficulté est liée au volume de données pouvant être incorporées dans une *blockchain* publique. Dans les *blockchains* publiques, les frais de réseau peuvent en effet rapidement augmenter ce qui impose une limite importante vis-à-vis du nombre de transactions qui peuvent être réalisées.

Encadré : les freins liés à l'engorgement des *blockchains*

L'engorgement des réseaux *blockchain* publics est une conséquence des mécanismes présentés en introduction. Il existe une limite maximale de transactions validées dans le réseau pour une durée donnée. L'engorgement d'un réseau *blockchain* correspond à la situation dans laquelle il se rapproche de cette limite. Dans ce cas, les nœuds validateurs sélectionnent les transactions à valider en fonction des frais payés par transaction. L'engorgement peut constituer un blocage pour des cas d'usage nécessitant un volume important de transactions, tant les coûts peuvent rapidement s'élever dans un réseau fortement utilisé, blocage qui peut être levé par des mécanismes présentés ci-dessous (*sharding* et *layers 2*).

Il est donc nécessaire de trouver un juste équilibre entre offre et demande sur le réseau, et de réduire au maximum l'écart entre les deux. Côté offre, cela nécessite de trouver le bon moyen de prendre en charge l'ensemble des transactions sur le réseau, sans exposer son jeton à un risque inflationniste trop fort, ou en *layer 2*. Côté demande, cela nécessite d'attirer bon nombre d'utilisateurs, sans diluer leur participation, et a fortiori leur rémunération.

Pour répondre à cette difficulté d'ordre technique, les acteurs peuvent avoir recours à deux méthodes.

Première méthode : le *sharding*[73], qui est un concept courant en informatique, consiste à diviser une base de données pour en répartir la charge. C'est aujourd'hui une piste de solution au problème de l'engorgement et ses conséquences sur la scalabilité et les coûts de transactions au sein du réseau, en répartissant la charge sur plusieurs sous-réseaux coordonnés (appelés shards).

Le sharding est un concept qui peut s'implémenter principalement de deux manières avec leurs impacts spécifiques.

[73] https://ethereum.org/fr/upgrades/sharding/

- Pour diviser et mieux organiser la base de données associée à la *blockchain*. Avec ce type d'implantation du sharding, l'accès aux données est simplifié et plus rapide, mais l'engorgement du réseau reste inchangé. Il est indiqué que le nombre de shards augmentera dans le temps, et que la sécurité du réseau restera inchangée.
- Pour diviser la charge d'exécution des transactions. Ce type de sharding permet un vrai gain en termes d'efficacité et de scalabilité, mais avec tradeoff au niveau de la sécurité des transactions.

Deuxième méthode : les *layers 2*, sont un type de solution qui, contrairement au sharding, n'impactent pas l'infrastructure *blockchain* et la sécurité qu'elle propose, et permettent de pallier le problème de passage à l'échelle. C'est une solution viable qui est déjà déployée, même si elle n'est pas encore massivement répandue, dont l'usage s'est fortement accéléré dans l'écosystème, à l'image des *layers 2* sur Ethereum comme Optimism, Arbitrum ou encore la « side chain » Polygon.

Le fonctionnement d'un *layer 2* avec le Lightning Network de Bitcoin est décrit en Annexe 6.

Ainsi, il est préférable d'effectuer les opérations et les traitements de données en dehors de la *blockchain* (« off chain ») autant que possible. Cela permet de limiter les volumes et coûts de transaction sur la *blockchain*, tout en garantissant l'authenticité des preuves d'exécution des opérations en les inscrivant sur la chaîne (« on chain »). En d'autres termes, les entreprises peuvent utiliser la *blockchain* pour enregistrer les preuves immuables des transactions importantes, tout en effectuant la plupart des tâches hors de la chaîne (« off chain ») pour améliorer l'efficacité globale du processus de production. Cela évite de stocker les données directement sur la *blockchain*, ce qui serait coûteux. D'autre part, ce processus évite des coûts de transaction élevés et permet une plus grande rapidité.

La problématique de la maîtrise de l'engorgement demande de concilier à la fois sécurité et adaptabilité au volume de transactions. Il est à la

fois risqué et difficile d'agir directement sur les mécanismes propres à l'infrastructure de la *blockchain*, et c'est pour cette raison que la maîtrise de l'engorgement par utilisation de la méthode *layer 2* semble être une bonne approche.

Bonne pratique n° 2

Pour éviter la saturation des réseaux et réduire les frais élevés de transaction :

- utiliser un *layer 2* (ex: Lightning Network pour Bitcoin, Starkware ou Polygon pour Ethereum). Par exemple, cela permet de réduire de manière significative les frais de transaction, d'augmenter la scalabilité et d'ajouter de nouvelles fonctionnalités qui ne sont pas disponibles sur la chaîne principale ;
- réaliser les processus de production au maximum *« off chain »*, c'est-à-dire en dehors de la *blockchain*, et n'inscrire que les preuves *« on chain »*.

5.3. LEVER LA DIFFICULTÉ LIÉE À LA QUALITÉ DES DONNÉES

Toujours en matière d'échange de données, une seconde difficulté tient à la qualité des données. En effet, la *blockchain* ne certifie pas la qualité des données enregistrées, ce qui pose la question de la fiabilité de la donnée en général. En particulier, si l'enregistrement d'une donnée non fiable est suivi de l'enregistrement successif de données fiables, dans ce cas, on ne pourrait pas identifier l'enregistrement de la donnée erronée.

Il y a donc un véritable besoin de garantir que les données sources sont exactes, non manipulables et récoltées selon une méthode définie et transparente. En réalité, on ne peut garantir la véracité des données qui proviennent de la *blockchain*. Toute donnée importée de l'extérieur peut

être erronée et il s'agit alors de décider comment gérer ce risque. On peut notamment avoir recours à des oracles.

Les avis peuvent diverger sur l'augmentation du risque de manque de fiabilité de données selon l'utilisation d'une *blockchain* publique ou de consortium. Si la *blockchain* de consortium, par une gouvernance restreinte et à la main du consortium, peut mettre en place des dispositifs limitatifs d'enregistrement et d'accès aux données pour en augmenter la maîtrise, il peut être argué d'un autre côté que la probabilité de corruption dans un système fermé et petit est accrue, avec des alliances plus faciles à mettre en place et des enjeux clairement identifiés.

Pour améliorer la transparence et l'efficacité du processus de production, on peut utiliser Les méthodes agiles et DevSecOps pour permettre le suivi en temps réel de chaque étape de la production et la transmission des informations pertinentes de manière sécurisée.

Les méthodes agiles et DevSecOps sont des approches de développement de logiciels utilisées pour automatiser le suivi de la chaîne de production et l'incorporation des données dans la *blockchain*. Les méthodes agiles font référence à une approche de développement de logiciels qui favorisent la collaboration, l'adaptation et la livraison rapide de solutions fonctionnelles. Dans ce contexte, l'utilisation de méthodes agiles permettrait de créer des outils de suivi de la chaîne de production de manière itérative et en collaboration avec les parties prenantes, en s'adaptant rapidement aux changements et en livrant des résultats fonctionnels rapidement.

DevSecOps est une méthode de développement de logiciels qui vise à intégrer la sécurité tout au long du processus de développement, plutôt que de la considérer comme une étape ultérieure. Dans le contexte de l'utilisation de la *blockchain* pour suivre la chaîne de production, l'utilisation de DevSecOps permettrait d'assurer la sécurité des données et de la *blockchain* en intégrant des tests de sécurité tout au long du processus

de développement et de déploiement. Cela garantirait que les outils développés pour automatiser le suivi de la chaîne de production sont sécurisés et protègent l'intégrité des données inscrites dans la *blockchain*.

Ces méthodes permettraient de garantir l'intégrité des données tout en réduisant les erreurs et en améliorant la traçabilité des produits. Les entreprises pourraient ainsi mieux contrôler leur chaîne d'approvisionnement et répondre plus rapidement aux problèmes éventuels, ce qui pourrait améliorer la qualité des produits et renforcer la confiance des consommateurs.

Bonne pratique n° 3

Pour améliorer la qualité des données dans les *blockchains* :

- avoir recours aux oracles les plus fiables possibles et les moins contestables, sélectionnés en fonction du cas d'usage, voire les multiplier quand cela est possible ;
- responsabiliser les équipes en charge de la qualité des données au sein de l'organisation à l'enregistrement des données sur la *blockchain* ;
- développer des outils automatisant le suivi de l'ensemble de la chaîne de production et l'incorporation des données dans la *blockchain*, de type méthodes agiles et DevSecOps, entre autres.

5.4. LEVER LA DIFFICULTÉ LIÉE À L'INTEROPÉRABILITÉ DES *BLOCKCHAINS*

Une troisième difficulté tient à l'interopérabilité des *blockchains*. Il peut en effet parfois être nécessaire d'importer des données d'une *blockchain* à une autre. C'est par exemple le cas si une donnée de logistique, enregistrée sur une *blockchain* pour optimiser la *supply chain* d'une entreprise,

est nécessaire pour déclencher des opérations d'affacturage traitées dans une autre *blockchain*.

L'importation de ces données inter *blockchain* est principalement explorée *via* des « bridges »[74], centralisés ou décentralisés, unilatéraux ou bilatéraux. Un bridge est un protocole qui permet la mobilité des actifs entre plusieurs *blockchains*. Ils établissent une passerelle entre les réseaux par laquelle les *smart contracts*, les données, les *tokens* et diverses informations peuvent être transférés d'une chaîne à l'autre. Ils peuvent être créés pour permettre des échanges entre *blockchains* ou layers. Généralement, un *smart contract* sur la *blockchain* émettrice a pour rôle de bloquer des *tokens* pour qu'ils ne puissent plus être utilisés, et il réplique le *smart contract* sur la *blockchain* ou le layer de destination.

Les bridges inter *blockchains* sont souvent moins sécurisés que les *blockchains* elles-mêmes, notamment du fait d'un nombre plus faible de validateurs. Par exemple, en mars 2022, le bridge de Ronin a subi un *hack* très important de 620 millions de dollars[75]. Il s'agit de l'un des *hacks* de crypto-actifs les plus importants, qui a pu se produire, malgré les schémas de sécurité mis en place (décentralisation du protocole Ronin notamment).

Les oracles et les bridges sont des solutions qui apportent de l'interopérabilité, cruciale pour le développement de la technologie. Sans celle-ci, les *blockchains* et autres systèmes d'information sont imperméables entre eux, et donc peu propices à l'efficacité et l'adoption. L'objectif de l'interopérabilité est de permettre des interactions automatiques et sans faille par un langage et des normes communes, pour transférer des *tokens* par exemple.

[74] *https://cryptoast.fr/qu-est-ce-qu-un-bridge-pont-crypto-actifs-comment-ca-fonctionne/*

[75] *https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=w*

L'interopérabilité se traduit par des connecteurs entre infrastructures différentes et par des standards, domaines sur lesquels les entreprises anglo-saxonnes ont une emprise importante.

- Les connecteurs sont une brique clé à maîtriser pour connecter les « îlots » numériques ou les réseaux d'infrastructures différents.
- Les normes et standards sont également clés.

L'interopérabilité des *blockchains* peut conduire à des compromis en termes de sécurité. En effet, chaque réseau *blockchain* possède des caractéristiques distinctes telles que la vitesse, la scalabilité, la composabilité, la sécurité et la décentralisation et ces réseaux ne sont souvent pas construits pour communiquer entre eux. Ainsi, pour résoudre les problèmes d'interopérabilité, il a parfois été choisi de sacrifier la sécurité pour pouvoir déployer une solution rapidement. C'est ainsi qu'il y a notamment eu des dizaines de bridges mis en production, souvent avec de grosses failles de sécurité qui ont parfois conduit à des *hacks*, comme par exemple le *hack* de Ronin où le bridge correspondant était contrôlé par neuf validateurs seulement dont cinq ont été piratés. D'autres solutions sont plus sécurisées mais prennent plusieurs années à être mises en production.

Les experts interrogés dans le cadre de ce rapport appuient qu'il y a aujourd'hui suffisamment de portabilité et d'interopérabilité pour ne pas être cloisonné dans une technologie si elle n'est plus d'actualité.

Encadré : la question de l'interopérabilité par le biais de l'EBSI

L'interopérabilité est ainsi érigée comme priorité à l'échelle de l'Union européenne, par le biais de standards communs et collaboratifs. L''Infrastructure Européenne de Services Blockchain (EBSI) a justement pour objectif d'être un standard de conformité européenne. Il s'agit d'un projet de la Commission Européenne et du Partenariat Européen sur la Blockchain (PEB), centré sur l'utilisation de la *blockchain* dans le secteur des services publics, et introduisant les concepts de confiance, de sécurité, d'interopérabilité et de respect du RGPD. L'EBSI est une *blockchain* européenne, dont les différents nœuds validateurs sont répartis dans toute l'Europe. Il repose sur des normes ouvertes et avec une infrastructure de code accessible à tous, ce qui favorise la création de services transfrontaliers et interopérables. Les utilisateurs ciblés de cette *blockchain* sont les services publics, les entreprises et les citoyens européens. En tant que première infrastructure *blockchain* à l'échelle européenne et pilotée par le secteur public, l'EBSI repose sur cinq principes théoriques fondamentaux :

- limiter son utilisation aux projets apportant un bien public net aux citoyens des États membres de l'Union Européenne ;
- garantir des décisions prises par consensus des parties prenantes ;
- harmoniser les normes techniques et ainsi encourager l'interopérabilité des protocoles ;
- construire les codes sources des services en open source, pour garantir un certain niveau de sécurité, de confiance et une concurrence saine entre les acteurs ;
- développer des cas d'usage conformes aux exigences européennes, notamment au RGPD et au règlement eIDAS.

Bonne pratique n° 4

Pour améliorer l'interopérabilité des *blockchains* :

- définir des standards de sécurité avec les parties prenantes et participer à l'élaboration de nouvelles normes utilisables par tous afin de faciliter l'interopérabilité ;
- Utiliser des bridges ou des oracles pour faciliter l'importation de données fiabilisées inter *blockchains* ;
- Choisir des solutions sécurisées pour minimiser les risques de piratage, en réalisant des audits ou en obtenant des rapport d'attestation de sécurité informatique (SOC2, ISO 27001, SecNumCloud) ;
- Anticiper les problématiques liées à l'interopérabilité dès la conception des projets *blockchain.* Il est primordial de bien choisir la *blockchain* en fonction du cas d'usage initié ;
- utiliser des *blockchains* de *layer 0*, interopérables avec d'autres écosystèmes ;
- Se doter de procédures et de contrôles de sécurité informatiques dans la mise en place des différents outils utilisés.

5.5. LEVER LA DIFFICULTÉ LIÉE À LA CONFIDENTIALITÉ DES DONNÉES ET AU TRAITEMENT DES DONNÉES PERSONNELLES

La technologie *blockchain* peut présenter les risques suivants pour la gestion de la confidentialité des données :

- la transparence et l'immuabilité des données de la *blockchain* peuvent faciliter l'espionnage industriel ;
- la qualification et la maîtrise du risque cyber nécessite des compétences spécifiques et rares dans le cadre des projets *blockchain* ;
- l'application du droit à l'oubli est complexe en pratique car l'enregistrement d'une transaction est immuable sur une *blockchain.*

Les entreprises doivent veiller à trouver un équilibre entre les mesures de protection adaptées aux risques cyber auxquels elles sont exposées et la formation aux outils *blockchain* pour se prémunir contre ces risques.

Encadré : précisions techniques sur l'anonymisation des données sur une *blockchain*

La *blockchain* se caractérise par la transparence et la traçabilité des transactions, avec une identification pseudonyme, matérialisée par la clé publique sur le réseau. Par conséquent, la pseudonymisation est un traitement de données à caractère personnel qui permet de relier ces données à une personne physique uniquement *via* des informations supplémentaires, non disponibles à tous et généralement stockées sous forme de matrice.

Cette matrice qui relie pseudonyme à identité réelle est donc une « clé » qui permet *in fine* d'accéder :

- aux caractéristiques de l'ensemble des transactions effectuées (montants, destinataires pseudonymes, date) ;
- à l'ensemble des jetons détenus, des données inscrites et des activités sur le réseau ;
- aux identités réelles des personnes en lien avec un utilisateur déjà identifié (destinataire de transaction par exemple).

Des matrices de ce type existent d'ores et déjà puisqu'un KYC est obligatoire pour acheter des *tokens* auprès d'un intermédiaire ou d'une plateforme d'échange, même si elles sont conservées de manière privée.

Encadré : état des lieux de l'utilisation du ZKP

Des institutions financières l'appliquent à la *blockchain* en mode prototypage, notamment pour la gestion de la confidentialité des transactions. En effet, il permet par exemple à un tiers de s'assurer qu'une personne a réalisé un paiement, sans pour autant avoir de visibilité sur ses transactions antérieures, contrairement aux procédés actuels de KYC sur *blockchain* qui créent le lien entre identité réelle et pseudonyme, et donc de facto avec ses transactions passées.

Bonne pratique n° 5

Pour augmenter la garantie de confidentialité des données :

- privilégier le traitement des données *« off chain »*, et l'enregistrement de données cryptées et anonymisées *« on chain »* ;
- utiliser des solutions de Zero Knowledge Proof afin de garantir la confidentialité des données ;
- mettre en place un partenariat avec des acteurs directement en prise avec les enjeux RGPD sur *blockchain* dans l'objectif de développer une interprétation commune de l'application du RGPD à la *blockchain*, et de la communiquer à l'ensemble de l'écosystème sous la forme d'un guide de bonnes pratiques ;
- former les personnes en charge du maintien des solutions *blockchain* au risque cyber.

5.6. GÉRER LES RISQUES LIÉS À L'UTILISATION D'UNE *BLOCKCHAIN*

La technologie *blockchain* est une technologie encore considérée comme naissante et non massivement testée. En tant que telle, une *blockchain* peut fonctionner de manière inattendue ou non intentionnelle. Des hackers ou organisations malveillantes peuvent identifier et exploiter les faiblesses du réseau, provoquant un comportement inattendu ou non intentionnel.

Les problèmes techniques résultant de causes internes ou externes associées au développement d'une *blockchain*, telles que le manque d'évolutivité, les mécanismes de validation des blocs ou les utilisations frauduleuses, pourraient entraîner diverses conséquences néfastes, par exemple pendant des pics d'activité.

Le développement et la viabilité future des *blockchains* restent souvent imprévisibles avec par exemple le risque qu'un réseau ne perde en sécurité car plus administré par un nombre suffisant de nœuds Plus généralement, le développement et l'utilisation ultérieurs des *blockchains*, qui font partie d'une nouvelle industrie en évolution rapide, sont soumis à une variété de facteurs difficiles à évaluer.

Certains projets, protocoles et entreprises instaurent notamment la mise en place des primes *« bug bounty »*. Cela consiste à offrir une récompense financière à des personnes externes à l'entreprise pour qu'elles cherchent et signalent les failles de sécurité dans la *blockchain* avant son lancement. Cette pratique permet d'identifier les vulnérabilités de la *blockchain* avant que celle-ci ne soit déployée, ce qui permet aux entreprises de corriger les erreurs et de renforcer la sécurité avant que des pirates informatiques ne puissent exploiter ces failles. En offrant des primes attractives pour la découverte de ces vulnérabilités, les entreprises peuvent mobiliser des experts en sécurité informatique pour tester leurs systèmes et signaler les problèmes avant que ceux-ci ne causent des dommages importants. Cette pratique est de plus en plus courante dans l'industrie de la

blockchain et est considérée comme une étape importante pour assurer la sécurité des systèmes déployés.

Par exemple, en juin 2022, un *hacker* éthique aussi appelé « white hat » a reçu une prime *« bounty »* de six millions de dollars pour avoir trouvé une vulnérabilité technique sur le protocole *DeFi* Aurora[76].

De nombreuses structures font également certifier leur processus de cérémonie des clés par un tiers indépendant *via* un rapport de type ISAE 3000, qui consiste à garantir la transparence et la sécurité du processus de gestion des clés privées utilisées dans la *blockchain*. La cérémonie des clés est un processus important pour la sécurité de la *blockchain*, car elle permet de générer et de distribuer les clés privées qui permettent d'accéder aux actifs stockés dans la *blockchain*. En faisant certifier ce processus par un tiers indépendant, les entreprises peuvent prouver à leurs clients utilisateurs, prospects et auditeurs externes que leur processus de cérémonie des clés est fiable et conforme aux normes de sécurité établies. Le rapport ISAE 3000 est une norme internationale qui permet de garantir l'efficacité et la conformité des processus de contrôle interne. En obtenant une certification de ce type, les entreprises peuvent renforcer la confiance de leurs clients et de leurs partenaires dans leur système de *blockchain* et démontrer leur engagement en matière de sécurité et de transparence.

5.7. GÉRER LES RISQUES LIÉS AUX *SMART CONTRACTS*

Tout dysfonctionnement faisant suite à d'éventuelles évolutions technologiques, toute erreur de codage engendrant un fonctionnement inattendu du contrat autonome sous-jacent utilisé pour les jetons peuvent entraîner un fonctionnement inapproprié des jetons, ou un fonctionnement inattendu ou non intentionnel. Un *fork* intentionnel de la *blockchain* sous-jacente, c'est-à-dire la division des membres du réseau

[76] *https://coinacademy.fr/actu/defi-hacker-white-hat-bounty-6-millions-dollars/*

d'une *blockchain* résultat en deux groupes, chacun se fiant à une version différente de la *blockchain* originale, peut conduire au même résultat.

5.8. GÉRER LES RISQUES LIÉS AUX ÉVOLUTIONS RÉGLEMENTAIRES

Le cadre réglementaire applicable à la *blockchain* et à ses applications reste largement en développement, malgré une approche commune en matière de réglementation de marché de crypto-actifs au sein de l'Union européenne dans le cadre du règlement MiCA. En effet, en attente de son application, l'écosystème reste régi par des règles hétérogènes et mouvantes, et même après son application, des champs substantiels relèveront toujours du domaine national (comptabilité, fiscalité, etc.).

À noter en particulier les risques :

- En matière comptable : la diversité des actifs numériques et des cas d'usage rendent difficiles les analyses comptables, à plus forte raison que les équipes comptables peuvent manquer de la compétence technique nécessaire à l'appréhension des objets. Cela entraîne des insuffisances dans la valorisation des taux d'échange crypto/crypto ou crypto/fiat, en matière de valorisation, etc.

- En matière de contrôle interne : la conception du contrôle interne et l'efficacité de son fonctionnement ne sont souvent pas suffisamment robustes ni documentées depuis le début des activités de gestion de crypto-actifs au sein des entreprises. Un dispositif de contrôle interne robuste est nécessaire, notamment autour de l'architecture des clés et du wallet, la génération des clés, la sécurisation des clés, la séparation des tâches, la gestion du wallet et la réconciliation avec la *blockchain*.

- En matière fiscale : dans le cadre de la mise en place d'un dispositif spécifique dédié à la gestion des crypto-actifs et des actifs numériques au niveau de la trésorerie de l'entreprise, certaines problématiques de déclaration fiscale peuvent survenir. Il est notamment important de suivre avec précision toutes les transactions effectuées en crypto-actifs(échanges, achats) et entre actifs numériques, ainsi que leur valeur. Ce suivi est d'autant plus important que l'OCDE va renforcer la transparence fiscale liée aux transactions réalisées en crypto-actifs et/ou actifs numériques en imposant une nouvelle obligation déclarative aux intermédiaires de réception et de transmission d'ordres ou aux entités qualifiées d'institutions financières. Dans ce contexte, il semble opportun pour l'entreprise d'avoir une vision exhaustive d'un point de vue fiscal afin de gérer les interactions futures avec l'administration fiscale qui aura accès aux données et pourra interroger les entreprises concernées. Dans le cas d'un groupe, la mise en place d'un système central de trésorerie commun à toutes les sociétés qui le composent, entraînera des problématiques de prix de transfert.Il est donc clef d'identifier les données fiscales pertinentes afin de gérer les reportings internes et potentiellement futurs externes, dans le respect de la législation en vigueur (IS mais aussi TVA) et en anticipant les éléments de reporting à venir. De façon générale, les outils de mesure du risque sont encore peu évolués et doivent être construits par des experts, et beaucoup plus de garanties doivent être fournies que dans les systèmes classiques (KYC, AML, historique des transactions).

Dans ce contexte, il est intéressant de s'équiper d'outils de reporting comptables, fiscaux et ESG pour les activités *blockchain*. Cela permet d'assurer la conformité réglementaire et la transparence des opérations effectuées dans la *blockchain*. Comme toute activité économique, les opérations effectuées dans la *blockchain* sont soumises à des obligations comptables et fiscales, qui doivent être respectées par les entreprises qui utilisent cette technologie. En utilisant des outils de reporting spécialisés pour la *blockchain*, les entreprises peuvent générer des rapports automatisés qui permettent de suivre et de documenter les opérations effectuées de manière transparente et conforme aux normes comptables et fiscales en vigueur. De plus, la dimension ESG est devenue primordiale, et les entreprises doivent être en mesure de démontrer leur engagement. En utilisant des outils de reporting ESG pour les activités *blockchain*, les

entreprises peuvent rendre compte de leur impact lié à l'utilisation de cette technologie, renforçant ainsi leur engagement envers une gestion responsable et durable.

Bonne pratique n° 6

Pour limiter les risques d'utilisation de la blockchain :

- définir un plan de continuité pour pallier les risques technologiques des *blockchains* ;
- faire revoir par un tiers indépendant et qualifié le développement des *smart contracts* ;
- réaliser un audit de sécurité informatique par un tiers de l'infrastructure *blockchain* ;
- mettre en place des primes *« bug bounty »*, afin de détecter les failles de sécurité avant le lancement
- implémenter des solutions professionnelles de conservation des actifs numériques ;
- concevoir et mettre en place des processus robustes de contrôle interne adaptés à la *blockchain* ;
- faire certifier par un tiers indépendant son processus de cérémonie des clés *via* un rapport de type ISAE 3000 à partager avec ses clients utilisateurs des services ou prospects et auditeurs externes ;
- mettre en place une veille réglementaire et technologique relative à la *blockchain* et aux crypto-actifs pour agir en fonction de leurs évolutions ;
- former ou accompagner les équipes Finance, Juridiques et fiscales en expertises *blockchain* et crypto-actifs ;
- s'équiper d'outils de reporting comptables, fiscaux et ESG pour les activités *blockchains*.

5.9. MIEUX FLÉCHER LES FINANCEMENTS VERS L'ÉCOSYSTÈME

En 2023, les investisseurs institutionnels et les entreprises ont continué leur mouvement d'adoption des crypto-monnaies, à mesure du développement de nouvelles applications *blockchain* portées par les innovations en finance décentralisée *(DeFi)* et du développement de la technologie *blockchain* au-delà du domaine des crypto-monnaies dans l'IoT ou l'identité numérique.

Néanmoins, ces financements sont très concentrés, que ce soit à court-terme avec 55 % des fonds alloués à financer 5 entreprises au premier semestre de 2022, ou à long-terme avec 85 % des montants levés en France depuis 2017 par Ledger et Sorare.

Toutes ces entreprises ne développent pas de *blockchain* à proprement parler mais proposent des produits et des services destinés à capitaliser sur des *blockchains* existantes. Leur sur-représentation dans les montants levés par le secteur *blockchain* indique que les modèles classiques de valorisation et d'analyse du risque restent prédominants au sein du secteur.

Sur ce type de modèles d'affaires, le secteur est confronté aux mêmes défaillances de marché que l'écosystème français des startups, à savoir un manque de financement *late stage*, une insuffisante capacité opérationnelle d'accompagnement des projets dans les fonds en raison d'un manque d'expertise technologique et des difficultés réglementaires persistantes pour participer aux ICOs.

Sur le *late stage*, si toutes les « licornes » françaises dans la *blockchain* ont ouvert leur capital à au moins un actionnaire minoritaire au moment de *scaler*, elles n'ont pas pu éviter de faire appel à des fonds capables de mettre des tickets supérieurs à 100 M€ comme Andreessen Horowitz (a16z), Benchmark, Accel, Headline ou encore Atomico.

Sur la capacité opérationnelle des fonds à accompagner les projets *blockchain*, les fonds sont encore confrontés au manque de maturité du secteur et à l'effet *hype* autour de la technologie qui noie trop souvent des projets viables dans des projets sans roadmap ni vision. Compte tenu des contraintes propres aux *limited partners*, cela contribue à réduire le montant des prises de participation en *token* comme en equity des fonds d'investissement. Pour autant des levées de fonds majeures ont été conduites par des fonds de *venture capital* français à l'instar d'Arianee par Bpifrance ou de Bolero par Newfund. À cet égard, l'enjeu principal pour les fonds d'investissement est de distinguer les projets pour lesquels la décentralisation fait sens, de ceux qui pourraient très bien s'en passer.

D'après le dernier rapport global de PwC sur les opérations M&A et de financement du secteur, il est visible que la zone EMEA accuse d'un retard sur le nombre et le volume de transactions réalisées, dans un marché qui reste largement dominé par les États-Unis, ces derniers concentrant près de 80 % de la valeur des deals conclus au premier semestre de 2022.

La viabilité de projets *blockchain* s'apprécie à l'aune de nouveaux critères qui complexifient la valorisation des *tokens*. La nécessité de valoriser des *tokens* se retrouve dans deux types de projets : les *blockchains*, c'est-à-dire des développeurs à l'origine de la création d'un protocole *blockchain* comme Ethereum, Algorand, Tezos ou Solana pour opérer, et les applications adossées à ces protocoles *blockchain*, proposant des produits ou services accessibles uniquement sur leur *blockchain* avec leurs propres *tokens*, comme Morpho ou Decentraland. Que ce soit pour des services comme l'accès à de meilleures garanties au sein de pools de prêts ou pour des environnements immersifs dans lesquels des produits virtuels sont disponibles, leur accès est conditionné à la détention d'un « wallet » pour y faire des achats et réaliser des ventes en crypto-actifs. Les actifs numériques sont des moyens d'échange pour accéder à ces applications adossées à des protocoles *blockchain*.

Pour les *blockchain* de *layer 1* ou 2, la notion de rentabilité n'a pas de sens puisque leur valeur s'apprécie par l'usage qui en est fait. Pour réduire l'écart entre l'offre et la demande de jetons en circulation, la pratique de détruire des jetons délibérément (burning) permet d'atteindre cet objectif.

Une pression déflationniste sur l'offre peut avoir un impact positif sur le prix, ce qui peut augmenter mécaniquement sa valorisation. Pour limiter la quantité de *tokens* en circulation, il est possible de recourir au burning ou de faire des *buy-back* sur le modèle des BNB de Binance[77] ou de mettre en place des mécanismes de *vesting* impliquant l'acquisition de *tokens* avant leur minage à des prix très avantageux en contrepartie de l'obligation de les bloquer dans le projet durant une période déterminée. De fait, le prix unitaire d'un actif *blockchain* dépend non seulement de la demande mais aussi du nombre total d'actifs de ce type, comme l'illustre le cas du *token* CAKE de PancakeSwap où le nombre d'utilisateurs est très important, mais le nombre de *tokens* aussi, ce qui entraîne leur dilution.

Encadré : définitions utiles

- *Burning :* destruction de manière souvent intentionnelle et permanente d'un *token*, réduisant l'offre totale de *tokens* en circulation.
- *Vesting :* méthode de verrouillage des *tokens* souscrits par les investisseurs dans le projet après son lancement, pour diminuer le risque de perte de valeur du jeton à court-terme, et donner un gage de valeur à long-terme.
- *Buy-back :* rachat de *tokens*, souvent par le créateur du projet, parfois de façon automatisée pour burn les *tokens* rachetés.

[77] + 15 Mds$ équivalent BNB ont été brûlés en février 2022.

Côté demande, plus le *token* sera utilisé, plus le déséquilibre avec l'offre de *tokens* en circulation sera susceptible d'être réduit dans la durée, augmentant et stabilisant mécaniquement son prix. Cette utilisation se mesure par le nombre de nœuds sur le réseau et leur activité réelle qui est difficile à appréhender. Dans les cas de *blockchain* avec des *smart contracts*, les *contract calls*[78] donnent une bonne indication de l'activité réelle et durable des nœuds sur un réseau, dans la mesure où leur activation est payante, et donc généralement représentative de l'activité réelle du réseau.

Certains *tokens* vont être davantage utilisés que d'autres en fonction de la *blockchain* considérée : les *tokens* natifs sont essentiels au fonctionnement de la *blockchain* et sont par définition les plus utilisés. Les *tokens* sont très spécifiques selon l'usage qu'ils portent et la pertinence de cet usage pour l'écosystème d'utilisateurs auquel ils s'adressent. Les indicateurs de mesure de leur succès sont dès lors très variables et dépendant du contexte dans lequel ils sont émis. L'enjeu est d'aligner les intérêts entre toutes les parties prenantes du projet pour que la valeur fondamentale du projet s'apprécie et cela ne se retranscrit pas toujours à court terme dans le prix.

Les mécanismes de *staking* et de participation à la gouvernance d'une organisation autonome décentralisée (DAO) peuvent également avoir des effets incitatifs pour les utilisateurs. Dans le cadre du *staking*, ces incitations sont purement financières car le fait de participer aux phases initiales du projet (jusqu'à la fin des « périodes » de *staking*) permet de maximiser ses gains. Dans le cadre de la participation à la gouvernance d'une DAO, cela va au-delà des incitations financières car cela permet de mobiliser la communauté dans la durée autour de décisions, de construction de normes et de valeurs communes. Par exemple, dans le métavers de Decentraland, la DAO permet à la communauté de déterminer les objets autorisés ou interdits dans l'espace immersif après son lancement,

[78] *Entendu comme le fait de déclencher un smart contract pour effectuer une transaction donnée.*

certains éléments de modération de contenus ou l'organisation d'enchères spécifiques.

Pour les autres *tokens* (sauf les *security tokens*), les porteurs de projet sont tenus au départ par un objectif purement sociétal, détaché de tout objectif de profit (pour ne pas être requalifié en security *token*). Toutefois, des fonds Web3 se créent car ils parient sur le fait que la communauté associée au projet prendra la décision collégialement, à terme, de mettre la rentabilité du projet au premier plan, au moment où les fonds au sein du projet seront totalement décentralisés. Ces fonds sont totalement décentralisés en théorie lorsque les « epochs » de *staking* et que la période de *vesting* pour les investisseurs de départ arrivent à leur terme. On retrouve donc une logique classique propre au venture capital où le montant du ticket est décorrélé de la rentabilité initiale du projet, mais repose sur une promesse d'avenir innovante et impactante.

Encadré : metrics importants pour mesurer l'offre de *tokens*

- Metrics pour la quantité de *tokens* :
  - Offre maximale (max supply) : nombre maximum de coins ou de *tokens* qui seront mis en circulation ;
  - Offre : ensemble des *tokens* déjà créés moins ceux qui ont été détruits volontairement (retirés de la circulation) ;
  - Circulating supply (offre en circulation) : fraction de la total supply qui circule sur le marché à un instant t (sont exclus les *tokens* « stakés », soient les *tokens* détenus par le protocole sur une période définie par un nombre d'« epochs » et ceux détenus par les fondateurs sur une période déterminée par le vesting au lancement du projet et mentionnée dans le whitepaper).

- Market cap : capitalisation de marché d'un *token*, soit la quantité de jetons utilisable dans un écosystème à un instant t (circulating supply × prix du *token*)
- Fully diluted market cap : quantité de jetons maximale de l'écosystème (max supply × prix du *token*)

Source : https://cryptoast.fr/tokenomics-tout-comprendre-economie-tokens/

Pour les applications proposant des produits ou services uniquement accessibles sur leur protocole *blockchain*, la rentabilité doit au contraire être rapidement atteinte pour que le projet fonctionne, ce qui implique de rassembler et de mobiliser très rapidement de nombreux utilisateurs actifs.

Certains projets, notamment de *DeFi* proposant des services aux particuliers et aux entreprises de type placement, obtention ou octroi de prêts etc., sont dépendants de la *Total Value Locked* (TVL), permettant de mesurer un volume d'activité, correspondant à la valeur totale des *tokens* « verrouillés » dans le protocole d'un projet à un instant donné. Plus la TVL est élevée, plus le projet peut être considéré comme reconnu, car cela traduit un volume élevé de transactions potentielles. Ce ratio sert généralement à mesurer la robustesse d'un protocole de *DeFi*. Par exemple, Curve et AAVE sont des exemples de projet avec des TVL élevées, respectivement à $5 et $4.8 milliards au 28 février 2023[79].

Toutefois, il est important de noter que la TVL n'est pas un indicateur pertinent pour tous les projets de protocoles avec des *tokens*, à l'instar du projet Audius[80]. Dans ce projet, les *tokens* sont générés en continu sans perdre de valeur à mesure de « epochs », pour privilégier la création de

[79] https://defillama.com/

[80] https://audius.co/

[81] https://whitepaper.audius.co/AudiusWhitepaper.pdf

nouveaux contenus[81]. Ainsi, la baisse de la TVL ne renvoie pas forcément à une baisse de transactions potentielles, au contraire, elle pourrait même suggérer une croissance continue des transactions liées au projet.

Les applications utilisateurs adossées à un protocole ne peuvent toutefois pas faire l'objet d'une analyse de TVL sans un regard averti en matière de tokenomics, dans la mesure où la TVL peut être manipulable par la pratique de certains investisseurs mal intentionnés et volatile car exprimée en dollar. Dans un marché marqué par une absence de liquidités, des techniques de manipulation de cours appelées hiding whales peuvent engendrer le blocage artificiel de jetons dans un projet pour faire monter artificiellement son prix, au détriment des investisseurs minoritaires. Pour rappel, la TVL de Terra s'était élevée à + 20 Mds$ fin mai 2022. Et *in fine*, la question de la rentabilité des protocoles se pose : au-delà de la TVL, il reste crucial que les frais prélevés permettent d'assumer les coûts sous peine d'abandon à terme d'un projet.

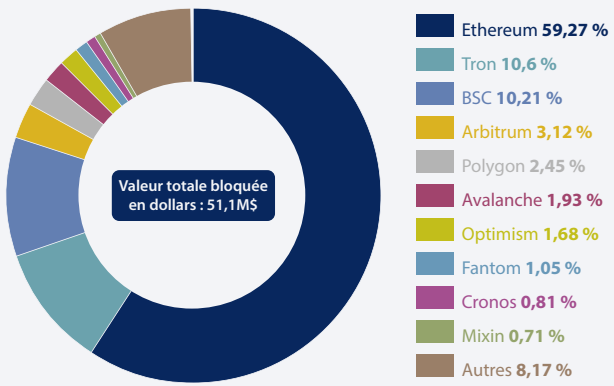
Encadré : modalités de calcul de la TVL

La TVL représente le volume d'actifs stockés à un instant donné dans un protocole.

Ratio de TVL = nombre de *tokens* en circulation du projet × prix actuel / TVL.

Si ce ratio est inférieur à 1, cela renvoie un message positif, car cela signifie que la valeur du jeton est sans doute sous-évaluée par le marché, dans la mesure où un grand nombre d'investisseurs font le choix de maintenir leurs jetons bloqués dans le protocole.

Répartition de la TVL en *DeFi*



Données actualisées le : 16/02/2023.
Source : https://defillama.com/chains

Au-delà des DAOs à l'origine de la création de protocoles *blockchain* et au-delà des applications adossées à ces protocoles *blockchain*, de nombreux services/infrastructures prometteurs sont à créer/renforcer, et des investissements seront là aussi nécessaires.

La valorisation actuelle des NFT est également médiatisée car elle peut sembler déconnectée de la réalité en raison de spéculations excessives dans ce domaine. Les NFT sont devenus très populaires, en particulier dans le domaine de l'art numérique, où certaines transactions ont atteint des sommes astronomiques. Ils permettent aux créateurs de contenus numériques de monétiser leurs œuvres de manière plus directe et transparente, et offrent des possibilités intéressantes dans des domaines tels que les fan *tokens* ou les systèmes de jeu « play-to-earn ». Il est probable que les valorisations deviennent plus en phase avec les usages réels qui se basent sur de vraies fonctionnalités, plutôt que sur une simple spéculation.

Bonne pratique n° 7

Orienter les financements venture capital vers les couches basses de la technologie *blockchain.*

Lexique

Clé de chiffrement : suite de caractères alphanumériques, permettant de chiffrer/déchiffrer une donnée.

Clé publique/ Clé privée : un utilisateur intègre un réseau *blockchain* en générant une clé privée à garder secrète, lui permettant de signer ses interactions sur le réseau. La clé publique est dérivée de la clé privée, et une fois communiquée aux autres utilisateurs du réseau, leur permet de vérifier l'authenticité des signatures générées par la clé privée sans toutefois la dévoiler.

Crypto-actifs : les crypto-actifs, représentent l'ensemble des actifs numériques émis sur une *blockchain* ou une autre technologie de registre distribué (DLT). Contrairement aux crypto-monnaies, ils ne sont pas uniquement conçus pour être utilisés comme moyen de paiement ou pour stocker de la valeur, mais également pour représenter un actif physique, une utilisation ou un droit par exemple. Les crypto-actifs englobent l'ensemble des formats de *token* numériques (NFT, *token* fongibles…).

Crypto-monnaie : une crypto-monnaie est une monnaie numérique qui utilise une technologie de registre distribué (DLT), et bien souvent une *blockchain*.

DAO : organisation autonome décentralisée fonctionnant par le recours aux *smart contracts*.

***DeFi* :** ensemble des protocoles, applications et cas d'usage basés sur la technologie *blockchain*, permettant de répondre à des besoins financiers spécifiques sans intermédiaire financier centralisé.

ICO : Initial Coin Offering, il s'agit d'un mode de financement participatif effectué au lancement d'un projet *blockchain* avec *tokens*, dans lequel tout type d'acteur (dont les particuliers) peut obtenir une quantité déterminée de *tokens* en fonction de son investissement.

Fork : un fork se produit lorsqu'une *blockchain* se divise en deux branches distinctes, généralement en raison d'une mise à jour logicielle ou d'un désaccord entre les nœuds du réseau.

Layer 2 : surcouche publique d'un réseau *blockchain*, profitant de sa sécurité, et ayant un intérêt supplémentaire pour ses utilisateurs par rapport à celui-ci (diminution des frais de transaction, gain de confidentialité, de rapidité d'exécution…).

Métavers : né de la contraction des mots méta (signifiant « au-delà ») et univers, le métavers désigne un environnement numérique et immersif, utilisant la 3D et d'autres technologies immersives telles que la réalité virtuelle (VR) et/ou la réalité augmentée. On peut y interagir socialement avec d'autres personnes incarnées par leur avatar. On peut également y interagir économiquement *via* l'échange d'actifs numériques, d'où l'importance du Web3 au sein de ces mondes virtuels qui permettent la création d'une réelle économie numérique au sein même de ces univers.

MiCA : Markets in Crypto-Assets. Il s'agit du nom du règlement européen en cours de finalisation visant à réglementer les crypto-actifs (notamment les *stablecoins*) et les usages associés.

Oracle : source d'informations initialement hors *blockchain*, permettant d'intégrer automatiquement des données et variables spécifiques dans la *blockchain*, pour personnaliser davantage les *smart contracts* par exemple.

PSAN : prestataire de services sur actifs numériques. Il s'agit d'un statut créé par la loi PACTE en 2019 applicable aux entités offrant des services sur actifs numériques (par exemple : conservation d'actifs numériques, plateforme d'échange, etc.). En l'état, les PSAN exerçant en France doivent être enregistrés.

PSCA : prestataire de services sur crypto-actifs. Il s'agit du futur statut européen créé par le règlement MiCA. Tous les PSCA exerçant dans l'UE devront être agréés.

Scalabilité : au sein du trilemme des *blockchains*, la scalabilité représente la viabilité d'utilisation d'un réseau à une échelle importante. Elle représente la capacité d'une *blockchain* à s'adapter aux volumes de transactions, afin que la vitesse d'exécution des transactions et ses frais ne soient pas affectés négativement.

Sharding : le sharding est un concept qui peut s'implémenter principalement de deux manières avec leurs impacts spécifiques.

- Pour diviser et mieux organiser la base de données associée à la *blockchain*. Avec ce type d'implantation du sharding, l'accès aux données est simplifié et plus rapide, mais l'engorgement du réseau reste inchangé puisque l'exécution des transactions s'effectue encore au niveau du réseau, et non des shards. Après The Merge en Septembre 2022, la roadmap d'Ethereum annonce The Surge, l'implémentation de ce type de sharding sur la *blockchain*. Il est indiqué que le nombre de shards augmentera dans le temps, et que la sécurité du réseau restera inchangée.
- Pour diviser la charge d'exécution des transactions, c'est-à-dire que les shards développent une forme d'indépendance vis-à-vis du réseau dans son entièreté. Une transaction sur le réseau est alors validée au niveau d'un shard, ce qui vaut validation à l'échelle du réseau entier. Ce type de sharding permet donc un vrai gain en termes d'efficacité et de scalabilité, mais avec tradeoff au niveau de la sécurité des transactions. En effet, le nombre de validateurs pour chaque transaction est divisé par le nombre de shards déployés.

Smart contract : les *smart contracts* peuvent être définis comme des scripts persistants auto-exécutés hébergés sur une *blockchain*.

Token : représentation numérique d'un bien, d'un service ou d'un droit, permise par le recours aux *smart contracts*.

Annexe 1

Les apports concrets de la technologie *blockchain*

Sécuriser l'enregistrement de données ou la preuve de leur existence

1/ En produisant des documents certifiés et infalsifiables :
- enregistrer les données brutes ou fournir des preuves d'existence de documents ou de qualifications à un moment donné, par exemple pour les diplômes ;
- fournir des solutions d'authentification de certificats de naissance pour des publics manquant de preuves pour justifier de leur identité (réfugiés, sans domicile fixe), sur le modèle du e-residency programme estonien ;
- faciliter et certifier les échanges, facturations et indemnisations, en rattachant des droits définis par les porteurs de projet à chaque *token* émis. Les *tokens* permettent d'économiser des frais de transaction, en plus d'être échangeables de manière instantanée et sécurisée.

Il convient néanmoins de préciser que la *blockchain*, notamment dans le cadre des *blockchain* privées, permet d'identifier avec certitude l'émetteur d'un document. Néanmoins, il est toujours possible pour un agent malveillant d'usurper l'identité de l'émetteur (en lui volant ses clés privées par exemple). En conséquence, la *blockchain* en tant que telle, n'offre pas des garanties absolues en matière de certification.

2/ En améliorant la transparence et la traçabilité des informations et activités:
- améliorer la transparence et la traçabilité des compensations de carbone sur les marchés volontaires (Toucan Protocol, Cambridge Center for Carbon Credits, Moss, Klima DAO, Climate Trade, Wen) ;

- faciliter la traçabilité des biens et services dans une chaîne de production ;
- suivre les transactions et activités de mise en conformité sur des marchés très fragmentés et faisant intervenir de nombreuses parties prenantes (eau, alimentation, énergie) ;
- enregistrer en temps réel de la provenance de pièces sur la chaîne logistique pour des rappels ciblés, résoudre des problèmes logistiques, ou enregistrer des conteneurs d'expédition au gré de leur progression ;
- suivre de manière différenciée des cargaisons dans la logistique de fret ;
- commercer et échanger plus facilement, rapidement et de manière sécurisée, notamment à l'international.

3/ En conciliant la protection des données sensibles et leur partage à grande échelle pour faire progresser la science et l'innovation :
- réduire le risque cyber de la centralisation de l'information dans le *cloud*, comme c'est le cas *blockchain* Filecoin qui interagit avec le protocole InterPlanetary File System (IPFS) ;
- mieux gérer des données de santé en empêchant la falsification d'antécédents, en fiabilisant la collecte *via* des oracles et en automatisant le partage d'informations pour statuer plus rapidement sur des dossiers médicaux sans erreur, etc. ;
- utiliser des smarts contracts pour optimiser le suivi de la couverture de l'assurance maladie (par exemple, l'EBSI pour mettre en œuvre la vérification transfrontalière de la couverture sociale des travailleurs détachés).

Exécuter des logiciels ou des applications décentralisées

1/ En faisant interagir des dispositifs entre eux sans tiers de confiance :
- octroyer une identité numérique à des tiers pour faciliter les transactions (notamment *via* un KYC décentralisé) ;
- renforcer les technologies existantes qui permettent à des objets de marque différente d'interagir entre eux sans passer par un opérateur centralisé ;

- créer des places de marché décentralisées pour négocier en continu l'accès à des ressources limitées comme l'électricité ;
- donner la possibilité de créer des dispositifs intelligents de type IoT doté de la capacité d'effectuer des transactions économiques directement dans la *blockchain*.

À noter que si des dispositifs sont capables de communiquer en Peer to Peer, il est possible que des objets de marques différentes puissent interagir entre eux, sans avoir nécessairement recours à une *blockchain*.

2/ En automatisant des conditions de déclenchement d'un contrat pour réduire le risque d'erreur :

- traiter de manière automatisée des dossiers d'assurance pour indemniser plus rapidement les clients ;
- fiabiliser la vérification de la réalité d'un événement assurable.

Encadré : *blockchain* et tokenisation, des réalisations notables dans le secteur de l'assurance

Appliquée à des cas d'usages bien choisis, la *blockchain* engendre des gains financiers et d'optimisation de gestion importants. En s'appliquant à tout type de secteur d'activité, elle apporte une plus-value réelle pour les agents économiques. Par exemple, Wakam a développé un outil interagissant avec une *blockchain* qui va être rendu open source permettant la gestion de millions de contrats d'assurance dont des centaines de milliers sont déjà gérés par ce biais. Dans certains cas, il est possible d'avoir un coût d'interaction avec la *blockchain* de quelques centimes par contrat.

Permettre aux procédures existantes de gagner en efficacité et en pertinence

1/ En standardisent les méthodologies et les produits : par exemple, des acteurs dans la cosmétique expérimentent la *blockchain* pour l'analyse du cycle de vie et le scoring des produits, la promesse étant une simplification des processus par une standardisation de marché. Dans un autre secteur comme l'assurance, des acteurs utilisent la *blockchain* pour standardiser le processus et les informations de facturation des contrats.

2/ En digitalisant des processus :

- de production, ce qui permet d'optimiser la *supply chain* en homogénéisant les informations et les documents, notamment entre différents acteurs d'une même chaîne de production. Cette digitalisation *via blockchain*, combinée parfois même à la suppression d'intermédiaires n'ayant plus de réelle valeur ajoutée, permet de réduire certains délais et certains coûts ;
- d'économie circulaire. Ce cas d'usage récent mais prometteur est en train d'émerger pour l'économie circulaire en B2B. Concrètement, la *blockchain* est utilisée pour la réutilisation et le recyclage. Sur certaines industries, comme les biotechnologies, la question de la provenance des matières premières est clef d'autant plus, que ce secteur est, comme peut l'être l'industrie financière, très réglementé avec des processus de transparence et de conformité intrinsèque à la production et la distribution de ces matériaux.

3/ En améliorant la relation client, en particulier pour les acteurs en B2B2C :

- offrir des possibilités intéressantes pour les entreprises dans le domaine de la gestion de la relation client (CRM), avec des fonctionnalités telles que des programmes de fidélité personnalisés, des récompenses numériques et des transactions transparentes et sécurisées ;
- permettre aux entreprises de mieux comprendre les besoins de leurs clients et automatiser certaines interactions avec eux à l'aide de

smart-contract, ce qui peut conduire à certaines automatisations et réductions des coûts. Les données chiffrées et sécurisées sur la *blockchain* offrent également une meilleure protection des informations clients.

Produire des ressources numériques dans des environnements virtuels

1/ En décentralisant l'architecture du Web pour permettre à chacun d'en posséder les ressources :
- « décentraliser » des secteurs ou des disciplines dont la majeure partie de la valeur repose sur l'engagement individuel et les idées (sciences, identité, etc.) ;
- permettre à chaque participant d'une chaîne de valeur d'en tirer profit de manière automatique par des mécanismes de redistribution multi-acteurs codés dans des *smart contract* ;
- acquérir des biens non fongibles comme des terrains dans différents métavers, ou des produits et/ou services représentés par NFT.

2/ En créant des espaces de convivialité pour les utilisateurs :
- fédérer des communautés pour assister à des événements uniques. Après avoir fait un concert exclusif dans Sandbox générant des revenus records, l'artiste a lancé ses « Snoopverse Early Access Pass », qui donnent accès à « toutes les expériences Snoopverse avant tout le monde », et qui regroupent 1 100 propriétaires, avec plus de 1,7 million de dollars de ventes fin juillet 2022. Pour son nouvel album B.O.D.R, Snoop a émi 10 000 NFT en édition limitée, vendus en moins d'une semaine pour une valeur totale de 44 millions de dollars ;
- fournir des jeux demandant un engagement variable de la part des utilisateurs parmi lesquels Roblox, Rockstar Games, entre autres.

3/ En créant des incitations à la création décentralisée de contenu :
- monétiser les interactions volontaires des utilisateurs à l'aide de *tokens*, et non à leur insu comme c'est le cas sur les réseaux sociaux (Steemit puis Hivepar exemple) ;

- inciter les individus à produire du contenu sur la durée par la tokenisation.

Faire émerger de nouvelles formes d'organisation plus participatives

1/ En créant de nouvelles méthodes de gouvernance plus efficaces :
- en instaurant un vote quadratiques ou autres méthodes de type consensus holographique ;
- en permettant l'ouverture du réseau *blockchain* à différents acteurs industriels afin qu'ils interagissent sur une ou plusieurs chaînes de valeur. En effet, lorsque le réseau *blockchain* est ouvert entre différents industriels interagissant sur une ou plusieurs chaînes de valeur, il permet de fédérer des acteurs qui peuvent être compétiteurs ou partenaires. Cela favorise la « coopétition » entre acteurs et l'adoption de nouveaux standards en fédérant des communautés d'acteurs industriels.

2/ En faisant émerger des modèles décisionnels "bottom up" plus inclusifs (ex. la démocratie liquide). Lorsque le réseau est ouvert au consommateur final, la *blockchain* permet de :
- rendre le consommateur plus autonome et responsable ;
- rapprocher consommateurs et producteurs en apportant de la transparence, voire en faisant émerger des « prosumers », des consommateurs, qui, par leur participation au process de fabrication et grâce à la *blockchain*, pourront récolter une partie de la valeur générée ;
- renforcer la confiance à l'échelle d'une organisation ;
- permettre à un consommateur individuel de devenir producteur ou fournisseur, par exemple à travers un *smart contract* dans un immeuble intelligent qui produit de l'électricité et permet à quiconque - y compris ne résidant pas dans l'immeuble de consommer l'électricité produite.

Encadré : la *blockchain* pour ouvrir le marché de la distribution d'énergie

Dans le secteur de la distribution d'énergie, le développement croissant des *smart grids* illustre l'ouverture croissante des marchés permise par la *blockchain*. Les *smart grids* sont des réseaux de distribution électrique qualifiés d'« intelligents » car adaptables à l'offre, à la demande et aux surplus des producteurs. Ils se développent dans un contexte de consommation électrique mondiale croissante (qui a plus que doublé lors des trente dernières années), et de pertes durant l'acheminement de l'électricité. Ils répondent à 4 problématiques importantes pour le secteur de l'énergie :

- réussir à corréler efficacement l'offre des producteurs et la demande des consommateurs dans le marché de l'énergie ;
- aboutir à un réseau sécurisé ;
- réaliser des économies d'énergie ;
- réduire les coûts pour les différents acteurs.

Selon une étude[82] de l'association Think Smartgrids, le marché français des *smart grid* a été évalué à 1,6 milliard d'euros en 2020, et est estimé à 6 milliards d'euros pour 2030. Cette croissance estimée du marché serait accompagnée de nombreuses créations d'emplois (estimés à 60 000 en 2030 en France). L'étude pointe que le secteur français des *smart grids* est en avance sur ses voisins européens, mais son essor est notamment sous contraintes d'investissements croissants et durables dans la recherche et le développement de nouvelles technologies de rupture.

Pour le bon fonctionnement de ces réseaux, un enjeu majeur est de susciter l'intérêt du consommateur pour permettre une adoption à plus grande échelle :

- en certifiant l'origine de l'électricité ;
- En diminuant les coûts de l'électricité (le réseau coûte moins cher à entretenir et est plus efficace dans un *smart grid*) ;
- en lui permettant de devenir lui même producteur pour le réseau *smart grid*.

Ce sont les réseaux *blockchain* qui sont privilégiés pour le développement de *smart grids*, puisqu'ils peuvent s'implanter directement dessus et bénéficier de leur sécurité, leur résilience et leur ouverture aux particuliers. Les réseaux *blockchain* publics sont privilégiés, ils ne reposent pas sur un acteur central, ce qui facilite la création de consortiums ainsi que l'inclusion du consommateur final dans la chaîne de production.

C'est notamment l'objectif de la Fondation Energy Web, une organisation à but non lucratif qui participe à la transition vers une énergie plus durable, en développant des solutions technologiques open-source pour les systèmes énergétiques. Initiée par un partenariat entre Rocky Mountain Institute et Grid Singularity, l'Energy Web Chain est une *blockchain* de consortium, adaptée au secteur de l'énergie et regroupant déjà plus d'une centaine de compagnies d'électricité dans le monde. En novembre 2022 le Japan's Electricity Power Exchange, mandaté par le gouvernement japonais, est devenu le tout nouveau membre d'Energy Web. L'objectif d'Energy Web est d'ouvrir le marché de l'électricité à tout le monde, en permettant de connecter des appareils générateurs d'électricité (panneaux solaires, éoliennes, pompes à chaleur, batteries, etc…) et de les connecter à la *blockchain* Energy web. L'Energy Web Chain gère le flux d'électricité, et l'envoie au plus offrant à l'endroit le plus proche où il y en a besoin, permettant ainsi de diminuer les pertes dues au transport longue distance de l'électricité. Le but premier est de participer à la décarbonisation

[82] *https://www.ey.com/fr_fr/power-utilities/le-marche-francais-des-smart-grids-en-2030*

de l'énergie mondiale, en optimisant et en régulant la distribution de l'électricité, et en ouvrant ce marché aux particuliers.

Rendre le système financier plus performant, intègre et inclusif

1/ En palliant les limites actuelles des systèmes financiers :

- envoyer des fonds transfrontaliers dans un contexte où les systèmes de paiement internationaux ne permettent pas d'échanger en temps réel et à faible coût de l'argent à l'international malgré les efforts du réseau SWIFT (exclusion de certaines banques) et des opérateurs spécialisés comme Western Union (frais de commission prohibitifs) ;
- augmenter l'accessibilité du système bancaire pour emprunter, épargner et investir dans un contexte où 1,7 milliard de personnes n'ont pas accès à leur compte bancaire dans le monde (Global Findex de la Banque Mondiale) ;
- réduire les coûts d'accès à certains produits financiers pour les consommateurs.

2/ En optimisant et en automatisant le fonctionnement du système financier :

- permettre aux intermédiaires financiers de réduire les coûts de réconciliation de comptes et d'opérations de mise en conformité (KYC avec ALASTRIA et EBSI) ;
- faciliter l'échange de devises (le protocole Ripple identifie le parcours le plus court pour échanger des devises de manière distribuée dans un réseau de pair à pair) ;
- renforcer la transparence et l'auditabilité des opérations des acteurs financiers, pour faciliter leur mise en conformité réglementaire ;
- créer des instruments financiers automatisés grâce à l'utilisation des *smart contracts* de type smart securities et smart derivatives ;
- adresser les points de friction classiques dans cette industrie et apporter des solutions d'automatisation :

  - réconciliations, souvent faites à travers des tableaux excels partagés entre différents acteurs de la chaîne de valeurs comme les courtiers et les producteurs pour les calculs de commissions, ou entre les banques et les chambres de compensation (CCP) pour les activités de clearing, ou tout simplement entre les assureurs et réassureurs pour les calculs de flux sur base de traités manuels de réassurance ;
  - redondance ou mirroring des processus, entraînant des pertes d'efficacité et des surcoûts pour la première catégorie, et simplement des surcoûts pour la seconde. C'est par exemple le cas pour les processus de KYC/AML et conformité, ou de gestion de fraude dans les sinistres ;
  - provenance, avec la nécessité d'avoir en permanence une piste d'audit pour tracer les actifs ;
  - renforcer la transparence et l'auditabilité des opérations des acteurs financiers, pour faciliter leur mise en conformité réglementaire.

- optimiser les coûts de production et de gestion, et a fortiori augmenter le pouvoir d'achat des acheteurs en particulier sur des produits complexes.
  - C'est par exemple le cas pour des produits financiers structurés pour lesquels la tokenisation permet de faire des gains de gestion importants, ou pour des produits non fractionnables comme l'immobilier qui ont du mal à trouver un marché quand il y a une forte barrière à l'entrée ou au sein duquel les intermédiaires de l'échange bénéficient d'une rente de position.
  - Au rang des précurseurs de la tokenisation immobilière, RealT se démarque en offrant une solution novatrice pour l'investissement fractionné, ce qui lui vaut une position de leader dans ce secteur. Nombre de projets émergent dans ce créneau, mais la majorité se confronte aux obstacles juridiques, particulièrement en France.
- standardiser les méthodologies et les produits plus efficacement, en ayant recours à des *smart contracts* massivement utilisés et interopérables dans les processus de production (*smart contract* ERC20 par exemple), notamment pour les produits complexes de type produits

financiers où le *smart contract* permet d'automatiser des opérations de clearing étant manuellement faites par les équipes.

3/ En le rendant plus ouvert :
- introduire des solutions plus interopérables pour faciliter l'innovation en rendant le système financier plus libre et plus ouvert ;
- créer des monnaies locales complémentaires aux monnaies nationales pour stimuler l'économie réelle ;
- construire de nouveaux standards pour rendre la finance plus inclusive (ouverture de l'accès au crédit avec HiveOnline par exemple), plus verte (Sun Exchange pour démocratiser le financement des énergies renouvelables) ou plus intègre (preuve d'impact avec IXO Foundation) ;
- stimuler l'innovation en diminuant les barrières à l'entrée pour les entreprises de la Fintech ;
- inclure tous les acteurs du marché, en leur donnant la possibilité d'y participer plus activement, par exemple les "prosommateurs" sur le marché de l'énergie ;
- réaliser des paiements et micro-paiements dans un réseau pair à pair.

Transformer les business models

Au-delà des apports purement technologiques, la *blockchain* permet une transformation massive des Business Models et induit la notion de souveraineté numérique : comment rendre le pouvoir aux personnes, qu'il s'agisse d'individus, de sociétés ou d'États, comment permettre aux personnes de se réapproprier leur propre patrimoine numérique. C'est une question de gouvernance, de confiance et de valeur.

- Pour une marque, cela signifie créer un véritable patrimoine numérique durable et d'exister au sein de l'internet et non à la périphérie comme c'est souvent le cas aujourd'hui, parce que ce sont les plateformes technologiques comme les GAMAM qui disposent de l'infrastructure informatique qui leur permettent de posséder la plupart des données et de capturer la plupart de la valeur.

- Avec le web3, la souveraineté numérique des individus, des entreprises et des États est repensée, et par là même, la notion de création et de partage de la valeur, au cœur de la constitution des Business Models.

La *blockchain* a, de ce fait, très certainement un rôle crucial à jouer dans la gestion de tout type de marché et de réseau, apportant performance, sécurité et facilité d'intégration. En rendant possible l'ouverture des marchés financiers aux particuliers, comme le fait la *DeFi* par exemple, la *blockchain* se place comme une technologie qui permet de lutter contre les monopoles et les distorsions de concurrence, tout en supprimant les externalités négatives associées tels certains frais de transaction dûs à une intermédiation sans valeur ajoutée. À noter que de nombreuses fraudes ont pu voir le jour, dues au manque d'éducation des utilisateurs et au manque d'intermédiaire régulé.

Faciliter la vie des citoyens dans une société plus numérique et connectée

Encadré : la solution ARK pour gérer le *staking* en respectant le KYC

ARK permet au régulateur de remonter au KYC en cas de besoin réel, dans la mesure où il est permissionné.

ARK vise à relier différentes *blockchains* entre elles pour leur permettre de communiquer entre elles et de déclencher des évènements choisis, de type autorisation au régulateur de remonter au KYC en cas de besoin vérifié.

Cette interconnexion peut se faire par d'autres acteurs que les développeurs d'ARK, ce qui la dote d'une avancée majeure en matière d'interopérabilité.

En matière de *staking*, le Delegated Proof-of-Stake (DPoS) permet d'attribuer des récompenses aux 51 délégués actifs les mieux classés par leurs électeurs, et de partager ensuite ces récompenses avec les électeurs.

Annexe 2

Les limites écologiques de l'utilisation de la *blockchain*

La communauté Blockchain a pris la mesure de l'importance de limiter l'impact carbone de la technologie, aussi bien pour des raisons écologiques que pour des raisons économiques et avec une logique opérationnelle pour éviter des coupures de courant liées à de grosses activités de minage. Les mineurs des *blockchains* PoW sont plus responsables, ont souvent recours à des énergies recyclables, ou installent les serveurs dans des zones géographiques où la population ne consomme pas l'ensemble des énergies disponibles.

Certains acteurs de la communauté s'appuient désormais sur la *blockchain* et le web3 pour développer des applications contribuant à accélérer la transition vers une société plus durable et responsable avec des innovations technologiques et scientifique pour résoudre les grands enjeux sociétaux et environnementaux, dans la lignée du mouvement Impact France[83] de la TechforGood.

Encadré : exemple d'initiatives pour rendre la *blockchain* plus durable

Dans cet esprit, PwC partage avec la fondation d'utilité publique ELYX, l'ambition d'explorer si le potentiel du Web3 permettra de transformer les modèles existants pour être à la hauteur des enjeux du monde contemporain que les 193 États membres de l'ONU se sont donnés comme objectifs communs à travers l'Agenda 2030 (ODD). Conjointement, à partir de fin janvier 2023, ils rassembleront des entreprises du Web3 ou utilisatrices du Web3, des institutions, des académiques et chercheurs ainsi que différents acteurs issus de la société civile pour réfléchir et prototyper des solutions durables autour de 10 intuitions (liées aux ODD) visant à rendre le web3 durable. Par exemple, intuition numéro 1: il est possible que de développer des infrastructures faiblement consommatrices en énergie, ou intuition numéro 2 : le web3 peut contribuer à une répartition plus juste de la valeur.

Contre les défis sociaux et environnementaux causés par les systèmes financiers traditionnels, un mouvement mondial se lève, promouvant des pratiques économiques plus justes et plus durables.

Dans la même lignée, Blockchain For Good[84] est une association qui œuvre pour le partage d'expériences entre des acteurs du secteur *blockchain* et du développement durable. Son objectif est de favoriser et d'accompagner la mise en place d'expérimentations pour promouvoir un cadre législatif et normatif adapté à ce contexte d'innovation.

[83] *https://www.impactfrance.eco/communautes-thematiques/tech-for-good*

[84] *https://www.google.com/url?q=https://blockchainforgood.fr&sa=D&source=docs&ust=1676563718121591&usg=AOvVaw3UVGSxZEz-LSFPds9YFKhT*

L'organisation autonome décentralisée (DAO) française Cardashift[85] a ainsi pour principal objectif de contribuer à créer un système financier plus équitable et durable, à la fois pour les personnes et pour la planète. Elle fournit ainsi une infrastructure autorégulatrice avec des normes et des interactions, où les membres seraient en mesure de contrôler la trésorerie, ses investissements et l'écosystème technique. La DAO est basée sur une structure juridique unique s'appuyant sur le cadre légal français des associations (1901) permettant aux détenteurs de jetons d'être facilement intégrés dans le processus de prise de décision.

Ces acteurs utilisent la *blockchain* avec une vision « Tech for Good ». Cette notion fait référence à l'utilisation de la technologie pour résoudre des problèmes sociaux ou environnementaux, en créant des solutions innovantes et durables. Cela implique l'utilisation de la technologie pour améliorer la vie des individus, des communautés et de la planète, en favorisant des résultats positifs sur le long terme. Les entreprises et les organisations qui adoptent cette approche cherchent à avoir un impact positif en utilisant la technologie de manière responsable, éthique et durable.

Il y a une prise de conscience réelle de ces enjeux environnementaux au niveau des entreprises et des régulateurs.

- Le projet de règlement européen sur les marchés de crypto-actifs, MiCA[86], rendra obligatoire le reporting de l'empreinte environnementale par les prestataires de services sur crypto-actifs (CASPs[87]) exerçant en Europe. Les CASPs devront suivre des Standards Techniques Réglementaires (RTS[88]) préparés par l'Autorité Européenne des Marchés Financiers (AEMF / ESMA[89]). MiCA devrait entrer en vigueur à la fin de l'année 2023 ou début 2024[90].
- Dans le secteur privé, 50 % des entreprises françaises prennent en compte le coût énergétique de la *blockchain* dans leurs choix, contre 21 % des entreprises au niveau mondial, selon PwC en avril 2022[91]. En outre, des initiatives telles que le Global Impact Investing Network (GIIN) se sont données pour objectif de concilier impact et profit en misant sur les crypto-actifs dans la phase d'amorçage pour financer des projets à impact.

Hormis le choix d'une *blockchain Proof of Stake* plutôt qu'une *blockchain Proof of Work*, et le mix énergétique du pays dans lequel la *blockchain* est opérée, il existe des innovations permettant de réduire l'impact environnemental de la *blockchain*, à des échelles plus ou moins importantes.

- Certains pays développent leur réseau électrique, et proposent dans un premier temps une offre bien supérieure à la demande. Dans ce contexte, les mineurs investissent sur de l'énergie qui aurait été gaspillée sans leur intervention, sauf à ce que des solutions de stockages soient disponibles[92].
- Dans certains cas, une partie de la chaleur produite par les machines de minage peut être récupérée. Par exemple, la société canadienne Mintgreen devrait collaborer avec la ville de North Vancouver pour fournir cette même chaleur à 100 bâtiments comptant un ensemble de 7000 appartements[93].
- Le minage de Bitcoin peut contribuer à atténuer le torchage du méthane produit par l'extraction de pétrole[94].

[85] https://cardashift.com/

[86] *MiCA ou MiCAR de l'anglais Markets in Crypto Assets Regulation.*

[87] *CASPs de l'anglais Crypto-Assets Service Providers.*

[88] *RTS de l'anglais Regulatory Technical Standard.*

[89] *ESMA de l'anglais European securities and markets authority.*

[90] *En trilogue depuis le 31 mars 2022. Un accord provisoire a été obtenu le 30 juin 2022.*

[91] https://www.pwc.fr/fr/publications/blockchain/blockchain-crypto-comment-les-entreprises-en-tirent-enfin-benefice.html

[92] https://a.storyblok.com/f/155294/x/0c3f3837c8/coinshares_bitcoin_mining_report_jan_2022.pdf

[93] https://vancouversun.com/news/local-news/Bitcoin-could-be-heating-homes-in-north-vancouver-next-year

[94] *Destruction contrôlée et volontaire d'un gaz combustible dans une torchère.*

- D'après Arcane Research, un investissement de 1 000 dollars dans un système de minage de Bitcoins utilisant le méthane qui se dégage de l'extraction de combustibles fossiles pourrait réduire les émissions de 6,32 tonnes d'équivalents CO_2 par an, contre 1,3 pour l'éolien et 0,98 pour le solaire[95].
- La société Crusoe Energy a développé une solution de minage de Bitcoin permettant de réduire de 80 % le gaz rejeté dans l'atmosphère par l'extraction de pétrole.
- Les protocoles ont vocation à évoluer pour produire moins de déchets électroniques et à incorporer les énergies renouvelables de manière croissante dans le processus de minage. Une étude de Blockchain Partners montre que les puces utilisées pour le processus de minage sont de plus en plus efficientes. En outre, le mix énergétique du minage évolue vers plus de durabilité à la fois parce qu'il intègre de plus en plus d'hydroélectricité (source: Coinshare) mais aussi parce que de plus en plus d'activités de minage se relocalisent au Canada et aux États-Unis dans des régions où les capacités en énergies renouvelables sont excédentaires, énergies renouvelables représentant près de 80 % du total du minage du Bitcoin dans ces régions[96].

Annexe 3

Explications détaillées des failles et *hacks*

- Plusieurs failles sont liées aux utilisateurs :
  - Les arnaques aux faux projets, fausses levées de fond, fausses promesses de rentabilité sont ce qu'on appelle des *Rug Pulls* (« tirage de tapis » en anglais). Le faux projet a pour ambition d'attirer des investisseurs en grand nombre (crowdfunding) puis d'utiliser ces mêmes investisseurs pour participer à la communication du projet (montrer un projet très soutenu et attendu de ses investisseurs). L'arnaqueur vole ensuite l'intégralité de l'argent qui a été investi dans son faux projet.
  - Les arnaques ciblées sont aussi beaucoup utilisées dans le domaine. L'objectif peut être par exemple d'arriver à faire signer un utilisateur avec sa clef privée une transaction non souhaitée ou un *smart contract* malveillant, ou d'arriver à lui soutirer directement sa clef privée avec pour conséquence d'accéder aux fonds de l'utilisateur. Ce genre d'arnaques est très similaire à celles que l'on retrouve dans nos quotidiens (un mail bancaire frauduleux dans le but de soutirer des informations par exemple), et n'est en rien spécifique au domaine.
- D'autres failles sont liées à des développeurs mal intentionnés :
  - Les *hacks* de *smart contracts* révélant des failles non identifiées lors de la production du code. Ce risque explique la croissance rapide des pratiques d'audit des *smart contracts*.
- D'autres failles encore sont liées aux plateformes :
  - Ces failles sont des cibles pour les hackers, car les plateformes détiennent des sommes considérables. Elles sont diverses et variées et ne reposent pas sur des erreurs individuelles. Ce sont des failles dangereuses car pouvant affecter un grand nombre d'individus simultanément. Les plus gros *hacks* sont représentés par les plateformes d'échange de crypto-actifs. Binance a par exemple a subi ce qui pourrait représenter son premier piratage d'envergure[97] le 7 mai 2019, pour un montant de 7 000 BTC. Bien souvent, ce sont les plateformes et dépositaires centralisés qui sont la cible de ce type de *hacks*.

Ces failles ou arnaques ne sont finalement pas liées aux *blockchain* elles-mêmes, mais plus aux lacunes dans la mise en place de processus de contrôles internes.

[95] *https://arcane.no/research/reports*

[96] *Source : Coinshare.*

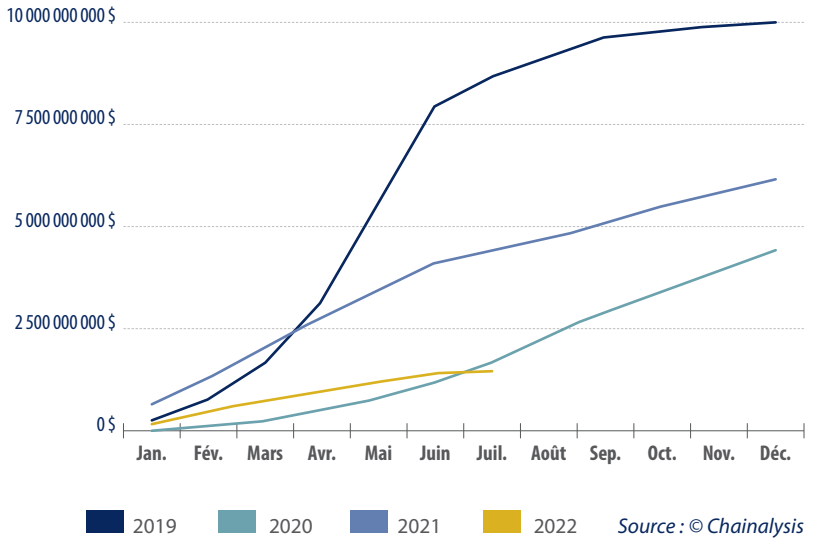
[97] *https://journalducoin.com/exchanges/binance-hack-42-millions-dollars-Bitcoins-pirates/*

Quelques faits et chiffres :

• Les arnaques en crypto-actifs représentent des sommes colossales.
- Le *Rug Pull* a été durant l'année 2021 la plus grande source de revenu pour les arnaqueurs de détenteurs de crypto-actifs, et a représenté 36 % de l'argent obtenu illégalement.
- Selon la Federal Trade Commission (FTC), une agence indépendante du gouvernement des États-Unis, plus de 46 000 personnes lui ont déclaré s'être fait escroquer des crypto-actifs entre janvier 2021 et juin 2022. L'étendue des vols s'élève à plus d'un milliard de dollars, la perte individuelle médiane déclarée est de 2 600 dollars et les vols de Bitcoin représentent environ 70 % des fonds dérobés.
- Toujours selon la FTC, du 1er janvier 2021 au 31 mars 2022, les crypto-actifs ont été identifiés comme le mode de paiement de 24 % des pertes en dollars déclarées (tout type de perte confondus).

• Néanmoins, le montant des arnaques semble diminuer au cours des dernières années.
- En ce qui concerne l'année 2022, selon ce graphique de Chainalysis, société spécialisée en investigation de flux de crypto-actifs, on constate une grande diminution des gains des arnaqueurs. Cependant, à garder en tête qu'il s'agit de sommes en dollars, et que cette diminution semble corrélée avec la baisse des cours de nombreuses crypto-actifs en 2022. Un refus de paiement de rançons en crypto-monnaies pourrait également expliquer cette baisse. Cette « résistance » s'expliquerait à la fois par une meilleure protection des sauvegardes et l'interdiction faite aux entreprises dans certains pays de payer les rançons, mais les récentes opérations de démantèlement pourraient également expliquer cette baisse.

Valeur mensuelle cumulée reçue par les escrocs par année



Source : © Chainalysis

Exemples de *hacks* et arnaques ces dernières années

Année / Affaire	Type d'arnaque	Description	Somme dérobée
2017 Onecoin	*Rug Pull*	Un des *Rug Pull* les plus connus est celui de Ruja Ignatova et son projet OneCoin. Il s'agissait d'une pyramide de Ponzi dans laquelle tout nouvel investisseur rémunérait en fait les anciens investisseurs. Elle est actuellement en cavale, et figure parmi les 10 fugitifs les plus recherchés par le FBI.	Minimum 4 milliards de dollars dérobés, issus de plus de 70 pays.
Avril 2021 Thodex	*Rug Pull*	Les 400 000 utilisateurs de la plateforme d'échanges centralisée Thodex se sont fait subtiliser l'ensemble de leurs actifs numériques. Le fondateur est soupçonné d'en être à l'origine, il s'est fait arrêter en août 2022, après plus d'un an de cavale.	Catégorie juridique et réglementation dédiées.

Année / Affaire	Type d'arnaque	Description	Somme dérobée
Août 2021 Poly Network	*Hack* de plateforme	Le hackeur s'en est pris à Poly Network, une plateforme qui permet le transfert d'actifs entre *blockchains*. La totalité des fonds volés ont ensuite été restitués à l'entreprise, et le hackeur a aidé l'entreprise à réparer la faille informatique dont il s'est lui-même servi. Cela lui a valu le surnom de Mr White Hat.	Plus de 600 millions de dollars en crypto-monnaie dérobés puis rendus.
Septembre 2021 Liquid	*Hack* de plateforme	Le hackeur s'en est pris à la plateforme d'échange japonaise Liquid. L'entreprise a tout de même survécu, notamment grâce au prêt d'une autre plateforme d'échange : FTX.	L'équivalent de 97 millions de dollars en BTC, TRX, XRP, ETH et jetons ERC-20 dérobés.
Février 2022 Wormhole	*Hack* de bridge	Wormhole est un bridge permettant de transférer des fonds entre la *blockchain* Ethereum et Solana. Une faille dans le code a permis de siphonner des centaines de milliers d'ETH des wallets des utilisateurs au tout début du mois de février 2022, pour un montant de de 326 millions de dollars.	300 millions de dollars.
Mars 2022 Axie Infinity	*Hack* de plateforme	Fin mars, 173 600 ETH sont volés du célèbre jeu Play to Earn Axie Infinity. Soit environ 600 millions de dollars au moment du vol. En exploitant une faille, les hackeurs soupçonnés d'être le groupe nord-coréens Lazarus, ont mis à mal la *blockchain* Ronin sur laquelle tournait le jeu.	600 millions de dollars.
Mars 2023 Euler Finance	*Hack* de plateforme	Euler Finance est un protocole de prêt hébergé sur Ethereum. Ainsi, il permet aux utilisateurs de sauvegarder et d'emprunter des crypto-monnaies de manière décentralisée. Le protocole de prêt basé sur Ethereum Euler Finance a été victime d'une attaque par flash loan qui a entraîné le vol d'environ 200 millions de dollars des actifs numériques du projet.	200 millions de dollars.

Annexe 4

Criminalité financière liée aux crypto-actifs

La démocratisation de l'usage des crypto-actifs a engendré une nouvelle criminalité financière qui fait l'objet d'une vigilance accrue des régulateurs. Tracfin a ainsi observé une augmentation du nombre de déclarations de soupçons : 528 reçues en 2018 sur les crypto-actifs, soit deux fois plus qu'en 2017 (rapport annuel d'activité de Tracfin de 2018).

La criminalité financière liée aux crypto-actifs se traduit sous la forme de 5 grandes catégories de délits :

- Blanchiment de capitaux : Les crypto-actifs peuvent être utilisés dans le cadre de blanchiment de capitaux en raison du pseudonymat et de leur capacité à effectuer des transactions transfrontalières sans l'intervention des banques. Cela peut représenter une difficulté d'identification des personnes impliquées dans ces transactions. La *blockchain* étant transparente, il est en réalité complexe de blanchir de l'argent *via* cette technologie. En 2021, les échanges illicites ont concerné 0,15 % des transactions sur l'ensemble des transactions de l'écosystème selon une étude de la société Chainalysis.
- Financement du terrorisme : De la même façon, les crypto-actifs peuvent être utilisés pour financer des activités terroristes. Des *blockchain* anonymes sont ainsi privilégiées, tel que Monero par exemple, car elles permettent des échanges financiers anonymes et décentralisés qui échappent souvent à la surveillance et à la réglementation traditionnelles.
- Contournement des mesures de gel des avoirs et sanctions internationales : La *blockchain* peut être une infrastructure technologique utilisée pour contourner les mesures de gel des avoirs et les sanctions internationales dû à la décentralisation du réseau qui ne permet pas d'arrêter une transaction ou empêcher une adresse d'effectuer un échange financier.

- Évasion ou fraude fiscale : nombreux sont les acteurs soit qui fuient vers des localisations ou la réglementation en matière de crypto-actifs est plus accueillante, soit qui ne déclarent pas leurs gains afin d'éviter qu'ils soient taxés. Barclays évalue ainsi à 50 milliards de dollars la fraude fiscale liée aux gains en crypto-actifs aux États-Unis en 2022.

Certaines solutions existent aujourd'hui pour aider les acteurs régulés à identifier et gérer ces risques.

- Chainalysis : Fondé en 2014, Chainalysis propose des enquêtes sur les activités illégales des crypto-monnaies et des services de conseils en conformité. La société de surveillance américaine est devenue un acteur majeur dans ce secteur avec des clients très importants comme des gouvernements, par exemple. Elle se place par ailleurs en pointe dans la lutte contre le financement d'activités à caractères terroristes.
- Scorechain : Fondée en 2015, cette société luxembourgeoise fournit des solutions de conformité contre le blanchiment d'argent pour les crypto-actifs. Scorechain accompagne plus de 200 clients dans plus de 40 pays, dont des banques, cabinet d'audit, plateforme d'échange…
- Napier : Napier propose des solutions de lutte contre le blanchiment d'argent pilotées par l'IA.
- D'autres solutions existent telles que TRM Labs, Sumsub, Solidus Lab, Elliptic.
- Certains cabinets de conseil accompagnent les acteurs régulés dans la revue ou la refonte des dispositifs de sécurité financière.

Annexe 5

L'exemple du PIIEC sur le *cloud*, une dynamique qui pourrait inspirer un EDIC *blockchain*

Étape 1 : une impulsion nationale a d'abord été donnée par le biais de la stratégie nationale « *cloud* au centre » de 2021 :
- le *cloud* devient l'hébergement par défaut des services numériques de l'État sur l'un des deux *clouds* interministériels ou chez des fournisseurs privés présentant des garanties ;
- pour ne pas entraver l'autonomie de prise de décision des pouvoirs publics et la sécurité numérique des citoyens un label Cloud a été mis en place avec un double niveau de sécurisation juridique (visa SecNumCloud) et technique (garanties de réversibilité, interopérabilité, portabilité et transparence).

Étape 2 : dans ce cadre, un soutien direct a été porté au niveau national aux projets avec le plus de valeur ajoutée dans le cadre du 4ème Plan d'Investissements d'avenir (PIA) et de France Relance. Un appel à manifestation d'intérêt (AMI) a permis d'identifier 60 projets pour une assiette totale de 1,5 Md€ (pour un co-financement public-privé de 5Mds€ au total).

Étape 3 : les plus importants d'entre eux ont ensuite été financés par un projet industriel d'intérêt européen commun (PIIEC) réunissant 12 États-membres avec l'ambition de développer une offre *cloud* plus verte dans des domaines d'innovation de rupture comme l'edge computing. L'objectif est de développer des services et des infrastructures *cloud* européennes dans le cadre de la stratégie européenne pour créer un marché unique de la donnée, incarnée par le Data Governance Act.

Annexe 6

Illustration du fonctionnement d'un *layer 2* avec le Lightning Network de Bitcoin

Une transaction sur un réseau *blockchain* constitue un engagement « inarrêtable » : une fois publié, l'engagement sera exécuté par un validateur. Le réseau Lightning Network consiste à créer des canaux de paiement entre utilisateurs pour échanger des paiements validés dans le réseau principal sans être publiés sur ce réseau. Ce layer bénéficie de la sécurité du réseau principal, sans avoir à publier constamment les transactions, ni attendre leurs validations et payer les frais associés. Il est nécessaire de recourir à un wallet Lightning compatible comme Breez, Simple Bitcoin Wallet, ou encore le wallet Phoenix développé par l'entreprise française Acinq.

Le réseau Lightning Network existe déjà et fonctionne, en étant capable de traiter 1 000 000 de transactions par seconde[98] lorsque le réseau principal (Bitcoin) est limité à environ 7 transactions par seconde. Voici certaines de ses caractéristiques :

- L'intérêt du Lightning Network est en théorie multisecteur, même s'il est principalement utilisé dans le secteur du paiement ; il s'agit de pouvoir transférer instantanément, à moindre frais et sans risque des sommes représentant principalement de faibles valeurs unitaires correspondant à des achats de biens et de services du quotidien. D'ailleurs, l'unité couramment utilisée est le satoshi : 1 Bitcoin = 100 millions de satoshis.
- Il nécessite cependant un déploiement efficace. Les canaux de paiement du réseau Lightning Network sont pair à pair, et la capacité de paiement d'un canal, c'est-à-dire le montant maximal de Bitcoins pouvant être échangés, est définie à son ouverture. Une bonne couverture des canaux de paiements et une capacité adaptée sont clés pour le bon fonctionnement de ce type de réseau, un peu comme l'est à la fois la couverture de bornes wifi et le débit maximum possible.
- Aussi, pour utiliser le Lightning Network et détenir ses propres Bitcoins, chaque individu ou organisation peut déployer son propre nœud sur ce second réseau. Cela demande d'allouer de manière persistante un ordinateur à cette tâche.
- Il est toujours possible d'utiliser ce *layer 2* sans déployer son propre nœud, mais il faudra dans ce cas se référer au nœud d'un tiers pour garantir la sécurité des transactions.

Le Lightning Network est un exemple de *layer 2* sur Bitcoin, mais il en existe de multiples, avec leurs propres caractéristiques (Polygon pour les paiements instantanés sur Ethereum, Starkware qui développe une technologie de preuve de connaissance zéro sur Ethereum, etc.).

[98] *https://actualiteinformatique.fr/blockchain/definition-lighting-network#:~:text=Le%20Lightning%20Network%20est%20capable,environ%207%20transactions%20par%20seconde*

Remerciements

L'Institut Montaigne remercie l'ensemble des personnes ayant contribué à l'élaboration de ce travail :

PRÉSIDENTS DU GROUPE DE TRAVAIL

- **Pauline Adam-Kalfon,** associée, responsable des activités Blockchain et crypto, PwC France et Maghreb
- **Olivier Jaillon,** président du Conseil d'administration, Wakam

MEMBRES DU GROUPE DE TRAVAIL

- **Sébastien Choukroun,** consultant Blockchain & DeFi, Wakam
- **Primavera De Filippi,** directrice de recherche au CNRS et chercheuse associée au Berkman Center for Internet & Society (Université de Harvard)
- **Louise Frion,** cofondatrice Medici & Cie (rapporteur)
- **Julien Prat,** chercheur CNRS au CREST et co-porteur de la chaire « Blockchain@X »
- **Milo Rignell,** responsable de projets et expert résident – Nouvelles technologies, Institut Montaigne
- **Marc Ripault,** directeur, PwC (rapporteur)
- **Klara Sok,** analyste et co-gérante du fonds R-co Blockchain Thematic Global Equity, Rothschild & Co.

Le groupe de travail remercie également les personnes suivantes pour leur aide précieuse :

- **William Blanc,** PwC
- **Max Feyler,** consultant Blockchain, PwC
- **Laurent Olivier,** consultant Blockchain, PwC
- **Anastasia Schenkery,** assistante chargée d'études, Institut Montaigne
- **Marcus Woodcock,** assistant chargé d'études, Institut Montaigne

PERSONNES AUDITIONNÉES

- **Brahim Azmi,** *Digital Innovation Product Owner,* Sanofi
- **Guillaume Bazouin,** directeur des programmes startup et intrapreneur, Leonard (VINCI)
- **Lina Bendifallah,** *Project Manager,* VIATYS
- **Laurent Benichou,** Fondateur, Scratch Tech
- **Emmanuel Bertin,** Directeur de programme Blockchain, Groupe Orange
- **Hervé Bonazzi,** président, Archipels
- **Stéphanie Cabossioras,** directrice juridique France, Binance
- **Nicolas Cantu,** président, 4NK
- **Pierre Chabrol,** sous-directeur du financement des entreprises et du marché financier, Direction Générale du Trésor
- **Simon Chantry,** cofondateur et *Chief Information Officer,* Bitt
- **Bruno Daunay,** *Head of AI Program,* Leonard (VINCI)
- **Ivan de Lastours,** *Blockchain/Crypto Lead,* Bpifrance
- **Jérome de Tychey,** président d'Ethereum-France et directeur général de Cometh
- **Hubert de Vauplane,** associé Kramer Levin
- **Noémie Dié,** doctorante, Télécom Paris et Bpifrance
- **Maxime Donadille,** conseiller technologies d'avenir, espaces immersifs et cybersécurité, ministère chargé de la Transition numérique et des Télécommunications
- **Ambroise Fargère,** *Head of M&A and Corporate Development*, +Simple
- **Faustine Fleuret,** présidente-directrice générale, Adan
- **Paul Frambot,** président Morpho Labs

- **Thomas France,** cofondateur, Ledger & Cygni
- **Jean Galand,** consultant stratégie sénior, Enedis
- **Jean-Charles Griviaud,** *Chief Security Officer,* Cisco Systems France
- **Franck Guiader,** directeur de Gide 255 - Innovation & FinTech - Gide Loyrette Nouel
- **Nicolas Kozakiewicz,** *Chief Innovation Officer,* Worldline
- **Charles Kremer,** directeur, Général Eniblock
- **Frédérick Lacroix,** avocat associé, *Head of Financial Regulations & Fintech,* Clifford Chance
- **Thibault Langlois-Berthelot,** fondateur & administrateur, KRYPTOSPHERE®
- **Éric Larchevêque,** cofondateur, Ledger, Coinhouse, ALGOSUP
- **Xavier Lavayssière,** chercheur en régulation des cryptoactifs, Université Paris 1 Panthéon-Sorbonne
- **John Le Guen,** collaborateur, Service Financiers – FinTech, Gide Loyrette Nouel
- **Danaelle Le Mao,** responsable du département ingénierie, Zurich France
- **Nicolas Lecocq,** *Global Head of BeautyTech Accelerators,* L'Oréal
- **Charles Leonardi,** directeur général Supply Chain, Nestlé France
- **Romain Liquard,** Études Économiques, Crédit Agricole
- **Nicolas Louvet,** président-directeur général, Coinhouse
- **Antoine Maisonneuve,** *Orange Business Blockchain Program Manager & President,* Alliance Blockchain France
- **Jean-Francois Michalczyk,** *Managing Consultant - Blockchain & innovation,* IBM Consulting
- **Michaël Miramond,** *Vice President Chief Digital Officer,* CMA CGM
- **Frédéric Montagnon,** président, Arianee
- **Charles Moussy,** directeur Innovation Finance digitale, Autorité des marchés financiers (AMF)
- **Jean-Michel Pailhon,** *NFT Art Advisory Board and Investor,* Ledger
- **Mathieu Pauwels,** *Chief Operating Officer,* Zurich France
- **William Piquard,** cofondateur, Atka
- **Aymeric Pontvianne,** conseiller économie et innovation, CNIL

- **Mahasti Razavi,** *Managing Partner,* August Debouzy
- **Thibaut Reymond,** *Strategic Project Manager,* Edenred
- **Vincent Sebag,** ancien vice-président, Cathay Innovation
- **Jean-Marc Stenger,** directeur général, Société Générale-Forge
- **Sara Tucci,** directrice de laboratoire, CEA List
- **Pierre Westphal,** Business development manager IT offers SGS ICS

Les opinions exprimées dans ce rapport n'engagent ni les personnes précédemment citées ni les institutions qu'elles représentent.

Retrouvez nos autres notes et rapports sur les mêmes sujets :

Tech

- Mobiliser et former les talents du numérique (mai 2023)
- Investir l'IA sûre et digne de confiance : un impératif européen, une opportunité française (avril 2023)
- Géopolitique et technologie : le tournant de la stratégie européenne (mars 2022)
- Fintech chinoise : l'heure de la reprise en main (avril 2021)

Europe

- La présidence française de l'Union européenne à la loupe (décembre 2021)
- Réinvestir le secteur bancaire européen (novembre 2021)

Innovation

- Innovation française : nos incroyables talents (octobre 2021)
- Enseignement supérieur et recherche : il est temps d'agir ! (avril 2021)

L'ensemble de nos travaux et publications
est disponible sur notre site institutmontaigne.org

Président

Henri de Castries président, Institut Montaigne

Membres

David Azéma associé, Perella Weinberg Partners
Emmanuelle Barbara *Senior Partner*, August Debouzy
Marguerite Bérard directrice des Réseaux France, BNP Paribas
Jean-Pierre Clamadieu président du Conseil d'Administration, ENGIE
Paul Hermelin président du Conseil d'administration, Capgemini
Marwan Lahoud président, Ace Capital Partners
Natalie Rastoin présidente, Polytane ; *Senior Advisor*, WPP
René Ricol président, Ricol Lasteyrie
Jean-Dominique Senard président du Conseil d'administration, Groupe Renault
Arnaud Vaissié président-directeur général, International SOS
Natacha Valla économiste ; doyenne de l'École de Management et d'Innovation, Sciences Po
Florence Verzelen directrice générale adjointe, Dassault Systèmes
Philippe Wahl président-directeur général, Groupe La Poste

Président d'honneur

Claude Bébéar fondateur et président d'honneur, AXA

L'Institut Montaigne vous propose de contribuer à la réflexion sur ces enjeux afin d'élaborer collégialement des propositions au service de l'intérêt général.

Les adhérents

INSTITUT Montaigne

ABB France
Abbvie
Accenture
Accuracy
Adeo
ADIT
Aéma
Air France - KLM
Air Liquide
Airbus
Allen & Overy
Allianz
Amazon
Amber Capital
Amundi
Antidox
Antin Infrastructure Partners
Archery Strategy Consulting
Archimed
Ardian
Arquus
Astrazeneca
August Debouzy
Avril
AXA
Bain & Company France
Baker & Mckenzie
Bearingpoint
Bessé
BG Group
BNP Paribas
Bolloré
Bouygues
Brousse Vergez
Brunswick
Capgemini
Capital Group
CAREIT
Carrefour
Casino
Chubb
CIS
Cisco Systems France
Clifford Chance
Club Top 20
CMA CGM
CNP Assurances
Cohen Amir-aslani
Compagnie Plastic Omnium
Conseil supérieur du notariat
Crédit Agricole
D'angelin & Co.Ltd
Dassault Systèmes
De Pardieu Brocas Maffei
DIOT SIACI
Doctolib
ECL Group
Edenred
EDF
EDHEC Business School
Egis
Ekimetrics France
Enedis
Engie
EQT
ESL & Network
Ethique & Développement
Eurogroup Consulting
FGS Global Europe
Fives
Getlink
Gide Loyrette Nouel
Google
Groupama
Groupe Bel
Groupe M6
Groupe Orange
Hameur Et Cie
Henner
Hitachi Energy France
HSBC Continental Europe
IBM France
IFPASS
Inkarn
Institut Mérieux
International SOS
Interparfums
Intuitive Surgical
Ionis Éducation Group
iQo
ISRP
Jeantet Associés
Jolt Capital
Kantar Public
Katalyse
Kea & Partners
Kearney
Kedge Business School
KKR
KPMG S.A.
Kyndryl
La Banque Postale
La Compagnie Fruitière
Linedata Services
Lloyds Europe
L'Oréal
Loxam
LVMH - Moët-Hennessy - Louis Vuitton
M.Charraire
MACSF
MAIF
Malakoff Humanis
Mazars
Média-Participations
Mediobanca
Mercer
Meridiam
Michelin
MicroPort CRM
Microsoft France
Mitsubishi France S.A.S
Moelis & Company
Moody's France
Morgan Stanley
Natixis
Natural Grass
Naval Group
Nestlé
OCIRP
ODDO BHF
Oliver Wyman
Ondra Partners
Onepoint
Onet
Optigestion
Orano
Ortec Group
PAI Partners
Pelham Media
Pergamon
Prodware
PwC France & Maghreb
Raise
RATP
RELX Group
Renault
Rexel
Ricol Lasteyrie
Rivolier
Roche
Rokos Capital Management
Roland Berger
Rothschild & Co
RTE
Safran
Sanofi
SAP France
Schneider Electric
Servier
SGS
SIER Constructeur
SNCF
SNCF Réseau
SNEF
Sodexo
SPVIE
SUEZ
Taste
Tecnet Participations SARL
Teneo
The Boston Consulting Group
Tilder
Tofane
TotalEnergies
UBS France
Unibail-Rodamco
Veolia
Verlingue
VINCI
Vivendi
Wakam
Wavestone
Wendel
White & Case
Willis Towers Watson France
Zurich

Institut Montaigne
59 rue La Boétie, 75008 Paris
Tél. +33 (0)1 53 89 05 60
institutmontaigne.org

Imprimé en France
Dépôt légal : mai 2023
ISSN : 1771-6764

Crédit visuel de couverture : © Pauline Faure

La *blockchain* possède tout le potentiel d'une infrastructure numérique de confiance. Il s'agit d'une infrastructure informatique qui permet d'échanger librement et de manière sécurisée des actifs numériques tels que des monnaies, des actes de propriété, des certificats ou des œuvres d'art, sans passer par un tiers de confiance.

Si les *blockchains* ont jusqu'à présent surtout permis d'échanger des actifs numériques à plus grande échelle, grâce à des crypto-monnaies comme Bitcoin, depuis la mise en place d'Ethereum en 2013 et des contrats autonomes (smart contacts), ses usages se sont diversifiés et propagés dans de nombreux secteurs (bancaire, artistique, légal, etc.). Son potentiel est particulièrement important pour quatre cas d'usage majeurs : l'identité numérique, la traçabilité, les opérations financières décentralisées, et les paiements. Ce dernier cas d'usage constitue un enjeu de souveraineté particulièrement important, puisque l'Europe pourrait rapidement se trouver en position de dépendance vis-à-vis d'acteurs non européens.

La France a été pionnière sur la technologie *blockchain* et dispose d'atouts incontestables : techniques, avec une expertise importante sur les contrats autonomes *(smart contracts)* et les langages formels, et réglementaires, avec un cadre pionnier proposé par la loi PACTE et récemment adapté à l'échelle européenne dans le cadre du règlement MiCA.

L'enjeu est désormais de développer notre avantage sur cette infrastructure numérique de confiance, en capitalisant sur ces avancées techniques et réglementaires d'une part, et en continuant à sécuriser le cadre juridique d'autre part. À l'échelle européenne, le développement d'infrastructures de paiement qui s'appuient sur la *blockchain* est clé pour notre souveraineté et pour notre compétitivité.

10 €
ISSN : 1771-6764
RAP2306-01