



**LES FONCTIONS
DE CONTRÔLE
FACE A
LA BLOCKCHAIN :
RISQUES
OU
OPPORTUNITES ?**

Emilie CHAPOT

MBA MRC 2021-2022

Management, Risques et Contrôle

Tutrice : Anne-Sophie MAURILIERAS

REMERCIEMENTS

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma gratitude.

Mes remerciements vont au directeur du programme Monsieur TABOURIN et à l'ensemble de l'équipe pédagogique.

Je voudrais particulièrement remercier ma Directrice de mémoire, Madame MAURILIERAS, pour son accompagnement, ses précieux conseils et ses encouragements. Votre expertise, pédagogie, écoute et confiance m'ont apporté une grande sérénité dans la réalisation de ce travail.

J'ai également beaucoup appris des échanges avec les professionnels qui ont accepté de me recevoir et prendre de leur temps.

Je tiens à les remercier pour leur disponibilité, ainsi que pour leurs contributions essentielles pour orienter ma réflexion.

Mes remerciements vont aussi à mes camarades de promotion 2021-2022. J'ai passé une année très enrichissante à leur côté.

Enfin, je voudrais remercier mes proches, pour leur soutien tout au long de ma démarche et leur aide précieuse pour la relecture de mon mémoire.



REMERCIEMENTS	2
SYNTHESE	5
INTRODUCTION	6
1. LA BLOCKCHAIN, C'EST QUOI ?	8
1.1- Définitions	8
1.1.1- Caractéristiques	
1.1.2- Blockchain publique, Blockchain privée, à Consortium : des différences de taille	
1.2- Histoire de la Blockchain	11
1.2.1- A l'origine : la création du Bitcoin et le mystère « <i>Satoshi Nakamoto</i> »	
1.2.2- L'émergence de la deuxième génération de Blockchain	
1.3- Principes et fonctionnement	14
1.3.1- Architecture non centralisée	
1.3.2- Consensus distribué	
1.3.3- Synchronisation et décentralisation des enregistrements	
1.3.4- Smart Contracts ou Contrats Intelligents	
1.3.5- Fonctionnement du Bitcoin en 5 étapes	
1.4- Avantages	16
1.4.1- Autonomie	
1.4.2- Transparence	
1.4.3- Traçabilité	
1.4.4- Horodatage	
1.4.5- Désintermédiation	
1.4.6- Sécurité	
1.4.7- Automatisation	
1.4.8- Limitation du risque de perte de données	
1.5- Les grands types d'usages de la Blockchain	17
1.5.1- Les typologies de crypto-actifs	
1.5.2- Les secteurs monétaires et financiers déjà mobilisés	
1.5.3- Les autres secteurs d'activité	

1.6-	Un cadre réglementaire mondial disparate... ... initialement mis en place localement par les états au sein de l'Union Européenne ... qui se construit désormais en commun	25
------	---	----

2. RISQUES, OPPORTUNITÉS ET DÉFIS 31

2.1-	Risques	32
2.1.1-	Risque de blanchiment d'argent	
2.1.2-	Risque de financement du terrorisme	
2.1.3-	Risque d'escroquerie et de fraude	
2.1.4-	Risque de fraude fiscale	
2.1.5-	Crypto-actifs anonymes ou pseudonymes ?	
2.1.6-	Risque lié à la protection de la clientèle	
2.1.7-	Risque lié à la sécurité	
2.1.8-	Risque lié à la gouvernance	
2.1.9-	Risque lié à la protection des données	

2.2-	Opportunités	46
2.2.1-	Nouveaux process à contrôler	
2.2.2-	Nouveau champ des possibles pour les fonctions de contrôle	
2.2.3-	KYC, un candidat pertinent	
2.2.4-	Surveillance des transactions	
2.2.5-	Reporting et consolidation	

2.3-	Défis	55
2.3.1-	Attirer les profils qualifiés, acquérir de nouveaux savoirs et maîtriser les outils	
2.3.2-	Se positionner en amont du changement	
2.3.3-	Faire le lien entre le monde physique et le monde numérique	
2.3.4-	Appréhender les nouvelles unités collaboratives	

3. POINTS D'ATTENTION « BLOCKCHAIN » POUR LES FONCTIONS DE CONTRÔLE 61

CONCLUSION	69
------------	----

GLOSSAIRE	71
-----------	----

BIBLIOGRAPHIE	78
---------------	----



SYNTHESE

« Technologie révolutionnaire », « disruption ultime », « machine à créer de la confiance », « innovation de rupture d'une ampleur inédite », « technologie qui va révolutionner la banque et l'assurance » ...

Les termes élogieux n'ont pas manqué et ont été largement présents dans les médias ces dernières années lorsqu'il s'agit d'évoquer la technologie Blockchain.

La Blockchain est une technologie qui permet la sécurisation des transactions d'un écosystème en rendant les données transparentes et non modifiables via la construction d'un registre partagé, infalsifiable, pour la parfaite traçabilité des échanges d'information.

Transparente et sécurisée, elle fonctionne sans organe de contrôle.

Cette technologie a connu son essor grâce aux cryptomonnaies. Mais la Blockchain peut être utilisée dans de nombreux autres secteurs d'activité, que ce soit, par les acteurs privés (art, banque, assurance, secteur du luxe, automobile....) ou par les acteurs publics (cadastre, vote, état-civil, etc.).

Cette transformation s'accompagne ainsi de nouveaux enjeux pour les fonctions de contrôles : Audit Interne, Contrôle Interne et Conformité.

Ce mémoire est destiné à tous ceux qui veulent découvrir la Blockchain.

En effet, les enjeux sont multiples, les sources de risques spécifiques, mais cette technologique offre également de nouveaux risques, de nouvelles opportunités et de nouveaux défis pour les fonctions de contrôle qu'il est nécessaire de bien appréhender.

L'objectif est de déclencher une réelle réflexion sur ce sujet et de stimuler les débats : sommes-nous face à une simple adaptation des fonctions de contrôle ou face à un bouleversement de plus grand ampleur ?



INTRODUCTION

“Mieux vaut prendre le changement par la main avant qu’il nous prenne par la gorge”

Winston Churchill

À la fin des années 1990, l’économiste américain, Paul Krugman, prévoyait la chute d’Internet pour l’année 2005 et affirmait alors qu’Internet n’aurait pas plus d’impact que le fax et que les réseaux sociaux n’auraient aucun succès, car la plupart des gens n’ont rien à se dire¹ »...

Il n’en fut rien, démontrant ainsi les limites de la prospective, mais aussi les difficultés à penser l’innovation. Internet n’étant pas régulé par les Etats, beaucoup de personnes pensaient donc qu’il ne pouvait pas fonctionner.

Aujourd’hui, c’est au tour de la Blockchain (ou « chaîne de blocs ») d’être au cœur des discussions.

La pression médiatique n’est quasiment pas retombée depuis le choix de placer la Blockchain à la une du magazine The Economist² en Octobre 2015 : « *Comment la technologie derrière le bitcoin pourrait changer le monde ?* »

¹ « *The growth of the Internet will slow drastically, as the flaw in 'Metcalfe's law'—which states that the number of potential connections in a network is proportional to the square of the number of participants—becomes apparent: most people have nothing to say to each other! By 2005 or so, it will become clear that the Internet's*



Certains citent en effet la technologie Blockchain comme étant une des meilleures inventions disruptives en introduisant une notion inédite, notamment la rareté numérique.

La Blockchain, qui utilise des mécanismes de cryptographie et de validation par consensus de données partagées et décentralisées, tout en assurant la traçabilité et l’intégrité des données échangées, gagne en effet chaque jour du terrain.

impact on the economy has been no greater than the fax machine's » - Paul Krugman

² Article de The Economist - « *The Trust Machine* » - 31/10/2015, disponible à l’adresse suivante : <https://www.economist.com/leaders/2015/10/31/the-trust-machine>

Cependant, cette technologie défraie la chronique avec son lot de louanges et de réserves : bitcoin, crypto-monnaies, protocoles de consensus distribués, NFTs...

En effet, les chiffres sont impressionnants³ et ce, malgré la chute récente des cryptomonnaies en 06/2022.

Souvent associée directement aux cryptomonnaies, la Blockchain peut pourtant être utilisée dans de nombreux secteurs et transformer l'échange de flux financiers, d'énergies, de biens, de données...

Mais qu'en est-il en 2022, quels sont les impacts de cette technologie, à présent et à l'avenir, pour les fonctions de contrôle ?

Il ne fait nul doute que les professionnels de l'Audit Interne, du Contrôle Interne et de la Conformité doivent prendre en compte et intégrer cette technologie dans leurs travaux.

Ce mémoire a donc pour objectif d'encourager les fonctions de contrôle citées ci-dessus à appréhender les enjeux de la Blockchain, en mesurant les risques associés, mais également en identifiant les nouvelles opportunités, les défis, ainsi que ses nouveaux usages.

Le présent mémoire propose enfin les points d'attention pour les fonctions de contrôle.

Cet écrit est le fruit d'un travail de revue et de recherche dans les littératures françaises et internationales.

Par ailleurs, pour comprendre aujourd'hui la réalité du terrain et envisager les changements auxquels, nous, fonctions de contrôle (Audit, Contrôle Interne et Conformité) allons devoir faire face, j'ai eu des échanges avec :

- ✓ **des acteurs qui font et pensent « Blockchain »** et ce, afin de recueillir leur vision en tant qu'acteurs et experts des rouages de cette technologie en perpétuelle évolution, dont les types d'usages sont en développement permanent ;
- ✓ **des professionnels de la Blockchain et de certaines fonctions de contrôle** pour recueillir leur point de vue et enrichir l'analyse des risques/opportunités sur la gestion des risques.

Il aurait été nécessaire de leur donner la parole plus longuement, tant le sujet est vaste, les défis conséquents et les perspectives dynamisantes. En fonction de l'entreprise, de son secteur d'activité, de sa fonction, la Blockchain a déjà ou aura quelque chose de différent à offrir...

Je vous souhaite une très bonne lecture, en espérant que ce mémoire suscitera un débat constructif autour de cette problématique que je trouve passionnante.

³ Selon un rapport sur le marché mondial de la technologie Blockchain publié par Sheer Analytics and Insights, le marché total était évalué à 6,1 milliards de dollars en 2020, avec une croissance à un TCAC élevé

de 36,8 % entre 2021 et 2031. On estime qu'il atteindra 183,2 milliards de dollars d'ici 2031.

1. LA BLOCKCHAIN, C'EST QUOI?

“ Le vieux monde se meurt, le nouveau tarde à apparaître et dans ce clair obscur surgissent les monstres ”

Antonio GRAMSCI

1.1- Définitions

1.1.1- Caractéristiques

Définir la Blockchain en quelques mots n'est pas chose aisée. Une des définitions les plus connues est celle du mathématicien Jean-Paul Delahaye : *« un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible ».*

Toutefois, la définition de la Blockchain reste complexe et peut être sujette à discussion. Il n'en reste pas moins qu'il s'agit :

- ✓ d'un **registre** (c'est-à-dire un fichier),
- ✓ **distribué** (des « nœuds » détiennent ce registre, aucune autorité centrale ne contrôle la Blockchain et il n'y a pas de tiers de confiance),
- ✓ **infalsifiable** (protégé par un système de confiance répartie – « consensus »),
- ✓ **partagé** entre les participants (partage des données, des opérations et du consensus),
- ✓ composé de **blocs** (ou pages),
- ✓ successivement **validés**, **datés** et **conservés** par ordre chronologique.

Les informations stockées peuvent être de toute nature : transactions, contrats, titres de propriété, œuvres d'arts, etc.

Également, deux définitions plus précises, issue de l'ouvrage Laurent Leloup ou celle émise par la CNIL, peuvent être proposées :

« Une blockchain est une base de données transactionnelle distribuée, comparable à un grand livre comptable décentralisé et partagé, qui stocke et transfère de la valeur ou des données de façon transparente, sécurisée et autonome (pas d'organe de contrôle). Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie (« consensus ») entre les membres ou participants (« nœuds »). Chaque membre du réseau possède une copie à jour du grand livre (en temps quasi réel) et le contenu est toujours en phase avec l'ensemble des participants. »

Extrait de « *Blockchain, la révolution de la Confiance* » - Laurent LELOUP - Eyrolles - 05/2021 - page 14

« La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Elle constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création, sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. »

Définition de la CNIL

La Blockchain peut être qualifiée de sous-catégorie des technologies de registres distribués (DLT- « *distributed ledger technology* »), caractérisée notamment par l'absence d'administrateur central et par le fait de ne pas dépendre d'une seule entité de stockage.

En résumé, la Blockchain est donc un registre distribué dans lequel tout le monde a le droit de lire et d'écrire, mais personne ne peut supprimer ce qui a été écrit. Mises à jour en permanence, les transactions sont infalsifiables.

Le Parlement Européen est venu définir en 2016 la Blockchain comme : « un ensemble de blocs intégrés dans un système partageant une base de données communes » dans sa résolution n°2016/2007 du 26/05/2016 sur les monnaies virtuelles.

La Blockchain a ensuite été introduite en droit français par le décret n° 2018-1226 du 24/12/2018 sous le nom de DEEP- dispositif d'enregistrement électronique partagé.

1.1.2- Blockchain publique, Blockchain privée, à Consortium : des différences de taille

Une distinction fondamentale existe entre Blockchain Publique, Blockchain Privée et Blockchain à Consortium.

▪ Blockchain publique

La Blockchain publique (de type Bitcoin/Etherum/Tezos...) est accessible à tous, elle repose sur le caractère ouvert à l'écriture sans restriction (envoi et validation de transaction) et à la lecture (libre accès au registre des transactions). Ouverte et transparente : toutes les données relatives aux transactions sont accessibles au public pour vérification.

Il est possible de devenir un « nœud » du réseau et vérifier l'intégralité des transactions historiques ainsi que les nouvelles transactions entrantes via le minage.

Chaque nœud, dans un réseau pair à pair, possède une copie complète à jour du registre.

Le terme sans permission « *permissionless* » est souvent utilisé en même temps que le terme public.

En effet, il n'existe pas d'autorité centrale/régulatrice pour autoriser la participation d'un nouveau membre et/ou son engagement dans le mécanisme de consensus, via le minage ou le staking.



▪ Blockchain privée

La Blockchain privée (de type Hyperledger) requiert, quant à elle, une autorité centrale pour valider de nouveaux membres. Elle accorde les droits en lecture ou en écriture pour modifier le registre. Les nœuds sont réservés aux membres du consortium.

Les Blockchains privées peuvent traiter plus de transactions par seconde que les Blockchains publiques. L'accès est limité à un certain nombre de participants, ce qui permet mécaniquement d'obtenir un consensus plus rapidement sur le réseau grâce à une probabilité plus faible de congestion.

Avec moins de nœuds, la Blockchain privée est cependant plus exposée aux attaques d'un hacker pour prendre le contrôle du réseau et manipuler les données.



Blockchain à Consortium

La Blockchain à Consortium (de type Ripple⁴, IBM Food Trust⁵, B3i⁶) dite « **permissionned** » s'est développée ces dernières années. Cette technologie, hybride, combine des éléments de la Blockchain Publique et de la Blockchain Privée.

Un des éléments clés se situe au niveau du consensus. Au lieu d'un système ouvert où n'importe qui peut valider des blocs (minage, staking...) ou d'un système fermé où les producteurs de blocs sont désignés par une autorité centrale, la Blockchain à consortium comporte une poignée de parties (les valideurs) équitablement puissantes pour la validation des blocs.

Une Blockchain de consortium a tendance à être plus évolutive (avantage notable concernant sa flexibilité pour opérer des modifications). Les changements peuvent être plus facilement déployés dans le cas où les validateurs parviennent à un consensus.

Cependant la Blockchain de consortium est moins transparente que la Blockchain Publique. Elle peut s'avérer être compromise dans le cas d'un nœud victime d'une faille de sécurité.



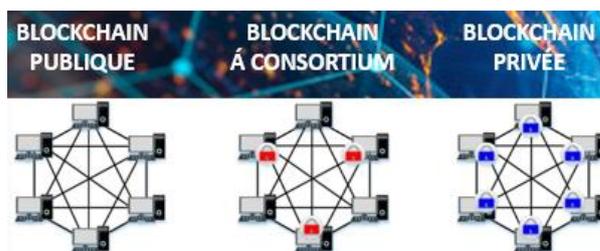
⁴ Ripple est un protocole de règlement bancaire, hébergeant la monnaie numérique « *Ripple* » ou « *XRP* ». Les transactions XRP sont accessibles par tous, toutefois la validation reste centralisée. En effet, Ripple fonctionne grâce à un ensemble réduit de nœuds choisis (société Ripple Labs).

⁵ IBM Food Trust est un registre distribué permissionné à l'écriture et à la lecture permettant une traçabilité de la nourriture. Elle rassemble un consortium d'entreprises incluant Walmart, Unilever, Nestlé et Carrefour.

Comparaison entre Blockchain Publique/Privée/à Consortium :

	Type de Blockchain		
	Publique	Privée	à Consortium
Sans permission ?	Oui	Non	Non
Qui peut la consulter ?	Tout le monde	Seulement les utilisateurs invités	Cela varie
Qui peut y écrire ?	Tout le monde	Des participants approuvés	Des participants approuvés
Propriété	Personne	Entité unique	Plusieurs entités
Participants connus ?	Non	Oui	Oui
Vitesse de transaction	Lente	Rapide	Rapide

Source : Binance Academy⁷ – Article du 06/01/2020 - « *Blockchain Privées, Publiques et à Consortium — Quelles sont les différences ?* »



En conclusion, les niveaux d'accessibilité, les protocoles de validation des blocs et les performances calculées en transaction par seconde peuvent grandement varier d'un type de Blockchain à une autre.

Au sein des catégories de Blockchains Publiques, Privées ou à Consortium, il existe plusieurs caractéristiques/spécificités. Il est donc indispensable de bien comprendre ces dernières pour pouvoir être pertinent dans son analyse.

⁶ B3i est une blockchain à consortium qui fédère plusieurs grands assureurs, développé sur l'infrastructure open source Corda.

⁷ Binance Academy - « *Blockchain Privées, Publiques et à Consortium — Quelles sont les différences ?* » - 06/01/2020, disponible à l'adresse suivante : <https://academy.binance.com/fr/articles/private-public-and-consortium-blockchains-whats-the-difference>

1.2- Histoire de la Blockchain

1.2.1- A l'origine: la création du Bitcoin et le mystère « Satoshi Nakamoto »

La Blockchain est née lors de la création du Bitcoin.

Le 31/10/2008, le monde découvre alors la première cryptomonnaie lorsque le créateur du Bitcoin, Satoshi Nakamoto, publie son livre blanc – « Bitcoin - A Peer-to-Peer Electronic Cash System ». Le document de 9 pages, concis, clair et technique, est accessible à tous⁸. Son auteur garde son identité secrète en se cachant derrière le pseudonyme de « Satoshi Nakamoto ».



Source bit2me ACADEMY

En 01/2009, Satoshi Nakamoto publie le logiciel Bitcoin, téléchargeable gratuitement. Après cette publication, il offre les clés de son invention aux internautes. Commence alors le développement de la cryptomonnaie Bitcoin, qui repose sur la technologie Blockchain pour conserver l'historique des transactions.

⁸ Satoshi Nakamoto - Livre blanc « Bitcoin: A Peer-to-Peer Electronic Cash System » - 31/10/2008, disponible à l'adresse suivante : <https://nakamotoinstitute.org/bitcoin/>

⁹ Eric Hughes - « A Cypherpunk's Manifesto » - 09/03/1993, disponible à l'adresse suivante : <https://www.activism.net/cypherpunk/manifesto.html>

¹⁰ L'objectif principal de Hashcash était de minimiser la réception de grandes quantités de courriels non désirés, en utilisant la collision de

Les Cypherpunks, groupe d'activistes de la région de San Francisco qui promouvaient un chiffrement fort dans le manifeste daté du 09/03/2013⁹, sont également très souvent évoqués lorsque l'on parle de Bitcoin.

Les Cypherpunks ont inspiré Satoshi Nakamoto lors de la conception de la monnaie numérique avec notamment le « HashCash¹⁰ ».

L'objectif était de créer une monnaie électronique infalsifiable et sans intermédiaire, mais un obstacle devait être levé, celui de la « double dépense¹¹ ». La double dépense fait référence à la difficulté d'empêcher ou de contrôler la duplication de contenu virtuel (l'information numérique était jusqu'alors facile à copier).

La création du Bitcoin a résolu le problème technologique de la double dépense et donc la problématique de la contrefaçon sur les réseaux et ce, en inventant l'unicité numérique, la transparence absolue.



Source : Les Echos Solutions

hachage pour ce faire. À l'origine, sa création visait à lutter contre le spam électronique et les attaques DDoS. Cependant, plus récemment, le système est devenu populaire avec le bitcoin et d'autres cryptomonnaies, en tant que pièce essentielle de l'algorithme de minage.

¹¹ Dr. Billal CHOULI, Frédéric GOUJON, Yves-Michel LEPROCHER - « Les Blockchains – De la théorie à la pratique, de l'idée à l'implémentation » - Collection Epsilon Editions ENI – 01/2017

Le réseau Bitcoin a été rapidement en développement actif et en production, en développant la possibilité de nouveaux échanges.

Un des épisodes connus est celui du 22/05/2010 lorsque le développeur Laszlo Hanyecz a cherché une bonne âme qui accepterait de lui livrer 2 pizzas en échange de 10.000 bitcoins. Ce jour est désormais connu comme le "Bitcoin Pizza Day", soit la première fois qu'un bien réel a été acquis grâce à la cryptomonnaie en tant que monnaie sans nécessité de garantie extérieure et en reposant sur la confiance de ses utilisateurs.

Ne s'agissant pas d'une monnaie étatique, le Bitcoin est alors une révolution, obligeant ainsi à se réinterroger sur ce qu'est que la monnaie.

En 12/2010, Satoshi Nakamoto publie son dernier message. Il disparaît en laissant planer le mystère sur son identité (il pourrait s'agir d'un individu ou d'un groupe d'individus), en laissant derrière lui plus d'un demi-million de bitcoin toujours intouchés et personne à qui s'adresser.

1.2.2- L'émergence de la deuxième génération de Blockchain

C'est avec l'émergence de la deuxième génération de Blockchain en 2015, axée sur le déploiement de Smart-Contracts, que les perspectives de désintermédiation se sont accentuées.



Source Cryptoast

Les Smart-Contracts sont : « des programmes déployés dans une blockchain. Concrètement il s'agit d'un code informatique qui exécutent automatiquement des conditions définies au préalable et inscrites dans la Blockchain. Ils fonctionnent comme toute instruction conditionnelle de type « if – then » (si telle condition est certifiée, alors telle conséquence s'exécute). »¹²

Ainsi, avec un Smart-Contract, les termes du « contrat »¹³ ou des protocoles automatisés, ne pourront pas être modifiés, ce qui a pour conséquence de réduire les coûts de vérification, d'exécution ou encore de fraude.

Les projets se sont concentrés par la suite sur :

- ✓ **la scalabilité** : terme utilisé dans le monde des cryptomonnaies pour désigner la capacité des Blockchains à « monter en charge », c'est-à-dire à pouvoir traiter plus de transactions à la seconde sans que cela n'impacte les performances ;
- ✓ **l'interopérabilité** : possibilité d'échanger des données entre différentes chaînes de blocs de manière transparente, comme s'il n'y avait pas de frontières ;
- ✓ **l'implémentation d'éléments de Machine Learning au sein des processus décisionnels** : technologie d'intelligence artificielle permettant aux machines d'apprendre sans avoir été au préalable programmées spécifiquement à cet effet.

Trois raisons principales peuvent expliquer l'émergence de la technologie Blockchain via notamment, la combinaison ingénieuse de technologies et de procédés existants :

¹² Définition de Blockchain France, disponible à l'adresse suivante : <https://blockchainfrance.net/2016/01/28/applications-smart-contracts/>

¹³ Un smart contract ne constitue pas en lui-même un contrat, il constitue une application technique

- ✓ une **puissance de calcul et de mémorisation** accessible largement grâce aux progrès des technologies de l'information (« loi de Moore »)¹⁴ ;
- ✓ la **cryptographie**, qui permet de transférer l'information de façon ciblée, et de s'assurer que seules les personnes destinataires de l'information pourront l'exploiter, sécurisant ainsi les échanges de données ou les transactions.
- ✓ la **technologie des réseaux pair à pair** (« peer-to-peer »), qui permet de réaliser un partage d'informations collectivement validées et protégées en reliant les utilisateurs sans serveur central et de constituer le registre partagé.



Puissance de calcul et de mémorisation

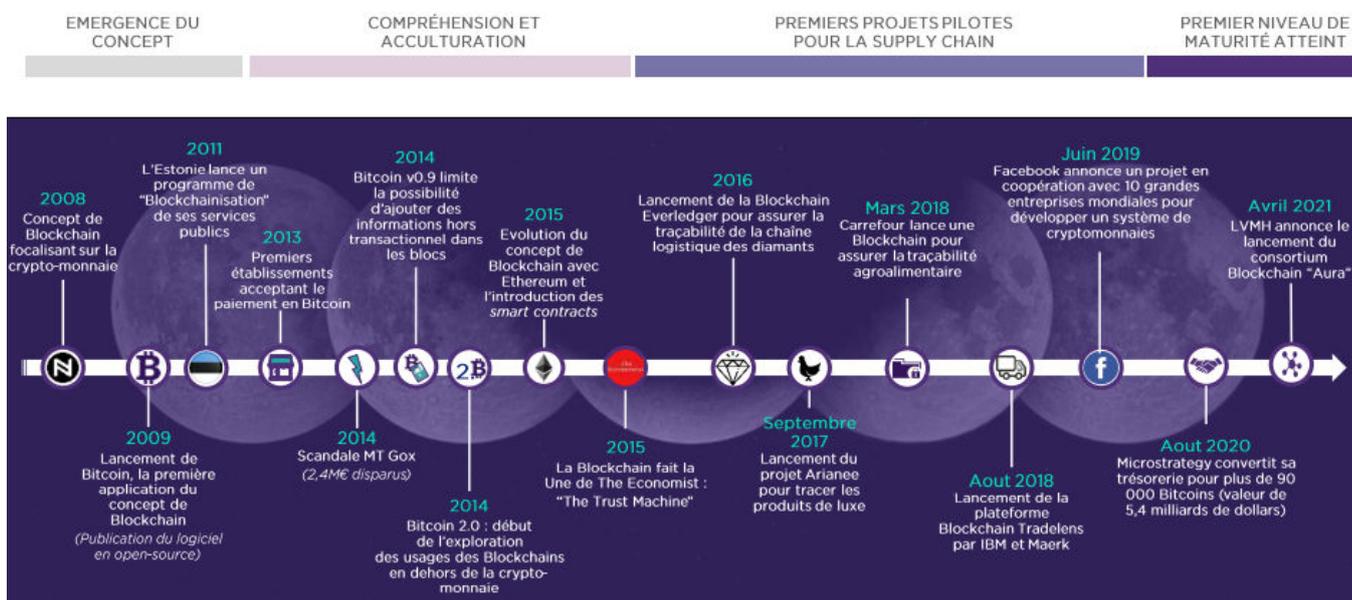


Cryptographie



Technologie de réseaux pair à pair

Ci-dessous, une chronologie sur le développement de la Blockchain et son application à la Supply Chain établie par le cabinet Wavestone :



Source :Wavestone¹⁵

¹⁴ La loi de Moore est une observation de 1965 faite par le cofondateur d'Intel, Gordon E. Moore, selon laquelle le nombre de transistors placés dans un circuit intégré (IC) ou une puce double environ tous les deux ans. Parce que l'observation de Moore a été fréquemment citée et utilisée pour la recherche et le développement par plusieurs organisations (et elle a été prouvée à plusieurs reprises), elle est connue sous le nom de loi de Moore.

¹⁵ Wavestone - Livre Blanc « Supply Chain x Blockchain » – 06/2021, disponible à l'adresse suivante : <https://www.wavestone.com/app/uploads/2021/06/Livre-blanc-Supply-Chain-x-Blockchain.pdf>

1.3- Principes et fonctionnement

Les grands principes inhérents à cette technologie Blockchain sont les suivants :

« La Blockchain dérive d'une vision de l'homme très particulière : des individus autonomes passent des contrats entre eux. Ils n'ont pas besoin de collectif, de communauté ».

Interview de « *Un rêve technocratique totalitaire* » - Michel Bauwens - Le Monde - 15/04/2016, disponible à l'adresse suivante : https://www.lemonde.fr/economie/article/2016/04/18/michel-bauwens-un-reve-technocratique-totalitaire_4904154_3234.html

1.3.1- Architecture non centralisée

L'architecture non centralisée de la Blockchain repose sur une architecture nodale. Les nœuds sont les ordinateurs reliés au réseau. Chaque nœud possède une copie de la base de données, retraçant l'ensemble de l'historique des transactions effectuées. Les membres de la Blockchain peuvent interagir de pair à pair sans avoir recours à une administration centrale. Se forme alors une chaîne de blocs reliés entre eux.

1.3.2- Consensus distribué

La transaction est réalisée lorsqu'elle est intégrée à un « bloc ». Elle ne pourra être intégrée que si l'ensemble des informations ont été préalablement vérifiées et déclarées conformes par des acteurs du réseau.

Ces derniers sont appelés les « mineurs », par exemple pour le Bitcoin. Via leur matériel informatique (importante puissance de calcul), les « mineurs » vérifient puis valident les blocs de transactions.

¹⁶ Disponible à l'adresse suivante : <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>

Lorsque le bloc est validé, il est horodaté et ajouté à la chaîne de blocs . La transaction est alors visible par tous les membres du réseau.

Représentation d'une chaîne de blocs



Source : Blockchain France¹⁶

Il existe 3 types de protocole permettant de valider les blocs ajoutés à la chaîne de blocs existante :

- Protocole de preuve de travail¹⁷

La validation des blocs repose sur la puissance de calcul de machines de minage capables de résoudre une équation cryptographique. Ce protocole est utilisé par exemple pour la cryptomonnaie Bitcoin.

- Protocole de preuve d'enjeu¹⁸

La validation des blocs repose sur les cryptomonnaies que les validateurs mettent sous séquestre pour valider les blocs. Si un valideur ne suit pas les règles du protocole, il risque par perdre tout ou partie des cryptomonnaies qu'il a mises sous séquestre. Ce protocole est utilisé par exemple pour la cryptomonnaie Ethereum.

- Protocole de preuve d'enjeu déléguée¹⁹

La validation des blocs repose sur des élus, via un système de notation de leur réputation afin d'assurer la sécurité des validations. Si l'un des validateurs ne suit pas les règles du protocole, il ne pourra plus refaire partie des validateurs

¹⁷ En anglais : PoW - Proof of Work

¹⁸ En anglais PoS - Proof of Stake

¹⁹ En anglaise: DPOS (Delegated Proof of Stake)

du réseau. Ce protocole est utilisé par exemple pour la cryptomonnaie Tezos.

Ce processus de validation des blocs peut prendre un certain temps selon la Blockchain en question : environ une dizaine de minutes pour Bitcoin, 15 secondes pour Ethereum.



Source : Wavestone – Livre Blanc « Supply Chain x Blockchain » - 06/2021

1.3.3- Synchronisation et décentralisation des enregistrements

Les informations constituant les transactions sont alors visibles par tous les membres du réseau (grand-livre hébergé par les membres du réseau sur leur espace de stockage local) et sont sécurisées par des procédés cryptographiques pour prévenir toute modification à posteriori.

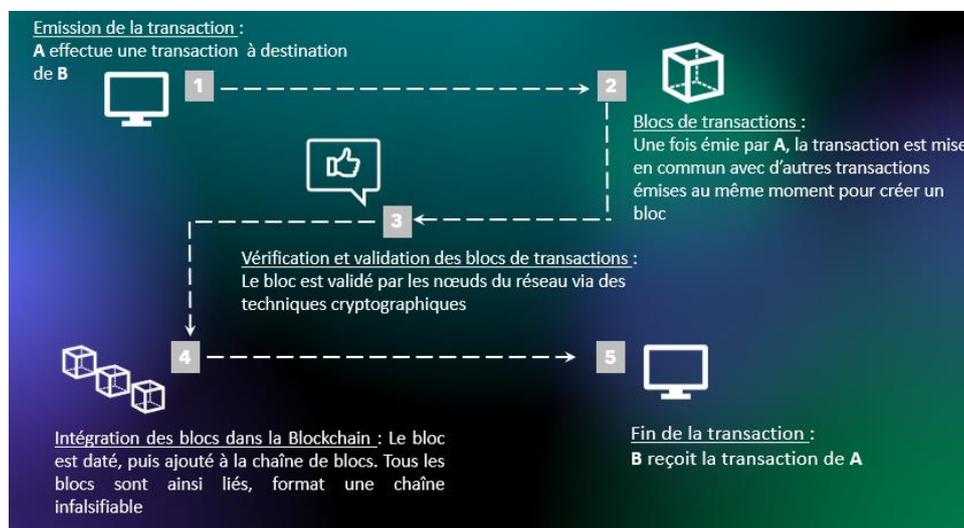
1.3.4- Smart Contracts ou Contrats Intelligents

Comme mentionné ci-dessus (paragraphe 1.2.2), les Smart-Contracts permettent l'automatisation de l'exécution d'une transaction et ce, de manière autonome.

1.3.5- Fonctionnement du Bitcoin en 5 étapes

Le fonctionnement de la Blockchain Bitcoin peut être illustré par les 5 étapes majeures ci-dessous :

- ✓ **Etape n°1 : Emission de la transaction** – deux parties (A et B) se sont accordées sur les termes d'une transaction ;
- ✓ **Etape n°2 : Blocs de transactions** - le registre est « scanné » par les membres du réseau. La transaction est mise en commun avec d'autres transactions émises pour créer un bloc ;
- ✓ **Etape n°3 : Vérification et validation des blocs de transactions** - la validation est encadrée par les règles du réseau. Si tel est le cas, la transaction est validée et ajoutée au dernier bloc de la chaîne ;
- ✓ **Etape n°4 : Intégration des blocs dans la Blockchain** – les blocs validés sont ajoutés à la chaîne de blocs et diffusés à l'ensemble du réseau ;
- ✓ **Etape n°5 : Fin de la transaction** – la partie B reçoit la transaction de A.



1.4- Avantages

1.4.1- Autonomie

La technologie Blockchain fonctionne selon les règles qui ont été établies par ses membres. Il n'y a donc pas besoin d'organe central de contrôle.

1.4.2- Transparence

Le fait que le code de la Blockchain soit ouvert et accessible à l'ensemble des membres du réseau rend le système transparent.

L'ensemble des transactions réalisées sont stockées sur un registre distribué (grand livre), ce qui garantit la transparence des données inscrites.

Ainsi, tous les membres du réseau disposant d'une autorisation d'accès voient les mêmes informations en même temps.

1.4.3- Traçabilité

La Blockchain crée une trace d'audit qui documente la provenance d'un actif à chaque étape de son parcours. Elle offre ainsi une source d'audit fiable, consultable par tous les membres de la Blockchain.

A titre d'exemple, dans les secteurs gangrenés par la contrefaçon et la fraude, cette trace d'audit de la Blockchain fait office de preuve.

1.4.4- Horodatage

La technologie Blockchain permet d'horodater des événements et des opérations sur des registres.

Ainsi l'horodatage, via la technologie Blockchain, permet de prouver qu'un fichier ou un document numérique existait à un certain moment. Ce fichier ou ce document peut être par exemple une pièce d'identité numérique ou un dossier numérisé.

1.4.5- Désintermédiation

La validation des transactions et des nouveaux blocs permet de passer d'une confiance centralisée à une confiance technologique décentralisée.

La vérification et la validation des blocs (« *minage* » pour le Bitcoin) sont effectuées sans avoir recours à un intermédiaire de confiance.

1.4.6- Sécurité

Un des avantages de la Blockchain est la sécurité qu'elle procure pour les transactions réalisées dans le réseau. Les informations insérées dans la Blockchain sont réputées comme étant sécurisées grâce au mécanisme de vérification et de validation des blocs.

Les données échangées sur la Blockchain sont cryptées. La validation des blocs fait appel à des concepts de cryptographie qui garantissent l'inviolabilité et la sécurité des transactions effectuées sur le réseau. Ainsi, une modification de l'historique de transactions engendre une désynchronisation du bloc par rapport aux autres, ce qui va mettre en lumière sa falsification.

Par ailleurs, en cas de tentative pour hacker le réseau et falsifier une transaction, le hacker va devoir corrompre simultanément plus de la moitié des nœuds (attaque dite des 51% - « *Goldfinger* »).

Ce type d'attaque, plus compliqué à mettre en œuvre, est détectable rapidement (incohérence par rapport à l'historique du système).

1.4.7- Automatisation

Les règles qui ont été pré-établies par les membres de la Blockchain, via les Smart-Contracts, permettent des traitements automatiques et autonomes, avec à la clé plus d'efficacité, de rapidité, ainsi que la certitude que le contrat sera exécuté comme convenu.

Les Smart-Contracts, réduisent notamment l'intervention humaine, les coûts de vérification et évitent de devoir faire appel à des tiers pour vérifier si les dispositions du contrat ont bien été respectées.

1.4.8- Limitation du risque de perte de données

Par rapport à un système centralisé, le risque de perte de données lié à une panne ou un piratage est moindre. En effet, les sauvegardes sont multiples compte tenu de son architecture non centralisée.

Pour résumer, la technologie Blockchain va permettre de garantir, sans faire appel à un tiers de confiance, la sécurité et l'application d'un contrat de pair à pair entre les membres d'un réseau. Elle accroît ainsi la transparence et la traçabilité des données et ce, en introduisant une efficacité nouvelle.

1.5- Les grands types d'usages de la Blockchain

L'engouement pour la Blockchain a gagné de nombreux secteurs de l'économie. En effet, les acteurs publics ou privés manifestent un intérêt grandissant pour la technologie Blockchain.

Il est possible de catégoriser les usages de la Blockchain en trois types :

▪ La Blockchain pour les transferts d'actif

La cryptomonnaie est le cas d'usage le plus connu du grand public en la matière. C'est d'ailleurs le premier usage avec la création du Bitcoin (cf. paragraphe 1.2.1).

Mais la Blockchain va au-delà du transfert monétaire, et permet de transférer tout type d'actifs : actions, obligations, titres de propriété, votes, etc.

▪ La Blockchain en tant que registre

Le caractère inaltérable et transparent de la Blockchain en fait un atout précieux pour des enjeux de traçabilité et de certification. En effet, la Blockchain permet de construire un grand livre distribué, visible de tous les membres, avec un protocole pour sa mise à jour et ce, sans besoin d'avoir recours à un tiers de confiance.

Ci-dessous quelques usages :

Lutte contre la Contrefaçon



Gestion de la preuve



Traçabilité



La Blockchain et le Smart-Contract

Le Smart-Contract est considéré par certains comme l'élément de la Blockchain ayant le plus grand potentiel applicatif.

Il est important de souligner que les Blockchains peuvent en effet être utilisés par tous les secteurs, autres que ceux en rapport avec les services financiers, pour désintermédier les systèmes transactionnels.

1.5.1- Les typologies de crypto-actifs

Il existe à ce jour plusieurs catégories de crypto-actifs et il est probable que de nouvelles typologies apparaissent au cours des prochains mois/années. Ci-dessous, quelques exemples (liste non-exhaustive) :

Crypto-monnaies

Il permet de réaliser des transactions numériques. Bien que le plus connue soit le Bitcoin, il en existe beaucoup d'autres. En date du 09/05/2021, selon CoinMarketCap, il existait 5 023 crypto-monnaies pour une valeur atteignant les 2 031 milliards d'€.



²⁰ Une « ICO » désigne une opération de levée de fonds par laquelle une société ayant un besoin de financement émet des jetons, aussi appelés « tokens », auxquels les investisseurs souscrivent principalement avec des crypto-monnaies. Ces jetons peuvent leur

Utility Token

- > Jetons fongibles
- > Liés à un produit
- > Valeur d'échange

Il est conçu pour permettre un usage ou un achat. On l'appelle « *Utility token* » et représente la majorité des tokens émis dans le cadre des « *ICO - Initial Coin Offering*²⁰ ».

L'Utility Token est ce qu'on appelle un jeton fongible, c'est-à-dire qu'il est remplaçable par n'importe quel jeton du même écosystème. Il peut être utilisé sur une plateforme en échange d'un service spécial ou pour recevoir un traitement préférentiel pour des services. Il est principalement utilisé par les entreprises afin de permettre aux utilisateurs d'accéder à leurs services. En effet, l'acquéreur d'un Utility Token n'attend pas nécessairement un retour sur investissement.

L'Utility Token n'est pas régulé en tant que tel.

Security Token

- > Jetons fongibles
- > Liés à un actif
- > Titre "on-chain"

Il donne droit à une forme de participation à l'entreprise, sous forme de droits de participation à la gouvernance ou d'intéressement aux profits futurs, c'est le « *Security token* ».

permettre d'accéder, dans le futur, à des produits ou services de cette société. L'investissement dans une ICO comporte des risques de perte partielle ou totale du capital investi.

Il représente la propriété sur un actif du monde réel (par exemple des actions, une dette ou un bien immobilier).

Ce type de token permet aux investisseurs de placer des fonds, de financer, mais aussi de spéculer sur un projet Blockchain.

Les investisseurs utilisant ce type de token espèrent tirer profit de leur investissement.

Le Security token est complexe car il y a des enjeux d'émission, de négociation mais également de conformité.

Le « *STO - Security Token Offering*²¹ », qui permet l'émission d'un Security token, fait l'objet d'une réglementation spécifique.

■ NFT - « *Non Fungible Token* »

- > **Jetons non fongibles**
- > **Preuve de propriété**
- > **Traçabilité**



Ce support numérique entre dans la famille des crypto-actifs. Il est créé et vendu via un système décentralisé de blockchain.

A la différence des autres typologies, le NFT représente un droit de propriété unique sur un actif et n'est pas interchangeable (identifiant numérique unique et inviolable qui permet d'authentifier un fichier numérique).

Le NFT est un actif certes unique, mais il est aussi vérifiable. Il permet une efficacité maximale pour prouver la propriété, identifier le caractère unique des biens et distinguer les contrefaçons des originaux.

Il est par nature non fongible d'où son nom « *Non Fungible Token* » ou « *Jeton Non Fongible* ».

En résumé, le NFT tient lieu de certificat d'authenticité et constitue une preuve numérique de provenance et de propriété unique d'un actif grâce à la technologie Blockchain.

Le cas d'usage le plus connu à ce jour est la transformation d'œuvres d'art ou d'objets de collection en NFT, ce qui permet d'en assurer la propriété.

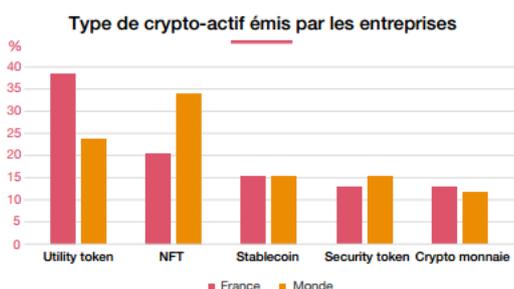
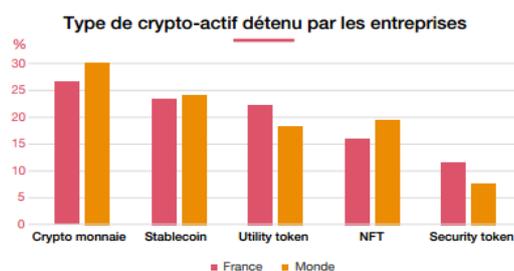
Toutefois, il est important de noter que ces catégories ne sont pas étanches. Dans les faits, il est parfois difficile d'établir une délimitation claire, certains tokens ayant des caractéristiques hybrides ou issues de plusieurs catégories.

Ainsi, une analyse au cas par cas est indispensable pour déterminer la nature et la fonction de chaque crypto-actif.

²¹ Une « *STO* » désigne une levée de fonds en cybermonnaie. Des jetons (tokens) financiers, appelés « *Security tokens* » sont émis et enregistrés sur une Blockchain. Comme pour les titres financiers, ils sont achetés par des investisseurs. Une fois acquis, ces « *Security*

tokens » confèrent à leurs détenteurs un droit juridique. Une « *STO* » est plus réglementé que l'« *ICO* » puisqu'il offre des droits aux possesseurs. Les « *Security tokens* » ont le statut de valeur mobilière comme des titres financiers. Ils sont liés à un actif sous-jacent.

■ Panorama en 2022



Source : « Blockchain & crypto : comment les entreprises en tirent enfin bénéfice », PWC, 2022²²

1.5.2- Les secteurs monétaires et financiers déjà mobilisés

La Blockchain fait partie des nouvelles technologies qui ont suscité un très vif intérêt des Etats et des entreprises du secteur financier, ci-dessous quelques exemples :

■ Focus sur la monnaie digitale des Banques Centrales

L'intérêt des gouvernements et des autorités publiques ne faiblit pas.

Dans une étude rendue publique en 01/2020²³, la Banque de Règlement Internationaux révèle que 80% des Banques Centrales étudient la création d'une monnaie digitale d'une manière ou d'une autre. C'est 10 points de plus qu'un an auparavant.

²² Disponible à l'adresse suivante : <https://www.pwc.fr/fr/publications/blockchain/blockchain-crypto-comment-les-entreprises-en-tirent-enfin-benefice.html>

« Les banques centrales envisagent de plus en plus la création d'une forme numérique de leurs monnaies. Et il faut l'admettre, l'idée soulève parfois des doutes, voire même des craintes, de la part des banques commerciales »

Extrait du discours de François Villeroy de Galhau - Gouverneur de la Banque de France – 12/07/2022

L'objectif en effet est de créer une « MDBC - monnaie digitale de banque centrale »; appelée également « MNBC - monnaie numérique de banque centrale » ou « CBDC - central bank digital currency ». Il ne s'agit pas de remplacer la monnaie fiduciaire mais plutôt d'en proposer une alternative.

A noter qu'il existe deux types de MDBC/MNBC/CBDC : celles dites de « gros » ou « wholesale » (exclusivement dédiées aux banques pour le règlement et la livraison d'actifs financiers) et celles de « détail » ou « retail » (uniquement destinées à une utilisation par le public).

La MDBC/MNBC/CBDC de « gros/wholesale », presque systématiquement de nature transfrontalière, est à ce jour au stade de démonstration de faisabilité. En France, deux cas d'usages déterminants sont en cours d'étude avec pour objectif l'amélioration de l'écosystème des paiements et ce, via le recours à la technologie Blockchain :

- ✓ tokenisation des titres avec un règlement de ces derniers ;
- ✓ règlements transfrontières et en devises.

²³ Etude de la Bank for International Settlements disponible à l'adresse suivante : <https://www.bis.org/publ/bppdf/bispap107.pdf>

A noter également l'existence d'initiatives communes entre les différentes Banques Centrales, notamment pour les paiements transfrontaliers.

Il existe également la MDBC/MNBC/CBDC, dite de « détail/retail », qui est uniquement destinée à une utilisation par le public. Cette dernière soulève de nombreuses interrogations, compte tenu notamment des priorités différentes entre les banques centrales des économies avancées et les banques centrales des économies émergentes.

Les premières s'attachent à la souveraineté des systèmes de paiement, tandis que les secondes cherchent, quant à elles, à améliorer l'accès à des systèmes de paiement de détails dans des pays où une partie de la population n'est pas bancarisée.

Les principales Banques Centrales du monde planchent sur le sujet, notamment au Royaume-Uni, aux Etats-Unis, ou encore en Inde, et en sont à des stades plus ou moins avancés.

Quelques pays ont cependant déjà lancé leur MDBC/MNBC/CBDC de « détail/retail », tels que :

- ✓ au Bahamas, où la Banque Centrale des Bahamas a lancé le « Sand Dollar » au printemps 2021 ;
- ✓ au Nigeria, où le « e-Naira » a été lancé à l'automne 2021 pour améliorer l'inclusion financière sur le territoire.

Les yeux sont également rivés sur la Chine, où la version pilote du yuan numérique²⁴, dit « E-yuan », en test depuis 2020, progresse à grand pas.

Déployé dans un nombre croissant de centres urbains et de Provinces, la Banque Populaire de Chine a d'ailleurs déclaré que les volumes de transactions utilisant le E-yuan avaient atteint 13 milliards de dollars fin 2021.

En Europe, la BCE a annoncé le 14/07/2021²⁵ le lancement d'une expérimentation concernant le recours à l'euro uniquement sur des supports numériques, avec une phase d'étude de 24 mois et ce, en vue d'un déploiement d'ici fin 2023²⁶.



■ Focus sur le secteur financier

L'étude publiée en janvier 2022 par l'ACPR²⁷ sur la transformation numérique dans les secteurs français de la banque et de l'assurance fait état des résultats suivants : « Dans le secteur de la banque, la technologie de registre distribué (Blockchain) fait l'objet d'appréciations contrastées : tandis que 25% des banques interrogées estiment cette technologie trop peu mature et les cas d'usage pertinents peu nombreux, près de 40%, jugent, à l'inverse, que l'impact de la Blockchain sur l'activité bancaire sera important, voire « disruptif ».

Les opérations interbancaires et de compensation font partie des premiers cas d'usage en matière de Blockchain et impliquent un grand nombre d'institutionnels et de grandes entreprises.

²⁴ Le gouvernement chinois a banni l'essentiel des activités privées en matière de cryptomonnaie.

²⁵ Communiqué de presse de la Banque Centrale Européenne - « L'Eurosystème lance un projet d'euro numérique » - 14/07/2021

²⁶ « Enfin, à la fin 2023, nous pourrions décider de lancer une phase de réalisation pour développer et tester les solutions techniques appropriées et les arrangements commerciaux nécessaires pour fournir un euro numérique », a déclaré Fabio Panetta. « Cette phase

pourrait prendre trois ans. » - Extrait du discours de M. Fabio Panetta, membre du directoire de la BCE en 05/2022

²⁷ Communiqué de presse de l'ACPR – « L'ACPR publie les résultats de son étude sur la transformation numérique dans les secteurs français de la banque et de l'assurance » - 14/01/2022, disponible à l'adresse suivante : https://acpr.banque-france.fr/sites/default/files/medias/documents/20220114_cp-_etudes_numeriques.pdf

Dans ce secteur, la technologie Blockchain ouvre la possibilité de valider des transactions sans l'intermédiaire d'une chambre de compensation, ce qui devrait permettre de certifier des opérations dans des délais beaucoup plus courts. Elle peut aussi réduire les coûts et les frais d'administration.

Dans le secteur de l'assurance, l'apport de la Blockchain tient par exemple à l'automatisation des procédures de remboursement et à l'allègement de certaines formalités à la charge des sociétés comme de leurs clients, sous réserve que les hypothèses et les conditions d'indemnisation et de préjudice soient clairement établies (recours au Smart-contract).

Autre exemple, la plateforme de paiement digitale et sécurisée fondée sur la technologie Blockchain, **MoneyTrack**, a levé 2,3 millions d'euros en 03/2021. Cette plateforme est reliée au système d'information des assureurs, ce qui permet de rapatrier toutes les garanties des contrats des assurés.

L'objectif est de permettre à une mutuelle / collectivité / institution de verser de l'argent à des personnes, qui peuvent alors les dépenser, sous condition, au sein d'un réseau de prestataire authentifié :

« Tout cela s'auto-exécute dans un Smart-contract pour générer derrière le paiement du compte de l'assureur au compte du praticien, sans que l'assuré n'ait à avancer des frais »²⁸.

“

Chez WTW, on a beaucoup d'interactions avec InsurTech France, France Meta et des starts-up, pour travailler sur les changements futurs du Business traditionnel dans l'Assurance face à la compétition de petites structures.

Il est donc nécessaire de se trouver le plus en amont possible de ces grands changements de tendance afin de pouvoir les intégrer et ne pas prendre du retard.

Il est important de souligner que toute la Blockchain n'est pas consolidée autour des crypto-monnaies.

Quand on regarde aujourd'hui dans le monde de l'assurance, ce qui viendra bouleverser le monde de l'assurance demain, ce sont les Smart-Contracts. Par exemple, en cas d'annulation ou de retard d'un avion, il était nécessaire d'envoyer un dossier et donc de prendre un temps certain pour se faire indemniser, générant ainsi des délais de traitements longs et parfois manuel, ainsi qu'un processus chronophage.

En se basant sur la technologie Blockchain et plus particulièrement sur les Smart-Contracts, les indemnisations pourront être déclenchées dès réception de l'information en provenance de l'aéroport, qui fera état du retard ou de l'annulation du vol et ce, de manière automatique.

Cela a un impact matériel sur le Business Model. ”

Benjamin Bouffard – Directeur de l'activité Strategic Risk Consulting pour l'Europe de l'Ouest chez WTW – 17/06/2022

²⁸ Propos de Christophe Doré - extrait de l'article French Web - « Blockchain: la FinTech MoneyTrack lève 2,3 millions d'euros et mène sa première acquisition » - 26/03/2021, disponible à l'adresse suivante :

<https://www.frenchweb.fr/blockchain-la-fintech-moneytrack-leve-23-millions-deuros-et-mene-sa-premiere-acquisition/418599>

Des groupes de travail se sont constitués dans le secteur financier, que ce soit en interne, au sein des entreprises, ou via des groupes de place.

A titre d'exemple, l'AFTI²⁹ – « Association française des professionnels des titres » est déjà mobilisée sur ces sujets, notamment au regard de l'actualité réglementaire européenne récente qui introduit :

- ✓ la création d'un régime pilote pour les infrastructures de marché reposant sur la technologie blockchain ;
- ✓ le règlement «Market in Crypto Assets» (MiCA), qui doit encadrer les cryptoactifs.

En effet, la technologie Blockchain pour la filière titres et le post-marché ouvre le champ des possibles via une efficacité opérationnelle inédite : intégration de l'exécution jusqu'au règlement-livraison, règlement-livraison instantané, disparition d'intermédiaires, fin des travaux de réconciliation.

Par ailleurs, le rôle des tiers de confiance pourra alors être assuré par la technologie, bouleversant ainsi les différents acteurs intervenant dans les différents processus.

1.5.3- Les autres secteurs d'activité

L'étude publiée en 2022 par PWC « *Blockchain & crypto : comment les entreprises en tirent enfin bénéfice* »³⁰ met en évidence le caractère incontournable de la Blockchain et des cryptoactifs dans les entreprises et révèle que les sponsors de la Blockchain se situent désormais au niveau des Directions Générales :

« Cette année, la direction générale devient le premier sponsor des projets blockchain, ce qui traduit un appui stratégique au plus haut niveau. A titre de comparaison, notre enquête de 2021 plaçait les départements innovation comme soutien principal (devant précisément les directions générales). »

Par ailleurs, l'ensemble des domaines et des métiers sont aujourd'hui concernés, notamment avec l'émergence du Web3, des NFT et du Métavers.

La France tire son épingle du jeu, au regard de son écosystème Blockchain dynamique³¹. Elle peut être utilisée dans de nombreux domaines et la liste s'agrandit chaque jour.

Ci-dessous un focus sur quelques secteurs phares :

■ Le secteur de la logistique



Dans ce secteur, la Blockchain présente deux intérêts majeurs : la traçabilité des produits et la coopération entre acteurs d'une filière.

A titre d'exemple, l'industrie alimentaire utilise déjà la technologie Blockchain pour sécuriser la chaîne d'approvisionnement. Elle connecte les agriculteurs, distributeurs, commerçants et consommateurs finaux afin d'apporter de la transparence.

Elle permet ainsi l'authentification des produits, une traçabilité sur l'ensemble du cycle de vie du produit et le suivi de la responsabilité de chacun des acteurs.

²⁹ L'AFTI - « Association Française des Professionnels des Titres », constituée en 1990, a pour objet de rassembler les professionnels des établissements du secteur bancaire et financier concernés par les activités sur les instruments financiers

³⁰ Etude de PWC - « *Blockchain & crypto : comment les entreprises en tirent enfin bénéfice* » - 2022, disponible à l'adresse suivante :

<https://www.pwc.fr/fr/publications/blockchain/blockchain-crypto-comment-les-entreprises-en-tirent-enfin-benefice.html>

³¹ A titre d'exemple, les licornes « Sorare » (vente de NFT de joueurs de football) et « Ledger » (portefeuille numérique) constituent des références à l'international de l'industrie Blockchain

A titre d'illustration, **Carrefour Bio** a annoncé la mise en place de la Blockchain sur ses produits à partir d'04/2022³².

▪ Le secteur immobilier

Le rapport « *Immobilier 3.0 : de la pierre papier à la pierre crypto* »³³, daté de 05/2022, met en lumière les grandes transformations que pourrait connaître le secteur immobilier grâce à la Blockchain. Au delà de l'usage de cette technologie pour la gestion du cadastre dans certains pays³⁴, la « tokenisation » immobilière (comparée au fractionnement immobilier), ainsi que le paiement de la transaction immobilière via les cryptomonnaies, commencent à émerger.

Aujourd'hui, le rapport mentionne qu'il existe une dizaine de sociétés dans le monde qui proposent la tokenisation de biens immobiliers.

A titre d'exemple, en 03/2019, l'entreprise **Brickblock** a tokenisé les actions de participation d'un SPV (Special Purpose Vehicle) afin de vendre un bien d'une valeur d'environ 2 millions d'euros, à Wiesbaden en Allemagne³⁵.

▪ Le secteur automobile

La Blockchain dans le secteur automobile est déjà à l'essai pour une multitude d'usages.

Plusieurs projets sont déjà lancés.

A titre d'exemple, **Faurecia**, **Groupe Renault**, **Knauf Industries**, **Simoldes** et **Coşkunöz**, en collaboration avec **IBM**, ont déployé une Blockchain pour tracer et certifier la conformité réglementaire des composants et sous-composants d'un véhicule.

L'initiative, baptisée XCEED – « *eXtended Compliance End-to-End Distributed* », a pour but de faciliter la traçabilité de l'ensemble des composants d'un véhicule de la conception à la production³⁶.

▪ Le secteur de l'énergie

Dans le secteur de l'énergie, un des usages est la gestion du réseau local électrique entre producteurs et consommateurs et ce, de façon indépendante dans une optique d'autoconsommation. Ainsi, l'objectif est l'échange/la revente des surplus d'électricité entre voisins, via des transactions sécurisées.

A titre d'exemple, le projet **Brooklyn Microgrid** permet aux utilisateurs de gérer localement et de façon indépendante leur propre réseau électrique, en s'appuyant sur la blockchain Ethereum. Les surplus d'électricité s'échangent entre voisins, via des transactions sécurisées.

Autre exemple, **BNP Paribas** et **EDF ENR** ont annoncé en 07/2022 leur collaboration afin d'émettre la première obligation distribuée sur la Blockchain sous forme de tokens.

³² Article de LSA Commerce Connecté - 13/04/2022, disponible à l'adresse suivante : <https://www.lsa-conso.fr/carrefour-applique-la-blockchain-a-ses-produits-bio-de-marque-propre,408776>

³³ Le rapport « *Immobilier 3.0 : de la pierre papier à la pierre crypto* » - 05/2022, disponible à l'adresse suivante : <https://drive.google.com/file/d/1FFmttsiF8PREQa1yZePVRbXr37NKwy5/view>

³⁴ Au Ghana, l'initiative de l'ONG « Bitland » a abouti à la mise en place d'un cadastre via la Blockchain. En Suède, le Landmäteriet (le service

national du cadastre) utilise la Blockchain pour l'enregistrement des titres de propriétés et des terrains

³⁵ Article de Cision -23/03/2019, disponible à l'adresse suivante : <https://www.prnewswire.com/news-releases/brickblock-tokenizes-the-first-property-in-europe-300820582.html>

³⁶ Voir communiqué de presse de Renault à l'adresse suivante : <https://www.renaultgroup.com/news-onair/actualites/xceed-e2-80-af-une-nouvelle-solution-de-blockchain-pour-les-usines-renault-en-europe/>

Les deux entités souhaitent ainsi :

- ✓ simplifier le financement des petits projets écologiques, qui peinent parfois à trouver les fonds nécessaires ;
- ✓ accroître la transparence avant investissement des projets, notamment sur les critères environnementaux, sociaux et de gouvernance (ESG).

▪ Le secteur du sport

La **FIFA** et la Blockchain **ALGORAND** ont annoncé le 03/05/2022 leur partenariat³⁷. ALGORAND va apporter une solution technique pour ce qui est des actifs numériques : portefeuille, développement d'infrastructure et stratégie sur actifs numériques, etc.

▪ Le secteur public

La Blockchain peut également être utile au secteur public, notamment en ce qui concerne l'identité numérique, la certification de documents et la traçabilité.

A titre d'exemple, en 10/2021, **l'Université de Lille** a émis un système d'attestations numériques de réussite aux diplômes fondé sur la Blockchain, dans le but notamment de lutter contre la fraude au diplôme³⁸.

L'objectif du projet est de délivrer à chaque diplômé une attestation de réussite accessible en ligne. Cette attestation, dite « vérifiable » ou « à valeur probante », est produite grâce à la technologie Blockchain.

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

1.6- Un cadre réglementaire mondial disparate...

Face à l'essor des crypto-actifs, les États tentent de réglementer ces nouveaux usages et d'établir un cadre légal.

Or, le premier frein à la mise en place d'une réglementation est constitué par l'essence même de la Blockchain, à savoir que le contrôle logique du système est opéré par l'ensemble de la communauté.

Dans le secteur bancaire et financier, la Blockchain entraîne un certain nombre de changements disruptifs compte tenu de :

- ✓ **l'arrivée de nouveaux acteurs**, tels que les sociétés technologiques dans les services financiers et de paiement, dont beaucoup sont à ce jour peu ou pas régulés ;
- ✓ **l'émergence de nouvelles formes d'actifs financiers ou de règlement** ;
- ✓ **l'apparition d'infrastructures de marché décentralisées** : les nouvelles technologies tendent à réduire le recours à des intermédiaires financiers ou à des systèmes centralisés développés souvent par les Banques Centrales ;
- ✓ **la suppression de certains intermédiaires** : les transactions se font directement entre utilisateurs finaux en se passant des intermédiaires bancaires et des infrastructures de marché.

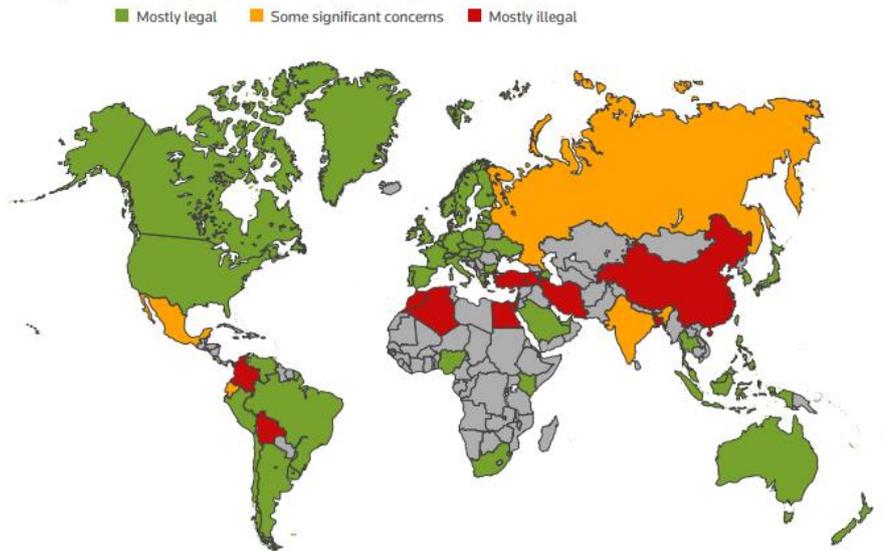
Face à cette situation, les approches des législateurs et régulateurs ont été hétérogènes selon les États.

³⁷ <https://coinacademy.fr/actu/fifa-algorand-partenariat/>

³⁸ Article d'Acteurs Publics - « *Quand la blockchain délivre des attestations de diplômes numériques inviolables* » - 05/11/2021,

disponible à l'adresse suivante : <https://acteurspublics.fr/articles/quand-la-blockchain-delivre-des-attestations-de-diplomes-numeriques-inviolables>

Cryptocurrency regulations by country



Source : Thomson Reuters –
« Cryptocurrency regulations by country » - 2022³⁹

Certains Etats ont interdit l'usage et le minage de crypto-actifs, alors que d'autres, au contraire, accueillent ce nouvel écosystème à bras ouvert.

Par exemple, la jurisprudence aux États-Unis a adopté une position stricte dès 2017, via l'application extensive de la réglementation financière aux crypto-actifs. Ils étaient alors assimilés à des instruments financiers, dits « securities ».

Au fur et à mesure, plusieurs réglementations locales ont vu le jour, avec pour objectif de prendre en compte les caractères multiples et variés des crypto-actifs.

Les intérêts propres de chaque Etat influencent également le déploiement des réglementations :

- ✓ **Le Salvador** a été le premier à adopter le Bitcoin comme monnaie officielle en 09/2021⁴⁰. Tous les paiements peuvent être effectués directement en Bitcoin ;
- ✓ **Le Kazakhstan** est devenu le deuxième Etat au monde avec le plus grand nombre de fermes de minage suite au bannissement des mineurs en Chine annoncé en 06/2021. A noter que le 04/05/2022, un arrêté ministériel a été publié afin que les mineurs s'enregistrent obligatoirement auprès des autorités. En effet, ce pays, qui a fait l'objet de pénuries énergétiques (coupures d'électricité), cherche désormais à endiguer le phénomène du minage illégal de crypto⁴¹ ;
- ✓ Autre exemple d'actualité, **la Banque Centrale russe** a accordé à Sberbank, une licence pour émettre et échanger des actifs financiers numériques⁴² ;

³⁹ Etude disponible à l'adresse suivante : <https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf>

⁴⁰ Article de La Finance pour tous – « Le Salvador a-t-il eu raison d'adopter le bitcoin comme monnaie officielle »- 04/05/2022, disponible à l'adresse suivante : <https://www.lafinancepourtous.com/2022/05/04/le-salvador-a-t-il-eu-raison-dadopter-le-bitcoin-comme-monnaie-officielle/>

⁴¹ Article du Journal du Coin - 06/05/2022, disponible à l'adresse suivante : <https://journalducoin.com/bitcoin/kazakhstan-mineurs-bitcoin-btc-enregistrement-regulation/>

⁴² Article de Zonebourse Coin - 17/03/2022, disponible à l'adresse suivante : <https://www.zonebourse.com/cours/action/PJSC-SBERBANK-6494829/actualite/La-banque-centrale-russe-accorde-a-Sberbank-une-licence-pour-emettre-et-echanger-des-actifs-numeriqu-39795250/>

- ✓ **Aux Etats-Unis**, le président américain a signé le 09/03/2022 un décret pour « *garantir le développement responsable des actifs numériques* ». Le texte reconnaît la croissance du secteur crypto, ainsi que l'attractivité de ses technologies. Les Etats-Unis, par ce décret, souhaitent développer rapidement une MNBC, ce qui correspond à un dollar numérique⁴³.

Au sein de l'Union Européenne, seuls quelques États membres depuis 2017 (dont la France) ont légiféré localement.

Finalement, ce n'est qu'à partir de 06/2019 avec l'annonce officielle de Facebook concernant le lancement de leur cryptomonnaie, appelée « *Libra* »⁴⁴, que les institutions Européennes se sont penchées collectivement sur la question. Compte tenu de l'opposition des régulateurs, des banques et des décideurs politiques, ce projet est aujourd'hui officiellement enterré⁴⁵.

...initialement mis en place localement par les Etats au sein de l'Union Européenne...

Face au développement des crypto-actifs, certains États de l'Union Européenne ont envisagé de réglementer les nouveaux usages et d'établir un cadre légal.

Compte tenu notamment de l'essor et de l'intérêt des citoyens pour les crypto-actifs, la France a légiféré localement. L'étude⁴⁶ de l'ADAN datée de 02/2022, réalisée avec KPMG France, mentionne que 8% des français détiennent des cryptomonnaies.

La **loi PACTE**, promulguée le 22/05/2019, a remodelé le paysage juridique des actifs numériques en France. Outre la question de la réglementation des ICO, en plein essor à l'époque des travaux législatifs, la loi PACTE s'est attachée à apporter un cadre clair aux « **prestataires de services sur actifs numériques** » (**PSAN**) en créant un régime d'enregistrement et d'agrément.

- **Le statut de prestataire de services sur actifs numériques (PSAN)**

Pour encadrer le développement des PSAN, la loi PACTE a mis en place deux types d'autorisations :

- ✓ un **enregistrement obligatoire** pour les services d'achat/vente, et de conservation de crypto-actifs pour le compte de tiers ;
- ✓ un **agrément optionnel** notamment pour la gestion d'une plateforme d'échanges et la gestion de portefeuille pour le compte de tiers.

Les PSAN sont soumis à un socle de règles communes à tous les services : assurance ou fonds propres, procédures de contrôle interne,

⁴³ Le décret est disponible à l'adresse suivante : <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/>

⁴⁴ Article du Journal Le Monde - 18/06/2019, disponible à l'adresse suivante : https://www.lemonde.fr/pixels/article/2019/06/18/ce-qu-il-faut-savoir-sur-le-libra-la-cryptomonnaie-de-facebook_5477887_4408996.html

⁴⁵ Article de Capital - 01/02/2022, disponible à l'adresse suivante : https://www.lemonde.fr/pixels/article/2019/06/18/ce-qu-il-faut-savoir-sur-le-libra-la-cryptomonnaie-de-facebook_5477887_4408996.html
<https://www.capital.fr/crypto/meta-facebook-met-officiellement-fin-a-son-projet-de-monnaie-numerique-diem-1427160>

⁴⁶ L'étude « *La crypto en France, structuration et adoption par le grand public* » - datée de 02/2022, établit un état des lieux de la place française autour de deux volets complémentaires : l'industrie des cryptos en France et la démocratisation des cryptos en France (sondage mené par l'institut IPSOS et analyse faite par KPMG France : <https://adan.eu/rapport/crypto-france-structuration-adoption#:~:text=En%20ce%20d%C3%A9but%20d'ann%C3%A9e%202022%2C%20l'Association%20pour,projections%20quant%20aux%20opportunit%C3%A9s%20%C3%A9conomiques>

système informatique résilient, politique tarifaire transparente, etc.

- **Le visa optionnel pour les levées de fonds en cryptomonnaies (ICO)**

Pour encadrer le développement des ICO, les acteurs qui souhaitent lever des fonds par émissions de jetons numériques (ICO) peuvent solliciter un visa auprès de l'AMF.

Afin d'assurer une meilleure information et protection des investisseurs, il est nécessaire de satisfaire plusieurs obligations, dont :

- ✓ l'obligation pour l'émetteur de jetons d'être constitué sous la forme d'une personne morale établie ou immatriculée en France ;
- ✓ la fourniture d'un document d'information destiné à donner toutes les informations pertinentes sur l'offre de jetons, le projet financé et l'entreprise ; la mise en place d'un dispositif permettant le suivi et la sauvegarde des actifs recueillis à l'occasion de l'offre ;
- ✓ le respect des règles en vigueur en matière de lutte contre le blanchiment et le financement du terrorisme.

Les levées de fonds, sans visa de l'AMF, restent cependant légales en France, le visa étant optionnel. Toutefois, les émetteurs qui n'ont pas reçu le visa de l'AMF ne pourront pas démarcher le grand public.

⁴⁷ Le décret n° 2021-387 - 02/04/2021 - « *Lutte contre l'anonymat des actifs virtuels et renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme* », disponible à l'adresse suivante :

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043328577#:~:text=Dans%20les%20r%C3%A9sum%C3%A9s-,D%C3%A9cret%20n%C2%B0%202021%2D387%20du%202%20avril%202021%20relatif,et%20le%20financement%20du%20terrorisme>

⁴⁸ Le décret n° n° 2021-446 - 15/04/2021 - « *Renforçant le cadre de lutte contre le blanchiment de capitaux et le financement du terrorisme* », disponible à l'adresse suivante :

Pour compléter le cadre légal de la loi PACTE, de **nouveaux textes** ont été publiés en **2021** :

- ✓ **l'ordonnance n° 2020-1544** du 09/12/2020
- ✓ **le décret n° 2021-387** du 02/04/2021⁴⁷ relatif à la lutte contre l'anonymat des actifs virtuels et renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme ;
- ✓ **le décret n° 2021-446** du 15/04/2021⁴⁸ renforçant le cadre de lutte contre le blanchiment de capitaux et le financement du terrorisme.

En conséquence, les PSAN enregistrés et les émetteurs de jetons ayant le visa AMF doivent réaliser l'identification de leurs clients à chaque opération, quels qu'en soient le montant et la nature et ne peuvent accepter le recours à la monnaie électronique anonyme pour l'achat d'actifs numériques.

De plus, depuis le 10/06/2021, à l'issue d'un délai de transition, il est interdit aux acteurs qui permettent l'échange crypto-crypto d'exercer sans être enregistrés auprès de l'AMF.

... qui se construit désormais en commun

Ce n'est qu'à partir de 2019 suite à l'annonce de Facebook concernant le lancement de sa cryptomonnaie, « *Libra* »⁴⁹ (aujourd'hui officiellement enterrée⁵⁰), que l'Europe s'est

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043378767#:~:text=Dans%20les%20r%C3%A9sum%C3%A9s-,D%C3%A9cret%20n%C2%B0%202021%2D446%20du%2015%20avril%202021%20renfor%C3%A7ant,et%20le%20financement%20du%20terrorisme>

⁴⁹ Article du Monde - 18/06/2019, disponible à l'adresse suivante : https://www.lemonde.fr/pixels/article/2019/06/18/ce-qu-il-faut-savoir-sur-le-libra-la-cryptomonnaie-de-facebook_5477887_4408996.html

⁵⁰ Article de Capital - 01/02/2022, disponible à l'adresse suivante : <https://www.lemonde.fr/pixels/article/2019/06/18/ce-qu-il-faut-savoir-sur-le-libra-la-cryptomonnaie-de->

penchée sur la question du cadre réglementaire.

Le 24/09/2020, la Commission Européenne a présenté deux textes afin de mieux réguler l'usage, l'échange et le stockage des cryptoactifs.

Les 29 et 30/06/2022, le Parlement Européen et le Conseil de l'Union Européenne sont parvenus à des accords politiques provisoires sur deux textes réglementaires majeurs qui vont changer le visage de l'industrie crypto européenne : le règlement Markets in crypto-assets (**MiCA**) et le règlement révisé sur les transferts de fonds (**TFR**).

▪ Focus sur le règlement européen MiCA (« Markets in Crypto-Assets »)

Le règlement européen MiCA vise les acteurs du secteur et a pour objectif de réguler les prestataires de services proposant des crypto-actifs de manière harmonisée sur l'ensemble du territoire de l'Union Européenne.

Il s'agit d'un règlement, donc d'un texte d'application directe (i.e. il n'a pas besoin d'être transposé en droit national). Ce règlement européen, qui vise à encadrer les crypto-actifs, couvre plusieurs domaines dont :

- ✓ l'offre au public et l'admission aux négociations de jetons ;
- ✓ l'offre au public et l'admission aux négociations de jetons de valeur stable (stablecoins⁵¹) ;
- ✓ la fourniture de services sur crypto-actifs par des prestataires ;
- ✓ la prévention des abus de marché sur crypto-actifs.

Ce règlement a vocation à remplacer les cadres nationaux mis en place jusqu'ici par certains Etats membres de l'UE (dont celui introduit par la loi PACTE en France). Il imposera l'obtention du statut de « crypto-assets services provider » « CASP ». Les prestataires qui seront agréés selon le règlement MiCA pourront bénéficier du passeport européen et fournir leurs services dans tous les Etats de l'Union Européenne.

A noter que :

- ✓ les NFT sont exclus du champ d'application du règlement MiCA, sauf s'ils remplissent certains critères spécifiques ;
- ✓ le règlement MiCA ne contient pas d'interdictions du minage en PoW. Cependant, les prestataires devront respecter des règles strictes en matière de déclaration des données liées à leur empreinte environnementale et climatique.

▪ Focus sur le règlement européen TFR (« Transfer of Funds »)

En parallèle, d'autres négociations se sont déroulées au niveau européen, dans le cadre de la révision du règlement TFR.

Ce dernier vise en effet à identifier les détenteurs de portefeuilles privés par le renforcement des procédures de vérification d'identité KYC⁵² et de lutte contre le blanchiment des capitaux et le financement du Terrorisme (LCB-FT). Par ailleurs, il rend obligatoire la fourniture des informations d'identification sur les transactions en cryptomonnaies : informations sur l'émetteur et le bénéficiaire des transferts de cryptoactifs.

<https://www.capital.fr/crypto/meta-facebook-met-officiellement-fin-a-son-projet-de-monnaie-numerique-diem-1427160>

⁵¹ Un Stablecoin est une monnaie numérique adossée à une valeur refuge « stable » comme le dollar américain ou l'or. Les Stablecoins

sont conçus pour réduire la volatilité par rapport aux cryptomonnaies non-adossées comme les bitcoins.

⁵² « Know Your Customer » ou connaissance du client, est le nom donné au processus permettant de vérifier l'identité des clients.

“

« En 2019, la loi a remodelé le paysage juridique des actifs numériques en France avec la création du statut de PSAN (prestataire de services sur actifs numériques – acteurs enregistrés/acteurs agréés).

L'optique de l'AMF, dans ce contexte, est de surveiller les innovations technologiques et financières, ainsi que la protection des investisseurs. Pour cela, il est nécessaire de réguler les acteurs, qui sont extrêmement diversifiés.

Concernant la gestion de l'actif, l'investissement dans ce type d'actifs numériques reste à ce jour limitée. Aujourd'hui, elle concerne 3 sociétés de gestion sur plus de 700 en France. Cela ne représente que quelques millions d'euros. Les crypto devises sont aujourd'hui interdites pour les OPCVM. Pour les « securities token », si le sous-jacent est bien un instrument financier éligible, l'usage d'un dispositif d'enregistrement électronique partagé est généralement considéré comme une simple modalité de tenue du passif.

Concernant la gestion du passif, les métiers du « post marché » et de la « conservation » sont très attentifs aux risques et opportunités que cette technologie engendre, pouvant avoir un impact sur la transformation de leur industrie.

Concernant les obligations en termes de protection de la Clientèle, MICA « Markets in Crypto-Assets » a vocation à réguler cette nouvelle classe d'actifs, via la mise en place d'un cadre juridique général. Cette version liste notamment les obligations en termes d'information, de gestion des conflits d'intérêts, de traitement des réclamations, d'organisation en termes de gestion des risques et de sauvegarde de l'information (évaluation via le recours à des entités tierces).

Didier Deleage – Directeur Adjoint de la Direction de la Gestion d'Actifs à l'AMF – 29/06/2022

Un accord provisoire sur le règlement TFR a été trouvé entre les différentes institutions européennes à Bruxelles, obligeant les acteurs à fournir des informations d'identification sur les transactions en cryptomonnaies.

Il s'applique à toutes les transactions depuis/vers les CASP dès le premier euro.

Le règlement TFR impose une connaissance du client à partir d'un virement de 1 000 euros entre une plateforme d'échange de cryptomonnaies et un wallet.

A noter que :

- ✓ le règlement TFR va s'appliquer également aux transferts depuis/vers des portefeuilles physiques dits "non hébergés" (portefeuille de type Ledger par exemple) vers un CASP.
- ✓ les transferts dits en "P2P", c'est à dire de personne à personne effectués sans prestataires, i.e. sans passer par des CASP, ne rentrent pas dans le champ du règlement TFR.

Les discussions techniques se poursuivent actuellement entre les co-législateurs sur chaque règlement avant leur publication au Journal Officiel de l'Union Européenne.

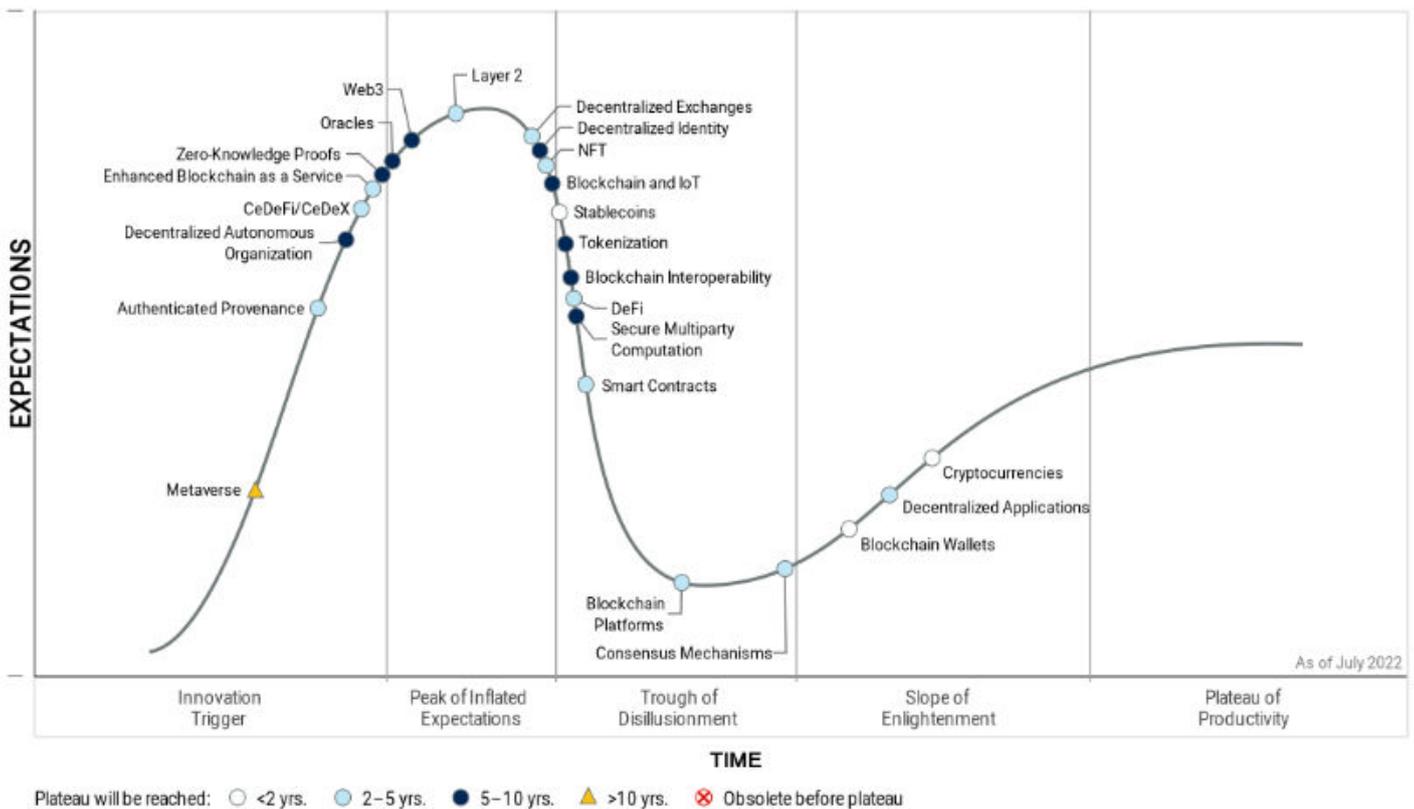


2. RISQUES, OPPORTUNITES ET DEFIS

Quand on parle de nouvelle technologie, la courbe de Gartner est souvent mentionnée.

D'après Gartner, il existe plusieurs phases, qui peuvent être résumées comme suit : la première correspond à une phase **d'enthousiasme excessif**, d'engouement médiatique qualifié de « **pic des illusions** ».

Ces illusions n'étant pas toujours justifiées (les attentes initiales ne sont pas toujours réalistes), s'ensuit la deuxième phase de « **désillusions** », avant de repartir ensuite sur une phase « **d'équilibre** » lorsque la technologie est maîtrisée, en phase avec des attentes réalistes.



Source : Etude Gartner – 07/2022⁵³

⁵³ Disponible à l'adresse suivante : <https://blogs.gartner.com/avivah-litan/2022/07/22/gartner-hype-cycle-for-blockchain-and-web3-2022/>

Si on applique cette courbe à la technologie Blockchain, le plateau de productivité n'est pas encore atteint et beaucoup d'initiatives se localisent dans le plateau « *creux des désillusions* » et « *pentés de consolidation* ».

Si on compare cette analyse par rapport à l'année dernière, on peut constater que le Web3 et le Metaverse ont fait leur apparition.

Compte tenu de cette analyse, on peut être amené à s'interroger sur ce qu'il en est pour les fonctions de contrôle⁵⁴.

Quels sont les risques qu'engendre cette technologie, quelles sont les nouvelles opportunités offertes, mais également quels vont être les défis à relever pour les fonctions de contrôle ?

2.1- Risques

" Il y a des inconnus connus, c'est-à-dire, qu'il y a des choses que nous savons que nous ne savons pas. Mais il y a aussi des inconnues inconnues, des choses que nous ne savons pas que nous savons pas "

Donald RUMSFELD

La place des tiers de confiance est impactée avec l'essor de la technologie Blockchain, remplaçant ainsi la confiance interindividuelle par une confiance de type algorithmique.

Or, dans de nombreux pays, les fonctions d'intermédiaires/tiers de confiance sont exercées par les institutions publiques, par des

grandes entreprises spécialisées et/ou des professions réglementées.

La Blockchain constitue une source de transformations économiques et sociales très importante, l'exposant ainsi aux risques suivants :

2.1.1- Risque de blanchiment d'argent

En France, le blanchiment est défini à l'article 324-1 du Code Pénal comme un délit consistant à faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect.

Il désigne également le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit.

Compte tenu de leur développement rapide, les crypto-actifs constituent des nouveaux vecteurs qui peuvent être utilisés à des fins de blanchiment d'argent.

Le service de renseignement français, TRACFIN met en lumière dans ses différents rapports annuels plusieurs risques de blanchiment d'argent avec pour vecteurs les crypto-actifs, tels que :

- **Crypto-actifs et Darknet**

Sur le Darknet, les criminels peuvent avoir recours aux crypto-actifs, via des plateformes d'achat et de vente de produits et contenus illégaux. Les prestations sont alors dénouées en crypto-actifs.

⁵⁴ Les fonctions suivantes ne sont pas couvertes par le présent mémoire : Audit Externe, Risk Management, Contrôle de Gestion.

A titre d'exemple, la place de marché russophone du Darknet, **Hydra Market**, a été démantelée en 04/2022 par la police fédérale allemande⁵⁵.

Hydra Market permettait de vendre et d'acheter des stupéfiants, des faux documents d'identité ou encore des offres de service de hackers censés permettre la prise de contrôle de comptes (réseaux sociaux, sites web, adresses e-mail, etc.). Ce site comptait alors 17 millions de comptes clients pour 19 000 comptes vendeurs.

23 millions de bitcoins ont ainsi été saisis par la police.

D'après la police fédérale allemande, cette place de marché intégrait une lessiveuse de blanchiment d'argent : « *Bitcoin Bank Mixer* ». Cette dernière avait pour but de mélanger des fonds potentiellement suspects avec d'autres fonds et ce, afin de brouiller les pistes jusqu'à l'origine des fonds.

Un service de conversion pour transformer les crypto-monnaies en monnaies fiduciaires était également proposé.



Source : Club informatique Provence Méditerranée - 31/05/2021

■ Bitcoin to plastic

Le bénéfice tiré du commerce de produits ou contenus illicites peut être également blanchi

par le biais de cartes « *Bitcoin to plastic* », utilisées pour retirer, en espèces, les profits illicitement acquis en bitcoins.

Ces cartes, apparues en 2013, permettent de payer les commerçants et/ou de retirer des espèces (fonction dite de « *cash out* ») dans les distributeurs automatiques des réseaux VISA et Mastercard. Elles permettent un haut degré d'anonymat.

A titre d'exemple, le cas cité dans le rapport TRACFIN pour l'année 2016⁵⁶ mentionne l'interpellation d'un cybercriminel français par le service de lutte contre la criminalité numérique de la gendarmerie nationale en 02/2016.

Ce dernier proposait à la vente des numéros de cartes bancaires volées, contre paiement en bitcoin. Les recettes étaient déposées par la suite sur une carte dite « *bitcoin to plastic* », permettant alors de convertir les sommes en espèces.

■ Crypto-actifs et conversion en matière première

Dans son rapport pour l'année 2016, TRACFIN a également communiqué que les crypto-actifs peuvent être convertis en matières premières par l'intermédiaire de certains prestataires de services de paiement.

A titre d'exemple, on peut citer le cas d'une plate-forme de e-commerce immatriculée au sein de l'Union Européenne, qui acceptait les paiements en crypto-monnaies pour l'achat et la revente de métaux précieux.

⁵⁵ Article issu de « *01net* » - 07/04/2022, disponible à l'adresse suivante : <https://www.01net.com/actualites/hydra-plus-grande-place-de-marche-du-darknet-et-machine-a-blanchir-les-bitcoins-demantelee-par-la-police-2055811.html>

⁵⁶ Rapport de TRACFIN - « *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2016* », disponible à l'adresse suivante : <https://www.economie.gouv.fr/files/rapport-analyse-tracfin-2016.pdf>

Une cellule de renseignement étrangère a informé TRACFIN qu'un individu résidant en France avait blanchi des revenus en bitcoins issus d'activités de carding (revente de coordonnées bancaires volées) en les convertissant en métaux précieux via cette plateforme.

■ ICO



Source : Business Digital

Les ICO peuvent également être utilisées pour blanchir des capitaux : des fonds illicites peuvent être investis en jetons, lesquels sont ensuite revendus à d'autres investisseurs, puis convertis en monnaie légale. Le blanchisseur justifie alors l'origine de ses fonds par le financement d'un projet et la rentabilité issue de cet investissement. Il est donc essentiel de vérifier l'origine des fonds des investisseurs lors du lancement d'un ICO.

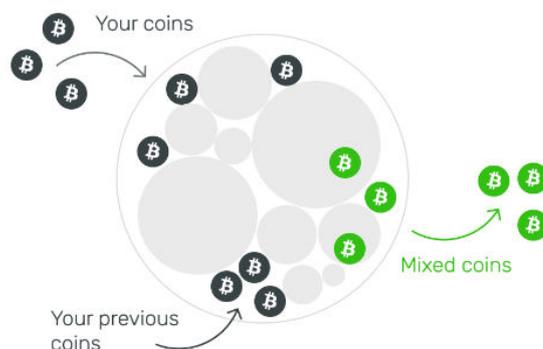
Dans son rapport 2021⁵⁷, TRACFIN mentionne que ce risque est de moins grande intensité compte tenu de l'état du marché. Cependant, le fonctionnement des ICO offre des vulnérabilités intrinsèques importantes en matière de blanchiment de capitaux.

⁵⁷ Rapport de TRACFIN « TRACFIN 2021 - Activité et analyse », disponible à l'adresse suivante : https://www.economie.gouv.fr/files/2022-07/Tracfin_2021_Web.pdf?v=1658933771

⁵⁸ Communiqué de Presse d'Europol - « Multi-million euro cryptocurrency laundering service Bestmixer.io taken down », disponible à l'adresse suivante :

■ Mixage des cryptoactifs

Un des points d'attention important est l'identification d'un « SMC », c'est-à-dire un système de mixage de crypto-actifs.



Source : Cointribune – 30/01/2020

Comme indiqué ci-dessus pour le cas mentionnant « Bitcoin Bank Mixer », un SMC a pour but de mélanger des fonds entre cryptoactifs dérivés d'activités délictueuses et cryptoactifs légaux, afin de les rendre anonymes et de blanchir ces actifs.

A titre d'exemple : le cas de la plateforme de mixage « Bestmixer.io »⁵⁸. En 06/2018, le service néerlandais d'information et de recherche en matière fiscale (FIOD) a enquêté en collaboration avec la société McAfee sur cette plateforme.

L'enquête a révélé que bon nombre des cryptoactifs mixés avaient une origine suspectieuse ou une destination illégale. Ainsi, le 17/02/2020, le FIOD a arrêté une personne physique soupçonnée d'avoir blanchi plus de 100 000 euros avec l'aide de deux complices grâce à cette plateforme.

<https://www.europol.europa.eu/media-press/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixer-io-taken-down>

▪ NFT

Le rapport du Trésor Américain « *Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art* », publié le 04/02/2022⁵⁹, fait état d'investissements dans les NFTs, exposés à l'afflux de fonds d'origine douteuse.

Il est mentionné que les NFTs peuvent être utilisés pour effectuer de l'auto-blanchiment, où les criminels peuvent acheter un NFT avec des fonds illicites et procéder à des transactions avec eux-mêmes.

« Furthermore, NFTs can be used to conduct self-laundering, where criminals may purchase an NFT with illicit funds and proceed to transact with themselves to create records of sales on the blockchain

...

These digital art assets are inherently easier to transfer between transacting parties than traditional art because, in most cases, the parties do not need to physically move the art or pay for shipping services such as insurance, transport, or customs duties, although users may incur transaction fees. The ability to transfer some NFTs via the internet without concern for geographic distance and across borders nearly instantaneously makes digital art susceptible to exploitation by those seeking to launder illicit proceeds of crime, because the movement of value can be accomplished without incurring potential financial, regulatory, or investigative costs of physical shipment.

Rapport du Trésor Américain - « *Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art* » - 02/2022

Un Smart-Contract peut être utilisé pour régir la propriété et la transférabilité d'un NFT, en générant des revenus à chaque transaction enregistrée sur la Blockchain.

Cela peut avoir pour conséquence d'inciter des transferts multiples sur une courte période (transfert sans distance géographique, en l'absence de déplacement physique et presque instantané) et ainsi rendre complexe l'identification de l'acheteur de l'œuvre.

En France, en l'absence de définition juridique précise, l'émergence des NFT offre aux criminels de nouvelles perspectives de blanchiment, en raison notamment des caractéristiques suivantes : difficultés relatives à la connaissance du client et le recours aux cryptoactifs (absence de KYC sur certaines plateformes).

2.1.2- Risque de financement du terrorisme

L'acte de terrorisme est défini en France à l'article 421-2-2 du Code Pénal comme le fait « *de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconques ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens utilisés ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme... indépendamment de la survenance éventuelle d'un tel acte.* »

Le financement du terrorisme est un système en réseau structuré avec des transferts d'argent de sources diverses et de nombreux montants relativement faibles pour contourner le système et se situer en dessous des seuils de contrôle.

⁵⁹ Rapport du Trésor Américain - « *Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art* » -

02/2022, disponible à l'adresse suivante : https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf

Le réseau utilise des formes variées de transfert pour faciliter le transit d'argent vers des pays à risques et ce, sans visibilité sur la contrepartie.

Les crypto-actifs constituent un vecteur risqué de financement du terrorisme compte tenu du fait que ces derniers peuvent être utilisés pour assurer le transfert de fonds au bénéfice de groupes djihadistes. TRACFIN a mis en lumière les risques de financement du terrorisme suivants :

- Exemple de transfert de fonds au bénéfice de groupes djihadistes via l'achat de coupons prépayés convertis en crypto-actifs

Dans le cas d'un circuit de financement du terrorisme innovant impliquant des crypto-actifs, les achats de coupons prépayés étaient convertis en crypto-actifs (bitcoin), qui ensuite étaient transférés sur des plateformes d'échanges situées dans des pays à proximité immédiate de la zone syro-irakienne.

TRACFIN fait état d'un montant de près de 250 000 euros à destination de membres d'Al-Qaïda, ainsi qu'à destination des djihadistes de l'organisation État islamique.

- Exemple de souscription de prêts à la consommation utilisés pour l'achat de crypto-actifs transférés vers un cluster lié à Al Qaïda

Plusieurs comptes étaient ouverts par une personne physique auprès d'une même néo-banque à l'aide d'identités usurpées.

En parallèle, cette dernière avait recours, sur la base de fausses identités, à plusieurs prêts à la consommation auprès d'autres établissements financiers.

Une fois les prêts à la consommation souscrits, elle alimentait avec les fonds issus des prêts les

comptes de la néo-banque afin d'acheter ensuite des crypto-actifs par l'intermédiaire de plateformes d'échanges européennes (françaises également).

Les crypto-actifs acquis étaient ensuite transférés en bitcoins, après plusieurs rebonds entre différentes adresses, vers un cluster identifié comme étant associé à Al Qaïda.

2.1.3- Risque d'escroquerie et de fraude

En France, l'escroquerie est définie à l'article 313-1 du Code Pénal comme le fait « soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge ».

Les ICO « *Initial Coin Offering* » sont exposées à des risques d'escroquerie.

En effet, l'investissement dans une ICO n'est pas sans risque puisque le capital investi peut être perdu en partie ou en totalité (absence de garantie sur le capital investi). Les ICO peuvent être un vecteur à des fins frauduleuses, via notamment l'intermédiaire de sociétés ou des projets fictifs.

A titre d'exemple, le cas ci-dessous a été relevé par TRACFIN : celui d'une société ayant recours à une ICO pour lancer un crypto-actif. Une personne physique a été à l'initiative d'une levée de fonds pour un projet dont la réalité économique a finalement posé question. A noter qu'une vingtaine de personnes physiques avaient investi dans ce projet.

Or, il s'est avéré que :

- ✓ le montant des investissements a été perçu par la personne physique sur des comptes détenus à l'étranger ou par l'intermédiaire d'une société transfrontalière, gérée par son concubin et ce, sans lien économique avec le projet ;
- ✓ aucune société émettrice de l'ICO n'a pu être identifiée ;
- ✓ les évolutions du cours du crypto-actif ont présenté les caractéristiques d'une manipulation de type « *pump and dump* » consistant à gonfler artificiellement le cours de l'actif par un achat massif afin d'attirer les investisseurs. Les personnes à l'origine du montage ont alors revendu leurs actifs, initialement achetés à bas prix, lorsque ces derniers ont atteint leur plus haute valeur. Le cours est ensuite retombé brutalement, ce qui a eu pour conséquence de générer de lourdes pertes pour les autres investisseurs.

Autre exemple avec les tentatives de fraude qui, elles, ont pour objectif de soutirer des informations confidentielles (mot de passe, code secret, informations relatives à l'identité d'une personne...) ou un consentement, via des moyens déloyaux, pour obtenir un avantage.

Ces tentatives de fraude peuvent se solder, en cas de réussite, par l'exécution de paiements à l'aide des informations dérobées et/ou de l'accord obtenu.

Ces risques de fraude vont concerner les investisseurs dans les crypto-actifs puisque ces derniers peuvent confier aux plateformes leurs clés privées. Cela a pour conséquence de leur déléguer la gestion de leur adresse.

Ces clés privées peuvent être stockées, soit dans un fichier connecté à Internet, soit sur un périphérique physique dédié.

Le fait de ne pas détenir sa clé privée sur un périphérique physique expose les investisseurs à un risque de fraude plus important. Leur vigilance doit être accrue.



Source : Cryptoast – 11/04/2018

Enfin, les transactions sur la Blockchain sont irréversibles.

Il convient de préciser qu'en cas de fraude avérée, il n'existe pas de mécanisme pour le rapatriement des fonds ou de solution pour récupérer, en partie ou en totalité, les fonds dérobés.

“

Les cas de fraude concernent le plus souvent des adresses dites « non hosted », des adresses de portefeuilles non hébergés (Metamask ou Ledger par exemple). Ce sont des adresses qui ne nécessitent pas de KYC aujourd'hui.

En cas de fraude pour les établissements bancaires, il existe un mécanisme de « recall » grâce auquel il est possible sous certaines conditions de rapatrier les fonds. Ce n'est pas le cas avec la technologie Blockchain, les transactions sont irréversibles.”

**Dorian Olivier – Compliance / Advisory à
Coinhouse – 21/06/2022**

2.1.4- Risque de fraude fiscale

La fraude fiscale consiste à se soustraire à la loi ou à utiliser des procédés illégaux pour échapper à tout ou partie de l'impôt : insuffisance, omission ou inexactitude dans la déclaration d'impôts. Elle ne doit pas être confondue avec l'évasion fiscale qui consiste à diminuer ses impôts en profitant de certaines lacunes de la loi fiscale. Les crypto-actifs constituent un vecteur propice à la dissimulation de l'origine des fonds auprès de l'administration fiscale.

A titre d'exemple, le 16/06/2022, l'IRS « *International Revenue Service* » a lancé aux Etats-Unis l'opération « *Hidden Treasure* » pour faire face à l'évasion fiscale liée aux crypto-actifs⁶⁰. Plusieurs techniques et méthodes de fraude fiscale sont mentionnées dans le rapport et permettent d'illustrer les procédés pouvant être utilisés, tels que :

- ✓ **structuration** : pratique qui consiste à effectuer fréquemment des transactions inférieures à certains seuils pour contourner les exigences de déclaration fiscale ;
- ✓ **recours à des sociétés écrans fictives** pour garder secrets les revenus liés aux crypto-actifs ;
- ✓ **échanges de chiffrement** permettant le commerce d'objets ou d'autres actifs numériques sans révéler leur identité par le biais de transactions anonymes.



Source : Finbold- 16/06/2022

2.1.5- Crypto-actifs anonymes ou pseudonymes ?

Les transactions en bitcoin, ainsi que la plupart des autres crypto-actifs, ne sont pas anonymes, mais pseudonymes. Pour réaliser une transaction, le détenteur d'un crypto-actif utilise son adresse publique via son portefeuille.

Cette adresse est en effet considérée comme pseudonyme car elle permet de consulter l'ensemble des transactions passées par le réseau sur la Blockchain.

“

On ne peut pas dire que la Blockchain soit anonyme. Elle est pseudonyme, on a accès à l'adresse publique. Par exemple les autorités judiciaires, autorités de police, vont suivre la transaction sur la Blockchain et regarder les adresses publiques. Dès qu'elles vont voir qu'une adresse publique est liée à un acteur enregistré, elles vont pouvoir solliciter l'acteur afin d'identifier l'identité de la personne derrière l'adresse publique. Le fait que les adresses ne soient pas rattachées à des acteurs centralisés pose problème. Les autorités judiciaires ne pourront pas alors avoir accès à l'information dans ce cas.

C'est une des préoccupations des règlements européens que l'Union Européenne est en train de voter (règlement TFR) – utilisation des portefeuilles non hébergés (Ledger/Metamask) qui ne nécessitent pas de KYC – comment tracer ces fonds là ? Il n'y a pas de KYC, pas d'entité centrale...

Concrètement, il va falloir déclarer à TRACFIN les clients qui font une transaction d'un portefeuille non hébergé.”

**Dorian Olivier – Compliance / Advisory à
Coinhouse – 21/06/2022**

⁶⁰ Article de Finbold, « *IRS launches 'Operation Hidden Treasure' to clamp down on crypto non-taxpayers* » - 16/06/2022, disponible à

l'adresse suivante : <https://finbold.com/irs-launches-operation-hidden-treasure-to-clamp-down-on-crypto-non-taxpayers/>

En revanche, il existe à ce jour des crypto-actifs totalement « anonymes ».

Ces derniers restent cependant minoritaires. Par exemple, l'Altcoin « *Monero* » (XMR), qui a basé son anonymat sur les « ring signatures » (signatures en cercle), cachant ainsi la provenance des transactions en créant des données de transactions factices pour masquer les données réelles.



Source : Cointribune – 21/08/2022

2.1.6- Risque lié à la protection de la clientèle

De manière générale, les investisseurs ne bénéficient d'aucune des garanties qui s'attachent aux marchés régulés. Ainsi, ils s'exposent à des risques de perdre, en partie ou en totalité, les montants investis et également à des risques de manipulation de cours.

■ Perte en capital

La récente débâcle de la Blockchain Terra Luna est l'illustration avérée du risque de perte en capital.

L'effondrement du « TerraUSD » s'est manifestée avec une grande rapidité, marquant ainsi l'histoire des crypto-actifs.

Répertoriée dans le top 10 mondial des cryptomonnaies, « TerraUSD » est passé de 80 dollars début 05/2022 à moins de 0,18 dollars le 12/05/2022 et ce, après que le Stablecoin TerraUSD (UST) ait perdu sa parité avec le dollar.

Pour garantir la valeur du Stablecoin TerraUSD (UST) par rapport au dollar (parité de 1 pour 1), un mécanisme d'arbitrage algorithmique⁶¹ était mis en place pour toujours équilibrer l'offre et la demande, avec un système de prêt-emprunt offrant une rémunération à hauteur de 19% pour les prêteurs.

Ce taux était assuré seulement en partie par les emprunteurs (4 à 5%) et le supplément était directement prélevé sur les réserves. Or, lorsque les prix des cryptomonnaies ont commencé à chuter, un grand nombre d'investisseurs ont souhaité échanger leur UST.

Face à cette vague massive de ventes, le mécanisme d'arbitrage n'a pas pu réagir assez vite, de sorte que le Stablecoin a vu sa valeur chuter progressivement, puis brutalement.

Il convient donc pour les investisseurs de se montrer prudent et de se renseigner sur le protocole utilisé, le parcours des fondateurs, la conservation des actifs, etc.

■ Wash trading et crypto-actifs

Les crypto-actifs peuvent être utilisés par les criminels dans une optique de wash trading.



Source : Cryptoast – 29/04/2020

⁶¹ Un mécanisme d'arbitrage était censé entrer en jeu pour maintenir le cours de l'UST. Si celui-ci baisse, les utilisateurs peuvent échanger

un UST contre l'équivalent d'un dollar en LUNA, afin d'augmenter sa valeur.

Le wash trading consiste pour un investisseur à vendre et acheter simultanément un actif à lui-même pour créer une activité artificielle trompeuse. Cette manœuvre entraîne une augmentation artificielle du volume des transactions, ce qui peut faire exploser la valeur du crypto-actif.

A titre d'exemple, en 03/2021, la plateforme d'échange de crypto-actifs, Coinbase, a fait l'objet d'une amende de 6,5 millions de dollars prononcée par la CFTC - « *Commodity Futures Trading Commission* » aux Etats-Unis⁶². Cette sanction a mis en lumière les faits suivants : manipulation du volume des transactions et tromperie des investisseurs via des pratiques de wash-trading sur des NFTs.

▪ Spoofing et crypto-actifs

Les crypto-actifs sont exposés au risque de spoofing.

Le spoofing est une technique illégale de trading haute fréquence (THF), qui consiste à charger un carnet d'ordres (émission d'une grande quantité d'ordres) pour ensuite les retirer avant exécution. L'objectif est de manipuler le marché à son avantage en gonflant le volume du carnet d'ordres.

Les crypto-actifs sont des proies idéales pour les opérations de spoofing, compte tenu des fluctuations rapides et parfois importantes de leurs cours. Les « Baleines »⁶³ ont alors la possibilité de manipuler le marché avec leurs transactions pour leur gain personnel.

L'infraction de spoofing s'avère généralement difficile à détecter.

▪ Délit d'initié et crypto-actifs

Un délit d'initié consiste pour une personne à réaliser des transactions sur le marché grâce à des informations privilégiées (confidentielles, précises, non publiques), pour pouvoir manipuler le marché à son avantage. Compte tenu des caractéristiques, mais également des nouvelles catégories de crypto-actifs, la question de l'infraction de délit d'initié/crypto-actifs se pose désormais.

Aujourd'hui, les cas d'inculpations au titre du délit d'initié viennent des Etats-Unis.

Le premier exemple de délit d'initié impliquant des NFTs a été révélé en 06/2022 avec la plateforme « *OpenSea* »⁶⁴.

L'ancien chef de produit de cette plateforme était informé à l'avance des NFTs, qui allaient être placés sur la page d'accueil du site avec pour conséquence, une augmentation de la valeur des jetons non fongibles en question.

De 06/2021 à 09/2021, ce dernier se procurait les NFTs avant qu'ils ne soient mis en avant, pour les revendre par la suite deux à cinq fois plus cher que leur prix initial.

En France, la problématique est la suivante : peut-on qualifier les NFTs d'instruments financiers ?

La réponse à cette question est à ce jour complexe au regard des différentes typologies de NFTs et des textes réglementaires en vigueur.

⁶² Communiqué de presse de la CFTC - « *CFTC Orders Coinbase Inc. to Pay \$6.5 Million for False, Misleading, or Inaccurate Reporting and Wash Trading* » - 19/03/2021, disponible à l'adresse suivante : <https://www.cftc.gov/PressRoom/PressReleases/8369-21>

⁶³ Surnom donné aux détenteurs de portefeuilles très importants d'un crypto-actif

⁶⁴ Article de SiecleDigital - « *Un ancien employé d'OpenSea accusé d'un délit d'initié lié aux NFT* » - 04/06/2022, disponible à l'adresse suivante : <https://siecledigital.fr/2022/06/04/un-ancien-employe-dopensea-accuse-dun-delit-dinitie-lie-aux-nft/>

Un autre exemple récent en provenance des Etats-Unis, qui constitue une première dans le domaine des crypto-monnaies⁶⁵ : le délit d'initié a en effet fait son entrée pour les crypto-monnaies le 21/07/2022, avec l'inculpation de 3 personnes physiques pour fraude électronique et délit d'initié par la SEC – « *Securities and Exchange Commission* » et le procureur fédéral de Manhattan.

Un ancien cadre (Directeur de produit) de la plateforme Coinbase donnait en effet des informations confidentielles à deux complices (son frère et un ami) et a été sanctionné.

- « Rug pull » et crypto-actifs



Crypto Rug Pull

Source : Nigeria Bitcoin Community

Le « *rug pull* » s'apparente à une escroquerie par laquelle les auteurs commercialisent des actifs numériques autour d'un projet fantôme.

Il existe plusieurs types de « *rug pull* », le plus connu étant le vol de liquidité. Les auteurs vont créer un jeton sur une Blockchain. Suite à la création du jeton en question, un apport de liquidité est effectué afin de permettre de l'échanger à plus grande échelle. Des investisseurs achètent alors le jeton pour faire monter le prix dans un court laps de temps et

créer un engouement afin que d'autres investisseurs achètent le jeton. Une fois l'objectif atteint par les auteurs de l'escroquerie, ces derniers vendront en masse leurs jetons. A noter que les « *rug pull* » sont souvent accompagnés via des campagnes de marketing autour d'influenceurs.

2.1.7- Risque lié à la sécurité

La technologie Blockchain apporte des mécanismes de sécurité, mais il ne s'agit pas d'une garantie absolue en termes de sécurité. Elle n'est pas à l'abri d'attaques provenant de personnes mal intentionnées, qui peuvent manipuler les vulnérabilités connues de l'infrastructure

Depuis quelques années, certains incidents/piratages impactant des Blockchains ont été mis en lumière et ont eu pour conséquence d'engendrer des pertes élevées pour les investisseurs.

- Risques liés à au réseau pair-à-pair

En l'absence de gouvernance centrale, si un ordinateur venait à être piraté, les impacts s'avèrent à première vue limités et ce, compte tenu de l'existence de plusieurs nœuds.

Toutefois, il existe des types d'attaques, comme celle dénommée « *attaque Eclipse* », dont l'objectif est d'isoler un nœud pour prendre connaissance des transactions de la Blockchain.

Cette attaque vise ensuite à occulter la connexion réseau du nœud qui est victime de l'attaque. Ce dernier reçoit alors de fausses informations sur le réseau Blockchain dont il fait partie.

⁶⁵ Article de LEDEVOIR - « *Inculpations pour délit d'initié sur Coinbase, une première dans les cryptomonnaies* » - 22/07/2022, disponible à l'adresse suivante :

<https://www.ledevoir.com/economie/736728/cryptomonnaie-inculpations-pour-delit-d-initie-sur-coinbase-une-premiere-dans-les-cryptomonnaies>

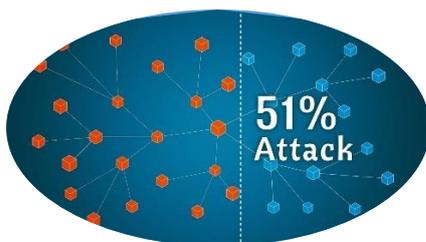
A noter que les Blockchains connues (Bitcoin ou Ethereum) ont mis en œuvre des mécanismes pour s'assurer de la diversité des nœuds connectés aux nœuds ciblés, ce qui permet ainsi de diminuer ce risque.

Un autre incident potentiel pouvant survenir est celui de l'exploitation de bugs dans le logiciel fonctionnant sur les nœuds. L'attaquant prend alors le contrôle de tous les nœuds, en les faisant, soit dysfonctionner via des transactions malhonnêtes, soit en les faisant s'arrêter.

A titre d'exemple, le bug lié à la Blockchain Solana, détecté puis corrigé par la société Neodyme⁶⁶. Il s'avère que pour éviter la survenance de ce type d'incidents, il est recommandé d'avoir une diversité des versions de logiciels fonctionnant sur les différents nœuds.

▪ Risques liés au protocole de consensus

Les protocoles de consensus peuvent également être la proie d'une attaque, avec notamment l'attaque dite des « 51% ».



Source : Cryptodisrupt

Lorsqu'ils disposent d'une majorité de la puissance de calcul du réseau de 51%, les attaquants peuvent alors annuler les

transactions effectuées par les autres utilisateurs. La légitimité des transactions ne peut alors plus être assurée. Cette attaque n'a pas été concluante à ce jour pour les Blockchain Bitcoin et Ethereum au regard de leur puissance de calcul.

Toutefois des Blockchains de plus petite taille ont été prises pour cible, engendrant alors des pertes conséquentes. L'exemple de la Blockchain ZenCash en 06/2021 peut être cité. Les attaquants ont pu s'emparer d'un demi-million d'euros⁶⁷.

▪ Risques aux algorithmes de signature cryptographique

L'un des fondamentaux de la technologie Blockchain repose sur le transfert de crypto-actifs, via une clé privée. La clé privée doit être conservée précieusement et ne doit pas être partagée avec d'autres personnes car cette dernière permet de signer une transaction et donc d'envoyer des cryptomonnaies.

Toute personne qui a la clé privée d'un crypto-actif peut en effet en disposer et le transférer.

En cas de vol ou de perte, il n'existe aucun moyen de récupérer les crypto-actifs, entraînant ainsi leur perte définitive. Il existe de nombreux exemples qui visent à voler les clés privées et ce, via des plateformes d'échange insuffisamment sécurisées.

A titre d'exemple, BitMart aurait perdu entre 150 et 200 millions de dollars en 12/2021⁶⁸ en Ethereum et en Binance Smart Chain.

⁶⁶ Article de Cryptoast, « Un bug lié à la blockchain Solana (SOL) aurait pu causer la perte de centaines de millions de dollars » - 04/12/2021, disponible à l'adresse suivante : <https://cryptoast.fr/bug-solana-perde-centaines-millions-dollars/>

⁶⁷ Article de Cryptonaute - « ZenCash (ZEN) victime d'une attaque des 51% » - 08/06/2021, disponible à l'adresse suivante : <https://cryptonaute.fr/zencash-zen-attaque-des-51-hack/>

⁶⁸ Article de Numerama, « Les vols de plateformes de crypto continuent : BitMart a perdu 150 millions de dollars » - 06/12/2021, disponible à l'adresse suivante : <https://www.numerama.com/cyberguerre/761891-les-vols-de-plateformes-de-crypto-continuent-bitmart-a-perdu-150-millions-de-dollars.html>

▪ Risques liés aux contrats intelligents

Des bugs dans des Smart-Contracts ont pu être exploités pour voler les crypto actifs. La bonne pratique est d'assurer un suivi sur du codage et d'effectuer des audits spécifiques concernant les Smart-Contracts. En effet, l'audit de sécurité d'un Smart-Contract examine son code.

Le piratage d'un contrat de DAO, s'appelant « *The DAO* » a constitué un véritable coup de tonnerre en mettant en lumière la vulnérabilité des Smart-Contracts. « *The DAO* » était conçu comme un fonds d'investissement décentralisé, permettant à chaque membre de participer à la gouvernance de l'entreprise en fonction de son niveau d'investissement.

Les membres composant la minorité de ses membres, pouvaient retirer leur investissement, lorsqu'une décision était prise par la majorité des membres en leur défaveur. Or, il s'avère que le Smart-Contract ne prévoyait pas de vérifier, avant tout retrait, le solde de l'investissement. Il a été alors possible, pour le même utilisateur, de retirer plusieurs fois le montant investi. Compte tenu de cette vulnérabilité, 50 millions de dollars ont été alors dérobés en 06/2016⁶⁹.

Autre exemple, le 01/08/2022, Nomad a été la cible d'une attaque avec pour conséquence le vol de 200 millions de dollars. Pour transférer des actifs numériques entre différents réseaux, les ponts exploitent des Smart-Contracts. Il s'avère que c'est une faille dans ces Smart-Contracts qui a été relevée dans ce cas⁷⁰.

2.1.8- Risque lié à la gouvernance

Le fonctionnement décentralisé de la Blockchain pose la question des risques liés à la gouvernance. Cette technologie bouscule les modes de gouvernance classique. Une faille dans le modèle de gouvernance constitue une source de risque importante pour son fonctionnement effectif.

En effet, la Blockchain nécessite de définir au préalable des règles précises. Les sujets suivants nécessitent ainsi d'être clarifiés : validité des transactions, émission de nouveaux actifs, règlement des litiges, processus d'adoption des mises à jour du code, protection contre les cyber-risques ou encore adhésion au réseau et la gestion des autorisations, etc...

“

Par définition, cette technologie est décentralisée. Il s'agit d'un tournant majeur car il y a quand même une perte de pouvoir de certains acteurs. Tout le monde peut contrôler les informations avec la Blockchain. Cependant aujourd'hui, c'est la question de la gouvernance qui prend du temps dans les projets Blockchain. Concrètement, on peut passer un an à discuter de la gouvernance et ensuite mettre 3 mois pour la mise en place de la Blockchain.”

**Benjamin Faraggi - CEO fondateur de Spuro
et Président de la Blockchain : Kagesecur –
06/07/2022**

⁶⁹ Article de L'Usine Digitale - « *DAO perd 50 millions de dollars lors d'un piratage* » - 17/06/2016, disponible à l'adresse suivante : <https://www.usine-digitale.fr/article/dao-perd-50-millions-de-dollars-lors-d-un-piratage.N397787>

⁷⁰ Article de Coins - « *Le pont crypto "sécurisé" Nomad piraté : près de 200M\$ volés* » - 02/08/2022, disponible à l'adresse suivante : <https://coins.fr/pont-crypto-nomad-hack-200-millions-dollars-vol/>

Au regard de son caractère protéiforme, il existe des modes de gouvernance variés d'une Blockchain à une autre, qui repose notamment sur plusieurs types d'acteurs ou de processus décisionnels :

- **Gouvernance centralisée ou partiellement décentralisée**

La gouvernance centralisée ou partiellement décentralisée fait référence aux Blockchains privées et aux Blockchain à Consortium. Le nombre de nœuds du réseau y est souvent limité. Ce modèle de gouvernance centralisé sur une ou plusieurs entités juridiques ne présente pas de difficultés additionnels spécifiques en termes de supervision.

- **Gouvernance décentralisée**

La gouvernance décentralisée fait référence aux Blockchains publiques. Le nombre de nœuds du réseau est illimité.

La gouvernance de ce type de Blockchain repose essentiellement sur des acteurs, qui effectuent le travail de vérification-sécurisation-enregistrement des blocs. Ce modèle de gouvernance décentralisé présente des difficultés additionnelles en termes de supervision.

- **Gouvernance avec un processus décisionnel « on-chain »**

La gouvernance « *on-chain* » signifie que le processus décisionnel et sa mise en œuvre s'effectue directement dans la Blockchain par le code.

La gouvernance avec un processus décisionnel « *on-chain* » s'effectue par des mécanismes de vote.

Les utilisateurs manifestent leur adhésion aux propositions de modifications directement sur la Blockchain.

2.1.9- Risque lié à la protection des données

La réglementation en matière de protection des données à caractère personnel s'est renforcée au niveau mondial, et particulièrement au sein de l'Union Européenne avec l'adoption du règlement général sur la protection des données (RGPD⁷¹), qui est entré en vigueur en 2018.

La technologie Blockchain suscite des questions quant à sa compatibilité avec le règlement RGPD.

Tout d'abord, ce règlement prévoit un droit d'effacement ou droit à l'oubli. En effet, les utilisateurs peuvent, sous certaines conditions, demander que leurs données personnelles soient effacées. Or avec la technologie Blockchain, les données sont immuables, elles ne peuvent pas être effacées une fois consignées. Il existe une trace de toutes les transactions effectuées sur le réseau depuis sa création.

De plus, le rôle de « *Responsable de traitement des données* » trouve son sens dans un écosystème de type centralisé.

Dans le cas d'une Blockchain publique, son application pose question au regard du principe de désintermédiation.

De plus, la gouvernance mise en place (voir ci-dessus) doit également être prise en compte.

⁷¹ Cette réglementation renforce les obligations faites aux entités réalisant la collecte et le traitement de données à caractère personnel : recueillement du consentement éclairé

des personnes concernées, mise en place de dispositifs techniques et organisationnels pour en assurer la conformité, mise en place de sanctions dissuasives, etc.

“

Une des caractéristiques de la Blockchain est l'impossibilité d'effacer les données. Toutes les informations que l'on intègre dans le registre sont premièrement en format « hash ». On ne peut donc pas revenir en arrière, et ces informations sont toutes chiffrées.

En outre, il existe une solution avec la Blockchain privée pour respecter le règlement général sur la protection des données (RGPD), en cas de demande de l'utilisateur pour que ces informations ne soient plus visibles. Il s'agit de « l'invalidation » des informations. On ne peut pas les effacer, mais on peut en quelque sorte les rayer pour que plus personne ne puisse pas les lire. Cela dépend des rôles attribués au sein de la Blockchain pour effectuer cette « invalidation ». D'ailleurs, pour les Blockchains, la CNIL recommande de trouver des moyens techniques afin de respecter le règlement. ”

**Benjamin Faraggi - CEO fondateur de Spuro
et Président de la Blockchain : Kagesecur –
06/07/2022**

Or, la Blockchain de par nature n'a pas de frontière.

En tout état de cause, une analyse d'impact sur la protection des données est incontournable pour analyser les risques en termes de protection des données.

Le rôle de « *Responsable de traitement des données* » revient-il naturellement au développeur à l'origine de la Blockchain ou davantage aux nœuds participants ?

Il est nécessaire de bien comprendre le rôle de ces derniers dans le traitement de la donnée afin de pouvoir répondre à cette question.

Autre problématique, le règlement autorise uniquement le transfert de données à caractère personnel vers des pays offrant un niveau de protection similaire à celui de l'Union Européenne.

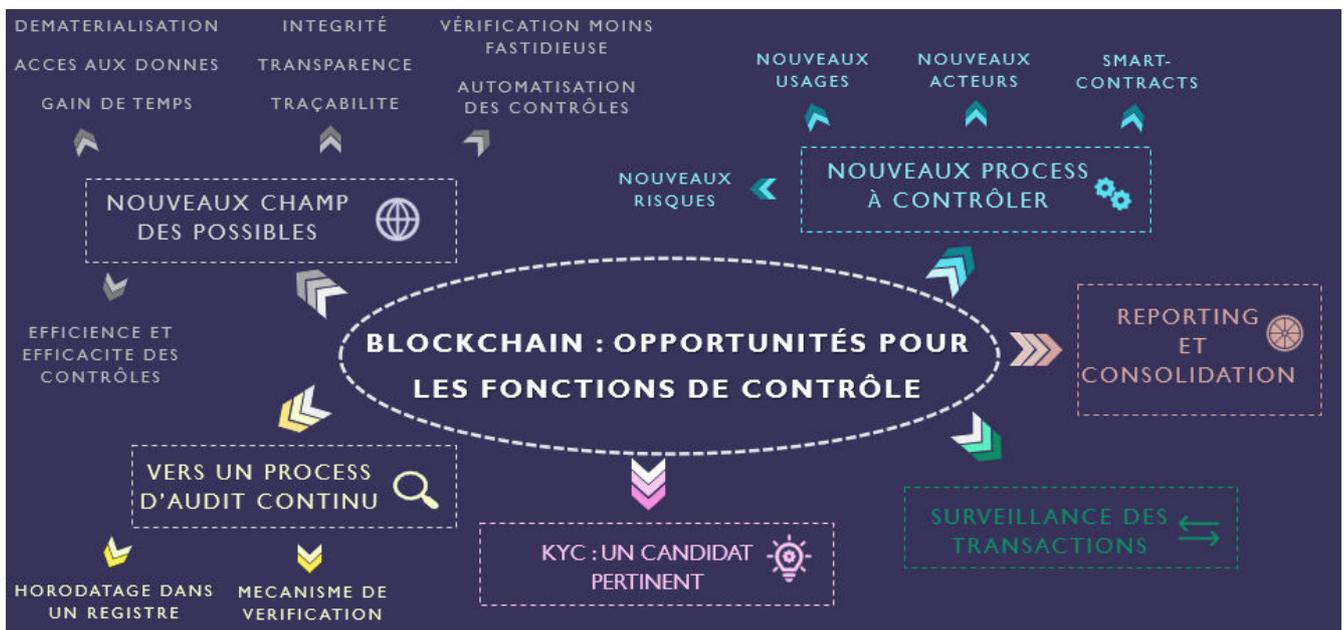
2.2- Opportunités

“ Chaque difficulté porte en elle le germe d'un avantage équivalent ou supérieur ”

Napoléon HILL

Cette technologie laisse entrevoir de nombreuses opportunités par ses possibles applications à des domaines où la confiance joue un rôle essentiel. Que ce soit les Blockchains publiques dont le code est disponible, accessibles à tous et décentralisées, ou que ce soit les Blockchains privées ouvertes à un nombre restreint de membres, elles ont un point commun, celui de permettre la désintermédiation et la certification.

Le déploiement de la Blockchain va impacter les organisations. A première vue, les fonctions de contrôle pourraient redouter l'essor de cette technologie. Cependant, cette dernière leur offre aussi plusieurs opportunités et constitue un virage à ne pas rater.



2.2.1- Nouveaux process à contrôler

La technologie Blockchain apporte une nouvelle génération de processus métiers compte tenu de ses impacts matériels sur les business model des entreprises. Ces processus devront être revus à la lumière des perspectives de transparence et de créativité qu'offre cette technologie et ce, sur

l'ensemble des chaînes de valeurs, tels que :

- ✓ Processus liés à de **nouveaux usages, couplés parfois avec de nouveaux acteurs** ;
- ✓ Process liés aux **Smart Contracts** ;
- ✓ Processus de **vérification des codes et patches potentiellement ajoutés** ;

- ✓ Processus liés **aux données** ;
- ✓ Processus liés **aux infrastructures de protection** ;
- ✓ Processus liés **à la continuité des activités et plans de rétablissements**, etc.

Ainsi, de nouveaux risques vont apparaître et devront être intégrés à la cartographie des risques.

Les fonctions de contrôle vont devoir s'assurer que ces derniers sont bien couverts par le dispositif de maîtrise des risques mis en place.

“

Mon point de vue personnel est que l'on ne va pas vers moins de contrôle. En effet, je ne suis pas certain qu'il y aura une disparition des tiers de confiance. Je ne suis pas sûr que beaucoup de gens croient encore au modèle tel qu'il était défini pour les crypto-actifs, avec un Bitcoin sans intermédiaire et de pair à pair. En effet, aujourd'hui, on part sur une réglementation plus forte avec des règlements Européens, le régime pilote, MICA. Je ne suis pas certain que les rôles de dépositaires centraux et d'agents disparaissent à l'avenir.

Au contraire, compte tenu de la complexité et des nouveaux modèles qui vont être mis en place, il y a des fonctions qui vont se renforcer.

Cela a pour conséquence l'arrivée de nouveaux acteurs, qui travaillent sur le KYC et qui montrent que les contrôles et les tiers de confiance vont être toujours présents. L'information est accessible, cependant un des points d'attention est qu'il est nécessaire d'avoir recours à des spécialistes afin de pouvoir exploiter les données.”

Frederick Beck – Head of Digital Process Enhancement - BNP Paribas Securities Services et Animateur du groupe AFTI Innovation – 27/07/2022

A titre d'exemple, les Smart-Contracts constituent un nouveau périmètre de contrôle pour les fonctions de contrôle.

« Dans les faits, seule une entreprise sur cinq réalise des audits et des revues de ces programmes par des experts ».

Propos de Pauline Adam-Kalfon, associée en charge de l'activité Blockchain et Crypto, PwC Franc et Magrehb, extrait de Option Finance - 16/07/2021

“

L'audit interne va être fortement impacté car toutes les transactions via des DEX doivent être auditées dans le cadre de leurs contrôles. Également, les Smart Contracts des DEX doivent être particulièrement revus.”

Pierre-Louis Missler - Data Analyst - Forensic & Integrity Services – Ernst&Young – 28/07/2022

2.2.2- Nouveau champ des possibles pour les fonctions de contrôle

Le fait que les données soient disponibles en temps réel, fiables et sécurisées, constitue un nouveau champ des possibles pour les fonctions de contrôle.

- **Dématérialisation, facilitation des accès aux données et gain de temps**

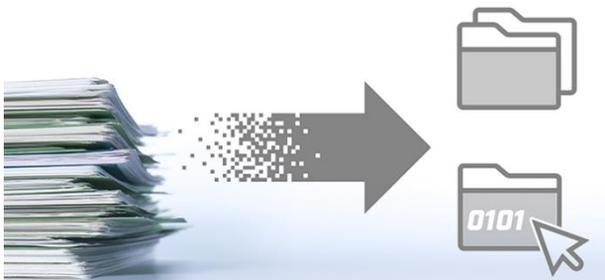
Tout d'abord, l'accès aux données va être simplifié, ce qui va avoir pour conséquence de faire gagner du temps aux fonctions de contrôle.



La technologie Blockchain utilisant un grand livre distribué, les transactions et les données sont enregistrées à l'identique à plusieurs endroits.

Les membres du réseau disposant d'une autorisation d'accès voient les mêmes informations en même temps (transparence).

Cette technologie se prête donc au partage des données dématérialisées entre plusieurs parties prenantes, dont les fonctions de contrôle.



Source : DafMAG.fr

“

Les fonctions de contrôle vont avoir accès dans une grande base de données, infalsifiable et sécurisée, à des informations leur permettant d'effectuer leurs revues de contrôle.

Un des impacts constituant une opportunité est donc le process de mises à disposition de documentations, de manière exhaustive et autonome. »

Rémi Rouet – Group Chief Data Officer – Les Mousquetaires – 11/07/2022

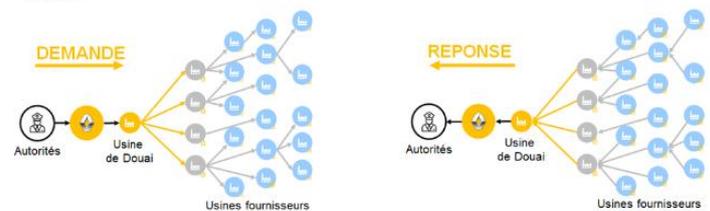
Également, la Blockchain permet d'avoir des échanges plus directs et de passer au temps réel ou au quasi temps réel. Les contrôles peuvent être effectués à distance, sans avoir la nécessité de consulter des documents sous format papier.

Si on prend le cas du secteur automobile, les véhicules sont composés de plusieurs milliers de pièces détachées sur toute la chaîne d'approvisionnement, devant répondre chacune à des certifications et des normes de sécurité différentes (caractéristiques de sécurité, réglementaires, géométriques, matériaux...).

Ainsi, lorsqu'un constructeur analyse l'état de conformité d'un véhicule à un instant donné, cela peut lui prendre un temps certain pour contacter directement toutes les parties impliquées.

A titre d'exemple, le projet ci-dessous de RENAULT baptisé « XCEED », lancé en 2019, peut être cité.

DEPUIS



VERS

INFORMATION DISPONIBLE EN TEMPS REEL



Source : Extrait de l'article de l'Usine digitale - « Renault déploie une blockchain pour tracer et certifier la conformité des pièces de ses voitures » - 10/09/2020, disponible à l'adresse suivante : <https://www.usine-digitale.fr/editorial/renault-deploie-une-blockchain-pour-tracer-et-certifier-la-conformite-des-pieces-de-ses-voitures.N1002224>

Ce projet concerne la traçabilité réglementaire des pièces détachées afin d'accéder rapidement aux informations relatives à l'état de conformité d'un véhicule.

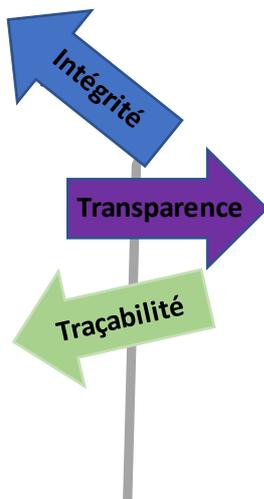
Auparavant, cela pouvait prendre plusieurs heures pour interroger directement les parties impliquées (usines fournisseurs) et de consolider leurs réponses.

Avec la technologie Blockchain, l'objectif est de faciliter l'accès aux données et le partage en temps réel.

« La blockchain permet d'avoir des échanges plus directs et de passer au temps réel ou au quasi *temps réel* ».

Propos d'Odile Panciatici, Vice-présidente Blockchain chez Renault, extrait de L'Usine Digitale - 10/09/2021

■ Intégrité, transparence et traçabilité



La technologie Blockchain permet de limiter le risque que les données et documents nécessaires à la réalisation des contrôles soient copiés ou altérés. En assurant leur intégrité de part leur caractère digitalement unique, la Blockchain offre ainsi une nouvelle garantie pour les fonctions de contrôle.

Les vérifications des fonctions de contrôle s'en voient alors positivement affectées.

“

La Blockchain constitue une opportunité pour les fonctions de contrôle puisque l'empreinte, la signature et l'horodatage, donc l'intégrité d'un document, est enregistrée dans le registre de la Blockchain.

La Blockchain permet par ailleurs la transparence et la collaboration entre les différentes parties prenantes, afin qu'elles aient toutes la même information et qu'il n'y ait pas moyen de la modifier.

Pour le contrôle, la traçabilité constitue une caractéristique très intéressante. Grâce à la Blockchain, il est possible de savoir qui a vu un document, qui l'a signé, qui l'a envoyé. Cette traçabilité est visible par tous les acteurs qui sont membres de la Blockchain.

En cas de litige, la simplification est l'un des avantages essentiels que permet la Blockchain. Par exemple, aujourd'hui, certains emails peuvent être contestés. Dans la Blockchain Kagesecur par exemple, ces emails sont intégrés et apportent ainsi une valeur probatoire. Ces nouvelles fonctionnalités sont intéressantes pour les fonctions de contrôle.”

Benjamin Faraggi - CEO fondateur de Spuro et Président de la Blockchain : Kagesecur – 06/07/2022

■ Vérifications moins fastidieuses et automatisation des contrôles

En les allégeant de certaines vérifications fastidieuses et répétitives, les fonctions de contrôle pourraient, grâce à la technologie Blockchain, voir leur rôle évolué.

A titre d'exemple, la mise en place de Smart-Contracts permettrait d'automatiser certaines revues pour vérifier que les données sont identiques (rapprochements).

Il est envisageable également que ces contrôles eux-mêmes puissent être tracés/inscrits dans la Blockchain, permettant ainsi une transparence pour tous les membres du réseau.

Dans le secteur de l'audit, on peut s'attendre à des changements de pratiques en cas de recours à cette technologie pour remplacer les procédures de circularisation ou de demande de confirmation en provenance des tiers.

En outre, les caractéristiques de transparence et traçabilité de cette technologie peut donner lieu à des projets communs entre fournisseurs, clients, partenaires, voire entre certains concurrents pour mettre en place des vérifications moins fastidieuses, chronophages et optimiser les vérifications via une automatisation des contrôles.

▪ **Effizienz et efficacité des contrôles**

Le gain de temps engendré va permettre aux fonctions de contrôle de concentrer leurs efforts sur les points les plus à risques, permettant ainsi d'améliorer l'efficacité des contrôles et d'accroître l'efficacité de leurs missions.



Par ailleurs, cela va engendrer des économies de coûts dans l'environnement de l'audit et du contrôle. Les revues peuvent être exhaustives, planifiées avec plus de souplesse et donner lieu à des conclusions offrant un niveau d'assurance plus élevé.

Cette couverture étendue améliorera donc considérablement le niveau d'assurance obtenu dans les missions d'audit concernées.

Il convient de noter que le recours à d'autres technologies comme le Big Data, la Robotics ou encore l'Intelligence Artificielle peuvent également venir s'ajouter à la Blockchain afin d'améliorer la pertinence des contrôles.

“

Le recours à la Blockchain est intéressant pour les fonctions de contrôle, s'il est couplé avec de l'intelligence artificielle.

En mettant en place un certain nombre d'indicateurs de type paramétrique, ces derniers pourront déclencher, soit un contrôle manuel, soit un contrôle automatique. En industrialisant et en couplant ce processus avec de l'intelligence artificielle, on va ainsi pouvoir réussir in fine à mieux identifier les zones prioritaires.

Par exemple, une entreprise qui est en charge de réaliser des visites de sites industriels utilise une application pour évaluer si les dispositifs de maîtrise des risques sont bien en place (extincteurs...). Le fait d'utiliser la Blockchain permet pour le management d'avoir un certain niveau de garantie concernant la pertinence des informations qui peuvent être collectées.”

Benjamin Bouffard – Directeur de l'activité Strategic Risk Consulting pour l'Europe de l'Ouest chez WTW – 17/06/2022

▪ **Vers un processus d'audit continu**

Les caractéristiques de la technologie Blockchain, de part son infrastructure, sont de garantir la transparence des données inscrites, l'existence d'une trace d'audit à chaque étape, l'horodatage des opérations sur un registre et la sécurité via des mécanismes de vérification.

A ce jour, certaines revues d'audit et de contrôles sont basées sur des données historiques, parfois arrêtées à une date précise.

Au lieu d'évaluations effectuées à une date arrêtée, l'un des avantages de la technologie Blockchain est de permettre d'avoir accès aux informations en temps réel ou quasi réel et d'être alors en mesure d'effectuer des évaluations continues tout au long de la période auditée, c'est-à-dire dès que les informations sont disponibles et vérifiées par les mécanismes de vérification mis en place.



Evaluation continue



Temps réel – quasi réel

La technologie Blockchain peut également être utilisée à des fins de certification des contrôles effectués.

Une fois ces derniers réalisés et sous réserve du respect de certaines conditions, les contrôles pourraient être encodés dans une identité numérique autonome pour être consultés par les autres membres de la Blockchain et ce, via des accès sélectifs.

Ainsi, ces derniers pourraient avoir accès aux éléments de contrôle et de conformité avec beaucoup plus de facilité qu'aujourd'hui.

2.2.3- KYC, un candidat pertinent

Les processus KYC (Know Your Customer) constituent une des pierres angulaires dans la lutte contre le blanchiment d'argent et le financement du terrorisme (LCB-FT).

Thomson Reuters a publié, en 2016, un rapport⁷² selon lequel il était estimé que les institutions financières dépensaient entre 60 et 500 millions dollars par an pour se conformer aux normes en KYC et « AML » - Anti-Money Laundering.

Or, malgré le déploiement de moyens conséquents (humains, systèmes...), le KYC demeure une source de risques dans de nombreuses institutions financières (processus fastidieux, duplication d'efforts, risque d'erreur, etc.).

Les institutions financières doivent constamment mettre à jour les informations sur leurs clients. Les clients multi-bancarisés, en contact avec plusieurs institutions, peuvent ainsi être devoir répondre à des questions identiques à plusieurs reprises.

Il s'avère qu'aujourd'hui les acteurs traditionnels sont fortement bousculés par des acteurs digitaux. Ces derniers proposent des entrées en relation plus rapides, au regard de leur capacité à agréger rapidement des briques technologiques innovantes, utilisées notamment pour l'établissement du KYC.

Le caractère sécuritaire de la Blockchain offre de nouvelles perspectives en termes d'échanges de données et ce, avec un niveau

⁷² Rapport de Thomson Reuters - « Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity » - 06/2016, disponible à l'adresse suivante :

<https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html>

de sécurité supérieur. Le processus KYC est un candidat pertinent de la technologie Blockchain compte tenu du caractère intrinsèque des données devant être partagées.

Cette dernière offre également des possibilités en termes de normalisation du stockage, de traçabilité et de partage de données fiables et certifiées, à destination d'acteurs concernés par le processus KYC.

“

Concernant les transactions financières, une des opportunités est le partage du KYC. Chaque établissement aujourd'hui établit son dossier KYC, un des usages intéressants est de capitaliser sur le partage du KYC entre plusieurs membres.”

Rémi Rouet – Group Chief Data Officer – Les Mousquetaires – 11/07/2022

A noter cependant que la diversité des exigences internes, des obligations réglementaires et de la spécificité de certaines activités, complexifient l'essor de ce nouvel usage.

A titre d'exemple, parmi les initiatives qui ont été lancées, on peut noter le projet KYC dénommé « *Synechron* » lancé à Dubai⁷³.

2.2.4- Surveillance des transactions

Le caractère sécuritaire de la Blockchain offre également des perspectives intéressantes de contrôle pour la surveillance des transactions.

Aujourd'hui les institutions financières automatisent en interne les contrôles et la surveillance dans les domaines de la lutte contre le blanchiment et le financement du terrorisme.

Intégrer la technologie Blockchain pour surveiller les transactions constitue ainsi une nouvelle opportunité pour les fonctions de contrôle.



Source : beincrypto.com

Précisons que selon le rapport « *PwC - Financial Services Technology 2020 and Beyond: Embracing disruption* »⁷⁴, les régulateurs pourraient aussi avoir la possibilité d'avoir un accès direct à ces outils.

Financial institutions can do their part

This is only the beginning. As financial institutions themselves continue to automate controls and monitoring in KYC/AML, trade surveillance, reconciliations and other areas, regulators will seek direct access to these tools – either on an ongoing basis or during supervisory reviews. As a result, firms will need to make data and control transparency priorities as they implement these tools and comply with data requests. It is shortsighted to focus solely on compliance with current regulations. Rather, firms should develop a better understanding of where their data and associated controls live. This will let them work with a growing range of interested regulatory bodies more quickly, easily and accurately, on everything from stress tests and periodic exams to individual requests. By doing so, they will improve their credibility with regulators today and be ready for the future.

Source : Extrait du rapport PwC "Financial Services Technology 2020 and Beyond: Embracing disruption

⁷³ Article de Ledger Insights - « *Know Your Customer blockchain consortium planned in Dubai* » - 01/08/2019, disponible à l'adresse suivante : <https://www.ledgerinsights.com/blockchain-know-your-customer-kyc-consortium-dubai/>

⁷⁴ Rapport PwC - « *Financial Services Technology 2020 and Beyond: Embracing disruption* » - 2020, disponible à l'adresse suivante : <https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf>

“

Les avantages de la Blockchain sont conséquents pour les fonctions de contrôle car tout est traçable. Il existe des cas où les clients font sortir leurs fonds des cryptomonnaies vers une adresse X, qui s'avère être in fine à destination du Dark Net et ce, via plusieurs rebonds.

Il est possible pour la plateforme d'identifier ce type de transfert grâce à la technologie Blockchain. D'un point de vue de gestion du risque, c'est assez puissant.

Avec des outils d'analyse de transactions qui permettent de filtrer toute la Blockchain (par exemple Scorechain), il est possible d'identifier les adresses de cryptomonnaies suspectes (escroquerie/Dark Web) et déclencher en conséquence des investigations. Des scénarios pourront alors être mis en place pour escalader ces alertes, de type : adresse ayant un lien avec le Dark web ou présence de multiples rebonds...”

Dorian Olivier – Compliance / Advisory à Coinhouse – 21/06/2022



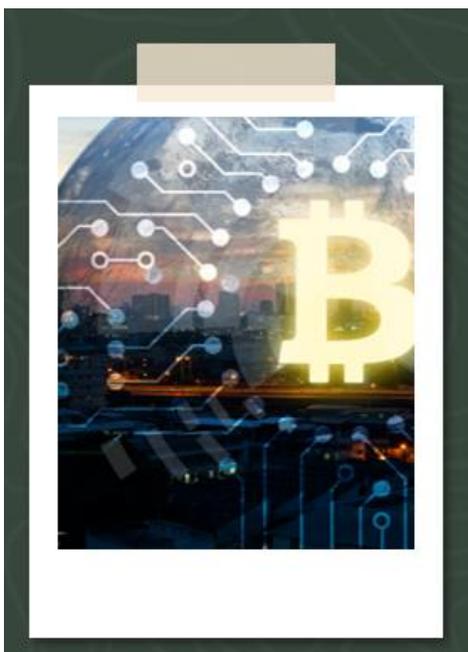
“

Si les banques repensent leur dispositif en modifiant certaines règles sous-jacentes, elles vont pouvoir intégrer beaucoup plus de choses, compte tenu de la technologie de la Blockchain (transparence accrue par essence par rapport au système financier classique) et en faire un vrai outil de contrôle. Avec la Blockchain, le déclaratif peut être vérifié et être prouvé avec le registre.

Concernant la surveillance des opérations, les entreprises et les agences américaines ont commencé en avance par rapport à l'Europe. Elles ont une vraie maîtrise de la technologie sous-jacente.

A titre d'exemple, elles utilisent « Chainalysis », qui a pu acquérir au fil des années, une sorte de bible/base de données assez unique des transactions, couplée à une « forme » d'intelligence. En Europe, on peut nommer la société luxembourgeoise « Scorechain », qui s'apparente davantage à un moteur de risque à paramétrer par rapport à « Chainalysis ». A noter qu'il existe aussi d'autres outils comme Elliptic, etc. ”

Ivan De Lastours - Blockchain lead chez Bpifrance - 25/07/2022



2.2.5- Reporting et consolidation

La technologie Blockchain peut être bénéfique pour la mise en œuvre des reportings, soumis parfois à des procédures multiples et contraignantes de consolidation.



Source : The Cryptonomist

Tel qu'il a été exposé par Olivier Desplebin, Gulliver Lux et Nicolas Petit⁷⁵, la Blockchain requiert :

- ✓ d'une part, que l'information soit validée par des entités différentes de l'émetteur pour qu'elle soit définitivement enregistrée dans le système ;
- ✓ d'autre part, que l'information soit enregistrée de façon collective et certifiée par l'ensemble des utilisateurs du système.

Ainsi, à travers les avantages offerts par le Smart-Contract, la Blockchain peut être utilisée pour alléger les processus consolidation de données et de reporting, en se basant sur une source unique et commune reconnue pour la véracité de chaque élément.

A titre d'exemple, les exigences réglementaires en termes de reportings

⁷⁵ « L'évolution de la comptabilité, du contrôle, de l'audit et de leurs métiers au prisme de la Blockchain : une réflexion prospective » de Olivier Desplebin, Gulliver Lux, Nicolas Petit, dans « Management & Avenir 2018/5 », pages 137 à 157, disponible à l'adresse suivante : <https://www.cairn.info/revue-management-et-avenir-2018-5-page-137.htm>

⁷⁶ La « DAC 6 » désigne la directive européenne (UE) 2018/822 du Conseil du 25/05/2018 relative à l'échange automatique et obligatoire d'informations sur les dispositifs transfrontières devant faire l'objet d'une déclaration. Elle vise à renforcer la coopération entre les

représentent aujourd'hui une charge de travail conséquente pour certains acteurs, tels que les établissements du secteur bancaire, les organismes du secteur de l'assurance, les sociétés de financement, les établissements de paiement, les sociétés cotées, etc...

Ces reportings pourraient être alimentés à partir de données enregistrées dans la Blockchain, permettant ainsi la simplification des processus pour fluidifier les interactions entre assujettis et régulateurs.

Autre exemple, celui à des fins de Conformité fiscale, à travers l'échange de données entre les contribuables et les Etats ou entre Etats. La Directive DAC⁷⁶ requiert des intermédiaires ou/et des contribuables de déclarer dans un délai de 30 jours, sous peine de s'exposer à une amende, les « dispositifs transfrontières de planification fiscale à caractère potentiellement agressif » visés par des « marqueurs ».

On peut donc considérer, comme Dorian Ravaute, que « Cette déclaration automatique d'informations pourrait être réalisée à travers un Smart-Contract, dès lors que le protocole permet l'identification des « marqueurs »⁷⁷.

La mise en place d'un Smart-Contract permettrait de combiner à la fois les intérêts :

- ✓ des entreprises, via un processus déclaratif automatisé, horodaté et enregistré ;
- ✓ des États visés par les dispositifs, qui pourraient alors accéder aux informations via la technologie Blockchain.

administrations fiscales des pays de l'UE en matière des montages potentiellement agressifs de planification fiscale. La déclaration DAC6 vise à déclarer des dispositifs transfrontières potentiellement agressifs au plan fiscal contenant certaines caractéristiques.

⁷⁷ Propos de Dorian Ravaute, extrait de l'article du Monde - « Blockchain : un outil pour la conformité fiscale » - 03/11/2020, disponible à l'adresse suivante : <https://www.lemonde.fr/blog/binaire/2020/11/03/blockchain-un-outil-pour-la-conformite-fiscale/>

2.3- Défis

" It's not the strongest of the species that survives nor the more intelligent, but the one most responsive to change "

Charles DARWIN

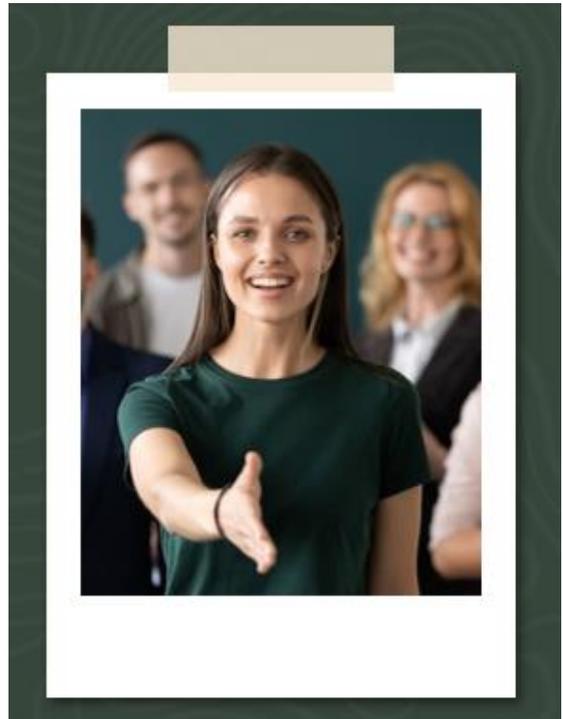
Les fonctions de contrôle font face à plusieurs défis pour lesquelles elles doivent dès à présent se mobiliser.

2.3.1- Attirer les profils qualifiés, acquérir de nouveaux savoirs et maîtriser les outils

Selon l'étude réalisée en 2017⁷⁸ par Dell et « l'Institut pour le Futur », un think tank américain, 85 % des emplois en 2030 n'existent pas aujourd'hui. Pour le travailleur du futur, le seul moyen de s'adapter sera notamment d'avoir la capacité d'acquérir de nouveaux savoirs rapidement. Ce pourcentage de 85% refléterait les grandes évolutions auxquelles le marché du travail doit faire face : développement de l'Intelligence artificielle, de la robotisation, de la numérisation, etc.

Ainsi, les auteurs de l'étude mentionnent que la capacité à acquérir un nouveau savoir vaudra plus que le savoir déjà appris : « *The ability to gain new knowledge will be more valuable than the knowledge itself* ».

Au regard de cette étude et de l'essor de la technologie Blockchain ces dernières années, les profils qualifiés capables de comprendre les sous-jacents de cette technologie et son potentiel constituent un défi pour les fonctions de contrôle.



“

L'avantage de la Blockchain, c'est qu'il y a une capacité d'audit très importante. En revanche, la technicité requise et les compétences nécessaires pour le faire constituent des limites dans la mise en œuvre des audits et contrôles.

Personnellement, je suis d'avis que les fonctions de contrôle doivent voir la Blockchain comme une opportunité de bien contrôler ce secteur, mais pour cela, elles doivent se former.”

Ivan De Lastours - Blockchain lead chez Bpifrance - 25/07/2022

⁷⁸ Etude « *Realizing 2030: Dell Technologies Research Explores the Next Era of Human-Machine Partnerships* » - disponible à l'adresse suivante :

<https://www.dell.com/fr-fr/dt/corporate/newsroom/realizing-2030-dell-technologies-research-explores-the-next-era-of-human-machine-partnerships.htm>

A titre d'exemple, la revue des Smart Contracts constitue un point majeur d'attention afin de s'assurer que leurs programmations sont bien conformes au cahier des charges. Il est nécessaire de vérifier que chaque ligne de code respecte les promesses contractuelles.

Ainsi, en sus des Data Scientists et Data Analysts, la revue des Smart Contracts nécessite de faire appel à des experts en cryptographie et en codage de langages informatiques.



“

Il y a une méthodologie à adapter car chaque Blockchain est spécifique et pour pouvoir avoir accès aux transactions, il est nécessaire d'avoir certaines compétences informatiques pour pouvoir le faire.

Ainsi, les méthodologies existantes de contrôle doivent être adaptées en prenant en compte la technologie sous-jacente. Cela a pour conséquence de revoir la composition des équipes de contrôles : up-skilling des équipes existantes ou des équipes hybrides.

Un des points d'attention est d'attirer dans les fonctions de contrôle des experts, or ces derniers ont des profils qui peuvent davantage être attirés par d'autres métiers liés à la Blockchain ;”

Rémi Rouet – Group Chief Data Officer – Les Mousquetaires – 11/07/2022

Le défi pour les fonctions de contrôle est de capter ces talents, tout en veillant à ce que ces derniers puissent maîtriser les outils pour faciliter leurs revues et être à jour des potentialités techniques qu'offre la technologie Blockchain.

“

En termes de connaissance, il est nécessaire que les fonctions de contrôle puissent être informées de ce nouveau monde et de la façon de fonctionner de tout ce système.

En termes de compétences, l'enjeu est de pouvoir utiliser les différents outils qui existent sur Internet, du type Etherscan pour la Blockchain Ethereum et Bitcoin Explorer pour la Blockchain Bitcoin. Ces outils sont des explorateurs de Blockchains qui fournissent des informations de type : adresses de portefeuille, montants des transactions, sources, etc.”

Pierre-Louis Missler - Data Analyst - Forensic & Integrity Services – Ernst & Young – 28/07/2022



Acquérir de nouvelles connaissances



Maîtriser les outils



Se former

“

Un des challenges pour les fonctions de contrôle est la prise en main et le paramétrage des outils d'analyse des données. Il y a une phase cruciale de prise en main et de compréhension de ce type d'outils. On peut avoir initialement l'impression qu'une transaction est risquée, alors qu'après investigation, il s'avère qu'elle ne l'est pas forcément.

Également, il y a cet aspect de rebonds à bien maîtriser. Une transaction peut faire jusqu'à 30,40, 50 rebonds (transfert d'une adresse, à destination d'une autre adresse... pour in fine une sortie des fonds via une adresse finale...) et ce, en divisant à chaque fois les fonds.

Un autre challenge est celui des « mixers » : un client brouille les pistes sur ses fonds en les mettant dans un pool, qui va alors mélanger les fonds. La lisibilité de ce type de transactions dans les outils n'est pas simple (traitement des cas de mixage de cryptomonnaie).

Enfin, il faut appréhender l'existence des Whitelists sur la Blockchain, c'est-à-dire des adresses qui vont être « whitelistées ». Cela va être utilisé par des protocoles décentralisés pour faire « une sorte » de KYC. C'est-à-dire, seules certaines adresses pourront accéder au protocole (Aave Arc par exemple).”

Dorian Olivier – Compliance / Advisory à Coinhouse – 21/06/2022

2.3.2- Se positionner en amont du changement



Face à l'adaptation croissante de la technologie Blockchain dans des domaines d'activité de plus en plus divers, la multiplication de ses usages et l'apparition de nouvelles déclinaisons, il est nécessaire que les fonctions de contrôle se positionnent en amont du changement.

Se pose alors la question de leur rôle dans ce contexte :

- ✓ **Comment adapter ma fonction de contrôle avant que d'autres ne le fassent pour moi ?**
- ✓ **Comment tirer avantage des propriétés de la technologie Blockchain pour améliorer le dispositif de contrôle de mon organisation ?**
- ✓ **Quelles sont les solutions, fondées sur la Blockchain, qui sont à ma disposition pour effectuer mes tâches ?**

Ce sont quelques-unes des pistes de réflexion qui peuvent être investiguées afin d'être proactif sur ce sujet. La réponse à ces questions peut aboutir à la réorganisation des équipes pour être en phase avec les nouveaux besoins d'expertise.

“

Dans le monde de l'Audit Interne, la traçabilité, la transparence, mais aussi l'autonomie constituent des points essentiels.

Ainsi, on peut être amené à se poser les 2 questions suivantes : comment la Blockchain peut être utile pour l'audit interne, mais aussi comment l'audit interne pourrait être utile pour la Blockchain ?”

Benjamin Bouffard – Directeur de l'activité Strategic Risk Consulting pour l'Europe de l'Ouest chez WTW – 17/06/2022

“

Sur les enjeux de traçabilité alimentaire, la technologie Blockchain est intéressante, mais il n'y a pas à ce jour de réglementation sur cette problématique dans le retail, notamment dans le secteur alimentaire.

Demain, je pense que cela va arriver. Dans le domaine, du retail, c'est donc le moment d'anticiper et être en amont de la réglementation.”

Rémi Rouet – Group Chief Data Officer – Les Mousquetaires – 11/07/2022

2.3.3- Faire le lien entre le monde physique et le monde numérique

Les fonctions de contrôles ont un rôle central, celui d'accompagner l'innovation et le développement de la Blockchain, tout en préservant la stabilité et les règles. Les attentes sont fortes en la matière. Elles seront également les garantes de l'adéquation entre systèmes numériques et évolutions réglementaires.

Comme mentionné dans l'article de Pascal De Lima publié dans Forbes en 2019⁷⁹ : « les possibilités offertes par la "conformité 3.0" pourraient tout aussi bien inciter les régulateurs à renforcer, en parallèle, leur niveau d'exigence, sans compter que certaines nouvelles technologies créent des vides juridiques qui vont devoir être comblés par des évolutions réglementaires dont la mise en œuvre sera elle-même porteuse de coûts... ».

Par ailleurs, les impacts de la technologie Blockchain sur le Business Model des

entreprises ne sont pas définis et/ou sont en constante évolution.

De nouveaux risques peuvent apparaître et/ou des risques existants peuvent être modifiés. Il convient de bien les évaluer en amont des projets pour sécuriser les dispositifs de contrôle interne et de conformité : cartographie des risques, adaptation des procédures de contrôle aux nouvelles infrastructures technologiques et processus opérationnels, demandes d'agrément, révision des risques informatiques et cyber, etc.

Ainsi, au sein des organisations exposées à la technologie Blockchain, les fonctions de contrôles sont d'ores et déjà appelées à revoir leurs procédures de contrôle, en créer de nouvelles, pour faire le lien entre le monde physique et le monde numérique.



“

Le modèle cible n'est pas défini aujourd'hui et le modèle opérationnel n'est pas clair. Ce qui change par rapport à ces dernières années, c'est qu'il existe dorénavant un consensus sur le fait que la Blockchain et les digital assets vont apporter une valeur.”

Frederick Beck – Head of Digital Process Enhancement - BNP Paribas Securities Services et Animateur du groupe AFTI Innovation – 27/07/2022

⁷⁹ Article publié dans Forbes - « La Conformité Bancaire A L'Heure De La Blockchain » - Pascal De Lima - du 11/09/2019, disponible à

l'adresse suivante : <https://www.forbes.fr/finance/la-conformite-bancaire-a-lheure-de-la-blockchain/>

“

Ce qui est compliqué c'est que l'on ne peut pas arriver avec une réponse holistique pour toute la chaîne, puisque les contrôles sont humains et potentiellement technologiques.

Le point d'attention est le suivant : arriver à faire le lien entre un milieu très « Tech » et un milieu très réglementé comme pour le secteur de la Banque/Assurance.”

Rémi Rouet – Group Chief Data Officer – Les Mousquetaires – 11/07/2022

“

Un des enjeux pour les fonctions de contrôle est d'avoir la capacité d'accompagner les métiers dans la définition des processus afin de s'assurer de la couverture des risques pour l'entité.

Par exemple, ils devront se poser la question suivante : quel est le bon processus de contrôle aujourd'hui ?

Il s'agit en effet d'aller au-delà de la simple transcription du dispositif de maîtrise des risques. Il est donc nécessaire d'être créatif et force de proposition, tout en restant très rigoureux.

Ces nouveaux actifs requièrent par exemple pour les Banques, de repenser leur dispositif de gestion des risques, ce qui les met dans une position inconfortable, entre leur volonté de contrôler ces nouveaux actifs, leurs obligations réglementaires en la matière et leur capacité de faire aujourd'hui dans les faits.”

Ivan De Lastours - Blockchain lead chez Bpifrance - 25/07/2022

2.3.4- Appréhender les nouvelles unités collaboratives

Comme mentionné dans l'étude de Deloitte « *Blockchain and Internal Control : the COSO perspective* »⁸⁰, l'un des changements les plus significatifs résultant de l'utilisation de la Blockchain est sa capacité de créer de nouvelles unités collaboratives, couvrant différentes entités, fonctionnant sur une base décentralisée mais qui restent liées (données partagées dans une base de données décentralisée).



Les trois objectifs du COSO, i.e. « opérations, rapports et conformité » peuvent alors être fortement affectés par le recours à cette technologie.

Observations and Implications

One of the more significant changes resulting from the use of blockchain relates to the hierarchy of the entity. Although the highest level of the hierarchy expressed in the *2013 Framework* as shown in Figure 1 is the Entity Level, drilling down to Division, Operating Unit, and Function, blockchain has the ability to create new collaborative units, spanning different entities, operating on a decentralized basis but bound together with shared data (i.e., a **decentralized database**). From shared ledgers and record-keeping to overarching governance (perhaps leveraging **smart contracts** for oversight and cross-organization internal controls), blockchain can change the concept of an “entity” in an internal control environment as well as the related responsibilities and requirements.

Source : Extrait du rapport de Deloitte - « *Blockchain and Internal Control : the COSO perspective* »

⁸⁰ Etude de Deloitte - « *Blockchain and Internal Control : the COSO perspective* » - Jennifer Burns, Amy Steele, Eric E. Cohen et Dr. Sri Ramamoort - 07/2020, disponible à l'adresse suivante :

file:///C:/Users/chapo/Downloads/us-audit-blockchain-and-internal-control-the-coso-perspective.pdf

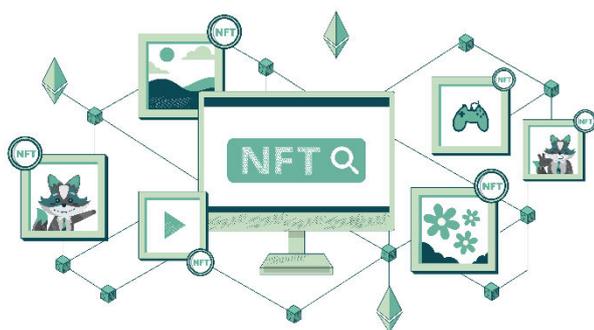
Les fonctions de contrôles, désireuses d'intégrer la technologie Blockchain, doivent en effet se préparer à quelques adaptations.

A titre d'exemple, pour réussir l'exercice de cartographie des risques, plusieurs préoccupations doivent être prises en compte par les fonctions de contrôle, telles que:

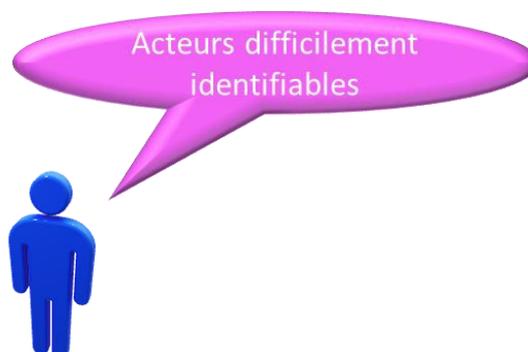
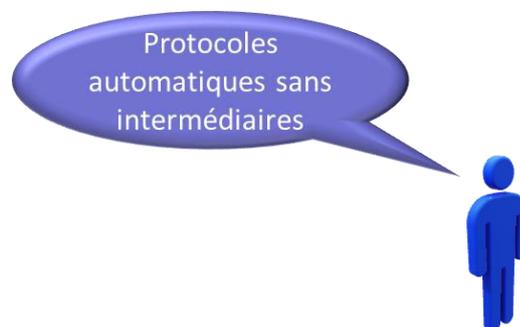
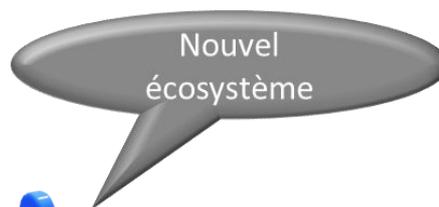
- ✓ l'écosystème mouvant et complexe ;
- ✓ l'existence de protocoles exécutés de manière automatique sans intermédiaires ;
- ✓ la problématique d'identification de la juridiction de rattachement pour les services proposés, notamment pour l'écosystème lié aux crypto-monnaies ;
- ✓ l'absence d'acteurs aisément identifiables dans certains cas.



Source : Journal du Coin



Source : Facett Crypto Blog



3. POINTS D'ATTENTION « BLOCKCHAIN » POUR LES FONCTIONS DE CONTRÔLE

*“You cannot swim for new horizons
until you have the courage to lose
sight of the shore”*

William Faulkner

Il existe une très grande variabilité suivant les projets Blockchain, avec des sous-jacents technologiques et ce, pour différents cas d'usages. Il faut donc regarder chaque projet, comme un cas particulier, car ce qui est vrai dans une Blockchain n'est pas forcément vrai dans une autre Blockchain.

Compte tenu des risques et des opportunités apportés par cette technologie, il est nécessaire de bien comprendre le fonctionnement de la Blockchain que l'on va contrôler. En effet, les choix opérés entre une Blockchain Publique, Privée ou à Consortium sont différents, ce qui a pour conséquence d'impacter, à la hausse ou à la baisse, leur exposition à certains risques.

Cadre de gouvernance	Le partage de données au sein de la Blockchain constitue un élément clé, fondamentalement différent des systèmes traditionnels	
	Approbation	Approbation formelle par les instances de gouvernance de l'organisation, ainsi que des autres parties prenantes le cas échéant
	Formalisation	Revue de la documentation relative à la gouvernance et des procédures afférentes afin de clarifier les rôles/responsabilités, ainsi que le partage de données
	Formation	Formation des instances de gouvernance sur la technologie Blockchain et sur ses spécificités
	Information	Information appropriée des comités de gouvernance : sécurité, incident, actions correctrices, suivi des changements opérés, projet d'évolution, etc.
	Supervision et suivi	Supervision et suivi des contrats avec les tiers

Gestion du changement	La gestion du changement au sein de la Blockchain nécessite un suivi spécifique et périodique afin de s'assurer que les changements déployés n'affectent pas le fonctionnement de la Blockchain, ainsi que le dispositif de maîtrise des risques mis en place	
	Codes et autorisation	Gestion du code et des autorisations pendant la période de Change Management
	Procédures	Formalisation des procédures de change management, approbation et communication aux différentes instances de gouvernance
	Données	Exhaustivité et exactitude des données au sein de l'organisation en cas de transfert entre les anciens systèmes et la Blockchain déployée (interfaces, etc.)
	Data migration	Migration des données et vérification relative à la conversion de données



“

Là où la Blockchain va apporter beaucoup, c'est en termes de traçabilité.

Par exemple, quand aujourd'hui on a un problème de maladie d'origine bactérienne, du type légionellose dans des produits, il est très difficile de retracer toute la piste d'audit.

Est-ce que la Blockchain règle le problème ? En tout cas, la Blockchain apporte une solution puisque cette technologie est infalsifiable sur la traçabilité, encore faut-il que le personne remplisse la bonne information et le fasse correctement. La qualité des données constitue un impondérable.

Donc aujourd'hui pour que cela fonctionne bien, il y a un énorme travail de change management. ”

Rémi Rouet – Group Chief Data Officer – Les Mousquetaires – 11/07/2022

Smarts-Contracts	Même si les Smart-Contracts s'exécutent de manière automatique lorsque certaines conditions sont remplies, ces derniers sont toutefois exposés à certains risques IT	
	Accès	Revue des accès aux Smart-Contracts
	Gestion du changement	Analyse du processus de gestion du changement applicable au Smart-Contract : développement, test, mise à jour, correction, etc.
	Gestion des incidents	Contrôle relatif à la gestion des incidents : identification, plan correctif, suivi et information, etc.
	Conformité	Adéquation parfaite entre les termes de l'accord et la retranscription informatique
	Code	Existence de revue périodique du code par un tiers indépendant
	Ajout	Revue du processus en cas d'ajout des Smart-Contracts



“

Là où la Blockchain va apporter beaucoup, c'est en termes de traçabilité.

Par exemple, quand aujourd'hui on a un problème de maladie d'origine bactérienne, du type légionellose dans des produits, il est très difficile de retracer toute la piste d'audit.

Est-ce que la Blockchain règle le problème ? En tout cas, la Blockchain apporte une solution puisque cette technologie est infalsifiable sur la traçabilité, encore faut-il que le personne remplisse la bonne information et le fasse correctement. La qualité des données constitue un impondérable.

Donc aujourd'hui pour que cela fonctionne bien, il y a un énorme travail de change management.”

Rémi Rouet – Group Chief Data Officer – Les Mousquetaires – 11/07/2022

Sécurité	Les différentes couches de sécurité informatique pour protéger la Blockchain et surveiller son fonctionnement doivent être vérifiées	
	Accès	Revue de la gestion des accès : autorisation, processus, documentation, contrôles, etc. L'accessibilité des données doit être restreinte aux entités membres de la Blockchain La revue de contrôle devra couvrir l'ensemble des nœuds pour vérifier que tous les membres de la Blockchain ont un niveau de visibilité identique
	Mécanismes de consensus	Vérification des mécanismes de consensus : formalisation, niveau de détail, acceptation par tous les participants, gestion des incidents, etc. Lors de la conception de l'infrastructure, les droits et devoirs de l'ensemble des acteurs sont établis pour connaître les autorisations et les responsabilités de chacun
	Gestion des clés privées	Analyse concernant la gestion des clés privées : génération, stockage, élimination, etc.
	Scalabilité	Revue de la capacité de la Blockchain à « monter en charge », c'est-à-dire à pouvoir traiter plus de transactions/opérations à la seconde sans que cela n'impacte les performances
	RGPD	Contrôle de la Conformité au regard du RGPD : transferts internationaux de données personnelles, droit à l'effacement, rôle du « Responsable de traitement des données », etc.
	Cybersécurité	Evaluation au regard des risques de Cybersécurité : analyse des vulnérabilités/failles de sécurité, test d'intrusion, stratégie de défense, identification des incidents, etc.

“

Mon obsession, c'est la sécurité, avec pour objectif qu'aucune information ne disparaisse, qu'il n'y ait pas de hackers, qu'il n'y ait pas de manipulation du code source ou du registre, etc.

Comme cette technologie est très dispersée, très décentralisée, il faut être capable en temps réel de contrôler l'ensemble des nodes. C'est fondamental.”

Benjamin Faraggi - CEO fondateur de Spuro et Président de la Blockchain : Kagesecur – 06/07/2022

Intégrité des données	L'intégrité des données, en entrée ou en sortie, nécessite d'être vérifiée afin de s'assurer de leur fiabilité, exhaustivité, exactitude et cohérence	
	Pertinence des sources de données	Revue de la pertinence des sources de données pour s'assurer que seuls les membres autorisés peuvent être à l'origine des données enregistrées dans la Blockchain
	Sécurité	Existence de contrôles efficaces pour prévenir les attaques pouvant modifier les données sources
	Enregistrement des opérations	Efficacité des contrôles en place relatifs à l'enregistrement des transactions/opérations
	Immuabilité	Contrôle du caractère immuable des données

Continuité et reprise après sinistre	Les plans de continuité d'activité et de reprise après sinistre doivent être contrôlés afin de s'assurer du fonctionnement opérationnel de la Blockchain en cas d'évènement perturbateur et afin de vérifier l'existence de mesures de reprise après sinistre	
	Périmètre	Revue des plans de continuité d'activité et de gestion de reprise après sinistre pour s'assurer que ces derniers intègrent le périmètre de la Blockchain
	Contributeurs	Revue des plans de continuité d'activité et de gestion de reprise après sinistre pour vérifier que ces derniers prennent en compte les parties prenantes concernées
	Approbation	Approbation formelle par les instances de gouvernance

“

Dans le cas d'une Blockchain privée, ce sont le droit et la logique des consortiums qui s'appliquent. Finalement, il y a un moins de technicité et de points d'attention spécifiques à la technologie Blockchain à prendre en compte. Certains risques et contrôles d'une base de donnée partagée peuvent être repris. Il s'agit davantage d'une adaptation que d'une révolution copernicienne pour les fonctions de contrôle.”

Ivan De Lastours - Blockchain lead chez Bpifrance - 25/07/2022

“

En fonction du degré de permission, la/les personne(s) qui a/ont la main sur la Blockchain privée peuvent très bien décider de supprimer telles ou telles transactions, qui ne seront plus visibles dans la Blockchain.

D'un point de vue risque, je pense qu'il faut être très au clair sur qui a accès à la Blockchain privée et qui peut faire des actions sur la piste d'audit de cette Blockchain privée. En effet, le risque est le suivant : l'effacement des datas que l'on ne retrouve pas sur les Blockchain publiques.”

Dorian Olivier – Compliance / Advisory à Coinhouse – 21/06/2022

Gestion des risques juridiques et réglementaires	Le cadre juridique et réglementaire qui encadre la Blockchain, disparate au niveau mondial, est en cours de construction ou de renforcement selon les pays	
	Conformité et veille réglementaire	Analyse des réglementations applicables afin de s'assurer de respect de ces dernières : lutte contre le blanchiment des capitaux et financement du terrorisme, respect des mesures de gel des avoirs, protection des investisseurs, RGPD, etc.
	Suivi et supervision	Revue des informations relatives à la surveillance des risques réglementaires : compte rendu à destination des comités et instances de gouvernance, cartographie des risques, reporting, rapports réglementaires, informations partagées avec les parties prenantes concernées, etc.

Gestion des profils qualifiés	Les profils qualifiés capables de comprendre les sous-jacents de cette technologie et son potentiel constituent un défi pour les fonctions de contrôle	
	Capter et retenir les talents	Analyse des mesures prises pour attirer et retenir les talents avec les connaissances et compétences requises pour le déploiement de la Blockchain
	Formation	Formation des équipes existantes sur le fonctionnement et les potentialités de la technologie Blockchain

Gestion des risques liés aux tiers	La technologie Blockchain est exposée à des risques liés aux tiers : risque de réputation et de non respect de la réglementation	
	Réputation	Revue des interactions avec les nouvelles unités collaboratives (différentes entités qui fonctionnent sur une base décentralisée mais qui restent liées) afin de s'assurer de l'absence de risque pouvant nuire à la réputation de l'organisation
	Sélection	Définition et formalisation du processus de sélection des fournisseurs selon des critères, établis intégrant notamment les aspects suivants : talents et expérience, solidité financière, coûts, conflits d'intérêt, etc.
	Relation contractuelle	Existence de contrats avec les tiers
	Suivi et pilotage	Suivi et pilotage de la relation avec les tiers
	Evaluation périodique	Revue périodique sur la base de critères prédéfinis pour s'assurer notamment que les fournisseurs respectent les termes du contrat

Transactions	La revue du flux de transactions inscrites sur la Blockchain doit être effectuée afin d'identifier les risques auxquels l'organisation est exposée	
	Flux	<p>Vérification de l'existence des flux et des risques au regard du KYC (Know your Customer), KYA (Know your Address) et KYT (Know your Transaction)</p> <p>Revue des transactions via des DEX</p> <p>Suivi des rebonds et des transactions via des « mixers »</p>

“

KYC (Know your Customer), KYA (Know your Address) et KYT (Know your Transaction) sont des problématiques propres aux transactions sur des crypto-actifs que les entreprises doivent prendre en compte.

Un exchange est une plateforme qui permet de réaliser des transactions d'actifs, notamment des crypto-actifs.

Il existe 2 types d'échange, les CEX – centralized exchange et les DEX - decentralized exchange.

Les CEX sont des plateformes d'échange sur lesquelles il est possible d'effectuer des transactions en crypto-actifs en faisant appel à un intermédiaire. A titre d'exemple, c'est le cas de Binance, Coinbase, Kraken, Coinhouse, etc.

Dans ce cas, les transactions ne sont pas inscrites sur la Blockchain. C'est l'intermédiaire qui alloue une partie d'un crypto-actif, sans que l'investisseur ne le possède vraiment.

Les DEX permettent à des utilisateurs d'acheter ou vendre des crypto-actifs sans devoir confier ses actifs numériques à une plateforme classique. Les investisseurs possèdent en permanence leurs propres portefeuilles et ont un contrôle total sur ces derniers. Ainsi, c'est l'adresse propre de l'investisseur qui est inscrite dans la Blockchain avec toutes les transactions.

Concernant le KYC (Know your Customer), à ce jour, les commissions et les vérifications en termes de connaissance client sont souvent moindre par rapport aux CEX.

Concernant le KYA (Know your Address), aujourd'hui, il est difficile de savoir qui est la personne qui est derrière l'adresse avec laquelle elle effectue des transactions, cette adresse étant uniquement déclarative. Par ailleurs, il est possible de télécharger toutes les transactions de la Blockchain si on a une connexion dans cette Blockchain (par exemple à travers un rig de minage), et il est ensuite possible de faire l'analyse de l'activité de certaines adresses.

Concernant le KYT (Know your Transaction), il convient de s'assurer qu'il n'y a pas de personnes malveillantes qui soit en relation avec une personne avec qui on a un lien.

Pour une entreprise qui crée son propre NFT, la question LCB-FT est importante car elle met en jeu sa réputation dans le cas où l'entreprise se retrouve exposée à une personne effectuant ou ayant effectué des malversations, notamment pour les « secondes mains ». A titre d'exemple, si une entreprise du secteur du luxe émet un NFT et que ce dernier se retrouve in fine être revendu à un terroriste, il peut y avoir une exposition médiatique et donc un risque de réputation compte tenu du lien traçable via la technologie Blockchain.”

Pierre-Louis Missler - Data Analyst - Forensic & Integrity Services – Ernst& Young – 28/07/2022

CONCLUSION

*“If you do what you always did,
you will get what you always got” »*

Albert Einstein

Ces derniers mois sont en train de marquer un tournant majeur dans l’histoire de la Blockchain. Entre essor des NFT, le Métavers qui fait de plus en plus parler de lui et les cryptoactifs qui sont en train de vivre un « *bear market* », l’enjeu de la régulation conforte sa place en haut de l’agenda.

Toutefois, comprendre le fonctionnement et analyser les mérites et les dangers de la technologie Blockchain nécessitent de maîtriser sa complexité technique intrinsèque.

Une des difficultés est de ne pas la limiter à l’utilisation du Bitcoin et d’autres cryptomonnaies et d’entrevoir, pour les fonctions de contrôle, ce que j’appelle le « champ des possibles ».



Je pense que cette innovation va avoir un impact notable à moyen terme sur les métiers de l’Audit Interne, du Contrôle Interne et de la Conformité.

Cela, certes, ne va pas avoir lieu à très court terme. Il s’agit d’une opportunité à saisir car c’est d’ores et déjà maintenant qu’il faut acquérir de nouveaux savoirs et apprendre à maîtriser les outils. Cependant, la technologie Blockchain n’est pas arrivée à maturité, loin s’en faut.

Sécurisation des chaînes d’approvisionnement, valorisation de la donnée, fléchages des investissements / aides financières, renforcement de la coopération et de la standardisation, optimisation et fiabilisation des processus, solutions de financement, sont autant de sujets pour lesquels les business model des organisations vont se transformer...

Quoi qu’il en soit, on observe que les cryptoactifs prennent progressivement de l’ampleur et se diversifient partout dans le monde, notamment dans les économies faiblement bancarisées.

De nouveaux risques apparaissent et se révèlent.

Cependant, dans un contexte aussi mouvant et foisonnant, les fonctions de contrôle, au sein de leur organisation, doivent être vigilantes à cette lame de fond, qui va progressivement changer, les impacter et leur offrir de nouvelles opportunités compte tenu des éléments suivants :

- ✓ **nouveaux process à contrôler,**
- ✓ **la dématérialisation et la facilitation d'accès aux données,**
- ✓ **l'intégrité, la transparence et la traçabilité,**
- ✓ **l'efficience et l'efficacité des contrôles,**
- ✓ **les perspectives de processus d'audit continu et de certification des contrôles,**
- ✓ **l'utilisation pour des fins de KYC, de surveillance des transactions et de reporting/consolidation.**

En conséquence, le premier prérequis pour réussir sa revue d'une technologie Blockchain est de disposer des bonnes compétences. Les profils qualifiés, ayant la connaissance et la maîtrise de cette nouvelle technologie, vont être recherchés. Il sera nécessaire de connaître les nouveaux outils mis à disposition.

Également, faire le lien entre le monde physique (réel, soumis aux réglementations existantes et celles à venir) et le monde numérique (mouvant, innovant en mutation perpétuelle) constitue un défi auquel les fonctions de contrôle doivent s'atteler dès à présent.

En cela, les fonctions de contrôle ont tout intérêt à soigner leurs recrutements. Parallèlement, la formation des équipes existantes est la clé du succès.





GLOSSAIRE

ADAN : « Association pour le développement des actifs numériques », fondée en 01/2020, qui rassemble les professionnels du secteur des actifs numériques et des technologies Blockchain en France et en Europe

AFTI : « Association Française des Professionnels des Titres », constituée en 1990, a pour objet de rassembler les professionnels des établissements du secteur bancaire et financier concernés par les activités sur les instruments financiers

Altcoin : le terme « Altcoin » provient de la contraction des deux mots « Alternative » et « Coin ». Cette expression est utilisée pour désigner toutes les cryptomonnaies autres que le Bitcoin. Comme le Bitcoin, ce sont des actifs numériques basés sur la technologie Blockchain. Généralement, ces altcoins proposent des protocoles ou des fonctionnalités différents de ceux du Bitcoin. En 06/2022, il existe plus de 18 000 Altcoins

Asset tokens : ce sont des crypto-actifs qui représentent des droits sur les actifs d'une entreprise qui a procédé à une ICO (*Initial Coin Offering*) et qui ont été cédés aux investisseurs, en contrepartie des fonds qu'ils ont apportés

Baleines : surnom donné aux détenteurs de portefeuilles très importants d'un crypto-actif

BCE : la Banque Centrale Européenne regroupe les 19 pays de l'Union européenne utilisant l'euro

Bear market : un marché décrit comme étant un bear market désigne une phase de marché durant laquelle le prix des valeurs - typiquement des actions, ou des obligations, mais cela peut s'appliquer également au marché de l'or ou des crypto-monnaies - évoluent à la baisse

Bitcoin Explorer : il s'agit d'un outil qui aide les utilisateurs à trouver transactions en bitcoins dans la blockchain Bitcoin. Il fournit également aux utilisateurs une interface pour rechercher facilement des informations

Blockchain publique : une Blockchain publique suit un mode de gouvernance décentralisé, l'intégrité de la donnée étant garantie par les nœuds qui la conservent et les mineurs qui la valident

Blockchain à consortium : ce type de Blockchain se situe sur la limite entre chaînes publiques et privées, combinant des éléments des deux côtés. La différence la plus notable par rapport à chaque système peut être observée au niveau du consensus. Au lieu d'un système ouvert où n'importe qui peut valider des blocs ou d'un système fermé où seule une seule entité nomme les producteurs de blocs, une chaîne à consortium comporte une poignée de parties équitablement puissantes qui fonctionnent simultanément en tant que validateurs

Bull Run : période de temps durant laquelle les marchés des cryptomonnaies connaissent un fort moment haussier, constituant ainsi une opportunité de faire des bénéfices

CASP : « *Crypto-assets services provider* »

CBDC : « *Central bank digital currency* »

CEX : « *Centralized exchange* » permet à des utilisateurs d'acheter ou vendre des crypto-actifs sans devoir confier ses actifs numériques à une plateforme classique. Les investisseurs possèdent en permanence leurs cryptoactifs et ont un contrôle total sur ces derniers

Clé privée : La clé privée est comparable à un code PIN : elle est gardée secrète et permet de signer des transactions et transférer des cryptomonnaies. Grâce à la clé privée, on peut calculer la clé publique (l'inverse n'est pas possible)

Clé publique : cette clé permet de calculer l'adresse

COSO : « *Committee Of Sponsoring Organizations of the Treadway Commission* », le COSO est une commission à but non lucratif qui établit en 1992 une définition standard du contrôle interne et crée un cadre pour évaluer son efficacité. La version de 2013 qui tient compte de l'évolution de l'environnement économique et réglementaire dans lequel évoluent les organisations - nouveaux risques, attentes accrues en matière de gouvernance, rôle toujours plus important de la technologie, recours intensifié à l'externalisation, exigences de reporting au-delà de la communication financière

CRIPP : « *Cadre de Référence Internationale des Pratiques Professionnelles de l'audit interne* » - le CRIPP comprend les lignes directrices approuvées par l'Institute of Internal Auditors

Cryptographie : c'est l'art de chiffrer des informations pour les rendre inintelligibles sauf à ceux qui ont la clé pour la décoder

Cypherpunk : Composé à partir de deux mots anglais que sont « cipher » (ou cypher) signifiant chiffrement et « punk » désignant un esprit rebelle, les cypherpunks forment un groupe informel de personnes intéressées par la cryptographie. Leur objectif est d'assurer le respect de la vie privée par l'utilisation proactive de la cryptographie

DAC 6 : La « *DAC 6* » désigne la directive européenne (UE) 2018/822 du Conseil du 25/05/2018 relative à l'échange automatique et obligatoire d'informations sur les dispositifs transfrontières devant faire l'objet d'une déclaration. Elle vise à renforcer la coopération entre les administrations fiscales des pays de l'UE en matière des montages potentiellement agressifs de planification fiscale

DAO : « *Decentralized autonomous organization* » ou « *Organisation autonome décentralisée* » est une organisation qui se fixe une mission et qui fonctionne grâce à un ensemble de Smart-Contracts permettant d'établir et de fournir des règles de gouvernance à une organisation

Darkweb : le darkweb, aussi appelé web clandestin ou encore web caché, est le web non indexé et non accessible par des moyens standard. Ce terme est aussi généralement utilisé pour désigner le web criminel au sens large, indépendamment de son indexation ou de son accessibilité. Dans l'imaginaire collectif, le Darkweb regroupe donc ces deux définitions, c'est-à-dire à la fois les sites dédiés aux activités criminelles et les sites, qu'ils soient dédiés au cybercrime ou non

Darkenet : le darkenet vient du mot anglais « *dark* », sombre, et « *Net* ». C'est l'ensemble des réseaux permettant de partager de manière anonyme des données cryptées inaccessibles aux moteurs de recherche traditionnels. Espace de liberté pour les dissidents politiques et les lanceurs d'alerte, notamment, le darknet est aussi le lieu d'un grand nombre d'activités illégales : pédophilie, trafic d'armes, terrorisme, etc. Ces réseaux sont dits « superposés » car ils reposent sur un autre pour fonctionner, internet en l'occurrence. Pas d'internet, pas de darknet...

DEEP : « *Dispositif d'enregistrement électronique partagé* » – introduction en droit français de la Blockchain sous le terme DEEP

DeFi : finance décentralisée – la DeFi permet de réaliser des opérations financières complexes sans faire appel à un tiers de confiance ». Son objectif est de démocratiser l'accès aux services financiers en se passant d'une banque, d'un assureur ou même d'un teneur de marché

DEX : « *Decentralized exchange* » permet à des utilisateurs d'acheter ou vendre des crypto-actifs sans devoir confier ses actifs numériques à une plateforme classique. Les investisseurs possèdent en permanence leurs cryptoactifs et ont un contrôle total sur ces derniers

DLT : « *Distributed ledger technology* » - voir définition ci-dessous concernant la technologie de ledger distribué

EBA : « *European Banking Authority* ». L'Autorité bancaire européenne est une autorité qui œuvre afin de garantir un niveau de réglementation et de surveillance prudentielles efficace et cohérent dans l'ensemble du secteur bancaire européen. Ses principaux objectifs sont de maintenir la stabilité financière dans l'Union Européenne et de garantir l'intégrité, l'efficacité et le bon fonctionnement du secteur bancaire

ESMA : « *European Securities and Markets Authority* ». L'Autorité européenne des marchés financiers est une autorité de surveillance européenne indépendante, installée à Paris. Son rôle est d'assurer la stabilité et l'efficacité du système financier dans l'Union Européenne à court, moyen et long terme

Ethereum : protocole d'échanges décentralisés permettant la création par les utilisateurs de contrats intelligents « Smart-Contracts ». L'Ethereum utilise une unité de compte dénommée Ether comme moyen de paiement de ces contrats. L'Ethereum est la deuxième plus importante cryptomonnaie avec une capitalisation supérieure à 448 milliards d'euros en octobre 2021

Etherscan : il s'agit d'un explorateur de blocs, c'est-à-dire que lorsque une transaction est effectuée sur la Blockchain Ethereum, il est possible de voir son état d'avancement, de vérifier l'adresse de départ, d'arrivée

E-yuan ou e-CNY : monnaie de banque centrale numérique chinoise

Forgeage : de nombreuses cryptomonnaies utilisent le concept de preuve d'enjeu (Proof-of-Stake - POS). Avec le POS, les possibilités d'attribution de nouvelles pièces ne se mesurent pas en fonction de la performance de travail, mais en fonction du «stake» personnel, c'est-à-dire de la part actuelle dans la cryptomonnaie correspondante. Dans le cas du POS, il fait référence au «forgeage» (forging en anglais) de nouvelles pièces et, dans le cas du PoW, il est fait référence au «minage» (mining)

Fork : un fork se produit dès qu'une communauté modifie le protocole de la Blockchain ou un ensemble de règles élémentaires. Le cas échéant, une division a lieu et fait naître une deuxième Blockchain qui partage l'ensemble de son historique avec celle d'origine tout s'orientant vers une nouvelle direction

Front running : Le Front Running est une pratique illégale compte tenu d'une connaissance préalable des événements susceptibles d'affecter le marché et ce, afin d'obtenir un avantage économique

ICO : « *Initial Coin Offering* » désigne une opération de levée de fonds par laquelle une société ayant un besoin de financement émet des jetons, aussi appelés « *tokens* », auxquels les investisseurs souscrivent principalement avec des crypto-monnaies. Ces jetons peuvent leur permettre d'accéder, dans le futur, à des produits ou services de cette société. L'investissement dans une ICO comporte des risques de perte partielle ou totale du capital investi

IIA : « *Instance internationale de normalisation* » - l'IIA fournit aux auditeurs internes du monde entier des orientations qui font autorité. Elles figurent dans les dispositions obligatoires ou recommandées du CRIPP

Hachage : le hachage cryptographique génère une chaîne de caractères de longueur fixe à partir d'un ensemble de données de n'importe quel volume. Cet ensemble de données peut être un mot, une phrase, un texte plus long ou un fichier entier. Le hachage cryptographique peut être utilisé à des fins de sécurité. Il transforme un input de données aléatoire (clés) en une chaîne d'octets de longueur et de structure fixes (valeur de hachage). Le hash d'une transaction facilite l'identification de cette dernière sur la Blockchain

Hashcash : système de preuve de travail (POW – Proof of Work – voir définition ci-dessous) conçu pour limiter le spam et les dénis de service, et plus récemment est connu pour son utilisation dans le Bitcoin

Interopérabilité : possibilité d'échanger des données entre différentes chaînes de blocs de manière transparente, comme s'il n'y avait pas de frontières

KYC : « *Know Your Customer* » ou connaissance du client, est le nom donné au processus permettant de vérifier l'identité des clients

Livre blanc du Bitcoin : article scientifique technique qui établit les bases théoriques de la structure du réseau de Bitcoin. Le livre blanc est composé de neuf pages

Loi de Moore : lois empiriques qui ont trait à l'évolution de la puissance de calcul des ordinateurs et de la complexité du matériel informatique. La première de ces lois est émise par le docteur Gordon E. Moore en 1965, lorsque celui-ci postule sur une poursuite du doublement de la complexité des semi-conducteurs tous les ans à coût constant. Dix ans plus tard, il ajusta sa prédiction à un doublement du nombre de transistors présents sur une puce de microprocesseur tous les deux ans. Ce second postulat se révéla particulièrement exact, et popularisa le terme de « loi de Moore », si bien que ce dernier a fini par s'étendre au doublement d'une capacité quelconque en un temps donné

Machine Learning : Technologie d'intelligence artificielle permettant aux machines d'apprendre sans avoir été au préalable programmées spécifiquement à cet effet. Le Machine Learning est explicitement lié au Big Data, étant donné que pour apprendre et se développer, les ordinateurs ont besoin de flux de données à analyser, sur lesquelles s'entraîner. De ce fait, le Machine Learning, issu par essence du Big Data, a précisément besoin de ce dernier pour fonctionner. Le Machine Learning et le Big Data sont donc interdépendants

Métavers ou Metaverse : Il s'agit de la contraction de « *Méta* » (au-delà) et « *Universe* » (univers), i.e. des univers partagés virtuels collectifs, parallèles au nôtres, dans lesquels nous évoluerons et interagirons comme dans la vie réelle, nous livrant à de la sociabilisation, des jeux ou à un travail

MDBC/MNBC : Monnaie digitale de banque centrale aussi appelée « *CBDC* » en anglais

MiCA : « *Markets in Crypto-Assets* » - le projet de règlement européen a pour but de réguler les acteurs du marché des cryptomonnaies

Mixage de cryptomonnaie : le mixage de crypto-monnaies est un service offert dans le but de mélanger des fonds de crypto-monnaie potentiellement identifiables ou « contaminés » avec d'autres, afin d'obscurcir la piste jusqu'à la source d'origine du fonds

MNBC : Monnaie numérique de banque centrale

Utility token : crypto-actifs conçus pour permettre un usage ou un achat

NFT : « *Non Fungible Token* », il s'agit de tokens non fongible ou de jetons non fongibles. Un NFT est un identifiant numérique unique et inviolable qui permet d'authentifier un fichier numérique (une image, une photo, un vidéo, etc.). Unique et non modifiable, il tient lieu de certificat d'authenticité et constitue une preuve numérique de provenance et de propriété du document à laquelle il est associé

Noeuds : points de connexion au réseau

Pairs : point de connexion égaux

Peer-to-Peer ou Pair-à-Pair : permet à plusieurs ordinateurs ou nœuds de communiquer via un réseau, en y partageant des simplement et directement des informations. La singularité des systèmes Peer-to-Peer réside dans le fait que les données peuvent être transférées directement entre les deux nœuds connectés au réseau, sans transiter par un serveur central

POS : « *Proof of stake* » ou preuve d'enjeu accorde généralement, selon un système de tirage aléatoire pondéré, le droit de créer le prochain bloc à un validateur actif sur le réseau ayant mis en dépôt des unités de la cryptomonnaie de la Blockchain. Avec le POS, les possibilités d'attribution de nouvelles pièces ne se mesurent pas en fonction de la performance de travail, mais en fonction du « *stake* » personnel, c'est-à-dire de la part actuelle dans la cryptomonnaie correspondante. Ainsi, plus une personne possède des pièces, plus elle a des chances d'être sélectionné aléatoirement pour valider des transactions

POW : « *Proof of work* » ou preuve de travail – Une blockchain utilisant la POW fait appel à des mineurs pour vérifier les données entrantes sur le registre, valider l'authenticité des transactions et créer de nouveaux blocs. Pour récompenser l'ensemble des mineurs pour leur travail, la preuve de travail doit établir des règles permettant de choisir le mineur qui aura le droit d'émettre le prochain bloc de la chaîne

PSAN : « *Prestataire de services sur actifs numériques* ». Depuis l'entrée en vigueur de la loi PACTE le 22/05/2019, et de l'ordonnance n° 2020-1544 le 09/12/2020 renforçant le cadre de la LCB-FT applicable aux actifs numériques, les prestataires exerçant dans certains secteurs relatifs aux crypto-monnaies doivent remplir des conditions particulières pour exercer leurs activités. Ces acteurs répondant au nouveau statut de PSAN doivent s'enregistrer auprès de l'AMF, qui vérifie notamment qu'ils sont en mesure de respecter le dispositif légal relatif à la Lutte contre le Blanchiment et le Financement du Terrorisme (LCB-FT)

Pump and Dump : « *gonfler et larguer* », il s'agit d'une technique de manipulation de marché qui consiste à faire monter artificiellement le prix d'une action (pump) par des déclarations mensongères, dans le but de revendre ces actions, achetées à bas prix, avec une forte plus-value. La revente massive des actions surcotées par les organisateurs de la manipulation (dump) fait alors chuter leur prix et les autres investisseurs subissent de lourdes pertes

Rebonds : avec la cryptomonnaie, les fonds peuvent transiter en faisant de nombreux rebonds différents à travers la planète

Recall : lorsqu'une entreprise lance un ordre de virement, si une erreur est faite lors de la saisie des informations du bénéficiaire, du montant ou encore en cas de fraude, il existe la procédure de recall. Cette procédure consiste (sous certaines conditions), à rappeler les fonds auprès de la banque du bénéficiaire

RGPD : « *Règlement Général sur la Protection des Données* » - le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne

Rug Pull : le rug pull est un terme anglophone qui se traduit en français par « *tirage de tapis* ». Dans le secteur des crypto-actifs, il s'agit d'une arnaque où les fondateurs/développeurs abandonnent leur projet et s'enfuient avec les fonds des investisseurs

Scalabilité : ce terme employé dans le domaine de l'informatique matérielle et logicielle, pour définir la faculté d'un produit informatique à s'adapter aux fluctuations de la demande en conservant ses différentes fonctionnalités

Smart-Contracts ou Contrats Intelligents : contrats informatiques autonomes (morceaux de codes) qui permettent de fixer les conditions et les règles d'interaction et ainsi exécuter automatiquement une négociation ou une transaction sur la blockchain. Ils s'exécutent selon certaines conditions prédéfinies

Stablecoin : un Stablecoin est une monnaie numérique adossée à une valeur-refuge « *stable* » comme le dollar américain ou l'or. Les Stablecoins sont conçus pour réduire la volatilité par rapport aux cryptomonnaies non-adossées comme les bitcoins

Staking : c'est le fait d'immobiliser ses cryptomonnaies dans un Smart-contract de façon à participer aux opérations qui se déroulent sur la Blockchain

STO : « *Security Token Offering* » désigne une levée de fonds en cybermonnaie. Des jetons (tokens) financiers, appelés « *Security tokens* » sont émis et enregistrés sur une Blockchain. Comme pour les titres financiers, ils sont achetés par des investisseurs. Une fois acquis, ces « *Security tokens* » confèrent à leurs détenteurs un droit juridique. Une « STO » est plus réglementée que l'« ICO » puisqu'il offre des droits aux possesseurs. Les « *Security tokens* » ont le statut de valeur mobilière comme des titres financiers. Ils sont liés à un actif sous-jacent

Technologie de ledger distribué (DLT) : système numérique d'enregistrement des transactions de biens dans lequel les transactions et leurs détails sont enregistrés à plusieurs endroits en même temps. Contrairement aux bases de données traditionnelles, les Ledgers distribués n'ont pas de fonction de stockage central de données ou d'administration. Dans un Ledger distribué, chaque nœud traite et vérifie chaque élément, générant ainsi un enregistrement de chaque élément et créant un consensus sur la véracité de chaque élément

Token : actif numérique échangeable sur une Blockchain

TRACFIN : service de renseignement placé sous l'autorité du Ministère de l'Économie, des Finances et de la Relance. Il concourt au développement d'une économie saine en luttant contre les circuits financiers clandestins, le blanchiment d'argent et le financement du terrorisme. Le Service est chargé de recueillir, analyser et enrichir les déclarations de soupçons que les professionnels assujettis sont tenus, par la loi, de lui déclarer.

Utility token : ils sont conçus pour permettre un usage ou un achat. Ils sont principalement utilisés par les entreprises afin de susciter de l'intérêt pour leurs produits et de permettre aux utilisateurs d'accéder à leurs services

Wallet : un wallet crypto, en français un portefeuille crypto monnaie, est une solution permettant de stocker et de gérer en toute sécurité une monnaie virtuelle. À l'instar d'un compte bancaire classique, le portefeuille permet à son utilisateur de dépenser, de recevoir, mais aussi d'échanger des cryptomonnaies



BIBLIOGRAPHIE

- ACPR – « *Accompagnement des acteurs innovants: les crypto-actifs et la transformation de l'écosystème financier* » - 22/10/2021, disponible à l'adresse suivante : <https://acpr.banque-france.fr/accompagnement-des-acteurs-innovants-les-crypto-actifs-et-la-transformation-de-lecosysteme-financier>
- ACPR - Communiqué de presse - « *L'ACPR publie les résultats de son étude sur la transformation numérique dans les secteurs français de la banque et de l'assurance* » - 14/01/2022, disponible à l'adresse suivante : https://acpr.banque-france.fr/sites/default/files/medias/documents/20220114_cp_etudes_numeriques.pdf
- ADAN et KPMG - « *La crypto en France, structuration et adoption par le grand public* » - 02/2022, disponible à l'adresse suivante : <https://adan.eu/rapport/crypto-france-structuration-adoption#:~:text=En%20ce%20d%C3%A9but%20d'ann%C3%A9e%202022%2C%20l'Associati on%20pour,projections%20quant%20aux%20opportunit%C3%A9s%20%C3%A9conomiques adoption#:~:text=En%20ce%20d%C3%A9but%20d'ann%C3%A9e%202022%2C%20l'Associati on%20pour,projections%20quant%20aux%20opportunit%C3%A9s%20%C3%A9conomiques>
- BANK FOR INTERNATIONAL SETTLEMENTS – CODRUTA BOAR, HENRY HOLDEN, AMBER WADSWORTH – « *Impending arrival – a sequel to the survey on central bank digital currency* » - 01/2020, disponible à l'adresse suivante : <https://www.bis.org/publ/bppdf/bispap107.pdf>
- BANQUE CENTRALE EUROPEENNE - Communiqué de presse - « *L'Eurosystème lance un projet d'euro numérique* » - 14/07/2021, disponible à l'adresse suivante : <https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.fr.html>
- BINANCE ACADEMY - « *Blockchain Privées, Publiques et à Consortium — Quelles sont les différences ?* » - 06/01/2020, disponible à l'adresse suivante : <https://academy.binance.com/fr/articles/private-public-and-consortium-blockchains-whats-the-difference>
- BLOCKCHAIN FRANCE - « *Qu'est-ce qu'une blockchain ?* », disponible à l'adresse suivante : <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>
- BLOCKCHAIN FRANCE - « *Les applications prometteuses des smart contracts* » - 28/01/2016, disponible à l'adresse suivante : <https://blockchainfrance.net/2016/01/28/applications-smart-contracts/>
- CAPITAL - « *Meta (Facebook) met officiellement fin à son projet de monnaie numérique Diem* » - 01/02/2022, disponible à l'adresse suivante : <https://www.lemonde.fr/pixels/article/2019/06/18/ce-qu-il-faut-savoir-sur-le-libra-la-cryptomonnaie-de-https://www.capital.fr/crypto/meta-facebook-met-officiellement-fin-a-son-projet-de-monnaie-numerique-diem-1427160>
- CHALLENGES - FABIO PANETTA – « *La BCE pourrait lancer le développement de l'euro numérique d'ici fin 2023, dit Panetta* » - 16/05/2022, disponible à l'adresse suivante : https://www.challenges.fr/finance-et-marche/la-bce-pourrait-lancer-le-developpement-de-l-euro-numerique-d-ici-fin-2023-dit-panetta_813351

- CHRISTOPHE DORE - extrait de l'article FRENCH WEB - « *Blockchain: la FinTech MoneyTrack lève 2,3 millions d'euros et mène sa première acquisition* » - 26/03/2021, disponible à l'adresse suivante : <https://www.frenchweb.fr/blockchain-la-fintech-moneytrack-leve-23-millions-deuros-et-mene-sa-premiere-acquisition/418599>
- CISION – « *Brickblock Tokenizes the First Property in Europe* » - 28/05/2019, disponible à l'adresse suivante : <https://www.prnewswire.com/news-releases/brickblock-tokenizes-the-first-property-in-europe-300820582.html>
- CNIL - « *Blockchain* », disponible à l'adresse suivante : <https://www.cnil.fr/fr/definition/blockchain>
- COIN ACADEMY- « *Crypto : La FIFA s'associe au réseau blockchain Algorand* » - 03/05/2022, disponible à l'adresse suivante : <https://coinacademy.fr/actu/fifa-algorand-partenariat/>
- COINS - « *Le pont crypto "sécurisé" Nomad piraté : près de 200M\$ volés* » - 02/08/2022, disponible à l'adresse suivante : <https://coins.fr/pont-crypto-nomad-hack-200-millions-dollars-vol/>
- COMMODITY FUTURES TRADING SERVICES - Communiqué de presse - « *CFTC Orders Coinbase Inc. to Pay \$6.5 Million for False, Misleading, or Inaccurate Reporting and Wash Trading* » - 19/03/2021, disponible à l'adresse suivante : <https://www.cftc.gov/PressRoom/PressReleases/8369-21>
- CRYPTOAST - « *Un bug lié à la blockchain Solana (SOL) aurait pu causer la perte de centaines de millions de dollars* » - 04/12/2021, disponible à l'adresse suivante : <https://cryptoast.fr/bug-solana-perte-centaines-millions-dollars/>
- CRYPTONAUTE - « *ZenCash (ZEN) victime d'une attaque des 51%* » - 08/06/2021, disponible à l'adresse suivante : <https://cryptonaute.fr/zencash-zen-attaque-des-51-hack/>
- DELOITTE – « *An Internal Auditors guide to Blockchain* » – 2021, disponible à l'adresse suivante : [file:///C:/Users/chapo/Downloads/internal-auditors-guide-to-blockchain%20\(4\).pdf](file:///C:/Users/chapo/Downloads/internal-auditors-guide-to-blockchain%20(4).pdf)
- DELOITTE - « *Blockchain and Internal Control: the COSO perspective* » - Jennifer Burns, Amy Steele, Eric E. Cohen et Dr. Sri Ramamoort - 07/2020, disponible à l'adresse suivante : <file:///C:/Users/chapo/Downloads/us-audit-blockchain-and-internal-control-the-coso-perspective.pdf>
- DELL TECHNOLOGIES - « *Realizing 2030: Dell Technologies Research Explores the Next Era of Human-Machine Partnerships* » - disponible à l'adresse suivante : <https://www.dell.com/fr-fr/dt/corporate/newsroom/realizing-2030-dell-technologies-research-explores-the-next-era-of-human-machine-partnerships.htm>
- DORIAN RAVAUTE, LE MONDE - « *Blockchain : un outil pour la conformité fiscale* » - 03/11/2020, disponible à l'adresse suivante : <https://www.lemonde.fr/blog/binaire/2020/11/03/blockchain-un-outil-pour-la-conformite-fiscale/>
- DR. BILLAL CHOULI, FREDERIC GOUJON, YVES-MICHELLEPROCHER - « *Les Blockchains – De la théorie à la pratique, de l'idée à l'implémentation* » - Collection Epsilon Editions ENI – 01/2017
- EMILIE RAFFO – « *Le futur des espèces* » - Dunod – 09/2021
- ERIC HUGHES - « *A Cypherpunk's Manifesto* » - 09/03/1993, disponible à l'adresse suivante : <https://www.activism.net/cypherpunk/manifesto.html>
- EUROPOL – Communiqué de presse - « *Multi-million euro cryptocurrency laundering service Bestmixer.io taken down* », disponible à l'adresse suivante : <https://www.europol.europa.eu/media-press/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixer-io-taken-down>

- FRANCOIS VILLEROY DE GALHAU – Discours – « *La monnaie numérique de banque centrale (MNBC) et l'intermédiation bancaire à l'ère numérique* » - 12/07/2022, disponible à l'adresse suivante : <https://www.banque-france.fr/intervention/la-monnaie-numerique-de-banque-centrale-mnbc-et-lintermediation-bancaire-lere-numerique>
- FINBOLD - « *IRS launches 'Operation Hidden Treasure' to clamp down on crypto non-taxpayers* » - 16/06/2022, disponible à l'adresse suivante : <https://finbold.com/irs-launches-operation-hidden-treasure-to-clamp-down-on-crypto-non-taxpayers/>
- FLORIAN FREYSSENET - « *Immobilier 3.0 - De la pierre papier à la pierre crypto* » - 05/2022, disponible à l'adresse suivante : <https://drive.google.com/file/d/1FFmtltsIF8PREQa1yZePVRbXr37NKwy5/view>
- GARTNER - « *Gartner Hype Cycle for Blockchain and Web3, 2022* » - 07/2022, disponible à l'adresse suivante : <https://blogs.gartner.com/avivah-litan/2022/07/22/gartner-hype-cycle-for-blockchain-and-web3-2022/>
- JENNIFER BURNS, AMY STEELE, ERIC E. COHEN ET DR. SRI BURNSRAMAMOORT - DELOITTE - « *Blockchain and Internal Control: the COSO perspective* » - 07/2020, disponible à l'adresse suivante : <file:///C:/Users/chapo/Downloads/us-audit-blockchain-and-internal-control-the-coso-perspective.pdf>
- JOURNAL DU COIN - « *Au Kazakhstan, les mineurs de Bitcoin doivent passer à l'enregistrement* » - 06/05/2022, disponible à l'adresse suivante : <https://journalducoin.com/bitcoin/kazakhstan-mineurs-bitcoin-btc-enregistrement-regulation/>
- LA FINANCE POUR TOUS - « *Le Salvador a-t-il eu raison d'adopter le bitcoin comme monnaie officielle* » - 04/05/2022, disponible à l'adresse suivante : <https://www.lafinancepourtous.com/2022/05/04/le-salvador-a-t-il-eu-raison-dadopter-le-bitcoin-comme-monnaie-officielle/>
- LA FINANCE POUR TOUS – « *Qu'est-ce que la blockchain ?* » - 30/07/2021, disponible à l'adresse suivante : <https://www.lafinancepourtous.com/decryptages/finance-et-societe/nouvelles-economies/blockchain/quest-ce-que-la-blockchain/>
- LAURENT LELOUP – « *Blockchain, la révolution de la Confiance* » - Eyrolles – 05/2021
- LEDEVOIR - « *Inculpations pour délit d'initié sur Coinbase, une première dans les cryptomonnaies* » - 22/07/2022, disponible à l'adresse suivante : <https://www.ledevoir.com/economie/736728/cryptomonnaie-inculpations-pour-delit-d-initie-sur-coinbase-une-premiere-dans-les-cryptomonnaies>
- LES ECHOS – SADRY BOUHEJBA – « *Opinion / Internet et blockchain : d'une révolution à l'autre* » - 03/05/2019, disponible à l'adresse suivante : <https://www.lesechos.fr/idees-debats/cercle/opinion-internet-et-blockchain-dune-revolution-a-lautre-1015930>
- LE MONDE - « *Libra : tout ce qu'il faut savoir sur la cryptomonnaie de Facebook* » - 18/06/2019, disponible à l'adresse suivante : https://www.lemonde.fr/pixels/article/2019/06/18/ce-qu-il-faut-savoir-sur-le-libra-la-cryptomonnaie-de-facebook_5477887_4408996.html
- LE MONDE - Maxime VAUDANO - « *La première blockchain de l'histoire date de 1995, et elle est imprimée sur papier* » - 01/09/2018, , disponible à l'adresse suivante : https://www.lemonde.fr/big-browser/article/2018/09/01/la-premiere-blockchain-de-l-histoire-date-de-1995-et-elle-est-imprimee-sur-papier_5349082_4832693.html

- LE MONDE - Michel BAUWENS - « *Un rêve technocratique totalitaire* » - 15/04/2016, disponible à l'adresse suivante : https://www.lemonde.fr/economie/article/2016/04/18/michel-bauwens-un-reve-technocratique-totalitaire_4904154_3234.html
- LSA COMMERCE CONNECTE – « *Carrefour applique la blockchain à ses produits bio de marque propre* » - 13/04/2022, disponible à l'adresse suivante : <https://www.lsa-conso.fr/carrefour-applique-la-blockchain-a-ses-produits-bio-de-marque-propre,408776>
- L'USINE DIGITALE - « *DAO perd 50 millions de dollars lors d'un piratage* » - 17/06/2016, disponible à l'adresse suivante : <https://www.usine-digitale.fr/article/dao-perd-50-millions-de-dollars-lors-d-un-piratage.N397787>
- L'USINE DIGITALE – « *Renault déploie une blockchain pour tracer et certifier la conformité des pièces de ses voitures* » - 10/09/2021, disponible à l'adresse suivante : <https://www.usine-digitale.fr/editorial/renault-deploie-une-blockchain-pour-tracer-et-certifier-la-conformite-des-pieces-de-ses-voitures.N1002224>
- MATTHIEU QUINIOU – « *L'avènement de la désintermédiation* », Iste Editions – 07/2019
- NUMERAMA - « *Les vols de plateformes de crypto continuent : BitMart a perdu 150 millions de dollars* » - 06/12/2021, disponible à l'adresse suivante : <https://www.numerama.com/cyberguerre/761891-les-vols-de-plateformes-de-crypto-continuent-bitmart-a-perdu-150-millions-de-dollars.html>
- OLIVIER DESPLEBIN, GULLIVER LUX, NICOLAS PETIT – MANAGEMENT & AVENIR 2018/5 - « *L'évolution de la comptabilité, du contrôle, de l'audit et de leurs métiers au prisme de la Blockchain : une réflexion prospective* » - pages 137 à 157, disponible à l'adresse suivante : <https://www.cairn.info/revue-management-et-avenir-2018-5-page-137.htm>
- OLIVIER DESPLEBIN, GULLIVER LUX, NICOLAS PETIT – MANAGEMENT & AVENIR 2018/5 - « *L'évolution de la comptabilité, du contrôle, de l'audit et de leurs métiers au prisme de la Blockchain : une réflexion prospective* » - pages 137 à 157, disponible à l'adresse suivante : <https://www.cairn.info/revue-management-et-avenir-2018-5-page-137.htm>
- PASCAL DE LIMA - FORBES - « *La Conformité Bancaire A L'Heure De La Blockchain* » - 11/09/2019, disponible à l'adresse suivante : <https://www.forbes.fr/finance/la-conformite-bancaire-a-lheure-de-la-blockchain/>
- PWC - « *Blockchain & crypto : comment les entreprises en tirent enfin bénéfice* » - Edition 2022, disponible à l'adresse suivante : <https://www.pwc.fr/fr/publications/blockchain/blockchain-crypto-comment-les-entreprises-en-tirent-enfin-benefice.html>
- SATOSHI NAKAMOTO - Livre blanc - « *Bitcoin: A Peer-to-Peer Electronic Cash System* » - 31/10/2008, disponible à l'adresse suivante : <https://nakamotoinstitute.org/bitcoin/>
- SHEER ANALYTICS & INSIGHTS – « *Blockchain Technology Market - Market insights, analysis, trends, and forecast 2021-2031* » - 10/2021, disponible à l'adresse suivante : <https://www.sheeranalyticsandinsights.com/market-report-research/global-blockchain-technology-market-global-industry-analysis-21>
- SIECLEDIGITAL - « *Un ancien employé d'OpenSea accusé d'un délit d'initié lié aux NFT* » - 04/06/2022, disponible à l'adresse suivante : <https://siecledigital.fr/2022/06/04/un-ancien-employe-dopensea-accuse-dun-delit-dinitie-lie-aux-nft/>

- PWC - « *Financial Services Technology 2020 and Beyond: Embracing disruption* », disponible à l'adresse suivante : <https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf>
- PWC – « *Global PwC CBDC Index 2021 : vers une adoption mondiale des monnaies digitales de banque centrale - Enjeux des nouvelles infrastructures monétaires et opportunités pour les entreprises* » - 03/2021, disponible à l'adresse suivante : <https://www.pwc.fr/fr/publications/blockchain/monnaies-digitales-de-banque-centrale.html>
- RENAULT – Communiqué de presse - « *XCEED : une nouvelle solution de blockchain pour les usines Renault en Europe* » - 06/07/2021, disponible à l'adresse suivante : <https://www.renaultgroup.com/news-onair/actualites/xceed-e2-80-af-une-nouvelle-solution-de-blockchain-pour-les-usines-renault-en-europe/>
- THE DEPARTMENT OF TREASURY - Rapport - « *Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art* » - 02/2022, disponible à l'adresse suivante : https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf
- THOMAS FEAT - OPTION FINANCE - « Les directions financières découvrent la blockchain » - 16/07/2021, disponible à l'adresse suivante : <https://www.optionfinance.fr/innovation/les-directions-financieres-decouvrent-la-blockchain.html>
- THE ECONOMIST - « *The Trust Machine* » - 31/10/2015, disponible à l'adresse suivante : <https://www.economist.com/leaders/2015/10/31/the-trust-machine>
- THOMSON REUTERS - « *Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity* » - 09/05/2016, disponible à l'adresse suivante : <https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html>
- TRACFIN - « *TRACFIN 2021 - Activité et analyse* » - 2021, disponible à l'adresse suivante : https://www.economie.gouv.fr/files/2022-07/Tracfin_2021_Web.pdf?v=1658933771
- TRACFIN - « *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2016* », 2016 - disponible à l'adresse suivante : <https://www.economie.gouv.fr/files/rapport-analyse-tracfin-2016.pdf>
- US EXECUTIVE ORDER - « *Executive Order on Ensuring Responsible Development of Digital Assets* » - 09/03/2022, disponible à l'adresse suivante : <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/>
- WAVESTONE - Livre Blanc - « *Supply Chain x Blockchain* » – 06/2021, disponible à l'adresse suivante : <https://www.wavestone.com/app/uploads/2021/06/Livre-blanc-Supply-Chain-x-Blockchain.pdf>
- WEBINAR IFACI – « *Cryptoactifs : perspectives et risques* » - 24/03/2022
- ZONEBOURSE - « *La banque centrale russe accorde à Sberbank une licence pour émettre et échanger des actifs numériques* » - 17/03/2022, disponible à l'adresse suivante : <https://www.zonebourse.com/cours/action/PJSC-SBERBANK-6494829/actualite/La-banque-centrale-russe-accorde-a-Sberbank-une-licence-pour-emettre-et-echanger-des-actifs-numeriqu-39795250/>

- 01 NET – « *Hydra, plus grande place de marché du Darknet et machine à blanchir les bitcoins, démantelée par la police* » - 07/04/2022, disponible à l'adresse suivante : <https://www.01net.com/actualites/hydra-plus-grande-place-de-marche-du-darknet-et-machine-a-blanchir-les-bitcoins-demantelee-par-la-police-2055811.html>