ACCOMPAGNER LA RÉVOLUTION

BLOCKCHAIN

& RÈGLEMENTER LES

CRYPTO-MONNAIES

Les études du Centre Jean Gol *www.cjg.be*

Cette étude a été portée par **Olaf van der Straten**, collaborateur au Sénat et **Laurent Carra**, étudiant. Elle a été coécrite et supervisée par **Corentin de Salle**, Directeur scientifique du Centre Jean Gol.

Je les en remercie.

Je remercie également **Pierre Brassinne**, conseiller au Centre Jean Gol pour son travail de documentation. Je remercie **Jean-Vianney Philippe**, Senior Vice President, Head of digital at Weber Shandwick, **Jolan Vereecke**, conseiller spécial du président du MR, **Philippe Moraldo**, conseiller au cabinet du Secrétaire d'Etat Mathieu Michel et **Mathieu Bihet**, député fédéral pour leur aide et leurs conseils.

Je remercie également **Marc Toledo**, managing director de la plateforme Bit4You, **Thibaut Verbiest**, avocat, essayiste et entrepreneur crypto, **Axel Legay**, professeur à l'Université Catholique de Louvain, ingénieur spécialisé dans la cybersécurité, **Claudia Lomma**, journaliste spécialisée dans le métaverse, **Gilles Quoistiaux**, journaliste à l'Echo et essayiste spécialisé dans le digital et **Faustine Fleuret**, présidente et CEO de l'ADAN (Association pour le Développement des Actifs Numériques) pour le temps et la précieuse expertise qu'ils ont partagés généreusement avec nos collaborateurs.

Je remercie enfin **Mathieu Michel**, Secrétaire d'Etat au numérique pour son intérêt, son aide, son expertise et ses conseils.

Je vous souhaite une excellente lecture de ce numéro des Études du Centre Jean Gol.

DANIEL BACQUELAINE
Administrateur délégué

Les Études du Centre Jean Gol sont le fruit de réflexions entre collaborateurs du CJG, des membres de son comité scientifique, des spécialistes, des mandataires et des représentants de la société civile.
Accessibles à tous, elles sont publiées sous version électronique et sous version papier.

résumé

Les partisans de la blockchain et des cryptomonnaies, application la plus connue de cette technologie, estiment que ces innovations ont le potentiel de changer profondément nos sociétés. En effet, les registres de données décentralisés permettent d'échanger, entre particuliers, des informations qui sont infalsifiables, indélébiles et ne nécessitant pas de tiers de confiance. Cela peut paraître anecdotique, mais comme nous le voyons dans cette étude, cette faculté offre d'innombrables possibilités.

La première partie est consacrée à la blockchain en tant que telle. Nous commençons par présenter cette technologie, son historique, ses caractéristiques et ses composantes. Ensuite, nous présentons des cas d'usages, dont certains sont fonctionnels, d'autres en phase test ou encore non implémentés. Ces exemples permettent d'appréhender l'étendue des possibilités et leur diversité. Ensuite, nous abordons les risques liés à cette technologie. Notamment, en termes de consommation énergétique, car ce point concentre la majorité des critiques faites à cette innovation.

La seconde partie traite des cryptomonnaies, qui ont popularisé la technologie blockchain. Leur historique, leur fonctionnement et les principales cryptomonnaies sont présentés. Suite à cela, nous abordons les risques associés à ces valeurs numériques. En particulier, nous discutons des dangers qu'elles peuvent représenter pour les acheteurs lambda. Nous concluons également cette seconde partie par des propositions concrètes.

Une étude réalisée par **OLAF VAN DER STRATEN, LAURENT CARRA & CORENTIN DE SALLE**

INTRODUCTION

Corentin de Salle

Les cryptomonnaies font beaucoup parler d'elles. La première d'entre elles, le bitcoin, est née en 2009. Suite à la crise financière de 2008, ses concepteurs posent un constat : si les banques centrales ne savent pas gérer la monnaie, autant la gérer nous-mêmes. En effet, une cryptomonnaie est décentralisée : elle n'est ni émise ni règlementée par une autorité centrale. Mais bien par la communauté de ses utilisateurs. Elle court-circuite les intermédiaires. Ainsi, les banques sont hors-jeu car la monnaie s'échange en dehors d'elles, « peer-to-peer », de particulier à particulier.

Bitcoin compte quantité de petites sœurs. On dénombre aujourd'hui pas moins de 20.000 cryptomonnaies ! La plupart sont éphémères voire farfelues mais cette vitalité dénote une activité économique en ébullition dans un écosystème qui se structure de plus en plus en passant par d'inévitables maladies de jeunesse.

Aujourd'hui, plus de 200 millions de personnes dans le monde - dont 500.000 Belges - détiennent des cryptomonnaies. C'est un investissement risqué en raison de son extrême volatilité. Mais s'agit-il réellement de « monnaies » ? Plusieurs experts préfèrent parler de « cryptoactifs » car on ne peut pas encore acheter avec elles des produits de consommation courante.

Assiste-t-on à une bulle spéculative ? Beaucoup le pensent. Mais la vérité est qu'aucune bulle financière n'a jamais duré dix ans comme c'est le cas des cryptomonnaies. Surtout quand, en dépit de chutes brutales et sporadiques, le cours de ces cryptoactifs ne cesse d'augmenter depuis 13 ans.

Pourquoi s'intéresser à ces prétendues « monnaies » ? Pour au moins trois raisons.

Premièrement, parce que les cryptomonnaies sont l'application la plus visible d'une technologie révolutionnaire dont la signification et les potentialités débordent largement de ces dernières : la technologie blockchain. Cette technologie va probablement jouer un rôle très important dans le futur et il s'avère indispensable d'en comprendre le fonctionnement aujourd'hui. Il sera amplement question de cette technologie et de son potentiel dans la présente étude.

Deuxièmement, les cryptomonnaies sont nées en vertu d'un projet philosophique libertarien de décentralisation. Elles ont initialement pour ambition d'affranchir les individus des politiques monétaires centralisatrices et de reconstituer un outil à vocation mondiale et qui ne fait plus dépendre d'un Etat les utilisateurs d'une monnaie. Cet idéal s'est affadi avec le temps mais la volonté de décentralisation est au cœur du web 3.0 qui est en train d'apparaître.

Troisièmement, derrière les cryptoactifs se profile tout un écosystème d'entreprises proposant différents services en pleine gestation et basés sur la technologie blockchain, sorte de gigantesque registre public, décentralisé et transparent qui assure aux transactions anonymes une sécurisation et une traçabilité à toute épreuve.

Ainsi, la « DEFI » (ou finance décentralisée) est un univers qui voit aujourd'hui se développer une myriade de systèmes de prêt, d'assurance, de protection des données, d'authentification de la propriété et même de smart contract (ou « contrats intelligents ») qui permettent d'activer automatiquement des dispositifs quand des conditions contractuelles surviennent durant une période considérée.

La finance décentralisée permet aujourd'hui une démocratisation de la finance. Ce n'est pas sans dangers car cela met à la merci d'influenceurs peu scrupuleux une masse de personnes qui, en manipulant simplement leur smartphone, achètent et revendent des actifs. Personnes qui, auparavant, n'auraient jamais accédé à ce monde assez fermé et hermétique aux non-initiés. Mais cela permet aussi d'assurer plus de transparence de l'information qui cesse ainsi d'être le monopole de milieux dit « bien informés » qui sont ceux de l'establishment. On assiste, par exemple, à un engouement chez les « cryptonatives » pour les achats « fractionnés ». La technologie permet désormais, par exemple, d'acheter (et de vendre) aisément un fragment d'immeuble situé ailleurs dans le monde et de toucher un fragment du loyer.

Comme le précise le professeur Mikael Petitjean,[1] ce qui est positif, c'est une plus grande liquidité dans les actifs. On peut les échanger beaucoup plus facilement qu'avant. Des actifs à la fois matériels (maison qu'on peut fragmenter) mais aussi des actifs numérisés (des œuvres d'art numérique : la technologie permet de les rémunérer de façon beaucoup plus optimale, sûre et rapide).

1 Propos tenus par l'intéressé dans le cadre d'une conférence donnée au siège du Mouvement Réformateur le 29 juin 2022

Au tiers-monde, la technologie blockchain permet, par exemple, d'assurer la bancarisation du tiers-monde. En effet, aujourd'hui, 1,7 milliards de personnes dans le monde ne peuvent accéder au secteur bancaire car trop onéreux pour elles : elles dépendent alors totalement du secteur bancaire clandestin et illégal pratiquant des taux usuraires. Heureusement, la blockchain RCN pourrait désormais permettre à certains d'entre eux d'accéder, via des smart contracts, à des prêts à faible coût d'un secteur légal et reconnu.

Les cryptoactifs ne sont peut-être pas une monnaie dans le monde réel mais ils permettent d'acheter quantité de choses (des objets numériques) dans un univers virtuel qui se développe parallèlement, à savoir le métaverse. C'est l'objet d'une autre étude publiée, parallèlement à celle-ci, par le Centre Jean Gol.

PARTIE I : LA BLOCKCHAIN

I. DÉFINITION ET HISTORIQUE

DÉFINITION

Étant l'une des infrastructures fondamentales du métavers, la **blockchain**, ou chaîne de blocs en français, peut être définie comme étant une technologie transparente et sécurisée de stockage et de transmission d'informations, fonctionnant sans organe de contrôle[2].

Elle constitue une base de données numérique infalsifiable qui contient l'historique de tous les échanges effectués entre ses utilisateurs et ce, depuis sa création[3]. La blockchain est ainsi partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne.

Il existe tant des **blockchains publiques**, ouvertes et accessibles à tous, que des **blockchains privées**, dont l'accès et l'utilisation sont limités à un nombre restreint d'acteurs[4]. Les **blockchains dites « à consortium »** représentent quant à elles des blockchains hybrides se situant entre chaînes publiques et privées [*figure 1*][5].

Figure 1 : Types de blockchain[6]

TYPES 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 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

2 Jeanneau Clément et al., ***La Blockchain décryptée****, Paris, Netexplo, 2016, p. 1.*

3 Pignel Marion, « La technologie blockchain : une opportunité pour l'économie sociale ? », ***Pour la Solidarité****, 2019, p. 4.*

4 Jeanneau Clément et al., ***La Blockchain décryptée****,* ***op. cit.****, p. 7.*

5 « Blockchain Privées, Publiques et à Consortium – Quelles sont les différences ? », ***Binance Academy****, 6 janvier 2020, disponible à l'adresse suivante : www.academy.binance.com/fr/articles/private-public-and-consortium-blockchains-whats-the-difference (consultée le 4 avril 2022).*

6 « Blockchain Privées, Publiques et à Consortium – Quelles sont les différences ? », ***op. cit.***

Une blockchain publique peut être dès lors assimilée à un vaste registre public, anonyme et infalsifiable. L'informaticien et mathématicien Jean-Paul Delahaye propose de l'imaginer plus simplement comme *« 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 »*[7].

L'**absence d'autorité centrale** apparaît sans doute comme l'élément le plus caractéristique des blockchains, voire des réseaux distribués au sens large. Leurs utilisateurs placent ainsi leur confiance dans de telles technologies, plutôt que dans un intermédiaire comme de manière traditionnelle. Dès lors, telles qu'émises par Poullet et Jacquemin, deux questions se posent : Comment créer de la confiance alors qu'aucune autorité centrale n'existe ? Comment s'assurer que toute évolution du registre distribué soit fiable et sécurisée tout en restant transparente pour tous les membres du réseau ?[8]

HISTORIQUE

L'architecture derrière la technologie de la blockchain est décrite dès 1991 par Stuart Haber et W. Scott Stornetta[9]. Ces deux chercheurs ont en effet mis en application une solution informatique permettant l'horodatage de documents numériques afin que ceux-ci ne soient jamais antidatés ou falsifiés. Par la suite, en 1992, le concept d'arbre de Merkle est incorporé à leur système, rendant son fonctionnement plus efficace en permettant à plusieurs documents d'être rassemblés en un seul bloc[10].

D'après le chercheur Ittai Abraham, le premier système de certification décentralisé est par ailleurs celui de la société *Surety* (fondée par ces mêmes Haber et Stornetta) qui, depuis 1995, publie hebdomadairement un certificat cryptographique de sa base de données dans la rubrique « Annonces et objets trouvés » du journal The New York Times (rendant ainsi impossible pour quiconque d'antidater ou d'altérer les dépôts)[11].

En 2004, l'informaticien Hal Finney lance un système appelé « Reusable Proof of Work » (RPoW) que l'on peut considérer comme un premier prototype et une première étape dans l'histoire des cryptomonnaies[12].

La première chaîne de blocs en tant que technologie n'a donc été conceptualisée que récemment, en 2008, par une personne ou une équipe connue sous le pseudonyme de Satoshi Nakamoto. Sur base de cette blockchain sera créé un an plus tard le Bitcoin tel que nous le connaissons aujourd'hui et qui popularisera cette technologie. Gagnant de plus en plus d'attention auprès du grand public et étant déjà utilisée dans une multitude d'applications, la technologie blockchain est en passe de bouleverser nos habitudes et les relations que nous entretenons avec les institutions centralisées.

---

*7 « Blockchain », **CNIL**, disponible à l'adresse suivante : www.cnil.fr/fr/definition/blockchain (consultée le 17 février 2022).*

*8 Poullet Yves et Jacquemin Hervé, « Blockchain : une révolution pour le droit ? », **Journal des Tribunaux**, 2018, vol. 36, n°6748, p. 802-803.*

*9 « L'histoire de la Blockchain », **Binance Academy**, 6 décembre 2018, disponible à l'adresse suivante : www.academy.binance.com/fr/articles/history-of-blockchain (consultée le 4 avril 2022).*

*10 **Ibid.***

*11 Vaudano Maxime, « La première blockchain de l'histoire date de 1995, et elle est imprimée sur papier », **Le Monde**, disponible à l'adresse suivante : 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 (consultée le 4 avril 2022).*

*12 « L'histoire de la Blockchain », **Binance Academy**, **op. cit.***

II. QUELLES SONT LES COMPOSANTES DE LA BLOCKCHAIN ?

La blockchain est la combinaison de **trois principales composantes** :

1. un registre distribué peer-to-peer s'appuyant sur
2. la cryptographie asymétrique et sur
3. un processus de validation.

Ces différentes composantes garantissent un niveau élevé de sécurité et permettent par conséquent de mieux comprendre la confiance accordée de la part des utilisateurs envers cette technologie.

1. LA BLOCKCHAIN FONCTIONNE SOUS LA FORME D'UN REGISTRE DISTRIBUÉ (DISTRIBUTED LEDGER, DL)

Cela signifie que chaque nœud (ou participant actif) du réseau possède une copie du registre qu'il peut consulter ou modifier en résolvant un problème cryptographique.

Aucun organe central de contrôle n'est ainsi requis. Par extension, un tel registre repose sur un réseau de type **peer-to-peer** (pair-à-pair ou P2P), où chaque entité est à la fois client et serveur (contrairement au modèle client-serveur traditionnel).

Autrement dit, un registre distribué peut être perçu comme un « grand livre comptable » qui enregistre et gère les données de tous les utilisateurs d'un réseau, et qui est reproduit ou reproductible en temps réel en chaque point du réseau.[13]

Un aspect important de la sécurité offerte par la blockchain réside dans ce caractère « distribué » des données, qui se différencie d'une base de données centralisée. En effet, pour falsifier les informations, celles-ci devront être modifiées sur tous les nœuds du réseau où la base de données est répliquée, ce qui est difficilement envisageable, voire impossible.

Il est important de noter que la blockchain ne constitue qu'un type de technologies de registres distribués (Distributed Ledger Technology, **DLT**)[14]. Les réseaux utilisant la DLT peuvent en effet ne pas recourir à la blockchain spécifiquement. S'ils le font néanmoins, le registre se structure alors comme une suite chronologique de « blocs » constatant les opérations et se liant les uns aux autres pour former une « chaîne de blocs », la blockchain[15].

2. DANS LA BLOCKCHAIN, LES INFORMATIONS STOCKÉES DANS LES BLOCS SONT PROTÉGÉES PAR UN SYSTÈME DE CRYPTOGRAPHIE ASYMÉTRIQUE

Cela leur permet d'assurer leur intégrité et leur confidentialité. En effet, pour avoir accès aux données ou pour pouvoir les modifier, il est nécessaire de disposer non seulement d'une clé publique mais également d'une clé privée. Par convention, la clé de chiffrement du message désigne la clé publique, connue de tous, et la clé de déchiffrement du message correspond à la clé privée, connue uniquement par son titulaire[16].

À l'aide d'une clé publique, l'expéditeur code dans un algorithme de chiffrement un message qui ne pourra être décodé ou résolu que par le destinataire détenteur d'une clé privée, donnée en entrée d'un algorithme de déchiffrement. Il en résulte que le récepteur du message pourra ainsi décoder la transaction à travers l'utilisation de la cryptographie asymétrique.

---

13 ***Ibid.***

*14 « Difference Blockchain and DLT », **Marco Polo Network**, 31 janvier 2018, disponible à l'adresse suivante : www.marcopolonetwork.com/distributed-ledger-technology/ (consultée le 4 avril 2022).*

*15 Poullet Yves et Jacquemin Hervé, « Blockchain : une révolution pour le droit ? », **op. cit.**, p. 803.*

*16 « Cryptographie asymétrique : tout sur la méthode de chiffrement », **Journal du Net**, 11 février 2019, disponible à l'adresse suivante : www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1209336-cryptographie-asymetrique/ (consultée le 4 avril 2022).*

3. UN PROCESSUS DE VALIDATION

En réalité, différents **processus de validation** sont à l'œuvre dans les blockchains. Dans ces processus, les « mineurs » – les acteurs du réseau – valident les diverses transactions en s'assurant de l'identité et de la capacité des émetteurs de transactions à effectuer celles-ci. Cette validation est opérée selon les règles de fonctionnement de la blockchain adoptées par consensus.

Les deux mécanismes de validation les plus importants sont la preuve de travail (*proof-of-work*) et la preuve d'enjeu (*proof-of-stake*).

Concernant la **preuve de travail**, il implique que les mineurs qui proposent de nouveaux blocs démontrent, en résolvant des problèmes mathématiques complexes, qu'ils ont consacré un effort suffisant, prenant la forme d'une dépense de puissance de calcul. Ce mécanisme permet ainsi d'éviter les blocs frauduleux et de décourager les nœuds malveillants. Une récompense est octroyée au premier mineur ayant réussi à valider un bloc lui-même ensuite validé par au moins 51 % des mineurs[17]. Le « minage » est l'appellation qui désigne cette opération de validation.

Il est à noter que seuls les équipements d'une très grande force de calcul permettent aux mineurs de résoudre la complexité des calculs[18]. De plus, la preuve de travail est le mécanisme de validation le plus ancien et est utilisé notamment par la blockchain du Bitcoin, la plus importante cryptomonnaie. Il fait aujourd'hui l'objet de débats en raison de ses coûts économiques et écologiques non négligeables.

Concernant la **preuve d'enjeu**, la validation dépend non plus de la force de calcul détenue mais bien de la quantité de cryptomonnaies que l'investisseur possède. En effet, pour avoir une chance de valider les blocs et de toucher une récompense, celui-ci doit apporter la preuve de détention de cryptomonnaie par une mise en gage. L'algorithme « proof-of-stake » choisit ensuite parmi les investisseurs éligibles quel sera celui qui obtiendra le droit de valider le prochain bloc de la blockchain[19]. Le principe dans ce mécanisme de validation est le suivant : plus une personne possède de cryptomonnaies, moins celle-ci a intérêt à falsifier la blockchain[20].

La preuve d'enjeu possède l'avantage d'être plus écologique et performante que la preuve de travail. En effet, à l'inverse de cette dernière, la preuve d'enjeu ne nécessite pas un équipement de minage coûteux et excessivement énergivore. L'autre grand avantage de cette méthode cryptographique réside dans la sécurité et la décentralisation plus marquées qu'elle permet : une poignée de mineurs ne peuvent détenir la majorité des infrastructures.[21]

---

*17 Poullet Yves et Jacquemin Hervé, « Blockchain : une révolution pour le droit ? », **op. cit.**, p. 803.*

*18 **Ibid.***

*19 Launay Vincent, « Qu'est-ce que la preuve d'enjeu ? », **Central Charts**, 3 décembre 2018, disponible à l'adresse suivante : www.centralcharts.com/fr/gm/1-apprendre/1-crypto-monnaie/44-minage/930-proof-of-stake-preuve-enjeu-participation (consultée le 4 avril).*

*20 Gayte Aurore, « L'Ethereum va passer à la « proof of stake » : tout comprendre à cette révolution dans les cryptomonnaies », **Numerama**, 15 août 2021, disponible à l'adresse suivante : www.numerama.com/tech/713345-lethereum-passe-a-la-proof-of-stake-tout-comprendre-a-cette-revolution-dans-les-cryptomonnaies.html (consultée le 4 avril 2022).*

*21 « Qu'est-ce que la preuve d'enjeu dans la blockchain ? », **Business AM**, 29 août 2018, disponible à l'adresse suivante : www.fr.businessam.be/quest-ce-que-la-preuve-denjeu-dans-la-blockchain/ (consultée le 4 avril 2022).*

III. A QUOI SERVENT LES BLOCKCHAINS ?

En raison de ces trois composantes techniques, plusieurs **caractéristiques** peuvent être associées à la blockchain :

- désintermédiation et décentralisation ;
- traçabilité et transparence ;
- immuabilité et caractère infalsifiable ;
- autonomie,
- sécurité et
- confiance[22].

Toutes ces caractéristiques rendent ainsi compte du potentiel innovateur de cette technologie.

Trois fonctions principales sont généralement retirées de la technologie blockchain[23].

La première consiste à servir de registre de données.

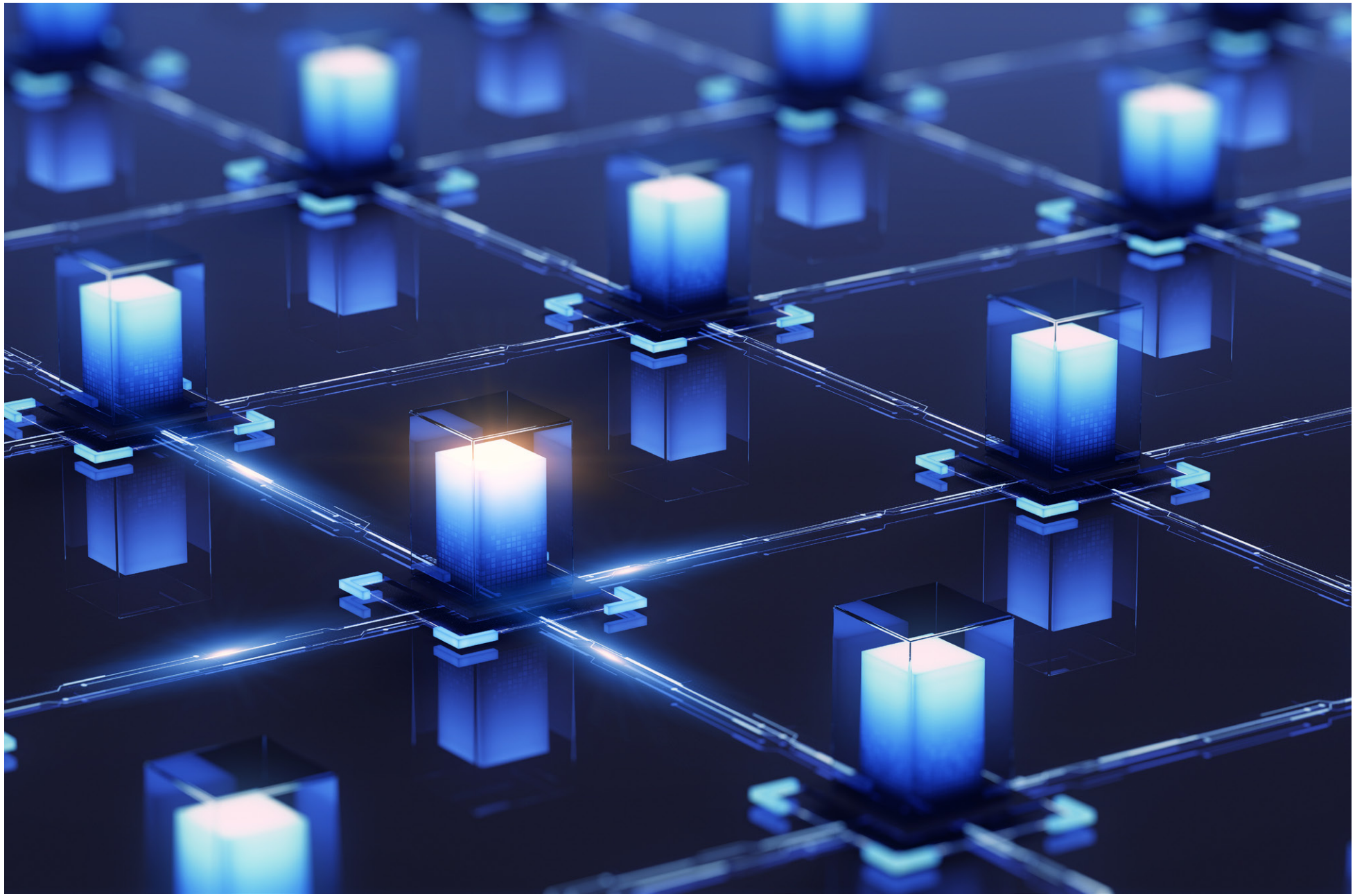
Complémentaires à la première, les deux autres fonctions portent sur le transfert de cryptoactifs et/ou l'exécution automatique de certaines opérations, par le recours à des smart contracts[24].

La blockchain est à la base des cryptomonnaies, dont sa première application est celle liée au Bitcoin depuis 2009. Mais au-delà de son aspect monétaire, cette technologie possède un **fort potentiel d'application** dans de nombreux autres domaines de la vie économique, sociale et publique, tels que :

- Des applications basées sur des smart contracts (exécutant automatiquement des actions validées au préalable par les parties prenantes) ;
- Des moyens de réduire les coûts de paiements et les coûts de transaction ;
- Le développement d'assurances peer-to-peer ;
- La gestion et la protection tant de la création que de l'exploitation des œuvres et des inventions ;
- La traçabilité et l'authenticité de produits divers ;
- Les énergies alternatives et le phénomène de l'autoproduction de l'énergie ;
- Le vote électronique (e-voting) et le gouvernement électronique (e-gouvernement) ;
- L'économie collaborative ;
- Etc.

Plus généralement, le potentiel de la blockchain pourrait s'appliquer à tous les domaines impliquant un échange, une sauvegarde ou même une preuve, ce qui pourrait donner lieu à des usages révolutionnaires dans de nombreux aspects de notre société[25].

*22 Pignel Marion, « La technologie blockchain : une opportunité pour l'économie sociale ? », **op. cit.**, p. 5-6.*
*23 Jeanneau Clément et al., **La Blockchain décryptée**, **op. cit.**, p. 10-11.*
*24 Mahabir Amanda, « Quelles sont les fonctions de la Blockchain ? », **Articlaw**, 22 novembre 2018, disponible à l'adresse suivante : www.articlaw.net/publications/legal/quelles-sont-les-fonctions-de-la-blockchain/*
*25 Pignel Marion, « La technologie blockchain : une opportunité pour l'économie sociale ? », **op. cit.**, p. 7.*



IV. QUATRE CONCEPTS CLÉS DE LA BLOCKCHAIN : DEFI, SMART CONTRACTS, DAO & NFT

Quatre concepts clés doivent encore être introduits :

1. la finance décentralisée (DeFi),
2. les contrats intelligents (smart contracts) et
3. l'organisation autonome décentralisée (DAO).
4. Les jetons non fongibles (non-fungible tockens : NFT)

1. DEFI, OU FINANCE DÉCENTRALISÉE

Il s'agit d'un écosystème financier basé sur la technologie blockchain. Il permet aux utilisateurs d'acheter et de vendre des actifs et des services financiers sous la forme d'investissement ou de financement sans intermédiaire.[26]

Comme nous l'avons vu précédemment, la blockchain relie ici les utilisateurs sans serveur central et transfère des données et actifs en toute sécurité, sous le regard des utilisateurs eux-mêmes. De plus, les transactions sont régies par des « smart contracts », c'est-à-dire des programmes informatiques qui utilisent également la blockchain et s'exécutent automatiquement lorsque les paramètres fixés à l'avance par les parties sont respectés (nous y reviendrons). Autrement dit, la blockchain est utilisée pour stocker et transférer des actifs numériques tandis que les contrats intelligents permettent de s'assurer que les parties respectent leur part du marché.[27]

Phénomène récent, le potentiel et l'utilisation de DeFi dépendront largement des besoins des utilisateurs et de la réglementation. Les particuliers et les entreprises investissent et obtiennent des fonds grâce aux **applications décentralisées, ou dApps**, qui font le lien entre l'offre et la demande, en utilisant la blockchain pour garantir la sécurité des transactions[28].

Les dApps ont un code ouvert, ce qui signifie que toute personne disposant d'Internet peut utiliser, créer, et proposer des services, ainsi que combiner des services existants[29]. Les logiciels et systèmes DeFi sont mis (gratuitement) à la disposition du public et peuvent même être copiés, améliorés ou adaptés aux besoins des utilisateurs.

Pour accéder à ces dApps, un portefeuille virtuel est nécessaire pour stocker des jetons. Les utilisateurs de la finance décentralisée qui cherchent un retour sur investissement en jetons peuvent dès lors programmer un contrat intelligent pour vendre des cryptomonnaies à un certain prix. Et les utilisateurs qui souhaitent acheter des jetons peuvent préparer un contrat intelligent pour les acquérir automatiquement lorsqu'ils atteignent la valeur souhaitée. Dans les deux cas, les transactions sont automatiques et il n'y a pas d'intermédiaire.

À long terme, la finance décentralisée pourrait par conséquent rendre obsolète un grand nombre d'activités nécessitant de passer par des intermédiaires[30]. Malgré son avenir très prometteur, DeFi a néanmoins un long chemin à parcourir, particulièrement en ce qui concerne son adoption par le grand public.

*26 « What is decentralized finance? », **Santander**, 3 mai 2022, disponible à l'adresse suivante : www.santander.com/en/stories/decentralized-finance (consultée le 5 mai 2022).*

*27 **Ibid.***

*28 « Qu'est-ce que la DeFi ? », **Coinbase**, disponible à l'adresse suivante : www.coinbase.com/fr/learn/crypto-basics/what-is-defi (consultée le 26 avril 2022).*

*29 Wojno Marc, « Qu'est-ce que DeFi ? Tout ce que vous devez savoir sur la finance décentralisée », **ZDNet**, 20 janvier 2022, disponible à l'adresse suivante : www.zdnet.fr/pratique/qu-est-ce-que-defi-tout-ce-que-vous-devez-savoir-sur-la-finance-decentralisee-39936009.htm (consultée le 26 avril 2022).*

*30 Ichbiah Daniel, « DeFi : qu'est-ce que c'est ? », **Futura Tech**, disponible à l'adresse suivante : www.futura-sciences.com/tech/definitions/cryptomonnaies-defi-19670/ (consultée le 26 avril 2022).*

2. LES CONTRATS INTELLIGENTS, OU « SMART CONTRACTS »

Il s'agit de programmes stockés sur une blockchain qui s'exécutent lorsque des conditions prédéterminées sont remplies. Ils sont généralement utilisés pour automatiser l'exécution d'un accord afin que tous les participants puissent être immédiatement certains du résultat, sans intervention d'un intermédiaire, ni perte de temps. Ils peuvent également automatiser un flux de travail, en déclenchant l'action suivante lorsque les conditions sont remplies.[31]

À la différence d'un contrat traditionnel dont l'exécution est régie par un cadre juridique, celle du smart contract est, en tant que protocole informatique, régie par le code informatique[32]. Comme pour chaque programme informatique, la complexité est variable d'un contrat intelligent à un autre. Certains fonctionnent en suivant des conditions simples de type « if this... then that... » écrites en code sur une blockchain, alors que d'autres sont davantage complexes.

Un réseau d'ordinateurs exécute ensuite les actions lorsque les conditions prédéterminées ont été remplies et vérifiées. Ces actions peuvent inclure le déblocage de fonds aux parties concernées, l'envoi de notifications, l'enregistrement d'un véhicule, ou encore l'émission d'un ticket. La blockchain est enfin mise à jour lorsque la transaction est terminée. Cela signifie que la transaction ne peut pas être modifiée, et que seules les parties qui ont reçu l'autorisation peuvent voir les résultats.

Le concept de smart contract a été développé en 1994 par l'informaticien et cryptographe Nick Szabo pour désigner la technologie permettant de sécuriser des échanges contractuels noués entre des parties qui ne se connaissent pas et qui, dès lors, ne se font pas confiance a priori[33].

Parmi la multitude de blockchains permettant de déployer des smart contracts, Ethereum est à ce jour la plus connue. Au sein de celle-ci, de nombreuses applications décentralisées programmées via des contrats intelligents sont en cours de développement dans les secteurs de la santé, l'assurance, l'énergie, ou encore l'immobilier. Bien que l'économie des smart contracts soit encore embryonnaire, celle-ci semble promise à un bel avenir.

3. L'ORGANISATION AUTONOME DÉCENTRALISÉE, OU DAO

Il s'agit d'une organisation décentralisée dont les règles de gouvernance sont automatisées et inscrites de façon immuable et transparente dans une blockchain. En théorie, une DAO se distingue d'une entité classique de trois manières :

- elle ne peut pas être arrêtée ou fermée ;
- aucune personne ou organisation ne peut la contrôler ; et
- tout y est transparent et auditable.[34]

Comme son nom l'indique, une DAO possède deux caractéristiques principales : l'autonomie et la décentralisation. Une DAO est autonome dans le sens où le fonctionnement de l'organisation se fait automatiquement par le biais de contrats intelligents. En effet, ceux-ci établissent les règles fondamentales, exécutent les décisions convenues et, à tout moment, les votes et même le code lui-même peuvent faire l'objet d'un audit public. De plus, une DAO est décentralisée dans le sens où elle est entièrement gouvernée par ses membres individuels. Ce sont ces derniers qui prennent collectivement des décisions critiques sur l'avenir du projet, comme les mises à niveau techniques et les allocations de trésorerie.[35]

En règle générale, les membres de la communauté créent des propositions sur les opérations futures du protocole et se réunissent ensuite pour voter sur chaque proposition. Les propositions qui atteignent un certain niveau de consensus prédéfini sont alors acceptées et appliquées par les règles instanciées dans le contrat intelligent. La collaboration communautaire est favorisée dans un tel cadre au détriment des structures hiérarchiques traditionnelles : chaque membre individuel de la DAO supervise le protocole à un certain niveau.[36]

L'élégance de ce cadre réside en partie dans l'alignement des incitations. En d'autres termes, il est dans l'intérêt de chacun d'être franc dans son vote et de n'approuver que les propositions qui servent le mieux les intérêts du protocole lui-même. Un protocole sain et robuste sera plus utilisé et, à son tour, augmentera la valeur des jetons que chaque membre de la DAO possède. Ainsi, si le protocole réussit, il en va de même pour les détenteurs de jetons.[37]

---

*31 « What are smart contracts on blockchain? », **IBM**, disponible à l'adresse suivante : www.ibm.com/topics/smart-contracts*

*32 Bobée Floriane, « Qu'est-ce qu'un smart contract ? », **Journal du Coin**, 21 février 2022, disponible à l'adresse suivante : www.journalducoin.com/lexique/smart-contract/*

*33 **Ibid.***

*34 « Qu'est-ce qu'une DAO ? », **Blockchain France**, 12 mai 2016, disponible à l'adresse suivante : www.blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/*

*35 Comitogianni Kévin, « Qu'est-ce qu'une organisation autonome décentralisée (DAO) ? », **Crypto News**, 5 février 2022, disponible à l'adresse suivante : www.fr.cryptonews.com/exclusives/quest-ce-quune-organisation-autonome-decentralisee-dao.htm*

*36 Shuttleworth David, « What Is A DAO And How Do They Work? », **ConsenSys**, 7 octobre 2021, disponible à l'adresse suivante : www.consensys.net/blog/blockchain-explained/what-is-a-dao-and-how-do-they-work/*

*37 **Ibid.***


NFT

4. LES JETONS NON-FONGIBLES (NFT)

Un NFT est un jeton non-fongible, dont la propriété par un utilisateur est inscrite dans la blockchain.

Juridiquement un bien est qualifié de « fongible » s'il est interchangeable avec un autre de même qualité et de même quantité. Par exemple, un billet de banque. Ou une pièce de monnaie. Ou même un bitcoin.

Par contre, les jetons non fongibles sont uniques, singularisés. Thibaut Verbiest et Alain Van Gelderen les définissent de la manière suivante : « éléments cryptographiques et virtuels sur la blockchain avec des codes d'identification uniques et des métadonnées (auteur, signature, date, type, ...) qui les distinguent les uns des autres ».[38] Ils fournissent à leurs propriétaires une preuve de propriété unique et infalsifiable.

La question de la propriété intellectuelle semble être la plus intéressante à ce sujet, étant donné l'ampleur de l'utilisation des NFT dans l'industrie artistique.

Traditionnellement, l'outil clé dans ce domaine est le droit d'auteur. Il est activé pour la propriété littéraire et artistique lorsque l'œuvre est créée sans qu'un dépôt soit nécessaire. Par conséquent, le droit d'auteur est généralement utilisé lorsqu'un auteur souhaite tirer profit de son œuvre en cédant ses droits transférables ou en agissant face à une contrefaçon. L'auteur doit alors démontrer que son œuvre est, juridiquement parlant, considérée comme «originale» et qu'elle a été produite avant l'autre œuvre en question en cas de désaccord. L'auteur peut recourir à une société d'auteurs pour dater cette composition. Il est donc envisageable que le NFT soit une solution alternative, permettant non seulement de dater la création de l'œuvre mais aussi de s'assurer de sa bonne utilisation.

En effet, comme pour les titres de propriété industrielle, l'utilisation de smart contracts permettrait d'automatiser les processus liés aux droits patrimoniaux d'auteur (par exemple pour la perception de redevances lorsque l'œuvre est utilisée ou transmise). Le NFT peut se développer comme un nouveau support pour tous les titres de propriété industrielle (brevet, marque, dessins et modèles). Cette application des NFT peut contribuer à faire progresser la défense des inventeurs. En effet, l'utilisation des NFTs permettra de combiner la puissance des smart contracts alors que de plus en plus de transactions ont lieu en ligne.

Avec l'aide de ces contrats intelligents, différentes actions, comme, par exemple, la récupération des droits d'exploitation d'une licence, peuvent être exécutées automatiquement. En outre, le NFT pourra être liée à des outils permettant de trouver les contrefacteurs.

La technologie blockchain s'est déjà révélée être un outil utile en matière de preuve. Les services de certification de documents et d'horodatage sont largement disponibles. C'est notamment le cas des services de certification d'emails comme Woleet, Ipocamp ou Mailstone.

38 Verbiest Thibault et Van Gelderen Alain, ***Tout ce que vous avez toujours voulu savoir sur les cryptomonnaies sans jamais oser le demander****, Lucpire éditions, 2022, p.60*

V. QUELS SONT LES DANGERS ET DÉFIS DE LA BLOCKCHAIN ?

1. UNE CONSOMMATION ÉNERGÉTIQUE EXCESSIVE

Cette critique est récurrente et interpelle à juste titre. Ainsi, selon une étude de 2020, la consommation d'électricité du Bitcoin (à travers la technologie blockchain) pour une seule transaction s'élèverait à plusieurs centaines de kWh et correspondrait donc à la consommation d'électricité d'un ménage allemand pendant plusieurs semaines (voire plusieurs mois). Ce chiffre nécessite cependant quelques précisions. Il a été obtenu en divisant la consommation électrique total du réseau Bitcoin sur une année par le nombre de transactions faite sur la même période de temps. Or, le nombre de transactions n'a aucun effet sur la consommation énergétique du traitement d'un block. En effet, le nombre total de transactions enregistrées par un block peut être augmenté sans que la consommation nécessaire pour traiter ce block n'augmente.[39] Cependant, les besoins énergétiques quotidiens des réseaux Bitcoin seraient les mêmes que ceux d'un petit pays comme l'Irlande ! Cela conduit à la critique de cette technologie en termes de viabilité.

Cependant, il est regrettable que les discussions ne soient pas différenciées entre le Bitcoin et la technologie des registres distribués (ou blockchain). En effet, la technologie blockchain est loin d'être homogène, non seulement en ce qui concerne ses applications (qui vont bien au-delà des crypto-monnaies comme nous l'avons vu), mais aussi en ce qui concerne ses caractéristiques techniques et, en particulier, sa consommation énergétique. Bien que le Bitcoin et d'autres blockchains « proof-of-work » consomment effectivement beaucoup d'énergie, des solutions alternatives de blockchain, avec une consommation d'énergie considérablement plus faible, sont déjà disponibles, et de nouveaux concepts prometteurs sont testés et pourraient réduire encore davantage la consommation énergétique des grands réseaux blockchain dans un avenir proche. Par conséquent, bien que la critique de la consommation électrique du Bitcoin soit légitime, elle ne doit pas être utilisée pour en déduire un problème de la technologie blockchain en général. Dans de nombreux cas d'utilisation d'outils numériques, nous pouvons même nous attendre à des économies d'énergie nettes par rapport à l'utilisation de technologies antérieures.[40]

Il faut également avoir en tête les ordres de grandeur. La technologie blockchain, en particulier son utilisation dans le secteur de la cryptomonnaie, consomme beaucoup d'électricité mais par rapport à quoi ? Une étude de Galaxy Digital[41] évalue la consommation énergétique du réseau Bitcoin à 113,89 Twh mais estime aussi que la consommation énergétique du système financier est de 263,72 Twh.[42] Les cryptomonnaies ne nécessitent pas, en effet, toute l'infrastructure du système financier (en ce compris les dizaines de milliers de distributeurs automatiques de billets de par le monde).

Par ailleurs, notons également qu'il est important de distinguer la consommation d'énergie et la production de celle-ci. En effet, le réseau blockchain du Bitcoin consomme beaucoup d'énergie, mais si cette dernière est produite avec des énergies renouvelables, son impact sur le changement climatique est proche de zéro.

À titre d'exemple, citons l'initiative de Jack Dorsey (fondateur de Twitter et Block) qui pose les premiers jalons d'une mine de bitcoins alimentée par de l'énergie solaire, au Texas. Le projet comporte des panneaux photovoltaïques produisant 3,8 mégawatts et des batteries de 12 mégawatts, provenant de l'entreprise Tesla. L'installation est conçue pour démontrer qu'il est possible de miner du Bitcoin à grande échelle avec des énergies 100 % renouvelables.[43]

L'électricité provenant de barrages hydrauliques est déjà utilisée pour miner des Bitcoins. Citons l'exemple d'une centrale hydroélectrique alimentée par la rivière Poas, au Costa Rica.

*39 Sedlmeir Johannes et al., « Recent Developments in Blockchain Technology and their Impact on Energy Consumption », **Informatik Spektrum**, 2021, p. 4.*

*40 Sedlmeir Johannes et al., « Recent Developments in Blockchain Technology and their Impact on Energy Consumption », **op. cit.**, p. 1.*

*41 Galaxy Digital Mining (2021) citée dans Person Pierre, « Monnaies, banques et finance : vers une nouvelle ère crypto » , **Rapport d'information de l'Assemblée Nationale Française**, 8 juin 2022, p.204.*

42 Chiffres à prendre avec précaution car plusieurs postes de la finance traditionnelle ne sont pas comptabilisés dans ce calcul.

*43 Sigalos MacKenzie, « Crypto world : Tesla, Block and Blockstream team up to mine bitcoin off solar power in Texas », **CNBC**, 2022, disponible à l'adresse suivante : www.cnbc.com/2022/04/08/tesla-block-blockstream-to-mine-bitcoin-off-solar-power-in-texas.html , (consultée le 18 mai 2022).*

Celle-ci alimente plus de 650 machines qui fonctionnent en continu, disposées dans huit conteneurs, conçus pour le minage de crypto-monnaies.

La centrale a été contrainte de se réinventer après 30 ans de fonctionnement, car le gouvernement a cessé d'acheter l'électricité qu'elle produisait, en raison d'un excédent d'énergie pendant la pandémie, dans ce pays d'Amérique centrale où l'État a le monopole de la distribution d'énergie.[44]

Enfin, il est possible de valoriser la chaleur produite par les ordinateurs qui minent des Bitcoins. En effet, de la chaleur est créée par les calculs effectués par les puces informatiques. En fait, l'énergie électrique se transforme en chaleur à cause de ces calculs. À titre d'exemple, citons le chauffage *Heatbit*, qui se vend 1 150 dollars, et qui peut chauffer jusqu'à 15 mètres carrés, tout en minant des bitcoins, à un taux de 14 hashs par seconde, en utilisant 1 300 watts d'électricité. Sur base d'un cours du bitcoin à 44 000 dollars et en supposant que le prix de l'électricité est de 0,10 dollar par kilowattheure, cela permet de gagner environ 47 dollars par mois, ou 557 dollars par an.[45]

2. UNE MENACE SUR LES DONNÉES PERSONNELLES

Les « nœuds » d'une même blockchain peuvent se trouver dans plusieurs endroits différents dans le monde, il est souvent difficile de déterminer les lois et les réglementations qui s'appliquent à un outil qui utilise cette technologie.[46]

De plus, les questions de protection des données pour les applications faisant appel à la technologie blockchain font l'objet de débats intenses. De nombreux chercheurs universitaires ont notamment affirmé que cette technologie est incompatible avec les lois sur la protection de la vie privée telles que le Règlement Général sur la Protection des données (RGPD) de l'Union européenne.

L'objectif de la blockchain est de faciliter les transactions entre pairs sans l'intervention d'une partie centrale.

Dans un système public de blockchain public sans autorisation, aucune partie en particulier n'est responsable du contrôle ou la sécurité du réseau, et tous les utilisateurs du système peuvent avoir accès aux données contenues dans le réseau. Ces caractéristiques sont en conflit avec l'idée centrale des lois sur la vie privée, qui exigent que la partie qui contrôle les données d'un individu soit en devoir de protéger la sécurité et la confidentialité de ces données au nom de l'utilisateur. Comme les réseaux de blockchain sont exploités par tous les utilisateurs dans un environnement de réseau peer-to-peer, il est difficile de définir si les utilisateurs sont des contrôleurs (donc soumis à la législation RGPD) ou de simples utilisateurs.[47]

---

*44 Murillo Alvaro, « Costa Rica hydro plant gets new lease on life from crypto mining », **Reuters**, 2022, www.reuters.com/technology/costa-rica-hydro-plant-gets-new-lease-life-crypto-mining-2022-01-11*
*45 Donovan Kevin et Stewart Monte, « Is crypto mining the next home heating trend? », **Capital.com**, 2022, disponible sur : www.capital.com/is-crypto-mining-the-next-home-heating-trend (consultée le 18 mai 2022).*
*46 Salmon John et Myers Gordon, « Blockchain and Associated Legal Issues for Emerging Markets », **IFC World Bank Group**, 2019, vol. 63, p. 3.*
*47 **Ibid.***

VI. QUELLES INNOVATIONS PROMETTEUSES PEUT-ON ATTENDRE DE LA BLOCKCHAIN ?

1. CADASTRER LE TIERS-MONDE

« Cadastrer » la société occidentale, c'est-à-dire répertorier tous les biens immobiliers, les authentifier, déterminer leurs propriétaires respectifs et retracer l'historique de leur transmission est un travail méconnu qui a nécessité plusieurs siècles. Il n'est pas, loin de là, achevé au tiers-monde. Et cela explique, notamment, le fait que ces pays voient, pour une large part, leur économie dominée par le secteur informel. Cela explique aussi pourquoi une large partie des hommes et des femmes sur terre n'ont pas - faute de pouvoir mettre en gage les biens qu'ils possèdent de facto – la possibilité d'accéder au crédit.

Le cadastre est l'un des cas d'usage le plus répandus pour la technologie blockchain. En revanche, les bénéfices, pour une économie, de posséder un tel registre sont moins connus.

L'économiste péruvien Hernando de Soto a travaillé sur cette question en particulier. Célèbre auteur du best-seller « Le mystère du capital »,[48] ce dernier est un partisan chevronné du renforcement des droits de propriété dans les pays en développement pour lutter contre la pauvreté. Il a inventé le terme « capital mort » pour décrire les actifs dépourvus de droits de propriété formels et qui ne peuvent donc pas être facilement échangés ou utilisés comme garantie pour un crédit. En raison de l'absence de titres de propriété, le capital mort est également soumis à une menace d'expropriation, ce qui peut décourager l'investissement.

Les premiers travaux de De Soto sur les droits de propriété et l'informalité - par exemple, la constatation empirique qu'il fallait 289 jours pour ouvrir une petite entreprise au Pérou en 1983 - ont inspiré le développement du rapport « Doing Business » de la Banque mondiale. Depuis sa deuxième édition en 2004, ce rapport contient une section sur l'enregistrement des biens. Dans ce domaine, la numérisation du registre foncier s'est révélée être une mesure particulièrement efficace pour accélérer les processus de transfert. Entre 2010 et 2015, 37 économies ont numérisé leur registre foncier. Cela a permis de réduire de 38 % le temps nécessaire à l'enregistrement d'un transfert de propriété dans ces pays, contre une réduction de 7 % dans les pays qui n'ont pas numérisé leur registre foncier. La prochaine étape prometteuse qui s'appuie sur les données numériques pourrait être de mettre les registres fonciers sur une blockchain.[49]

Même de petites améliorations peuvent avoir un effet considérable dans ce domaine, car le volume du capital mort mondial est estimé par de Soto à 20 000 milliards de dollars, qui sont détenus par 5,3 milliards de personnes dans le monde. Cette absence massive de droits de propriété a des conséquences économiques considérables. Régler ce problème pourrait, selon de Soto, conduire à «des taux de croissance chinois ou indiens dans le monde entier». Cependant, cet enthousiasme n'est pas incontesté. Oliver Williamson scinde le raisonnement de Soto en deux hypothèses et mène une enquête sur la littérature empirique pour tester les deux : «1) Les droits de propriété ont un impact sur le développement en modifiant la capacité et les incitations à la formation de capital, 2) La délivrance de titres fonciers fournit les moyens de sécuriser les droits de propriété.»[50]

Alors que la première hypothèse est largement incontestée dans la littérature empirique, les preuves de la deuxième hypothèse sont mitigées. Kerekes et Williamson identifient une raison potentielle de l'efficacité limitée des titres fonciers : les banques privées au Pérou ne font pas suffisamment confiance aux titres fonciers pour accorder à leurs détenteurs des avantages par rapport aux détenteurs de terres sans titre.

48 de Soto, Hernando, Le mystère du capital, Champs Flammarion, 2010

*49 Ohnesorge Jan, « A primer on blockchain technology and its potential for financial inclusion », **Deutsches Institut für Entwicklungspolitik**, 2018, vol. 2, p. 19-21.*

*50 **Ibid.***

En fait, les banques privées péruviennes utilisent des terres détenues de manière informelle et formelle comme garantie. Pour compenser l'insécurité perçue de la garantie, les banques facturent des primes de taux d'intérêt, indépendamment de l'existence de titres fonciers. Kerekes et Williamson affirment que l'incapacité de l'État à faire respecter les droits de propriété pourrait être à l'origine de ce résultat.[51]

Il est donc important de souligner qu'un registre foncier blockchain doit être intégré à des mécanismes d'application qui fonctionnent pour garantir efficacement les droits de propriété. Ces conditions ne sont actuellement pas réunies dans de nombreux pays en développement, où la situation se caractérise par des droits fonciers contestés et des mécanismes d'application de la loi dysfonctionnels. Il convient de noter que les cryptomonnaies n'ont généralement pas à s'appuyer sur des mécanismes d'application autres que leurs propres mécanismes basés sur le code contre les activités malveillantes.

Le jeton virtuel (par exemple, le bitcoin) est lui-même l'objet de valeur, ce qui permet au logiciel de le protéger. Ce n'est qu'en cas d'échec de cette protection - par exemple, si un attaquant parvient à voler la clé privée d'une adresse Bitcoin - que des mécanismes d'application étatiques (c'est-à-dire la police et les tribunaux) sont nécessaires.

En revanche, un registre foncier contient des titres, c'est-à-dire des représentations abstraites d'objets de valeur physiques qui se trouvent en dehors du registre. Ainsi, toutes les propositions actuelles de registres fonciers à registres distribués s'appuient sur des mécanismes d'application étatiques pour fonctionner correctement. Ainsi, les registres de propriété dépendent des mécanismes d'application de l'État.

En outre, la création initiale des entrées du registre distribué ne peut pas être entièrement automatisée et nécessite un système judiciaire opérationnel pour garantir que les revendications conflictuelles sur un bien donné sont légalement réglées avant que le bien n'entre dans le registre. Benito Arruñada souligne que la production d'informations fiables est en effet le principal défi des registres de propriété et que la technologie blockchain ne semble pas pouvoir résoudre ce problème. Une fois le registre distribué mis en place, le transfert de jetons de propriété pourrait théoriquement être traité de manière analogue au transfert de bitcoins ou d'autres jetons de crypto-monnaie. Toutefois, cela entraînerait d'énormes problèmes en cas de perte ou de vol de la clé cryptographique d'un jeton de propriété. Pour cette raison et pour d'autres, les projets qui visent à faire migrer le registre foncier d'un pays vers un grand livre distribué essaient généralement de concevoir un système plus sophistiqué qui ne repose pas entièrement sur le fait que les utilisateurs gardent leurs clés cryptographiques en sécurité.[52]

Malgré cela, la technologie du registre distribué peut révolutionner le cadastre en offrant une architecture sécurisée pour stocker les transactions foncières à l'aide d'un protocole cryptographique. Cette technologie a de nombreux avantages pour ce cas d'usage. Cela permet d'avoir plus de transparence car chaque nœud a un aperçu complet du réseau et détient un historique des transactions qui peut être visible par n'importe qui et à tout moment. La confiance est accrue car les archives sont immuables. Les données sont stockées à plusieurs endroits ce qui accroît la fiabilité des données et empêche leur falsification. De plus, les coûts d'administrations sont grandement diminués car aucune tierce partie humaine n'est impliquée pour la validation des données. Les transactions automatisées réduisent également les risques d'erreurs commises par les humains. Enfin, les risques de compromission des données par la corruption d'agents sont grandement réduits. Des projets pilotes sont menés dans de nombreux pays, notamment au Japon, en Georgie, en Russie, en Suède, au Brésil, au Canada, au Ghana, en Inde, aux Etats-Unis et au Pays-Bas.[53]

2. RÉSEAU ÉLECTRIQUE INTELLIGENT

Les réseaux électriques intelligents offrent aux consommateurs d'énergie la possibilité de devenir indépendants des grands fournisseurs d'énergie. Au sein d'une communauté fermée, les petits producteurs d'énergie privés, comme des ménages équipés de systèmes photovoltaïques par exemple, peuvent vendre leur énergie excédentaire à leurs voisins qui en ont besoin. Pour ce faire, on utilise un micro-réseau physique de distribution d'énergie, qui relie les différentes maisons, et un micro-réseau virtuel, qui relie les compteurs intelligents qui mesurent et surveillent la production et la demande d'énergie de chaque foyer. Dans une blockchain, des contrats intelligents réalisent des enchères en faisant correspondre toutes les offres d'achat (personnes qui ont besoin d'énergie) et de vente (personnes qui ont de l'énergie à vendre) et en inscrivant chaque transaction énergétique sur la blockchain. Cette façon d'échanger de l'énergie permet de fournir un accès à l'énergie en temps quasi réel, dès que le besoin s'en fait sentir. Actuellement, un prototype de ce protocole est testé à New York.[54]

3. ASSURANCE AGRICOLE

Rien qu'en Afrique, on compte environ 300 millions de petits exploitants agricoles, dont la majorité n'est pas assurée contre les risques climatiques tels que les inondations et la sécheresse. Les petits exploitants sont particulièrement vulnérables à la sécheresse car beaucoup d'entre eux n'ont pas accès aux techniques d'irrigation et dépendent des précipitations pour leurs cultures. Cela rend leurs moyens de subsistance, et leur principale source de nourriture, incroyablement précaire.

---

51 ***Ibid.***

52 Ohnesorge Jan, « A primer on blockchain technology and its potential for financial inclusion », ***op. cit.***

53 Shuaib Mohammed et al., « Blockchain-based framework for secure and reliable land registry system », ***Telecommunication, Computing, Electronics and Control****, 2020, vol. 18, n°5, pp. 2560-2571.*

54 Klein Sandra et al., « A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities », ***SIGCHI Conference****, 2017, p.5.*

C'est pour cela qu'une assurance peut être très utile, mais dans cette partie du monde, les assurances contre les intempéries sont soit trop chères, soit inexistantes. Dans les pays à faible revenu, moins de 3 % de la population agricole a une assurance agricole. Pour les compagnies d'assurance qui s'appuient sur des outils traditionnels de tarification et de gestion des sinistres, la protection des petits exploitants contre les événements climatiques n'est généralement pas rentable.[55]

En revanche, une assurance basée sur la blockchain pourrait être une solution viable. Dans ce système, les polices d'assurance sont hébergées sur des smart contracts qui sont connectés à des centres de relevés météorologiques. En cas de catastrophes naturelles ou de conditions météorologiques extrêmes, les contrats intelligents sont exécutés automatiquement, ce qui permet au bénéficiaire de toucher rapidement les primes qui lui sont dues. De plus, cela ne nécessite aucune intervention humaine, ce qui permet aux assureurs de réduire considérablement leur coût et donc d'être rentables même pour de toutes petites exploitations.[56]

4. COLLECTE DE TVA

En Europe, la fraude à la TVA est estimée à 50 milliards d'euros. L'une des fraudes les plus courantes est le «carrousel TVA». Le procédé est simple : une entreprise importe des marchandises dans un pays européen à un taux de TVA de 0 %, puis revend les marchandises dans un autre pays de l'Union au taux de TVA normal (20 % ou plus dans la plupart des pays de l'UE), puis disparaît, avec le montant de la TVA qu'elle devait reverser au gouvernement où elle opérait.[57]

Grâce à la blockchain, il est possible d'obtenir des informations claires et transparentes sur les transactions qui ont lieu. Cela permet de savoir quand et où la TVA a été payée, ce qui pourrait aider les gouvernements à lutter contre la fraude à la TVA. Les "carrousels TVA" peuvent être difficiles à détecter lorsqu'il s'agit de transactions transfrontalières et d'un réseau complexe d'acteurs impliqués (certaines entités peuvent même ne pas être conscientes qu'elles facilitent la criminalité financière). Actuellement, les régulateurs font de leur mieux pour prévenir la fraude et l'évasion fiscales en demandant des documents comptables et des rapports détaillés et précis pour justifier le traitement de la TVA sur chaque transaction. Cependant, ces processus sont coûteux et ne sont pas infaillibles. La technologie blockchain pourrait diminuer la charge de travail et permettre aux gouvernements de réduire les pertes fiscales causées par la fraude à la TVA, grâce à l'enregistrement automatique de données fiables en temps réel pour chaque transaction. Avec le développement des smart contrats, il serait possible d'aller encore plus loin : le versement de la TVA pourrait être automatique.[58]

Cette technologie pourrait faire office d'agent fiscal virtuel, en divisant automatiquement le montant payé lors de chaque transaction en deux parties. La première partie serait appelée «frais payés pour les biens ou services fournis» et serait directement versée sur le compte bancaire du fournisseur. La seconde partie serait appelée «TVA» et n'entrerait que momentanément sur le compte bancaire du fournisseur, avant d'être rapidement transférée sur le compte bancaire de l'autorité fiscale compétente. Cette approche rendrait la fraude pratiquement impossible. A nouveau, cela pourrait réduire la charge administrative, puisqu'aucun intermédiaire ne serait nécessaire pour exécuter le paiement fractionné. Théoriquement, il n'y aurait également plus besoin de faire de déclaration, ce qui diminuerait également la charge de travail des entreprises.[59]

---

55 Wininger Shai, « Introducing the Lemonade Crypto Climate Coalition », disponible à l'adresse suivante : www.lemonade.com/blog/crypto-climate-coalition/ (consultée le 29 mai 2022).

*56 Jha Nishant et al., « Blockchain Based Crop Insurance: A Decentralized Insurance System for Modernization of Indian Farmers », **Sustainability**, 2021, p.14.*

*57 Arman Pierre, « Could Blockchain transform the GCC's VAT system? », **Thomsons Reuters**, www.mena.thomsonreuters.com/content/dam/openweb/documents/pdf/mena/white-paper/vatandblockchain_whitepaper_hires_digital.pdf*

*58 **Ibid.***

*59 **Ibid.***


DECENTRALIZED * PEER TO PEER *
DIGITAL * BITCOIN * CRYPTOCURRENCY *
ethereum classic
DECENTRALIZED
ethereum classic
CARDANO
SECURE LAYERED SMART CONTRACTS
ADA

PARTIE 2 : CRYPTOMONNAIES

I. DÉFINITION ET PHILOSOPHIE

Les **cryptomonnaies** sont l'une des principales applications de la blockchain[60]. La confiance d'un large éventail d'utilisateurs permet de soutenir le système de valeur des cryptomonnaies et stimule à la fois la circulation et le commerce de celles-ci. À ce jour, selon CoinMarketCap, il existerait plus de 19.200 cryptoactifs émis dans le monde, et de nouvelles ne cessent d'apparaître chaque jour.

Tout comme le monde réel repose sur des monnaies fiduciaires, le futur **métavers** a inévitablement besoin de cryptomonnaies qui délivrent de la valeur lors de leur circulation, de leur paiement et de leur règlement. Plus précisément, les systèmes de blockchain mettent en œuvre une série d'opérations relatives aux cryptomonnaies, comme la création, l'enregistrement et le commerce. Toutes ces opérations sont fondamentales et nécessaires pour le métavers.[61]

« Monnaie virtuelle », « cryptomonnaie », « cryptoactif », ou encore « monnaie numérique » sont autant de **qualificatifs** qui foisonnent et témoignent de la complexité à laquelle le monde du droit est confronté lorsqu'il est question de qualifier le Bitcoin et d'autres cryptomonnaies[62]. Il est dès lors intéressant de s'attarder sur les définitions juridiques proposées aux niveaux du droit européen et du droit belge.

En **droit européen**, les devises virtuelles sont définies par la Banque centrale européenne (BCE) comme étant « une représentation numérique d'une valeur qui n'est pas émise par une banque centrale, un établissement de crédit ou un établissement de monnaie électronique et qui, dans certains cas, peut être utilisée comme une alternative à la monnaie »[63].

La cinquième directive AML de l'Union européenne définit, quant à elle, les monnaies virtuelles comme étant des « représentations numériques d'une valeur qui ne sont émises ni par une banque centrale ni par une autorité publique, qui ne sont pas nécessairement liées non plus à une monnaie à cours forcé mais qui sont acceptées comme moyen de paiement par des personnes physiques ou morales et qui peuvent être transférées, stockées ou échangées par voie électronique »[64].

En **droit belge**, l'arrêté royal belge du 8 février 2022 reprend une définition quasiment identique à celle citée précédemment. Les monnaies virtuelles y sont en effet définies comme des « représentations numériques d'une valeur qui ne sont émises ou garanties ni par une banque centrale ni par une autorité publique, qui ne sont pas nécessairement liées non plus à une monnaie établie légalement et qui ne possèdent pas le statut juridique de monnaie ou d'argent, mais qui sont acceptées comme moyen d'échange par des personnes physiques ou morales et qui peuvent être transférées, stockées et échangées par voie électronique »[65]. Cette définition est par ailleurs reprise par l'Autorité des services et marchés financiers (FSMA)[66].

De ces définitions, il est possible de dégager plusieurs **caractéristiques** concernant les cryptomonnaies (la plupart en lien avec la blockchain, étant la technologie qui les sous-tend). De ce fait, elles ont pour caractéristiques principales d'être virtuelles, au nombre limité, non émises par une banque centrale, sans cours légal, et basées sur la blockchain et la cryptographie.

---

*60 Yang Qinglin et al., « Fusing Blockchain and AI with Metaverse: A Survey », **op. cit.**, p. 8.*

*61 **Ibid.***

*62 Poullet Yves et Jacquemin Hervé, « Blockchain : une révolution pour le droit ? », **op. cit.**, p. 813.*

*63 « Avertissement sur les monnaies virtuelles », **Commission de Surveillance du Secteur Financier (CSSF)**, 14 mars 2018, disponible à l'adresse suivante : www.cssf.lu/fr/2018/03/avertissement-sur-les-monnaies-virtuelles*

64 Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE – article premier.

65 Arrêté royal du 8 février 2022 relatif au statut et au contrôle des prestataires de services d'échange entre monnaies virtuelles et monnaies légales et des prestataires de services de portefeuilles de conservation (Moniteur belge du 23 février 2022) – art. 3, ∫5.

*66 « Qu'entend-on par 'monnaies virtuelles' ? », **Autorité des services et marchés financiers (FSMA)**, disponible à l'adresse suivante : www.fsma.be/fr/faq/7-quentend-par-monnaies-virtuelles (consultée le 26 avril 2022).*

1. HISTORIQUE

La cryptomonnaie la plus emblématique, le Bitcoin, peut être perçue comme la réalisation, voire le dépassement des ambitions de l'économiste autrichien **Friedrich August von Hayek** consistant à mettre fin au monopole des États et des banques centrales dans l'émission de la circulation de la monnaie[67]. Dans son ouvrage *The denationalization of money* sorti en 1976, Hayek se prononce en effet en faveur d'un marché monétaire en dehors du monopole de l'État. Il y propose la création de monnaies émises de manière privée et soumises à la loi du marché et au principe de libre-concurrence. Selon lui, celles-ci deviendraient plus stables et plus fiables que les monnaies étatiques[68].

À cet égard, le Bitcoin a été pensé par ses fondateurs comme un système de paiement « sans confiance », au sens où la confiance ne reposerait plus sur un tiers, une autorité centrale, mais plutôt sur une infrastructure technique reposant sur un réseau décentralisé de pair-à-pair avec un protocole cryptographique, une chaîne de blocs et une activité de minage[69].

Ce projet d'un système de paiement échappant à la tutelle de toute institution centrale trouve plus généralement son origine dans la pensée libertarienne développée à la fin des années 1980 par les **courants cypherpunk et crypto-anarchiste**[70]. L'évolution des technologies et la possibilité de développer la cryptographie à grande échelle sont perçues par ces courants comme des moyens de mettre fin à l'omniprésence des contrôles étatiques[71].

A CYPHERPUNK'S MANIFESTO

La vie privée est un prérequis à une société libre et ouverte, à l'ère numérique. La vie privée est différente du secret. Lorsque quelque chose est privé, nous ne voulons pas que le monde entier le sache. En revanche, lorsque quelque chose est secret, nous voulons que personne ne le sache. La vie privée est la capacité de se révéler au monde de manière sélective. [...]

Par conséquent, la vie privée dans une société libre et ouverte nécessite des systèmes de transaction anonymes. Jusqu'à présent, c'est l'argent liquide qui remplissait ce rôle. [...]

Nous devons défendre notre vie privée si nous voulons en avoir une. Nous devons nous rassembler et créer des systèmes qui permettent des transactions anonymes. [...]

Nous, les Cypherpunks, nous nous consacrons à la construction de systèmes anonymes. Nous défendons notre vie privée à l'aide de la cryptographie, d'e-mail anonyme, de signatures numériques et de monnaie électronique. [...] [72]

Dès lors, la naissance des cryptomonnaies se fait par l'entremise de différents essais infructueux. En 1995, le cryptographe américain David Chaum crée « **Digicash** », une forme précoce de paiement électronique cryptographique décentralisé, intraçable et sécurisé[73]. Le système s'appuie sur un logiciel utilisateur pour retirer l'argent d'une banque et des clés cryptographiques spécifiques pour envoyer l'argent à un bénéficiaire. Digicash fait néanmoins faillite en 1998. Cette même année voit l'arrivée de deux projets de monnaies numériques en ligne. En effet, l'ingénieur informatique Nick Szabo conçoit un mécanisme de monnaie numérique décentralisée appelé « **Bit Gold** », souvent qualifié de précurseur direct de l'architecture du Bitcoin[74]. N'ayant pas reçu suffisamment de soutien, il n'a cependant jamais été implémenté. Également, Wai Dei, lui aussi ingénieur informatique, présente dans une brève note les bases d'une autre monnaie digitale, baptisée « **b-money** », qui demeurera à l'état de projet[75].

Ce n'est qu'une décennie plus tard, plus précisément le 31 octobre 2008, que l'histoire des cryptomonnaies amorce un véritable tournant. À cette date, un développeur (ou groupe de développeurs) publie sous le pseudonyme Satoshi Nakamoto un livre blanc intitulé *Bitcoin – A Peer to Peer Electronic Cash System* décrivant les fonctionnalités du réseau de blockchain **Bitcoin**[76]. Le domaine bitcoin.org est enregistré en août 2008 et reste à ce jour la page d'accueil de la cryptomonnaie la plus utilisée au monde. L'histoire du Bitcoin est alors en marche. En janvier 2009, le premier bloc du réseau (« genesis block ») est miné à hauteur de 50 bitcoins par Satoshi Nakamoto lui-même, dont personne ne connait l'identité.

---

67 Rolland Maël et Slim Assen, « Économie politique du Bitcoin : l'institutionnalisation d'une monnaie sans institutions », Économie et Institutions, 2017, vol. 26, p. 3.

*68 « Blockchain et crypto-monnaies : origines et histoire », **Microsoft experiences**, 3 octobre 2021, disponible à l'adresse suivante : www.experiences.microsoft.fr/articles/cybersecurite/blockchain-cryptomonnaies/*

*69 Rolland Maël et Slim Assen, « Économie politique du Bitcoin : l'institutionnalisation d'une monnaie sans institutions », **op. cit.**, p. 3.*

*70 **Ibid.***

*71 Ganascia Jean-Gabriel, « L'État peut-il rester tiers garant à l'heure de la blockchain ? », **L'ENA hors les murs**, 2018, p. 1.*

72 Hughes Eric, « A Cypherpunk's Manifesto », 1993, disponible à l'adresse suivante : www.activism.net/cypherpunk/manifesto.html (consultée le 25 mai 2022).

*73 « Une brève histoire de la crypto monnaie », **CryptoVantage**, disponible à l'adresse suivante : www.cryptovantage.com/fr/guides/une-breve-histoire-de-la-cryptomonnaie/ (consultée le 26 avril 2022).*

*74 « Blockchain et crypto-monnaies : origines et histoire », **Microsoft experiences**, **op. cit.***

*75 **Ibid.***

*76 « Une brève histoire de la crypto monnaie », **CryptoVantage**, **op. cit.***

La toute première transaction s'effectue en avril 2010 : un internaute échange 10.000 bitcoins contre deux pizzas[77]. Au prix maximum du Bitcoin, ces deux pizzas vaudraient bien plus de 600 millions de dollars !

Dès lors, les choses commencent à s'accélérer. De nouvelles cryptomonnaies apparaissent, telles que le **Litecoin** en octobre 2011. Étant des cryptomonnaies alternatives au Bitcoin établi, elles sont nommées « altcoins »[78]. En janvier 2013, peu de temps après une valorisation record de 1.000 dollars, le Bitcoin connaît un premier krach. La couverture médiatique est dès lors importante : de nombreuses personnes découvrent les cryptomonnaies dans le contexte de fortunes perdues chez des adeptes précoces. Un an plus tard, la plus grosse plateforme d'échange du monde à cette époque, Mt. Gox, s'effondre et annonce faillite, après avoir perdu 850.000 bitcoins à cause de hackers[79].

Lancé en 2015, le projet **Ethereum** apporte à la cryptomonnaie le concept des smart contracts (contrats intelligents), ouvrant le développement d'applications complexes et utiles dans une multitude de domaines et générant de nombreux projets différents[80]. De tels projets ont acquis des fonds de démarrage par le biais de crowdfunding, plus précisément par des Initial Coins Offerings (ICO) dans lesquelles de nouveaux jetons sont proposés aux investisseurs. Autrement dit, l'opération consiste à émettre des jetons (tokens) pour lever des fonds auprès du public[81]. Le modèle en ICO connaît un succès grandissant au point que les fonds récoltés par ce biais sont évalués à plus de trois milliards de dollars en octobre 2017[82].

Après avoir atteint des cours astronomiques frôlant les 20.000 dollars en décembre 2017, le Bitcoin ne parvient pas à maintenir son sommet. L'Ether, quant à lui, atteint un sommet en janvier 2018 pour une valeur d'environ 1.400 dollars. La croissance rapide de l'écosystème des cryptomonnaies devient cependant insoutenable : la bulle éclate et les prix commencent à décliner. Ces prix ne sont toutefois pas restés à la baisse et, depuis fin 2018, la plupart des cryptomonnaies – dont le Bitcoin et l'Ether – ont rebondi.[83]

---

*77 « Une brève histoire de la crypto-monnaie », **Kriptomat**, disponible à l'adresse suivante : www.kriptomat.io/fr/crypto-monnaies/une-breve-histoire-de-la-crypto-monnaie/ (consultée le 26 avril 2022).*

*78 **Ibid**.*

*79 « Une brève histoire de la crypto monnaie », **CryptoVantage**, **op. cit.***

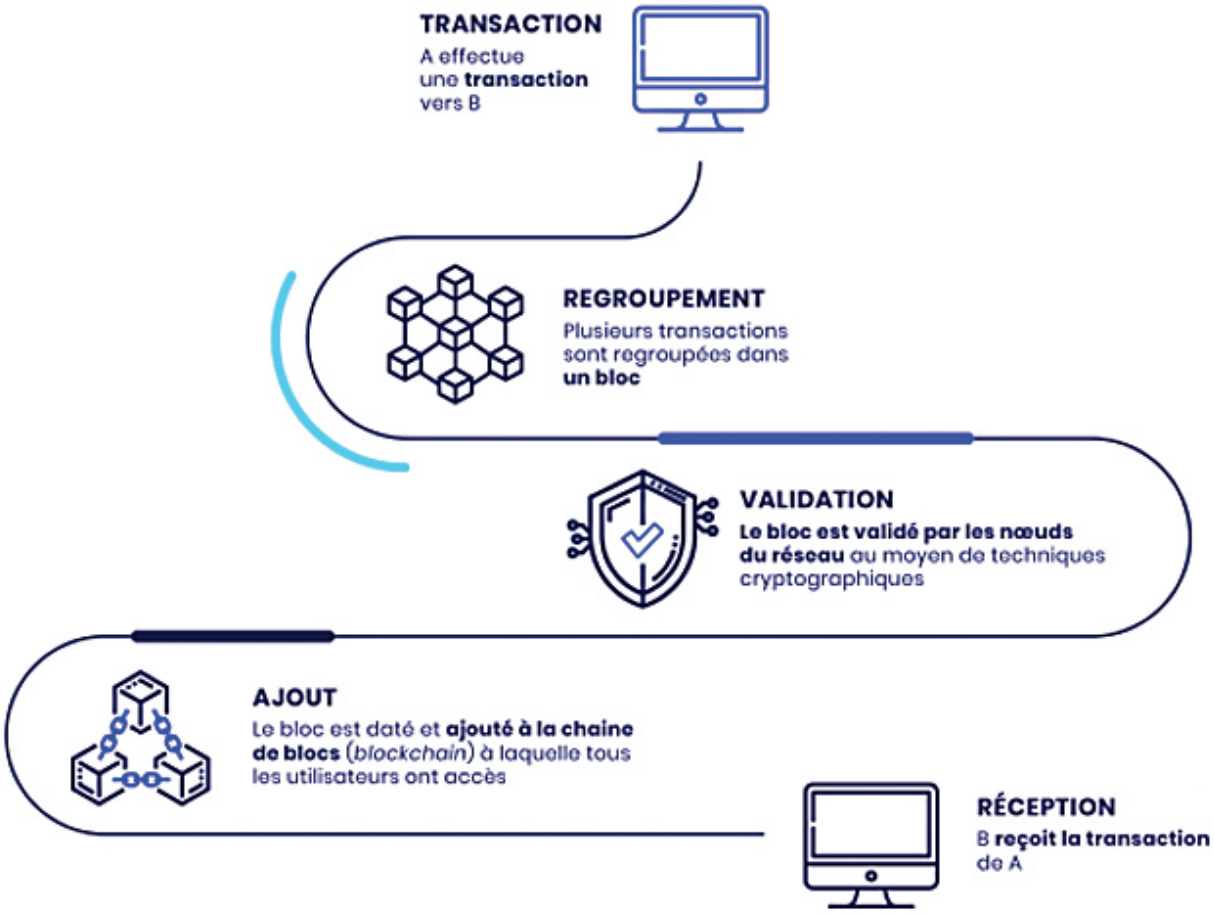
*80 « Une brève histoire de la crypto-monnaie », **Kriptomat**, **op. cit.***

*81 Poullet Yves et Jacquemin Hervé, « Blockchain : une révolution pour le droit ? », **op. cit.**, p. 815.*

*82 « Une brève histoire de la crypto-monnaie », **Kriptomat**, **op. cit.***

*83 « Une brève histoire de la crypto monnaie », **CryptoVantage**, **op. cit.***

Figure 2 : Mécanisme de transaction du Bitcoin



II. SA MAJESTÉ LE BITCOIN

Le **schéma** [*figure 2*] donne un aperçu du **mécanisme de transaction d'un bitcoin** d'un utilisateur A à un utilisateur B. Bitcoin est un exemple de monnaie programmable fonctionnant sur une blockchain publique.

Pour rappel, les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Les nœuds du réseau appelés les « mineurs » valident chaque bloc selon des techniques dépendant du type de blockchain. Dans la blockchain du Bitcoin, cette technique est la preuve de travail (proof-of-work) qui consiste en la résolution de problèmes algorithmiques. Une fois la validation du bloc effectuée, celui-ci est horodaté et ajouté à la blockchain. La transaction est dès lors visible aussi bien pour le récepteur que pour l'ensemble du réseau.[84]

Tout ce processus prend un certain temps suivant la blockchain considérée : toutes les dix minutes en moyenne, de nouveaux blocs viennent compléter la blockchain du Bitcoin. À chaque fois qu'un bloc est résolu, un tirage au sort désigne un des mineurs participants et le récompense d'un certain nombre de bitcoins créés ex nihilo.[85]

Les protocoles de Satoshi Nakamoto prévoient que la somme distribuée aux gagnants du minage soit divisée par deux tous les 210.000 blocs, c'est-à-dire tous les quatre ans environ. Étant donné que le nombre maximum de bitcoins pouvant être créés est de 21 millions, ce chiffre devrait être atteint aux alentours de 2140[86]. Aujourd'hui, miner un bloc de Bitcoin rapporte ainsi 6,25 bitcoins, loin des 50 bitcoins des débuts.

BITCOIN WHITE PAPER: A PEER-TO-PEER ELECTRONIC CASH SYSTEM

Voici comment s'exprime le mystérieux Satoshi Nakamoto, le prétendu père du Bitcoin. Ce passage résume sa philosophie.

Une version d'un système de paiement purement pair-à-pair permettrait des paiements en ligne directs d'une partie à l'autre sans passer par une institution financière. Les signatures digitales fournissent une partie de la solution, mais les principaux bénéfices sont perdus si un tiers de confiance est encore nécessaire pour éviter les doubles-paiements. Nous proposons une solution au problème de la double dépense en utilisant un réseau pair-à-pair. Le réseau horodate les transactions en les hachant en une chaîne continue de preuves-de-travail, formant un enregistrement de données qui ne peut pas être changé sans avoir à refaire la preuve-de-travail.

La chaîne la plus longue non seulement sert de preuve par témoignage de la séquence des événements, mais prouve qu'elle est issue du plus grand groupe de puissance CPU.

Aussi longtemps que la majorité de la puissance CPU est contrôlée par des nœuds non participant à une attaque du réseau, ils engendreront la plus longue chaîne et surpasseront les attaquants. Le réseau en lui-même exige une structure minimale. Les messages sont diffusés au mieux et les nœuds peuvent quitter et rejoindre le réseau à leur gré, en acceptant la plus longue chaîne de preuve-de-travail créée en leur absence.[87]

*84 Jeanneau Clément et al., **La Blockchain décryptée**, **op. cit.**, p. 3-4.*
*85 Delahaye Jean-Paul, « La cryptographie réinvente la monnaie : le Bitcoin », **Les nouvelles d'Archimède**, 2014, vol. 66, p. 14.*
*86 Delahaye Jean-Paul, « Bitcoin, la cryptomonnaie », **Pour la science**, 2013, vol. 434, p. 80-81.*
87 Nakamoto Satoshi, « Bitcoin: A Peer-to-Peer Electronic Cash System », 2008, disponible à l'adresse suivante : www.bitcoin.org/bitcoin.pdf (consultée le 25 mai 2022).

III. LES CRYPTOMONNAIES EMBLÉMATIQUES

BITCOIN (BTC) ET BITCOIN CASH (BCH)

En tant que premier actif numérique, le Bitcoin a été présenté en novembre 2008 par une personne ou un groupe de personnes sous le pseudonyme de Satoshi Nakamoto. Son code source a quant à lui été publié en 2009. Malgré sa forte volatilité, le Bitcoin reste la référence en matière de cryptomonnaies et ne cesse de gagner en popularité, notamment auprès du grand public.

Le Bitcoin Cash est une cryptomonnaie créée en août 2017 et issue du Bitcoin. Il s'agit plus précisément d'un fork du Bitcoin, c'est-à-dire que les deux cryptomonnaies partagent certaines caractéristiques communes mais fonctionnent sur des chaînes de blocs différentes depuis leur séparation. En effet, afin de subvenir à la croissance du nombre d'utilisateurs, le Bitcoin Cash a été créé en offrant davantage de transactions par bloc à moindre prix que le BTC.

ETHER (ETH)

Lancé en 2015, l'Ether est la cryptomonnaie nécessaire pour utiliser la blockchain Ethereum et ses applications décentralisées. Outre la gestion des transactions en Ether, la plateforme permet la création par les utilisateurs de smart contracts ou contrats intelligents, c'est-à-dire des programmes informatiques autonomes capables d'exécuter automatiquement et sans tiers de confiance un contrant en prenant en compte l'ensemble des conditions et des limitations prédéfinies au préalable par les différentes parties. Ether apparaît à la seconde place du marché des cryptomonnaies derrière le Bitcoin.

D'après son fondateur Vitalik Buterin, la force d'Ethereum repose sur son caractère complètement programmable, ce qui permet de créer une multiplicité d'applications, là où le Bitcoin est destiné uniquement aux transactions[88].

XRP / RIPPLE (XRP)

Créé en 2012 par la start-up Ripple, XRP offre un moyen d'effectuer des transactions transfrontalières sécurisées et quasi instantanées à faible coût. En effet, les transactions peuvent être validées en moins de quatre secondes contre deux à quatre jours ouvrables pour les virements numériques traditionnels.

Obtenant le soutien de plusieurs banques du monde entier, la technologie blockchain de Ripple a la spécificité de prendre en charge aussi bien les monnaies fiduciaires que les cryptomonnaies, ou d'autres unités de valeurs.

LITECOIN (LTC)

Lancé en 2011 par Charlie Lee, le Litecoin a été l'une des premières crypto-monnaies distribuées sous licence libre à suivre les traces de Bitcoin dont il est techniquement similaire.

Le Litecoin se base sur une blockchain améliorée par rapport à celle du Bitcoin. Cela a notamment permis d'accélérer le processus de vérification et donc d'augmenter la rapidité des transactions. Par ailleurs, ses frais de transaction sont bien plus faibles que ceux du Bitcoin. Le Litecoin est ainsi particulièrement destiné aux transactions quotidiennes.

À l'instar du Bitcoin et de la plupart des cryptomonnaies, le Litecoin sera produit dans un nombre limité. Son taux d'émission atteindra à terme 84 millions de litecoins (contre 21 millions de bitcoins).

MONERO (XMR)

Lancé en avril 2014 pour répondre entre autres aux problématiques de confidentialité du Bitcoin, Monero est une cryptomonnaie axée sur la vie privée et la décentralisation. Bien que construit sur une technologie open-source, la particularité de Monero est l'anonymat complet qu'il offre. Ses transactions ne peuvent pas être retracées, ce qui protège les détenteurs de Monero des regards indiscrets du public.

*88 Madelaine Nicolas, « Vitalik Buterin : 'Les blockchains géreront des milliards d'utilisateurs dans cinq ans' », **Les Echos**, janvier 2016, disponible à l'adresse suivante : www.lesechos.fr/2016/01/vitalik-buterin-les-blockchains-gereront-des-milliards-dutilisateurs-dans-cinq-ans-193107*


BTC /BUSD M
SHIB /BUSD M
ADA /BUSD M
DOGE /BUSD M
[ETH]
DECENTRALIZED PLATFORM THAT RUNS SMART CONTRACTS

IV. LE CADRE NORMATIF EN GESTATION

Le cadre normatif réglementant les cryptomonnaies est encore en pleine gestation. Comme on va le voir, les choses avancent plus vite en France. Au niveau européen, la règlementation MiCA (Market in Crypto Assets), encore en négociation, entrera en application durant l'année 2023 ou, plus probablement, en 2024.

Petit tour d'horizon en commençant par la France.

1. FRANCE : LOI PACTE (2019) ET ENREGISTREMENT PSAN

Première du genre, la loi PACTE (Plan d'Amélioration pour la Croissance et la Transformation des Entreprises) promulguée en France le 22 mai 2019 contient un volet sur les acteurs de la cryptomonnaie et a notamment pour objectif de réguler les Initial Coin Offering (ICO) qui, précédemment, n'étaient pas encadrées.

Précisons qu'une « Initial Coin Offering » (ou ICO), littéralement « offre de jetons au public» est 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.

Le texte permet, aux entreprises qui le souhaitent, d'obtenir un visa auprès de l'Autorité des marchés financiers française (AMF) moyennant certaines exigences visant à assurer une meilleure information et protection des investisseurs. Ces exigences sont les suivantes :

- L'obligation pour l'émetteur de jetons de le constituer en personne morale établie ou immatriculée en France.
- L'obligation de fournir une documentation informative destinée à contenir toutes les informations pertinentes sur les offres de jetons, les projets financés et les entreprises.
- La mise en place d'un système permettant le suivi et la sécurisation des avoirs collectés lors des offres.
- La conformité aux réglementations applicables en matière de prévention du blanchiment d'argent et de lutte contre le financement du terrorisme.

Notons que le financement AMF sans visa reste légal en France et les visas sont facultatifs. Cependant, les émetteurs qui n'ont pas de visa AMF ne pourront pas vendre au public. L'AMF publie une liste des ICO enregistrées.[89]

Ce visa est facultatif, ce qui signifie que les émetteurs de jetons ne sont pas interdits de lancer leur ICO auprès du public français s'ils ne demandent pas le visa ou ne l'obtiennent pas. Cependant, le visa offre certains avantages. Le plus important est l'accès illimité aux services bancaires : les émetteurs de jetons qui ont obtenu un visa ne peuvent pas se voir refuser l'accès aux services de dépôt et de compte de paiement par les établissements de crédit. Lorsqu'un tel refus se produit, ou si aucune réponse n'est reçue après 2 mois, les établissements de crédit doivent fournir à l'AMF et à l'ACPR (le superviseur bancaire français) les justifications de ce refus. L'ACPR peut alors offrir aux acteurs la possibilité de demander à la Banque centrale française de désigner un établissement de crédit, qui sera tenu de fournir les services. Il y a donc ici reconnaissance d'un véritable « droit au compte » pour les acteurs crypto.

Un autre avantage est que le visa peut être perçu comme un avantage concurrentiel comparatif. En effet, le visa peut devenir un élément dans la prise de décision des acheteurs potentiels de jetons. Enfin, les ICOs qui ont été approuvées par l'AMF obtiennent l'autorisation d'être commercialisées directement auprès du public français.[90]

89 "Vers un nouveau régime pour les crypto-actifs en France", AMF, 2019, disponible à l'adresse suivante : www.amf-france.org/fr/actualites-publications/actualites/vers-un-nouveau-regime-pour-les-crypto-actifs-en-france
90 "The French Regulatory Framework for Markets in Crypto-Assets", ADAN, 2020, disponible à l'adresse suivante : www.adan.eu/en/article/french-regulatory-framework-markets-crypto-assets

L'agrément en tant que prestataire de services sur actifs numériques (PSAN) est obligatoire pour les entreprises qui exercent l'une des activités suivantes :

- Stockage d'actifs numériques
- Achat et vente d'Actifs Numériques contre des monnaie ayant un cours légal
- Échange des actifs numériques contre d'autres actifs numériques
- Exploitation d'une plateforme de négociation d'actifs numériques

Ce type de service se réfère principalement à toutes les plateformes d'échange telles que Coinhouse, Kraken, Zebitex et Coinbase. Par commodité, un enregistrement auprès de l'AMF est requis si un cryptoactif est échangé contre de la monnaie fiduciaire ou si un autre cryptoactif et/ou la clé privée de l'investisseur est conservée. La loi française ne s'applique qu'aux entreprises qui ont des succursales en France ou qui s'adressent explicitement aux citoyens français. Cependant, des géants tels que Coinbase, Binance et Kraken ne s'adressent pas directement au public français (domaines .fr, publicité, etc.). Par conséquent, ces entreprises ne doivent pas demander d'enregistrement à moins qu'elles en fassent la demande volontairement.[91]

L'avantage d'être enregistré en tant que PSAN est l'accès sans restriction aux services bancaires. Comme les émetteurs de jetons dont l'ICO obtient un visa, les PSAN enregistrés auprès de l'AMF ne devraient pas se voir refuser par les établissements bancaires l'accès aux services de dépôt et de compte de paiement. Pourtant, les établissements de crédit se montrent encore réticents à s'engager dans des relations commerciales avec des acteurs impliqués dans des activités liées aux actifs numériques, même si un PSAN est enregistré auprès de l'AMF.[92]

Il serait souhaitable que les entreprises belges, enregistrées auprès de la FSMA en vertu de l'arrêté royal sur les monnaies virtuelles, puissent également avoir accès sans restriction aux services de dépôts des établissement bancaires.

2. BELGIQUE : ARRÊTÉ ROYAL DU 8 FÉVRIER 2022 SUR LES MONNAIES VIRTUELLES

Depuis le 1er mai 2022, les personnes établies en Belgique dont l'activité professionnelle régulière consiste à fournir des services d'échange de crypto-monnaies et à proposer des wallets sur le territoire belge seront tenues de s'enregistrer auprès de l'Autorité belge des services et marchés financiers (FSMA). L'obligation d'enregistrement ne s'applique qu'aux prestataires de services en monnaie virtuelle ayant une présence physique ou un établissement permanent en Belgique. Les guichets automatiques situés sur le territoire belge et permettant l'échange entre monnaie virtuelle et monnaie fiduciaire seront considérés comme un établissement en Belgique et déclencheront l'obligation d'enregistrement auprès de la FSMA.

Il est interdit aux personnes physiques ou morales régies par le droit d'un pays tiers (hors espace économique européen) de fournir ou d'offrir sur le territoire belge, à titre d'activité professionnelle ordinaire ou même à titre d'activité additionnelle ou complémentaire, des services d'échange entre monnaies virtuelles et monnaies fiduciaires, ou d'offrir des services de garde de portefeuille.

Les fournisseurs de monnaies virtuelles de l'espace économique européen peuvent, en revanche, librement fournir leurs services en Belgique sur une base transfrontalière sans être tenus de s'enregistrer auprès de la FSMA (pour autant qu'ils n'aient pas de présence physique en Belgique).

Pour obtenir l'enregistrement auprès de la FSMA, les prestataires de services en monnaie virtuelle doivent satisfaire à diverses conditions d'enregistrement, telles que l'obligation de posséder une fiabilité professionnelle et une expertise appropriée. En outre, des exigences minimales en matière de capital et de lutte contre le blanchiment d'argent (AML) s'appliquent. Les actionnaires doivent également être aptes à assurer une gestion saine et prudente de la société. L'obligation de s'enregistrer auprès de la FSMA s'applique également aux institutions financières réglementées (par exemple, les établissements de crédit, les établissements de paiement, les entreprises d'investissement, etc.) qui fournissent ou offrent, en plus de leurs services de base, des services d'échange de crypto-monnaies et/ou des services de portefeuille dépositaire. Toutefois, ils seront exemptés des conditions d'enregistrement qui leur sont déjà applicables en raison de leur autre statut réglementé.

3. QUELLE IMPOSITION SUR LES OPÉRATIONS DE TRADING DE CRYPTOMONNAIES EN BELGIQUE ?

Pour les entreprises et les magasins qui acceptent le paiement de biens ou de services en bitcoins, il n'y a aucune différence sur la manière dont les bénéfices imposables sont calculés, par rapport aux moyens de paiement standard.

Toute société belge ou entité étrangère active en Belgique qui génère un revenu (ou une perte) en tradant des bitcoins et/ou en échangeant des monnaies (virtuelles), sera assujettie aux règles standard de l'impôt sur les sociétés. L'impôt sur les sociétés sera également dû sur les gains provenant de trading liées aux bitcoins.

91Allouch Benjamin, "Qu'est-ce que le PSAN et comment obtenir ce statut ?", Cryptoast, 2020, disponible à l'adresse suivante : www.cryptoast.fr/psan-services-actifs-numeriques-obtenir-statut/
92 "The French Regulatory Framework for Markets in Crypto-Assets", ADAN, 2020, disponible à l'adresse suivante : www.adan.eu/en/article/french-regulatory-framework-markets-crypto-assets

Pour les particuliers, la question est plus compliquée. La question pertinente à se poser est de savoir si l'activité liée aux bitcoins doit être considérée comme un hobby ou une activité commerciale. La manière dont sont faits les investissements dans le bitcoin influence largement la qualification aux fins de l'impôt sur le revenu.

Les mineurs, les négociants, les échangeurs et les autres prestataires de services qui ne travaillent pas par l'intermédiaire d'une société peuvent potentiellement être soumis à l'impôt belge sur le revenu des personnes physiques. Si la profession du contribuable consiste à négocier la monnaie virtuelle, les bénéfices en bitcoins seront considérés comme des revenus professionnels et imposés comme tels.

Les taux d'imposition progressifs standard compris entre 25 % et 50 % (+ taxe communale) s'appliqueront. En outre, on peut également être soumis à des cotisations de sécurité sociale sur ces revenus. Toutefois, si l'investissement en bitcoins est fait en dehors d'une activité professionnelle, la situation est différente. Si ces opérations peuvent être considérées comme une gestion normale du patrimoine privé, tout gain en résultant sera exonéré de l'impôt sur le revenu. Si les investissements ne relèvent pas du principe de la gestion en bon père de famille et que les risques pris sont élevés, ces opérations seront considérées comme étant à caractère spéculatif aux yeux du fisc belge. Dans ce cas, la plus-value sera imposable comme revenu divers auquel s'appliquera un taux d'imposition forfaitaire de 33% (+ taxe communale).

Le Service des Décisions Anticipées (SDA) du SPF Finances est récemment arrivé à cette conclusion dans la situation où un étudiant en informatique a généré un bénéfice par le biais d'une plateforme de trading en ligne de bitcoins qu'il avait développée (Arrêt n° 2017.852, 5 décembre 2017).

Nous devons souligner que l'évaluation du caractère imposable (ou déductible) d'un bénéfice ou d'un gain dépendra toujours des faits et des circonstances. Les investisseurs potentiels doivent demander conseil pour savoir si leurs activités de trading peuvent être considérées comme un commerce professionnel ou une activité spéculative.

4. EUROPE : EXTENSION, EN 2022, DU TRANSFER OF FUNDS REGULATION (TFR) DE 2015 AUX CRYPTOACTIFS POUR LUTTER CONTRE LE BLANCHIMENT DES CAPITAUX

Selon la quatrième directive sur le blanchiment de capitaux, les fournisseurs de services de crypto-monnaies deviendraient des « sociétés assujetties ». Dès le premier euro, le TFR sera appliqué à toutes les transactions de et vers les prestataires de services de cryptomonnaies. Cela s'applique à tous les échangeurs (comme les plateformes d'échange centralisées, telles que Binance, Coinbase...).

Avec le TFR, les prestataires devront rassembler des données sur les parties prenant part à une transaction. Les transferts de et vers les « portefeuilles non hébergés » (également connus sous le nom de «cold wallets», tels que le portefeuille Ledger) vers une plateforme d'échanges seront également soumis à la législation TFR. Pour les transferts supérieurs à 1.000 €, lorsque le transfert est effectué vers ou depuis un portefeuille appartenant à un client de prestataire, la vérification de l'identité du bénéficiaire effectif du portefeuille non hébergé sera également requise.

Cela dit, les transferts dits P2P (c'est-à-dire les transferts qui ne passent pas par un prestataire) sont exemptés de la loi TFR. Le Parlement européen a déclaré dans un communiqué que les règles ne s'appliquent pas aux transferts de personne à personne effectués sans prestataire de services, comme les plateformes d'échange, ou entre prestataires de services agissant pour leur propre compte. Un utilisateur ayant un portefeuille non hébergé peut donc déplacer ses cryptomonnaies vers un portefeuille numérique décentralisé.

L'objectif est de rendre plus difficile l'utilisation des cryptomonnaies à des fins illicites par les criminels. Selon les institutions européennes, le nouvel accord permettra à l'UE de faire face aux risques de blanchiment d'argent et de financement du terrorisme associés à ces nouvelles technologies, dans un équilibre liant la compétitivité, la protection des consommateurs et des investisseurs, et la protection de l'intégrité financière du marché intérieur.

5. EUROPE : MARKETS IN CRYPTO-ASSETS (MICA) 2022

La réglementation MiCA (Markets in Crypto-Assets) s'appliquera dans toute l'Union européenne sans qu'il soit nécessaire d'adopter des lois nationales de mise en œuvre. Cette approche va dans le sens de la protection des consommateurs et de la garantie d'un accès efficace et harmonisé aux marchés des cryptoactifs dans l'ensemble du marché unique.

Le règlement sur les marchés des cryptoactifs poursuit quatre objectifs essentiels :

- le premier est de garantir la sécurité juridique en établissant un cadre législatif solide pour les cryptoactifs entrant dans son champ d'application et qui ne sont pas couverts par la législation existante sur les services financiers ;
- le deuxième est de soutenir l'innovation et la concurrence loyale afin de promouvoir le développement des cryptoactifs en instituant un cadre sûr et proportionné ;
- le troisième est, évidemment, de protéger les consommateurs, les investisseurs et l'intégrité du marché en tenant compte des risques associés aux cryptoactifs.
- Enfin, la réglementation MiCa vise à assurer la stabilité financière, avec l'inclusion de garanties pour faire face aux risques potentiels pour la stabilité financière.

Les émetteurs de cryptoactifs entrant dans le champ d'application de la MiCA, à savoir ceux qui proposent des cryptoactifs à des tiers, peuvent être soumis à plusieurs obligations.

La première est la publication d'un livre blanc présentant certaines similitudes avec les prospectus publiés en vertu du règlement sur les prospectus pour les produits financiers.

La deuxième est la nécessité d'être autorisé à émettre des cryptoactifs en respectant certaines règles prudentielles lors de la commercialisation de ceux-ci.

Les émetteurs ont l'obligation d'agir de manière honnête, équitable et professionnelle vis-à-vis des détenteurs de cryptoactifs, notamment en ce qui concerne la gestion des litiges et le maintien des protocoles de sécurité.

L'entrée en application du règlement sur les marchés des cryptoactifs était initialement prévue pour la mi-2023. Il est toutefois probable qu'elle soit reportée à 2024, car une période de 18 mois est prévue pour permettre l'adoption de mesures avant l'application du MiCA.

Malheureusement, de nombreux acteurs du secteur sont alarmés par les perspectives de MiCA. En premier lieu, ils regrettent l'absence de sollicitation des sociétés de crypto-monnaies européennes pour participer à ces débats, ce qui permettrait de mieux comprendre leurs activités. Elles sont en effet les meilleurs interlocuteurs pour évaluer les impacts des nouvelles propositions réglementaires et estimer quelles règles sont adaptées, proportionnées et efficaces. La réglementation MiCA affectera les entreprises et les emplois à un niveau micro et l'avenir de l'économie numérique européenne à un niveau macro : il est dangereux de prendre des décisions aussi importantes pour l'avenir sans une parfaite connaissance du secteur, des risques mais aussi des opportunités des crypto-actifs et des conséquences des évolutions réglementaires.

L'Association pour le Développement des Actifs Numériques (Adan) estime que MiCA pourrait manquer les objectifs de l'UE de trouver un juste équilibre entre la protection des investisseurs et le renforcement de l'innovation. C'est ce que nous a expliqué sa présidente Faustine Fleuret dans deux entretiens qu'elle nous a accordés.[93] L'Adan propos trois axes d'amélioration qui pourraient contribuer à rétablir cet équilibre.

Le premier axe est la proportionnalité. Les innovations apportées par les cryptoactifs sont construites par des nouveaux venus. Selon l'état des lieux de l'industrie des cryptomonnaies en 2020 réalisé par l'Adan, 83 % des cryptomonnaies françaises ont moins de cinq ans. Les 600 projets de crypto en France (selon la banque publique d'investissement Bpifrance) entrent dans différents secteurs économiques. A cet effet, miser sur les seuls acteurs historiques pour construire des marchés de cryptoactifs n'est pas une stratégie gagnante. S'il est évidemment normal de créer des passerelles entre les acteurs traditionnels et les nouveaux marchés pour s'appuyer sur leur expérience réglementaire, le profil spécifique des nouveaux pure players doit également être pris en compte.

A ce titre, selon l'état des lieux précité de l'Adan, 62 % des équipes ont moins de 10 salariés, la grande majorité des entreprises peinent à trouver des financements, etc. Cela implique des règles plus proportionnées pour les prestataires de services en cryptoactifs et les émetteurs de stablecoins (en termes d'exigences de fonds, de liquidité, etc.), un dimensionnement des exigences pour les entités en fonction de la taille et de la maturité de leurs activités, l'octroi des mêmes exemptions que celles dont bénéficient les autres intermédiaires financiers lorsque les acteurs crypto remplissent les mêmes conditions. La proportionnalité devrait être appréciée par la réalisation d'analyses d'impact des exigences MiCA par les autorités européennes.

Le deuxième axe est l'adaptabilité pour permettre l'exploitation des opportunités technologiques. Non seulement le MiCA ne s'appuierait pas suffisamment sur les opportunités technologiques, mais il ne prend pas non plus en compte les spécificités des cryptoactifs et des technologies blockchain. Si s'inspirer du paradigme réglementaire traditionnel est compréhensible dans un premier temps, une prochaine étape nécessaire consisterait à rationaliser les règles lorsqu'elles ne sont pas adaptées ou peuvent être simplifiées sans nuire à la protection des investisseurs ou à la stabilité des marchés. Les exigences de MiCA devraient s'appuyer sur les compétences opérationnelles et techniques des nouveaux acteurs et sur leur expérience en tant que pure players. Cela éviterait de créer des situations où les entreprises ne peuvent pas se conformer de facto et où des règles inefficaces et trop contraignantes nuisent à leurs activités.

Le dernier axe est le pragmatisme. En tant que secteur nouveau puis moins mature, l'industrie des cryptoactifs est encore en cours de structuration. L'introduction de réglementations ne doit pas remettre en cause le développement des entreprises ni leur compétitivité. Il est donc essentiel de rétablir la progressivité des règles du MiCA. Une approche plus réaliste est exigée également des superviseurs qui devront s'adapter à l'extension du champ des entités qu'ils supervisent, développer leurs compétences et se doter de tous les moyens nécessaires. La progressivité apparaît alors essentielle pour assurer une supervision efficace et ne pas pénaliser les acteurs. Elle devrait se traduire par la création d'une voie rapide pour les acteurs déjà autorisés dans le cadre des régimes nationaux (comme cela a été fait pour les acteurs du crowdfunding), l'octroi de périodes de tolérance plus réalistes pour qu'ils se mettent en conformité, la planification d'une mise en œuvre progressive de MiCA et d'autres réglementations s'appliquant aux acteurs de la cryptomonnaie (comme les réglementations sur la lutte contre le blanchiment d'argent et le financement du terrorisme) et l'engagement d'un travail à long terme sur les DeFi et les NFT.

93 Respectivement le 16 juin et le 21 juin 2022

V. DANGERS & DÉFIS DES CRYPTOMONNAIES

VOLS

Compte tenu du fait que les monnaies numériques sont virtuelles et stockées dans un portefeuille numérique, elles sont susceptibles d'être piratées, volées ou détournées de manière frauduleuse. Bien qu'aucune méthode de paiement ne soit sans danger, la monnaie virtuelle est encore plus risquée que les monnaies traditionnelles. En effet, malgré le fait que la contrefaçon de la propriété d'un Bitcoin (par exemple) est impossible (en raison du cryptage et de l'enregistrement des transactions par les mineurs), les pirates peuvent voler les données donnant accès aux portefeuilles électroniques. Si les clés du portefeuille d'un utilisateur sont volées, le voleur peut se faire passer pour le propriétaire initial du compte et a le même accès aux fonds du portefeuille que ce dernier. Une fois que le Bitcoin est échangé hors du compte et que l'échange est enregistré dans la blockchain, il est perdu à jamais pour le propriétaire initial.[94]

VOLATILITÉ

Les marchés de cryptomonnaies sont particuliers car la monnaie ne s'échange que sur demande des utilisateurs, sans organe de régulation. Comme l'offre de la monnaie est limitée, cette dernière peut être confrontée à des problèmes de liquidité et la rendre vulnérable aux manipulations du marché. En outre, en raison de sa faible adoption, la monnaie peut avoir tendance à être plus imprévisible que d'autres monnaies physiques, sous l'effet d'achats et de ventes spéculatives.[95]

En effet, la spéculation est l'une des causes les plus importantes de la volatilité des cryptomonnaies. En réalité, c'est l'incertitude du marché des cryptomonnaies qui attire les traders spéculateurs. Ils tentent de prédire les fluctuations à la hausse et à la baisse des marchés, afin de prendre des positions en fonction de ces prédictions et réaliser un bénéfice. Ces paris spéculatifs ajoutent de l'incertitude à un marché déjà agité.[96]

Aujourd'hui, le nombre d'usager des cryptomonnaies est assez faible en comparaison avec celui des usagers des monnaies classiques (comme le dollar et l'euro, par exemple). Par conséquent, la décision d'un petit nombre d'acteurs de vendre ou d'acheter peut influencer énormément les cours. Cependant, cette volatilité est amenée à se réduire au fur et à mesure que le nombre d'usagers d'une cryptomonnaie augmentera.[97]

*94 Khan Ruby et Hakami Tahani Ali, « Cryptocurrency: usability perspective versus volatility threat », **Journal of Money and Business**, 2021, p. 8.*
*95 **Ibid.**, p. 7.*
*96 **Ibid.**, p. 8.*
*97 « Perri Scope du jeudi 20 mai 2021 », **LCI**, disponible à l'adresse suivante : www.tf1info.fr/replay-lci/video-perri-scope-du-jeudi-20-mai-2021-2186600.html (consultée le 2 mai 2022).*

MAI 2022 : CRASH DU MARCHÉ DES CRYPTOMONNAIES

Pendant la pandémie de coronavirus, les gens se sont rués vers les cryptomonnaies : 16 % des Américains en possèdent désormais, contre 1 % en 2015, selon une enquête du Pew Research Center. Les premiers investisseurs sont probablement encore dans une position confortable. Mais les baisses rapides de cette semaine ont été particulièrement sévères pour les investisseurs qui ont acheté des cryptomonnaies lorsque les prix se sont envolés l'année dernière. La chute des cryptomonnaies s'inscrit dans un mouvement plus large de repli des actifs risqués, stimulé par la hausse des taux d'intérêt, l'inflation et l'incertitude économique causée par l'invasion de l'Ukraine par la Russie.[98]

Si le passé se répète, alors le creux actuel (ou le crash, selon les points de vue) pourrait rebondir comme il l'a fait l'année dernière, lorsque les prix ont chuté à des niveaux similaires avant de revenir aux niveaux d'avant le creux et même d'atteindre un sommet à l'automne. Mais bien sûr, cela pourrait ne pas être le cas. Les prix du bitcoin, en particulier, ont montré un certain degré de saisonnalité jusqu'à présent, semblant perdre de la valeur dans des proportions plus ou moins importantes au printemps avant de rebondir au début de l'été. Cependant, comme pour tout type d'investissement, les performances passées ne garantissent pas les résultats futurs.[99]

*98 Yaffe-Bellany David, « Cryptocurrencies Melt Down in a 'Perfect Storm' of Fear and Panic », **The New York Times**, 2022, disponible à l'adresse suivante : www.nytimes.com/2022/05/12/technology/cryptocurrencies-crash-bitcoin.html*
*99 Mark Hooson, « Crypto Market Crash: Is It The Right Time To Buy The Dip? », **Forbes**, 2022, disponible à l'adresse suivante : www.forbes.com/uk/advisor/investing/cryptocurrency/crypto-market-crash-is-it-the-right-time-to-buy-the-dip*

MANIPULATION DE MARCHÉ

Un type de manipulation de marché est le « pump and dumps », où le prix d'une cryptomonnaie est volontairement augmenté par un achat collectif et massif de cette cryptomonnaie, suivi d'une vente brutale au prix qui a été artificiellement surévalué. L'utilisation de cette technique dans l'univers crypto atteint des proportions jamais vues auparavant et, souvent, les systèmes « pump and dumps » ne sont même pas réalisés secrètement ou à l'insu des consommateurs.[100]

La vente d'actifs surévalués peut également être réalisée avec la méthode « traditionnelle » de la pyramide de Ponzi, où les nouveaux investisseurs qui achètent un cryptoactif paient pour les anciens détenteurs. Les systèmes de Ponzi ont souvent recours au recrutement actif de nouveaux détenteurs pour faire augmenter le prix des cryptoactifs possédés par les anciens détenteurs.[101]

BLANCHIMENT D'ARGENT

Avant d'aborder le blanchiment d'argent effectué via les cryptomonnaies, commençons par présenter brièvement le modèle classique. Le blanchiment d'argent est un processus en trois étapes : placement, superposition et intégration. La phase de placement consiste à placer l'argent acquis illicitement dans une entreprise légitime afin de créer une distance initiale entre l'argent et l'infraction principale. Au stade de la superposition, l'argent est utilisé dans de nombreuses transactions légales afin de créer une distance supplémentaire entre l'argent et l'acte criminel. L'étape finale est l'intégration où l'argent est réintroduit dans le système financier légitime.[102]

Le blanchiment d'argent avec les cryptomonnaies est semblable au blanchiment d'argent classique. Ce sont les propriétés inhérentes à la cryptomonnaie qui accroissent la difficulté pour lutter contre ce processus.

Le premier défi posé par les cryptomonnaies est la difficulté de relier directement un utilisateur physique à un token (qui est une unité de cryptomonnaie). Le deuxième défi est qu'il est presque impossible d'interrompre les transactions faites via les cryptomonnaies. Le troisième challenge est la présence d'un cryptage sophistiqué qui renforce le degré d'anonymat. Cette caractéristique complique les enquêtes, la récolte de preuves et la confiscation des cryptomonnaies acquises par le fruit d'un bénéfice illicite.[103]

Pire, bien que les transactions en Bitcoin, en Litecoin et en Dash soient difficiles à tracer, mais pas impossible, d'autres cryptomonnaies sont conçues spécialement pour assurer l'anonymat des détenteurs et des transactions (comme le Monero et le Zcash, par exemple).[104]

Un autre avantage pour les criminels est le fait que les cryptomonnaies sont de plus en plus acceptées comme forme de paiement par certains commerçants.[105]

Enfin, les cryptomonnaies peuvent être déplacées d'un pays à un autre, facilement, rapidement et à peu de frais. Dans l'étape de superposition du processus de blanchiment d'argent, les cryptomonnaies sont utilisées pour faire une myriade de transactions financières, mais aussi pour être transférées vers différents pays avec différentes juridictions, ce qui complique encore davantage le travail des enquêteurs.[106]

Cela dit, comme nous le verrons plus loin, il y a une grande exagération dans la critique selon laquelle les cryptomonnaies fournissent un terrain propice au blanchiment. La réalité est que, une fois l'infraction découverte, la poursuite des fraudeurs est beaucoup plus efficace en raison de la traçabilité.

EFFET DE LEVIER

Dans le trading de cryptomonnaie, l'effet de levier désigne l'utilisation de capitaux empruntés pour effectuer des transactions. Le trading à effet de levier peut amplifier le pouvoir d'achat ou de vente, ce qui vous permet de trader des montants plus importants. Ainsi, même si votre capital initial est faible, on peut l'utiliser comme garantie pour effectuer des transactions à effet de levier. Si le trading à effet de levier peut multiplier les profits potentiels, il est également soumis à un risque élevé - en particulier sur le marché volatile des crypto-monnaies. Des entreprises asiatiques, telles que BitMEX, autorisaient un effet de levier de x100 pour les échanges de crypto-monnaies.[107]

---

100 Horváth Ágnes, « Protection of consumers provided in the proposal for a regulation of markets in crypto assets », Édition Katarina Ivančević, 2021, p. 249.

*101 Horváth Ágnes, « Protection of consumers provided in the proposal for a regulation of markets in crypto assets », **op. cit.**, p. 252.*

*102 Albrecht Chad et al., « The use of cryptocurrencies in the money laundering process. » , **Journal of Money Laundering Control**, 2019, vol. 22, n°2, p. 211.*

*103 Mabunda Sagwadi, « Cryptocurrency: The new face of cyber money laundering », **International Conference on Advances in Big Data, Computing and Data Communication Systems**, 2018, p. 9.*

*104 Albrecht Chad et al., « The use of cryptocurrencies in the money laundering process. », **op. cit.**, p. 214.*

*105 Mabunda Sagwadi, « Cryptocurrency: The new face of cyber money laundering », **op. cit.**, 2018, p. 7.*

*106 **Ibid.**, p. 2.*

*107 « What Is Leverage in Crypto Trading? », **Binance**, 2022, disponible à l'adresse suivante : www.academy.binance.com/en/articles/what-is-leverage-in-crypto-trading, (consulté le 14 juin 2022).*

Si les prix baissent, ils doivent rembourser la société de courtage dans ce que l'on appelle un «appel de marge». Dans ce contexte, il y a souvent un prix fixe qui déclenche la vente afin de s'assurer que les traders peuvent rembourser la bourse. Le danger pour l'écosystème est qu'il y a un effet de foule : les prix de liquidations ont tendance à être proches les uns des autres. Donc, quand ce niveau est atteint, tous ces ordres de vente automatiques arrivent, et le prix descend en cascade». Cet effet accentue la volatilité de ces marchés.[108]

CONFIANCE

L'avantage des monnaies classiques, dites « fiat », est que leur stabilité est garantie par un État au travers d'une banque centrale. Cette caractéristique, que n'ont évidemment pas les crypto-monnaies, est source de confiance pour les utilisateurs. Cependant, dans l'émission Perri Scope du jeudi 20 mai 2021, Ferghane Azihari rappelle que les plus grandes catastrophes monétaires ont toutes été le résultat de politiques menées par des États (notamment l'hyperinflation sous la République de Weimar et les assignats sous la Révolution française).[109]

De plus, depuis les accords Bretton Wood, ces monnaies ne sont plus adossées à un actif (qui était l'or, précédemment). Cela a rendu possible l'impression de billets par les banques centrales, qui n'ont pas manqué d'y avoir recours. Or, le bitcoin, par exemple, est fondé sur la promesse qu'il n'y aura jamais plus de 21 millions d'unités en circulation. Ce qui est un avantage considérable pour un actif ayant comme objectif d'être une réserve de valeur.

*108 « Bitcoin traders using up to 100-to-1 leverage are driving the wild swings in cryptocurrencies », **CNBC**, 2021, disponible à l'adresse suivante : www.cnbc.com/2021/05/25/bitcoin-crashes-driven-by-big-margin-bets-new-crypto-banking.html, (consulté le 14 juin 2022).*

*109 « Perri Scope du jeudi 20 mai 2021 », **LCI**, **op. cit.***

VI. A QUOI SERVENT LES CRYPTOMONNAIES ?

PROTECTION CONTRE L'INFLATION POUR LES ÉPARGNANTS

Pour illustrer ce cas d'usage, nous allons nous focaliser sur le bitcoin, mais d'autres cryptomonnaies peuvent remplacer un rôle comparable. Le principal facteur qui fait de cet actif numérique une protection contre l'inflation est son offre limitée de tokens. Lorsque Satoshi Nakamoto a créé la plus grande crypto-monnaie du monde, il a intégré dans le code source du bitcoin un hard-cap qui limitait la circulation à 21 millions de bitcoins. Depuis lors, environ 19 millions de pièces ont déjà été générées, et il n'en reste plus que 2 millions. Personne ne peut modifier le code source du bitcoin pour augmenter l'offre. Par conséquent, les pièces qui existent déjà finiront par se raréfier, ce qui augmentera la demande et, par conséquent, le prix de l'actif. En outre, contrairement à l'or, le bitcoin est extrêmement portable. Il peut être transféré d'un coin du monde à un autre en quelques secondes. Il est également accessible à toute personne possédant un smartphone et ayant accès à l'internet. Il est donc accessible aux masses «non bancarisées». Théoriquement, il devrait être une excellente couverture contre l'inflation. Son offre est limitée, ce qui en fait un actif rare. Il est fongible, ce qui signifie qu'un bitcoin peut être échangé contre un autre sans perte de valeur. Il est également facilement accessible, jouit d'une large acceptation et a prouvé son appréciation.[110]

Cela dit, cet avantage est relatif. En effet, les « baleines » du bitcoin (à savoir les gros détenteurs de cette monnaie) ont également été en mesure de manipuler le prix de l'actif en achetant ou en vendant l'actif en masse. Cela indique que des forces spéculatives sont à l'origine du prix du bitcoin. Elles pourraient modifier le prix de l'actif, qu'il y ait ou non une période d'inflation.

Un autre problème du bitcoin est le nombre de réglementations auxquelles il est actuellement confronté de la part des législateurs du monde entier. Cela signifie que le prix de l'actif est souvent à la merci des institutions et des gouvernements. Et les réglementations strictes à l'encontre du bitcoin peuvent entraver l'adoption de l'actif, entraînant une dépréciation des prix.[111]

CRÉDITS À DESTINATION DE POPULATION NON-BANCARISÉE

En Amérique latine, sur une population de 644 millions d'habitants, plus de 400 millions de personnes n'ont pas de compte bancaire. C'est le ratio le plus élevé au monde de personnes non-bancarisées. L'impossibilité de contracter des crédits est un frein majeur pour le développement de ces économies. C'est pour y remédier que le Ripio Credit Network (RCN) a été créé.[112]

RCN, née en Argentine, a pour objectif d'étendre l'inclusion financière en proposant des crédits partout dans le monde et dans n'importe quelle devise locale. L'entreprise compte plus de 300 000 utilisateurs actifs et affirme être le produit blockchain le plus populaire d'Amérique latine. Le réseau fonctionne sur la base de contrats intelligents cosignés, reliant ainsi les emprunteurs, les prêteurs et les agents cosignataires. Ce dernier neutralise le risque de crédit du prêteur et, en cas de défaillance, dispose des outils nécessaires pour gérer la dette dans le pays de résidence de l'emprunteur.[113]

*110 «How does Bitcoin work as a hedge against inflation? », **CNBC**, 2022, disponible à l'adresse suivante : www.cnbctv18.com/cryptocurrency/how-does-bitcoin-work-as-a-hedge-against-inflation-13052422.htm*
*111 «How does Bitcoin work as a hedge against inflation? », **CNBC**, 2022, disponible à l'adresse suivante : www.cnbctv18.com/cryptocurrency/how-does-bitcoin-work-as-a-hedge-against-inflation-13052422.htm*
*112 Verbiest Thibault et van Gelderen Alain, « Tout ce que vous avez toujours voulu savoir sur les cryptomonnaies sans jamais oser le demander », **Lucpire éditions**, 2022, pp. 117-120.*
*113 Butcher Mike, « Ripio Credit Network launches, aiming to attack bank loan fees in emerging markets », **Techcrunch**, 2017, disponible à l'adresse suivante : http://tcrn.ch/2yprxBw*

RECOMMANDATIONS

Corentin de Salle & Olaf van der Straten

1. FAVORISER, LÀ OÙ C'EST POSSIBLE, LE PAIEMENT AVEC DE LA CRYPTOMONNAIE AFIN DE CRÉER DES ÉCOSYSTÈMES DE PAIEMENT ET FAIRE DE LA BELGIQUE UN HUB EUROPÉEN DES TECHNOLOGIES BLOCKCHAIN

Si la Belgique devenait un hub européen des technologies blockchain, les retombées économiques seraient considérables. Pour atteindre cet objectif, il faut envoyer des signaux forts d'ouvertures à ces technologies.

Un exemple serait, dans les transports en commun, de permettre aux utilisateurs qui le désirent de régler leurs tickets en cryptomonnaie. Cela favoriserait leur usage auprès des jeunes qui sont les plus friands de ces innovations. De plus, cette implémentation serait facile et peu coûteuse : le paiement peut se faire avec des QR codes et en convertissant automatiquement et instantanément les cryptomonnaies en euros, les entreprises de transports seraient prémunies du risque de fluctuation des cours.

2. ACCORDER À CHAQUE CITOYEN UN PORTEFEUILLE DE DONNÉES NUMÉRIQUES DÉCENTRALISÉ FONCTIONNANT GRÂCE AUX TECHNOLOGIES BLOCKCHAIN

Les grandes plateformes numériques permettent à leurs utilisateurs de se connecter à divers services en ligne, qu'il s'agisse de faire des achats ou de lire la presse, mais ces connexions ne permettent pas aux utilisateurs de contrôler totalement quelles données ils partagent lorsqu'ils s'identifient pour utiliser des services en ligne. L'Union européenne a fait des propositions pour créer des portefeuilles numériques personnels permettant aux citoyens de s'identifier numériquement, de stocker et de gérer des données d'identification et des documents officiels sous format électronique. Il peut s'agir d'un permis de conduire, d'une prescription médicale ou encore d'un diplôme d'études.

Avec le portefeuille numérique, les citoyens pourront prouver leur identité si cela est nécessaire pour accéder à des services en ligne, partager des documents numériques ou simplement prouver un attribut personnel spécifique, tel que l'âge, sans révéler leur identité ou d'autres données personnelles.

Les citoyens auront à tout moment le plein contrôle des données qu'ils partagent. En effet, les utilisateurs seront en mesure de contrôler les données à caractère personnel qu'ils souhaitent partager avec les services en ligne.

Le plein contrôle de ces données implique que ce portefeuille soit décentralisé, c'est-à-dire qu'elles ne soient pas toutes stockées et gérées par une entité centrale. L'identité est un ensemble d'attributs très disparates qui ne doivent pas être en possession d'une entité. Il faut au contraire un « triangle de confiance » faisant intervenir chaque fois un émetteur des certificats (par exemple le SPF Pensions, une école privée, une agence de voyage, etc.), un titulaire (le citoyen) et un vérificateur (une entreprise qui embauche, une autorité publique octroyant une allocation, etc.). L'autorité publique détient évidemment, depuis toujours, un certain nombre de données sur ses citoyens (notamment tout ce qui concerne l'état civil) mais pas l'intégralité de ces dernières car l'identité d'une personne ne se réduit pas, loin de là, à sa qualité de citoyen. C'est donc un émetteur parmi quantité d'autres.

Ce portefeuille pourrait permettre d'accéder à des services en ligne aussi bien publics que privés dans l'UE, en particulier ceux qui nécessitent une authentification renforcée de l'utilisateur. Il peut s'agir, par exemple, d'accéder à un compte bancaire ou de demander un prêt, de présenter des déclarations fiscales, de s'inscrire dans une université de votre pays d'origine ou à l'étranger et de nombreuses autres démarches faites avec un moyen d'identification habituel.[114]

*114 « La Commission propose une identité numérique fiable et sécurisée pour tous les Européens – Questions et réponses », **Commission européenne**, 3 juin 2021, disponible à l'adresse suivante : www.ec.europa.eu/commission/presscorner/detail/fr/QANDA_21_2664 (consultée le 9 mai 2022).*

Aujourd'hui, 19 systèmes d'identification électronique notifiés sont utilisés par 14 États membres, couvrant presque 60 % de la population de l'UE-27, mais le taux d'adhésion à ces systèmes est faible, leur utilisation est contraignante et leur usage commercial est limité.[115]

La Belgique, à l'initiative de Mathieu Michel, Secrétaire d'État à la Digitalisation, souhaite proposer à chaque citoyen, dès 2023, un portefeuille numérique. Des initiatives ont déjà été prises (eID, eBox, MyMinfin, MyPension, etc.). Mais avec un gros souci : elles ont été, le plus souvent, conçues et développées en silos, c'est-à-dire de façon compartimentée, ce qui ne facilite pas la vie des citoyens. L'objectif serait que ce nouveau portefeuille numérique permette de demander, entre autres, un renouvellement de carte d'identité ou un permis de conduire, un acte de naissance, la certification d'un diplôme ou l'accès à des tarifs sociaux en matière de télécoms.[116]

Ce portefeuille numérique pourrait être développé à l'aide des technologies blockchain, permettant de garantir que les données sont infalsifiables et que leur stockage est décentralisé.

3. GARANTIR UN « DROIT AU COMPTE » POUR LES ENTREPRISES LIÉES AUX CRYPTOACTIFS

L'une des principales difficultés pour les entrepreneurs crypto en Belgique est la quasi -impossibilité de créer un compte en banque pour leur société. En effet, ces activités n'étant pas régulées, les banques préfèrent ne pas prendre de risque et refusent simplement de travailler avec ces sociétés. Cela représente un frein majeur pour le développement de cet écosystème en Belgique.

Pour pallier cela, il suffirait que les autorités de régulation établissent des lignes directrices, à destination des banques. Celles-ci pourraient déterminer les précautions que le secteur bancaire devrait prendre pour mitiger le risque en travaillant avec des entreprises actives dans l'écosystème crypto.

En Angleterre, Sam Woods, le directeur de la Prudential Regulation Authority a adressé une lettre aux banques, compagnies d'assurance et entreprises d'investissement dans ce but précis. Dans celle-ci, il rappelle que les cryptomonnaies pourraient représenter un risque pour la stabilité financière notamment à cause des risques de contagion, des effets de levier et la faible liquidité de ces marchés. Dès lors, il invite les banques à agir de telle sorte que la sécurité et leur solidité soient conservées. Par conséquent, Sam Woods invite le secteur bancaire à agir de manière prudente, à avoir des stratégies de risque et des systèmes de gestion des risques efficaces et à traiter avec les régulateurs de manière ouverte et coopérative, en divulguant de manière appropriée tout ce qui devrait être porté à la connaissance de la Prudential Regulation Authority. Par exemple, certaines activités peuvent nécessiter une surveillance plus fréquente, une prise en compte plus grande de l'incertitude dans la modélisation ou l'évaluation des risques ou des seuils de tolérance au risque inférieurs à ceux qui sont généralement appliqués. Compte tenu de ces incertitudes, les entreprises doivent également envisager l'utilisation de stress test afin d'être sûres que les risques sont suffisamment pris en compte. Par ailleurs, les entreprises bancaires doivent prendre en compte l'extrême volatilité des prix de ces actifs pour déterminer la réserve de fonds propres appropriée.[117]

4. CRÉER UN CRYPTO EURO DE BANQUE CENTRALE

Depuis quelques années, on a vu apparaître la notion de « monnaie numérique de banque centrale » (MNBC). Concept assez paradoxal car, dans sa philosophie même, la cryptomonnaie est née, comme on le sait, dans la volonté de décentraliser la monnaie et retirer leur pouvoir monétaire aux banques centrales. Ces idéaux libertariens sont comparables à ceux qui animaient les fondateurs d'internet. Et ces derniers sont appelés à s'atténuer voire à se compromettre avec le pragmatisme du monde de la finance. Ainsi, plusieurs banques centrales sont désireuses de récupérer ces nouveaux objets que sont les cryptomonnaies et de bénéficier ainsi des avantages de la technologie blockchain.

Les banques centrales peuvent s'approprier certains des avantages d'une monnaie numérique sans abandonner leur politique monétaire en émettant leurs propres monnaies numériques qui seraient librement convertibles à un taux de change fixe de « un pour un ». Contrairement aux monnaies numériques privées, une monnaie numérique de banque centrale aurait cours légal, de sorte que la définition traditionnelle de la monnaie au sens étroit inclurait désormais, outre les dépôts à vue et les espèces détenues par le public, la monnaie numérique de la banque centrale. La monnaie numérique détenue par les banques traditionnelles dans la banque centrale serait considérée comme des réserves. La base monétaire comprendrait donc, outre les réserves bancaires et les espèces, également cette nouvelle monnaie. Il y a évidemment plus d'une façon de mettre en œuvre les détails d'une telle monnaie numérique de banque centrale. [118]

---

115 ***Ibid.***

116 Lovens Pierre-François, « Mathieu Michel veut offrir un 'portefeuille numérique' à chaque Belge dès 2023 », ***La Libre****, 18 octobre 2021, disponible à l'adresse suivante : www.lalibre.be/belgique/politique-belge/2021/10/18/mathieu-michel-veut-offrir-un-portefeuille-numerique-a-chaque-belge-des-2023-FNRIP34LHVDWHOMOQEW2FU4KGI/ (consultée le 9 mai 2022).*

117 Woods Sam, « Existing or planned exposure to cryptoassets », ***Prudential Regulation Authority****, 2022, disponible à l'adresse suivante : www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2022/march/existing-or-planned-exposure-to-cryptoassets.pdf?la=en&hash=9C23154F16580082C3DD6437B4C3352591A0F946 (consultée le 31 mai 2022).*

118 Cukierman Alex, « Welfare and political economy aspects of a central bank digital currency », ***Centre for Economic Policy Research****, 2019, p.7.*

Considérons les deux alternatives suivantes :

- **une version radicale** dans laquelle la banque centrale (profitant des économies pour les coûts de transaction permises par la nouvelle technologie) permet au grand public de tenir des comptes en monnaie numérique hébergée directement chez elle. En conséquence, les transactions privées peuvent être compensées directement par la banque centrale ;

- **une version modérée**, dans laquelle la banque centrale maintient la tradition institutionnelle selon laquelle seules les banques privées peuvent conserver des dépôts auprès de la banque centrale.

Dans les deux cas, le public a accès à la monnaie numérique de la banque centrale mais, dans la version modérée, cet accès est mis en œuvre via le système bancaire privé plutôt que directement. Ainsi, si un particulier souhaite acheter de la monnaie numérique émise par la banque centrale, il ne peut le faire que par l'intermédiaire d'une banque privée en échange de fonds provenant soit d'un dépôt, soit d'espèces. En revanche, dans la version radicale, le particulier peut obtenir la nouvelle monnaie numérique auprès d'autres particuliers ayant des comptes à la banque centrale sans l'intermédiaire du système bancaire privé. La différence entre la version radicale et la version extrême du point de vue du système bancaire privé est fondamentale. Dans le premier cas, les banques risquent de perdre une grande partie de leurs activités traditionnelles.[119]

Les avantages d'une monnaie numérique émise par la Banque centrale, dans sa version radicale, seraient multiples.

D'abord, les banques centrales ne pouvant pas faire défaut, les épargnants qui choisiraient d'épargner leur argent en crypto euro, hébergé par la Banque centrale, se prémuniraient du risque de faillite qui existe pour les banques classiques. En effet, même si la chose est peu connue, il faut savoir que la seule créance que le citoyen détient sur la banque centrale est issue des pièces de monnaies et des billets qui sont en leur possession. Pour le reste de la monnaie en circulation, il s'agit d'une créance sur les banques commerciales, entités privées. Les dépôts des citoyens sont assurés par la BCE mais uniquement pour un montant de 100.000 €. Or, avec un crypto euro, la monnaie numérique serait garantie par la Banque Centrale elle-même.

Ensuite, ce compte à la BNB pourrait être gratuit, à l'inverse des comptes à vue des banques traditionnelles qui sont souvent facturés aux clients. Cet e-euro pourrait permettre aux consommateurs et aux commerçants belges de faire des transactions sans frais. Un projet semblable a été formulé par le gouvernement estonien, qui a pour projet de créer un « Estcoin ».[120] Cet euro numérique permettrait aux citoyens européens qui le désirent de disposer d'une monnaie numérique qu'ils peuvent s'échanger d'individu à individu (de « wallet » à « wallet ») sans passer par un intermédiaire bancaire.

Enfin, un euro numérique est également nécessaire pour éviter que le dollar aujourd'hui, et l'e-yuan chinois demain, ne soient les seules monnaies de référence dans les échanges internationaux. Un euro numérique permettrait de renforcer la souveraineté monétaire de l'Union européenne.

Pour que cet e-euro soit adopté par une grande partie des citoyens, ceux-ci doivent être assurés de sa sécurité, en tant que moyen d'échange et de stockage de valeur, mais aussi de la confidentialité associée à leurs données personnelles. Le risque pour la Belgique, et plus largement l'Europe, serait d'emprunter une voie similaire à celle de la Chine. Il a été particulièrement éloquent de constater que, dans le cadre de la lutte contre le Covid-19, les nouvelles technologies ont été un atout pour les régimes autoritaires dans leur volonté d'imposer une centralisation extrême de l'information. A cet égard, le contrôle et la surveillance politique des citoyens chinois semblent être le but ultime de la politique monétaire numérique de la Chine. Il est essentiel que les pays européens suivent une voie radicalement différente. Cette nouvelle monnaie doit incarner les valeurs de notre vieux continent. Il est donc essentiel que le respect de la vie privée soit garanti. L'une des pistes pour atteindre cet objectif est l'utilisation de pseudonymes pour les titulaires de comptes qui ne pourraient être associés à une identité qu'en cas de demande spécifique d'un juge.[121]

Comme le suggère Thibaut Verbiest,[122] si on introduit une cryptomonnaie d'Etat, il faudrait, à tout le moins que, jusqu'à un certain montant, cette monnaie soit traitée comme est traité le cash dans le monde réel. En effet, aujourd'hui, il est impossible, par exemple, d'acheter une automobile avec du cash. La loi prévoit des montants plafond pour éviter le blanchiment de capitaux. Il faudrait faire la même chose avec les cryptomonnaies d'Etat : c'est-à-dire que, mettons jusqu'à 5.000 €, l'échange soit totalement anonyme. Au-delà, l'identification devient possible. La technologie permet aujourd'hui de faire cette distinction et de procéder de la sorte.

---

*119 Cukierman Alex, « Welfare and political economy aspects of a central bank digital currency », **op. cit.**, p.8.*

*120 Korjus Kaspar, « Estonia could offer 'estcoins' to e-residents », **Medium**, 22 août 2017, disponible à l'adresse suivante : www.medium.com/@kaspar.korjus/estonia-could-offer-estcoins-to-e-residents-a3a5a5d3c894*

*121 Person Pierre, « Monnaies, banques et finance : vers une nouvelle ère crypto » , **Rapport d'information de l'Assemblée Nationale Française**, 8 juin 2022, p.204.*

122 Propos tenus par l'intéressé dans le cadre d'une conférence donnée au siège du Mouvement Réformateur le 29 juin 2022

5. AUTORISER LE DÉVELOPPEMENT DE STABLECOINS EN EUROS PRIVÉS ET RÉGLEMENTÉS POUR PROTÉGER LES ACTEURS ÉCONOMIQUES ET DÉFENDRE LA SOUVERAINETÉ MONÉTAIRE EUROPÉENNE DANS LE NOUVEL ÉCOSYSTÈME

Les stablecoins – représentation de la monnaie étatique dans le monde numérique - sont devenus incontournables dans le système des cryptoactifs. Ils permettent normalement aux agents économiques de se prémunir contre la volatilité de ces actifs en garantissant leurs échanges avec un équivalent en monnaie fiduciaire. Il s'agit d'un outil de règlement des transactions et de transfert de la valeur prémunissant les acteurs d'une brusque chute des cours intervenant entre l'ordre de mouvement et la réception des fonds.

Ces stablecoins sont très diversifiés. Ils peuvent être centralisés (par exemple, USDC de Circle) ou décentralisés (par exemple, DAI de MakerDAO). Ils peuvent être règlementés (USDC) ou pas (USDT de Tether). Ils peuvent être adossés à des actifs ou pas (c'est le cas des stablecoin algorithmiques). Dans les stablecoin adossés à des actifs, on distingue encore entre les stablecoins adossés à actifs off-chain et les stablecoins adossés à actifs on-chain. La valeur des premiers est garantie par une réserve en actifs réels, traditionnels. Les seconds sont adossés à des cryptoactifs. Les premiers, tels que l'USDT de Tether et l'USDC de Circle ont, en principe, un dollar placé en en réserve en contrepartie de chaque USDT ou USDC émis. Ils peuvent aussi être adossés à d'autres catégories d'actifs, comme les métaux précieux ou un panier de devises. Quand un stablecoin est adossé à un actif, on dit qu'il est « collatéralisé ». Quand cet actif a une valeur supérieure à ce qu'il garantit (ratio supérieur à « un pour un », on dit qu'il est « surcollatéralisé ».

Lors de la récente crise, un stablecoin – l'UST – a paradoxalement perdu la quasi-totalité de se valeur. Il s'agit d'un stablecoin algorithmique. Les stablecoin algorithmiques ne sont adossés à aucune réserve matérielle ou immatérielle. Ils sont décentralisés et contrôlés uniquement par un algorithme. Cet effondrement d'un stablecoin algorithmique est donc une leçon importante à tirer.

Autoriser le développement de stablecoins privés en Euro permettrait aux acteurs économiques européens utilisant le crypto de se doter d'un outil protecteur contre la volatilité. A condition toutefois que ces stablecoins privés soient réglementés et garantis par des actifs off-chain, en l'occurrence une parité 1-1 en euros. Ce serait aussi un signal fort pour renforcer la place de l'Euro dans l'économie mondiale. Notons que cela mettrait fin à une situation absurde : la nature ayant horreur du vide, il existe aujourd'hui un stablecoin en Euros mais émis par une entreprise américaine.

6. FAVORISER LE « VERDISSEMENT » DU MINAGE DES CRYPTOMONNAIES

Le « minage » des blocs de la blockchain est souvent pointé du doigt en raison de son caractère énergivore.

Nous avons vu, d'une part, que cette critique ne tient généralement pas compte de toute l'énergie épargnée grâce à la suppression des intermédiaires. Notons d'ailleurs aussi que la technologie blockchain permet de déterminer avec précision et certitude la consommation énergétique du minage, ce qui est en soi une prouesse et que c'est loin d'être le cas, et c'est un euphémisme, des autres entreprises de la finance traditionnelle.

D'autre part, nous avons précisé que beaucoup d'initiatives étaient prises depuis longtemps pour améliorer la situation en « verdissant » *le minage.*

Nous pensons que l'Etat doit encourager ce processus de verdissement et cela de plusieurs manières :

- en favorisant fiscalement les partenariats entre les producteurs d'énergie et les mineurs de crypto-actifs. Il est effectivement possible de faire de la cogénération ou de récupérer la chaleur produite par le minage.

- Inversement, des fermes de minage peuvent être implantées sur des lieux de production énergétique. Ainsi, on pourrait supprimer les torchères des sites de production du pétrole. Ces torchères brûlent sur place le méthane inutilisable induit par la production de pétrole. En effet, les sites de production pétrolière sont situés très loin des habitations et rarement raccordés au réseau de distribution électrique. Ici, il serait possible de transformer ce gaz en électricité, laquelle serait directement consommée sur place par les fermes de minage.[123]

- en encourageant fiscalement le recours aux sources d'énergie décarbonées pour assurer le minage. Il est intéressant d'utiliser la production d'électricité verte durant les périodes où celle-ci est excédentaire, comme c'est souvent le cas durant l'année en Belgique.

123 Person Pierre, « Monnaies, banques et finance : vers une nouvelle ère crypto » , ***Rapport d'information de l'Assemblée Nationale Française****, 8 juin 2022, p.204.*

7. FAVORISER LE DÉVELOPPEMENT D'UNE NOUVELLE « LEX TECHNOLOGICA » (OU « LEX CRYPTOGRAPHIA »)[124] GRÂCE À LA MISE EN PLACE D'UN CADRE RÉGLEMENTAIRE MINIMAL ET PROVISOIRE (DIT « BAC À SABLE ») FAVORISANT L'ÉMERGENCE D'ENTREPRISES INNOVANTES

Au regard des innovations technologiques telles que la blockchain, les smart contracts, les NFT, une adaptation voire une refonte de notre droit s'avère nécessaire.

Faut-il, par exemple, reconnaître juridiquement les NFT ? Peut-on les considérer comme un mode de preuve ? Faut-il, en raison de la diversité des usages qui peuvent en être faits, leur donner un statut distinct des crypto-actifs ?

En effet, il semblerait opportun que le législateur se penche sur cette technologie NFT afin de reconnaître en droit les preuves provenant d'un enregistrement sur blockchain. L'utilisation des NFT pourrait être une solution plus simple, moins coûteuse, opposable à tous, sans risque de fraude, et sans frais en termes de gestion des données, alors que les méthodes actuelles pour faire reconnaître ses droits d'auteur sont coûteuses et parfois chronophages en termes de formalités administratives.

Il est donc raisonnable de s'interroger sur l'opportunité de lier l'attribution des droits d'auteur à un dépôt via les NFT.[125] Les NFT pourraient également être utilisées pour attester de la propriété d'un objet comme, par exemple, un vélo ou une voiture. Cela rendrait impossible le recel de ces objets.

En effet, si la vente d'un bien était conditionnée au transfert du NFT associé, un voleur ne serait pas en mesure de réaliser la transaction, car il ne posséderait pas le jeton attestant de sa propriété. Alfa Romeo a d'ailleurs décidé d'associer un token à son nouveau SUV Tonale. « Avec le consentement du client, le NFT enregistrera les données du véhicule, générant un certificat qui peut être utilisé pour assurer que la voiture a été correctement entretenue », indique le communiqué de presse d'Alfa Romeo. « Sur le marché des voitures d'occasion, la certification NFT représente une source supplémentaire de crédibilité de propriété sur laquelle les propriétaires ou les concessionnaires peuvent compter ».[126]

Pour construire cette législation, il est souhaitable de mettre en place une réglementation dite du "bac à sable" (« sandbox»). Cela consiste à laisser se développer les projets dans un cadre réglementaire minimal, cadre réglementaire soumis à évaluation. Ce régime, nécessairement transitoire, doit permettre à la fois d'éviter des abus sans néanmoins brider l'innovation tant qu'une réglementation pertinente et protectrice se soit développée sur le sujet.

En seulement quelques années de développement, cet outil réglementaire s'est déjà révélé très fructueux. Il a déjà été utilisé en Angleterre pour encadrer le développement des FinTech. Certaines recherches ont montré, grâce à cet exemple, qu'un bac à sable réglementaire présente de nombreux avantages non seulement pour les entreprises qui le rejoignent, mais aussi pour l'institution de supervision. Ils permettent aux participants d'obtenir des licences plus rapidement et de résoudre des doutes juridiques. La participation à un bac à sable réglementaire est également une forme de promotion pour les entreprises qui s'y soumettent et facilite la levée de capitaux. L'avantage le plus important pour les autorités de surveillance est que, grâce à cet outil, elles acquièrent des connaissances sur les nouvelles technologies et les nouveaux *business models*.[127]

La technologie blockchain permet de proposer des services financiers avec de nombreux avantages. Citons, notamment, la désintermédiation pour les échanges, mais aussi les prêts et les assurances. Cet outil permet de réduire sensiblement les opérations de *back office* pour les secteurs précités, grâce à l'automatisation des processus. Cela permet de réduire le coût de ces services et leur temps de réalisation tout en les rendant plus lisibles et plus efficaces.

De plus, comme le précise le député français Pierre Person dans son rapport d'information sur ce thème :

> ***« Quelle que soit l'origine, la couleur de peau, la croyance culturelle ou la nationalité de l'utilisateur, ce dernier pourra y avoir accès à n'importe quel service sans aucune discrimination de la part du protocole. Chaque personne est égale en droits devant les protocoles décentralisés. La blockchain a réussi là où les institutions publiques avaient échoué : instaurer une véritable universalité des services financiers sans contrainte entre les différents pays. »***

De surcroît, la totale transparence des protocoles de registres distribués offre la possibilité à l'ensemble de la société de contrôler l'action des institutions financières. Tout un chacun peut étudier le code et pointer du doigt les comportements déviants de certains acteurs. Notre société ne devra plus compter sur le courage de lanceur d'alerte isolé mais pourra compter sur un ensemble d'acteurs indépendants qui assurent la veille constante des marchés. Cela permet d'espérer l'émergence d'une finance plus juste, durable et à la portée de tous. Cette transparence bénéficiera également aux pouvoirs publics en capacité de mieux orienter leurs politiques économiques, de contrôler et de prévenir les comportements délictueux sur les marchés. Pour toutes ces raisons, il est capital de ne pas sur-réguler cet écosystème encore naissant, afin de le laisser se développer pour faire bénéficier à l'ensemble de la société les avantages que nous avons présentés.[128]

---

*124 Y. Poullet & H.Jacquemin, Blockchain : une révolution pour le droit ?, **Journal des Tribunaux**, 10 novembre 2018, n°6748, p.819*

125 Person Pierre, « Monnaies, banques et finance : vers une nouvelle ère crypto » , Rapport d'information de l'Assemblée Nationale Française, 8 juin 2022, p.91.

126 « Alfa Romeo Tonale : la Metamorfosi », Alfa Romeo, 2022, disponible à l'adresse suivante : www.media.stellantis.com/uk-en/alfa-romeo/press/alfa-romeo-tonale-la-metamorfosi, (consulté le 28 juin 2022).

*127 Hui Robin et al., « The development and regulation of cryptoassets: Hong Kong experiences and a comparative analysis », **European Business Organization Law Review**, 2020, volume 21, number 2, p. 319-347.*

128Person Pierre, « Monnaies, banques et finance : vers une nouvelle ère crypto », Rapport d'information de l'Assemblée Nationale Française, 8 juin 2022, p.188.

Un autre principe régulatoire essentiel en la matière est le fait qu'il faut toujours éviter de réguler les outils technologiques en tant que tels. C'est l'usage qui en est fait qui doit être régulé. Pas les outils eux-mêmes. Ainsi, dans les travaux initiaux du texte MICA (Market in Crypto Asset) au Parlement Européen, il avait été question d'interdire la technologie Proof-of-Work (POW) ou « preuve par le travail » sous prétexte qu'elle était trop énergivore. Soit la technologie blockchain utilisée par bitcoin pour sécuriser les échanges. Si cette proposition délirante avait été votée, nous nous serions privés d'une innovation fondamentale qui bénéficie pourtant aujourd'hui à quantité de secteurs.

8. INSTAURER LA POSSIBILITÉ, POUR LE CONTRIBUABLE, DE REPORTER LES MOINS-VALUES SUR CESSION D'ACTIFS NUMÉRIQUES SUR LES PLUS-VALUES DE MÊME NATURE, JUSQU'À 3 ANS APRÈS LEUR CONSTATATION

Les plus-values sur cryptomonnaies sont taxables. Dès lors, les moins-values devraient être déductibles. Mais uniquement sur des gains de même nature, soit des gains spéculatifs. Pour éviter, évidemment, que certains les déduisent sur leurs revenus professionnels ou immobiliers. Cela renforcerait l'attractivité de la Belgique sur le terrain fiscal. Le délai de trois ans (ou durée à déterminer) se justifie par la nécessité de tenir compte de la réalité cyclique de cet écosystème financier particulier.

9. ACCORDER AUX DAO LA PERSONNALITÉ MORALE ET LEUR IMPOSER CERTAINES RÈGLES

Les DAO sont de facto les personnes morales du web 3.0. Dès lors, il serait souhaitable qu'elles puissent être reconnues en droit. Cette reconnaissance pourrait résulter d'un enregistrement, comme c'est le cas des personnes morales traditionnelles. Cela permettrait d'imposer à ces organisations de se conformer à des obligations réglementaires qui garantissent le bon fonctionnement de l'économie et préviennent les abus de toutes natures. Il pourrait, par exemple, être exigé que les DAO enregistrées soient constituées selon des règles de gouvernance équilibrées. La divulgation de l'identité des détenteurs de tokens de gouvernance exerçant une certaine influence dans les prises de décision pourrait également être rendue obligatoire (comme c'est le cas pour certains associés disposant d'une part importante du capital d'une société).

Les nombreux avantages des DAO sur les personnes morales traditionnelles, notamment en termes de transparence, laissent penser que de nombreuses entreprises se constitueront grâce à ce type de gouvernance. Leur simplicité de fonctionnement séduira très probablement aussi les ONG et les partis politiques, entre autres. Il est donc capital que les pouvoirs publics s'attellent à poser dès aujourd'hui les bases du cadre réglementaire qui encadreront ces nouvelles entités qui seront probablement incontournables dans le futur.

CONCLUSIONS

Corentin de Salle

Face aux cryptomonnaies, une attitude courante consiste à affirmer que c'est de la spéculation à haut risque, que cela consomme trop d'électricité, que cela permet de blanchir de l'argent, etc.

Qu'en penser ?

Il y a, premièrement, une part de vérité dans ces critiques. Il est vrai que ce secteur est encore jeune, quasiment pas régulé et traverse des crises fréquentes, comme celle qui la frappe de plein fouet aujourd'hui. Mais la présente étude a démontré aussi que ces critiques étaient partiellement fausses et qu'elles devaient, à tout le moins, être nuancées. Comme le dit le professeur de Finances Mikael Petitjean,[129] il y a clairement de vrais dangers dans ce nouveau type d'actifs. Mais aussi des opportunités. Rien de neuf sous le soleil. Cela a toujours été le cas avec l'innovation. On a toujours connu un processus schumpétérien de « destruction créatrice ». On a connu, rappelle-t-il, une grave bulle financière avec les oignons de tulipe en Hollande au XVIIème siècle, bulle qui a fini par exploser. Un bulbe de tulipe valait le prix d'une maison dans le centre d'Amsterdam ! Pourtant, on n'a pas supprimé les bulbes de tulipe. On n'a pas supprimé les marchés sur lesquels on achète et on vend des choses. Ce sera la même chose pour toute une série de crypto-actifs. Certains vont subsister. Et, comme dans tout far west, il y en a qui vont disparaître. Comme précisé dans cette étude, le stablecoin algorithmique en a pris plein la figure. Un tri se fait. C'est normal. C'est une évolution classique.

129 Propos tenus par l'intéressé dans le cadre d'une conférence donnée au siège du Mouvement Réformateur le 29 juin 2022

Notons aussi que, dans une certaine mesure, ces mêmes critiques peuvent également être adressées au monde de la finance classique. En effet, la crise de 2008 a frappé la spéculation à haut risque de la finance classique et régulée. Laquelle consomme également énormément d'électricité si on totalise toutes les infrastructures qui sont nécessaires à son fonctionnement (alors que la désintermédiation induite par la cryptomonnaie permet de court-circuiter la nécessité de pareilles infrastructures). Au niveau de son coût énergétique, le bitcoin est 2,5 moins consommateur que l'or et 6,5 fois moins consommateur que le système bancaire mondial.[130]

Enfin, notons que blanchir de l'argent via la cryptomonnaie est une très mauvaise idée car, même si ces échanges peuvent bénéficier de l'anonymat, la technologie blockchain permet précisément de retracer avec précision tous les échanges : si la justice lève l'anonymat, tout le dispositif frauduleux et l'intégralité de ses bénéficiaires sont instantanément révélés. Raison pour laquelle la mafia évite généralement de recourir aux cryptomonnaies. Cette objection est donc en grande partie outrancière. Notons que Chainalysis, une société spécialisée dans l'analyse de transactions crypto, estime qu'en 2021, 8,6 milliards de dollars ont été blanchis en cryptomonnaies.[131] On estime que depuis 2017, le blanchiment s'élève à environ 33 milliards de dollars via les cryptomonnaies, soit une moyenne de 6,6 milliards par an. À titre de comparaison, l'Office des Nations Unies contre la drogue et le crime annonce près de 2.000 milliards de dollars de monnaies fiduciaires blanchies par an, soit plus de 300 fois le chiffre annuel du blanchiment d'argent lié à l'écosystème crypto. Par ailleurs, Chainalysi révèle qu'en 2021, seuls 0,15 % des cryptos étaient liées à des activités illicites.[132] C'est très nettement moins qu'en 2019 : à l'époque, 3,37 % des transactions crypto étaient le fait d'acteurs engagés dans des activités prohibées par la loi.

Deuxièmement, il faut toujours garder à l'esprit que ce qui motive principalement ces critiques, c'est la volonté de discréditer un nouvel entrant disruptif qui remet totalement en cause le modèle traditionnel (un peu comme Uber face au secteur traditionnel des taxis).

En effet, derrière la création des cryptomonnaies, on découvre l'activité vibrionnante d'une myriade d'entreprises novatrices et encore fragiles pour la plupart. Plusieurs d'entre elles ne survivront pas aux maladies de jeunesse et essais/erreurs de ce nouveau secteur.

C'est un secteur qui ne va probablement pas remplacer le secteur financier traditionnel qui est extrêmement sophistiqué et résilient. Mais qui peut coexister avec lui. A ce titre, il mérite d'être soutenu. Notamment contre les banques qui, hostiles aux entreprises de finance alternative, refusent aux entreprises actives dans le secteur des cryptoactifs et des métaverses, leur demande pour créer un compte. Comme en France, nous devons garantir aux entreprises crypto l'accès à un compte en banque, à savoir, consacrer le « droit au compte ».

Bien régulée, la finance décentralisée pourrait coïncider avec une démocratisation et une plus grande transparence de la finance jusqu'ici réservée aux initiés et aux personnes fortunées. Pourquoi ?

D'abord, elle permet, à ses risques et périls, au simple possesseur d'un gsm d'accéder aux produits financiers et d'investir sans devoir recourir à des intermédiaires ;

Ensuite, elle permet, par exemple, à un(e) jeune Belge d'acheter directement - sans notaires et sans fastidieuses et lentes procédures internationales - une portion infime d'un immeuble à Manhattan et d'en percevoir une partie du loyer

A travers les innovations technologiques derrière les cryptoactifs, ce qui est train de se mettre en place, c'est toute l'infrastructure du web 3.0. Il faut créer un cadre réglementaire minimal et provisoire (dit « bac à sable ») pour permettre à des entreprises innovantes d'émerger : cela consiste à laisser se développer les projets dans un cadre réglementaire minimal. Ce régime, nécessairement transitoire, doit permettre de ne pas brider l'innovation tant qu'une réglementation pertinente et protectrice se soit développée sur le sujet. Le secteur financier crypto est encore très jeune et n'a pas encore déployé son potentiel. On n'a pas encore assez de recul pour réglementer quelque chose qui n'existe pas encore. Ce secteur obéit à une autre logique que le secteur financier classique et cela n'a pas de sens d'appliquer ici des règles qui conviennent à un secteur déjà structuré et résilient

Ce ne sont pas les protocoles qu'il faut réguler (par exemple, interdire la proof of work) mais l'usage qui en est fait : si on avait voulu règlementer les protocoles internet à sa naissance, il ne serait jamais né.

La cryptomonnaie est une composante importante d'un phénomène beaucoup plus vaste : révolution numérique du « web 3.0 ». De quoi s'agit-il ?

- le web 1.0 a permis de consulter des contenus. L'internet à ses tout premiers débuts, c'est, pour ceux qui s'en souviennent, l'efflorescence d'une multitude de sites internet sur absolument tous les sujets et des mails qui sont transférés une multitude de fois ;

---

130 Verbiest Thibault et Van Gelderen Alain, ***Tout ce que vous avez toujours voulu savoir sur les cryptomonnaies sans jamais oser le demander****, Lucpire éditions, 2022, p.44*

131 Journal du Coin, Cryptomonnaies et blanchiment d'argent : le bilan alarmant de Chainanalysis, 28 janvier 2002, www.journalducoin.com/actualites/cryptomonnaies-blanchiment-argent-bilan-chainalysis/#author

132 Cagan Anne, La part d'activités criminelles dans les cryptos n'a jamais été aussi basse, Numerama, 6 janvier 2022, www.numerama.com/tech/810711-la-part-dactivites-criminelles-dans-les-crypto-na-jamais-ete-aussi-basse.html#:~:text=La%20soci%C3%A9t%C3%A9%20sp%C3%A9cialis%C3%A9e%20dans%20l,activit%C3%A9s%20prohib%C3%A9es%20par%20la%20loi

- le web 2.0 a coïncidé avec la possibilité de consulter mais surtout de créer des contenus. C'est l'ère des réseaux sociaux dans laquelle nous sommes encore plongés. L'ère du triomphe des GAFAM ;

- le web 3.0 permettra, lui, de consulter, créer et posséder des contenus aujourd'hui accaparés par des entités centralisées (Etat, GAFAM, etc.). Il vise à conférer à l'individu la possibilité de maîtriser, patrimonialiser et gérer ses données et contenus créés.

Pour qu'elles appartiennent pleinement à ceux qu'elles concernent et qui les produisent, les données doivent pouvoir être **« portables »** (par exemple si une personne veut quitter un réseau social pour un autre et rapatrier ses contenus dans cet autre réseau social) et « **interopérables »** (par exemple, si un individu désire continuer à échanger avec les contacts qu'il a noués sur un ancien réseau social : comme c'est, par exemple le cas des personnes qui sont sur des opérateurs téléphoniques différents).

La maîtrise individuelle des données passe par la création d'une identité numérique décentralisée. Ce « wallet » (portefeuille) auquel aucune autorité centralisée n'a accès permet à l'individu de choisir, au cas par cas, lesquelles de ses données il accepte de divulguer et celles qu'il entend garder secrètes. Il permet à une personne de prouver son identité directement si elle le désire (sans avoir à fournir des pièces justificatives) et est appelé à remplacer les contrats de partage de données que à l'orée de tel ou tel site, la plupart des gens signent sans les lire (et qui conduisent généralement, à céder beaucoup plus de données que nécessaires).

Ainsi, nous sommes favorables à l'accès des citoyens à une **carte d'identité numérique décentralisée** (DID : Decentralized Identity).

A la base de la création et de l'échange des cryptoactifs, la technologie blockchain « décentralise » car elle permet de se passer d'un tiers de confiance pour sécuriser les transactions. La transaction est pseudonymisée, enregistrée de manière irréversible et contrôlée par la communauté des utilisateurs.

Cette désintermédiation permet, par exemple, aux individus de faire des transactions numériques entre eux avec des cryptomonnaies sans passer par un intermédiaire financier (une banque).

Cette désintermédiation permettait, autre exemple, à l'Etat de verser directement et automatiquement aux citoyens des allocations sans passer par des tiers (syndicats et mutuelles), accroissant ainsi la vitesse et la sécurité de la redistribution et générant ainsi des économies colossales.

Une innovation technologique permet de consacrer la propriété d'un objet numérique en le liant à une personne : le « NFT ». Ce jeton non-fongible (non-fungible token), apparu en 2017, révèle, par son unicité et son caractère non-interchangeable, la volonté de créer de la rareté dans un internet où toute information, image ou vidéo est copiable à l'infini.

Ce nouveau support des titres de propriété permet de protéger plus efficacement les créateurs de contenu (auteurs, inventeurs, dessinateurs, photographes, réalisateurs, graphistes, etc.) et, à ce titre, devrait être consacré juridiquement afin de pouvoir tirer le maximum de profit de son extraordinaire potentiel dans quantité de domaines.

Ainsi, un usage de la NFT est de rendre les biens immobiliers plus liquides et donc plus cessibles. On divise un même immeuble en plusieurs très petites parties (des tokens) fongibles (tokenisation de l'immobilier) permettant de démocratiser l'accès au marché immobilier.

Il existe un autre élément fondamental inhérent à ce nouveau paradigme technologique : les « contrats intelligents » (ou **« smart contracts »**) qui prévoient, comme c'est le cas dans les contrats classiques, que telle ou telle conséquence suit la survenance d'un évènement, la réalisation d'une condition, l'arrivée d'un terme, etc. mais qui automatisent le processus. Exemple : mon vol est retardé ou annulé ; dès lors, une indemnité m'est instantanément et automatiquement versée.

Le **potentiel des smart contracts est colossal** lui aussi car il permet des utilisations alternatives de la blockchain autour de services financiers : prêts, assurances, paris, financements participatifs, contrats récurrents, locations, etc. La transaction financière a lieu automatiquement si les conditions définies dans le contrat sont réunies.

Le web 3.0 est une opportunité économique gigantesque pour les PME, et cela peu importe leur localisation, pour peu que le législateur européen et belge déterminent un cadre régulatoire adéquat, à savoir un cadre favorable à l'innovation, offrant souplesse et sécurité pour ses utilisateurs. Pour l'instant, seuls les Etats-Unis et la Chine se montrent pro-actifs en la matière, la première dans une perspective libérale, la seconde dans une voie totalitaire.

L'Europe, quant à elle, se cantonne pour l'instant dans une posture défensive et prohibitive.

Il y a 20 ans, l'Europe a raté le train des GAFAM. A nous de décider si elle montera ou pas dans celui du web 3.0...

BIBLIOGRAPHIE

OUVRAGES

DE SOTO, Hernando, *Le mystère du capital*, Champs Flammarion, 2010

Jeanneau Clément et al., *La Blockchain décryptée*, Paris, Netexplo, 2016, 143 p.

Quoistiaux G., *Les cryptomonnaies*, Renaissance du Livre (collection Dis, c'est quoi ?), 2022

Verbiest Thibault et Attia Jonathan., *Un nouvel internet est-il possible ?*, Bruylant, 2020

Verbiest Thibault et van Gelderen Alain, *Tout ce que vous avez toujours voulu savoir sur les cryptomonnaies sans jamais oser le demander*, Lucpire éditions, 2022

ARTICLES SCIENTIFIQUES

Albrecht Chad et al., « The use of cryptocurrencies in the money laundering process », *Journal of Money Laundering Control*, 2019, vol. 22, n°2, pp. 210-216.

Cukierman Alex, « Welfare and political economy aspects of a central bank digital currency », *Centre for Economic Policy Research*, 2019, p.7.

Delahaye Jean-Paul, « Bitcoin, la cryptomonnaie », *Pour la science*, 2013, vol. 434, pp. 76-81.

Delahaye Jean-Paul, « La cryptographie réinvente la monnaie : le Bitcoin », *Les nouvelles d'Archimède*, 2014, vol. 66, pp. 13-15.

Ganascia Jean-Gabriel, « L'État peut-il rester tiers garant à l'heure de la blockchain ? », *L'ENA hors les murs*, 2018, pp. 1-4.

Horváth Ágnes, « Protection of consumers provided in the proposal for a regulation of markets in crypto assets », Édition Katarina Ivančević, 2021, pp. 428-455.

Hui Robin et al., « The development and regulation of cryptoassets: Hong Kong experiences and a comparative analysis », European Business Organization Law Review, 2020, volume 21, number 2

Jha Nishant et al., « Blockchain Based Crop Insurance: A Decentralized Insurance System for Modernization of Indian Farmers », *Sustainability*, 2021, p.14.

Khan Ruby et Hakami Tahani Ali, « Cryptocurrency: usability perspective versus volatility threat », *Journal of Money and Business*, 2021, pp. 1-13.

Klein Sandra et al., « A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities », SIGCHI Conference, 2017, p.5.

Mabunda Sagwadi, « Cryptocurrency: The new face of cyber money laundering », *International Conference on Advances in Big Data, Computing and Data Communication Systems,* 2018, pp. 1-10.

Mallick Santosha Kumar, « Cryptocurrency: A New Money », *Journal of critical reviews*, 2020, vol. 7, n°4, pp. 4427-4431.

Ohnesorge Jan, « A primer on blockchain technology and its potential for financial inclusion », *Deutsches Institut für Entwicklungspolitik*, 2018, vol. 2, p. 19-21.

Poullet Yves et Jacquemin Hervé, « Blockchain : une révolution pour le droit ? », *Journal des Tribunaux*, 2018, vol. 36, n°6748, pp. 801-819.

Rolland Maël et Slim Assen, « Économie politique du Bitcoin : l'institutionnalisation d'une monnaie sans institutions », Économie et Institutions, 2017, vol. 26, pp. 1-20.

Salmon John et Myers Gordon, « Blockchain and Associated Legal Issues for Emerging Markets », *IFC World Bank Group,* 2019, vol. 63, pp. 1-8.

Sedlmeir Johannes et al., « Recent Developments in Blockchain Technology and their Impact on Energy Consumption », *Informatik Spektrum,* 2021, pp. 1-11.

Shuaib Mohammed et al., « Blockchain-based framework for secure and reliable land registry system », *Telecommunication, Computing, Electronics and Control*, 2020, vol. 18, n°5, pp. 2560-2571.

Yang Qinglin et al., « Fusing Blockchain and AI with Metaverse: A Survey », *arXiv*, 2022, pp. 1-15.

LÉGISLATION

Arrêté royal du 8 février 2022 relatif au statut et au contrôle des prestataires de services d'échange entre monnaies virtuelles et monnaies légales et des prestataires de services de portefeuilles de conservation (Moniteur belge du 23 février 2022).

Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE.

SITES INTERNET

« Avertissement sur les monnaies virtuelles », *Commission de Surveillance du Secteur Financier (CSSF)*, 14 mars 2018, disponible à l'adresse suivante : www.cssf.lu/fr/2018/03/avertissement-sur-les-monnaies-virtuelles/ (consultée le 26 avril 2022).

« Bitcoin traders using up to 100-to-1 leverage are driving the wild swings in cryptocurrencies », CNBC, 2021, disponible à l'adresse suivante : www.cnbc.com/2021/05/25/bitcoin-crashes-driven-by-big-margin-bets-new-crypto-banking.html, (consulté le 14 juin 2022).

« Blockchain », *CNIL*, disponible à l'adresse suivante : www.cnil.fr/fr/definition/blockchain (consultée le 17 février 2022).

« Blockchain et crypto-monnaies : origines et histoire », *Microsoft experiences*, 3 octobre 2021, disponible à l'adresse suivante : www.experiences.microsoft.fr/articles/cybersecurite/blockchain-cryptomonnaies/ (consultée le 26 avril 2022).

« Blockchain Privées, Publiques et à Consortium – Quelles sont les différences ? », *Binance Academy*, 6 janvier 2020, disponible à l'adresse suivante : www.academy.binance.com/fr/articles/private-public-and-consortium-blockchains-whats-the-difference (consultée le 4 avril 2022).

« Création d'un observatoire des droits de l'Internet en Belgique », *DroitBelge*, 2001, disponible à l'adresse suivante : www.droitbelge.be/news_detail.asp?id=50 (consultée le 7 juin 2022).

« Cryptographie asymétrique : tout sur la méthode de chiffrement », *Journal du Net*, 11 février 2019, disponible à l'adresse suivante : www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1209336-cryptographie-asymetrique/ (consultée le 4 avril 2022).

« Difference Blockchain and DLT », *Marco Polo Network*, 31 janvier 2018, disponible à l'adresse suivante : www.marcopolonetwork.com/distributed-ledger-technology/ (consultée le 4 avril 2022).

« L'histoire de la Blockchain », *Binance Academy*, 6 décembre 2018, disponible à l'adresse suivante : www.academy.binance.com/fr/articles/history-of-blockchain (consultée le 4 avril 2022).

« La Commission propose une identité numérique fiable et sécurisée pour tous les Européens – Questions et réponses », *Commission européenne*, 3 juin 2021, disponible à l'adresse suivante : www.ec.europa.eu/commission/presscorner/detail/fr/QANDA_21_2664 (consultée le 9 mai 2022).

« Perri Scope du jeudi 20 mai 2021 », LCI, disponible à l'adresse suivante : www.tf1info.fr/replay-lci/video-perri-scope-du-jeudi-20-mai-2021-2186600.html (consultée le 2 mai 2022).

« Qu'entend-on par 'monnaies virtuelles' ? », *Autorité des services et marchés financiers (FSMA)*, disponible à l'adresse suivante : www.fsma.be/fr/faq/7-quentend-par-monnaies-virtuelles (consultée le 26 avril 2022).

« Qu'est-ce qu'une DAO ? », *Blockchain France*, 12 mai 2016, disponible à l'adresse suivante : www.blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/ (consultée le 26 avril 2022).

« Qu'est-ce que la DeFi ? », *Coinbase*, disponible à l'adresse suivante : www.coinbase.com/fr/learn/crypto-basics/what-is-defi (consultée le 26 avril 2022).

« Qu'est-ce que la preuve d'enjeu dans la blockchain ? », *Business AM*, 29 août 2018, disponible à l'adresse suivante : www.fr.businessam.be/quest-ce-que-la-preuve-denjeu-dans-la-blockchain/ (consultée le 4 avril 2022).

« How does Bitcoin work as a hedge against inflation? », *CNBC*, 2022, disponible à l'adresse suivante : www.cnbctv18.com/cryptocurrency/how-does-bitcoin-work-as-a-hedge-against-inflation-13052422.htm, (consulté le 13 juin 2022).

« Une brève histoire de la crypto monnaie », *CryptoVantage*, disponible à l'adresse suivante : www.cryptovantage.com/fr/guides/une-breve-histoire-de-la-cryptomonnaie/ (consultée le 26 avril 2022).

« Une brève histoire de la crypto-monnaie », *Kriptomat*, disponible à l'adresse suivante : www.kriptomat.io/fr/crypto-monnaies/une-breve-histoire-de-la-crypto-monnaie/ (consultée le 26 avril 2022).

« What are smart contracts on blockchain? », *IBM*, disponible à l'adresse suivante : www.ibm.com/topics/smart-contracts (consultée le 5 mai 2022).

« What is decentralized finance? », *Santander*, 3 mai 2022, disponible à l'adresse suivante : www.santander.com/en/stories/decentralized-finance (consultée le 5 mai 2022).

« What Is Leverage in Crypto Trading? », Binance, 2022, disponible à l'adresse suivante : www.academy.binance.com/en/articles/what-is-leverage-in-crypto-trading, (consulté le 14 juin 2022).

Arman Pierre, « Could Blockchain transform the GCC's VAT system? », Thomsons Reuters, disponible à l'adresse suivante : www.mena.thomsonreuters.com/content/dam/openweb/documents/pdf/mena/white-paper/vatandblockchain_whitepaper_hires_digital.pdf (consultée le 28 mai 2022).

Bobée Floriane, « Qu'est-ce qu'un smart contract ? », *Journal du Coin*, 21 février 2022, disponible à l'adresse suivante : www.journalducoin.com/lexique/smart-contract/ (consultée le 26 avril 2022).

Butcher Mike, « Ripio Credit Network launches, aiming to attack bank loan fees in emerging markets », *Techcrunch*, 2017, disponible à l'adresse suivante : http://tcrn.ch/2yprxBw, (consulté le 13 juin 2022).

Comitogianni Kévin, « Qu'est-ce qu'une organisation autonome décentralisée (DAO) ? », *Crypto News*, 5 février 2022, disponible à l'adresse suivante : www.fr.cryptonews.com/exclusives/quest-ce-quune-organisation-autonome-decentralisee-dao.htm (consultée le 26 avril 2022).

Commission Européenne, « European Commission launches the EU Blockchain Observatory and Forum », 2018, disponible à l'adresse suivante : www.ec.europa.eu/commission/presscorner/detail/en/IP_18_521 (consultée le 7 juin 2022).

Donovan Kevin et Stewart Monte, « Is crypto mining the next home heating trend? », *Capital.com*, 2022, disponible sur : www.capital.com/is-crypto-mining-the-next-home-heating-trend (consultée le 18 mai 2022).

Gayte Aurore, « L'Ethereum va passer à la « proof of stake » : tout comprendre à cette révolution dans les cryptomonnaies », *Numerama*, 15 août 2021, disponible à l'adresse suivante : www.numerama.com/tech/713345-lethereum-passe-a-la-proof-of-stake-tout-comprendre-a-cette-revolution-dans-les-cryptomonnaies.html (consultée le 4 avril 2022).

Hooson Mark, « Crypto Market Crash: Is It The Right Time To Buy The Dip? », *Forbes*, 2022, disponible à l'adresse suivante : www.forbes.com/uk/advisor/investing/cryptocurrency/crypto-market-crash-is-it-the-right-time-to-buy-the-dip/, (consulté le 13 juin 2022).

Ichbiah Daniel, « DeFi : qu'est-ce que c'est ? », *Futura Tech*, disponible à l'adresse suivante : www.futura-sciences.com/tech/definitions/cryptomonnaies-defi-19670/ (consultée le 26 avril 2022).

Korjus Kaspar, « Estonia could offer 'estcoins' to e-residents », *Medium*, 22 août 2017, disponible à l'adresse suivante : www.medium.com/@kaspar.korjus/estonia-could-offer-estcoins-to-e-residents-a3a5a5d3c894 (consultée le 9 mai 2022).

Launay Vincent, « Qu'est-ce que la preuve d'enjeu ? », *Central Charts*, 3 décembre 2018, disponible à l'adresse suivante : www.centralcharts.com/fr/gm/1-apprendre/1-crypto-monnaie/44-minage/930-proof-of-stake-preuve-enjeu-participation (consultée le 4 avril).

Lovens Pierre-François, « Mathieu Michel veut offrir un 'portefeuille numérique' à chaque Belge dès 2023 », *La Libre*, 18 octobre 2021, disponible à l'adresse suivante : www.lalibre.be/belgique/politique-belge/2021/10/18/mathieu-michel-veut-offrir-un-portefeuille-numerique-a-chaque-belge-des-2023-FNRIP34LHVDWHOMOQEW2FU4KGI/ (consultée le 9 mai 2022).

MacKenzie Sigalos, « Crypto world : Tesla, Block and Blockstream team up to mine bitcoin off solar power in Texas », *CNBC*, 2022, disponible à l'adresse suivante : www.cnbc.com/2022/04/08/tesla-block-blockstream-to-mine-bitcoin-off-solar-power-in-texas.html , (consultée le 18 mai 2022).

Mahabir Amanda, « Quelles sont les fonctions de la Blockchain ? », *Articlaw*, 22 novembre 2018, disponible à l'adresse suivante : www.articlaw.net/publications/legal/quelles-sont-les-fonctions-de-la-blockchain/ (consultée le 4 avril 2022).

Murillo Alvaro, « Costa Rica hydro plant gets new lease on life from crypto mining », Reuters, 2022, disponible à l'adresse suivante : www.reuters.com/technology/costa-rica-hydro-plant-gets-new-lease-life-crypto-mining-2022-01-11/ , (consultée le 18 mai 2022).

Shuttleworth David, « What Is A DAO And How Do They Work? », *ConsenSys*, 7 octobre 2021, disponible à l'adresse suivante : www.consensys.net/blog/blockchain-explained/what-is-a-dao-and-how-do-they-work/ (consultée le 5 mai 2022).

Wininger Shai, « Introducing the Lemonade Crypto Climate Coalition », disponible à l'adresse suivante : www.lemonade.com/blog/crypto-climate-coalition/ (consultée le 29 mai 2022).

Wojno Marc, « Qu'est-ce que DeFi ? Tout ce que vous devez savoir sur la finance décentralisée », *ZDNet*, 20 janvier 2022, disponible à l'adresse suivante : www.zdnet.fr/pratique/qu-est-ce-que-defi-tout-ce-que-vous-devez-savoir-sur-la-finance-decentralisee-39936009.htm (consultée le 26 avril 2022).

Woods Sam, « Existing or planned exposure to cryptoassets », *Prudential Regulation Authority*, 2022, disponible à l'adresse suivante : www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2022/march/existing-or-planned-exposure-to-cryptoassets.pdf?

Yaffe-Bellany David, « Cryptocurrencies Melt Down in a 'Perfect Storm' of Fear and Panic », *The New York Times*, 2022, disponible à l'adresse suivante : www.nytimes.com/2022/05/12/technology/cryptocurrencies-crash-bitcoin.html, (consulté le 13 juin 2022).

ARTICLES DE PRESSE

Lovens Pierre-François, « Mathieu Michel veut offrir un 'portefeuille numérique' à chaque Belge dès 2023 », *La Libre*, 18 octobre 2021, disponible à l'adresse suivante : www.lalibre.be/belgique/politique-belge/2021/10/18/mathieu-michel-veut-offrir-un-portefeuille-numerique-a-chaque-belge-des-2023-FNRIP34LHVDWHOMOQEW2FU4KGI/ (consultée le 9 mai 2022).

Madelaine Nicolas, « Vitalik Buterin : 'Les blockchains géreront des milliards d'utilisateurs dans cinq ans' », *Les Echos*, janvier 2016, disponible à l'adresse suivante : www.lesechos.fr/2016/01/vitalik-buterin-les-blockchains-gereront-des-milliards-dutilisateurs-dans-cinq-ans-193107 (consultée le 4 avril 2022).

Vaudano Maxime, « La première blockchain de l'histoire date de 1995, et elle est imprimée sur papier », *Le Monde*, disponible à l'adresse suivante : 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 (consultée le 4 avril 2022).

AUTRES DOCUMENTS

FARDES DOCUMENTAIRES

« La blockchain », *Service Public Fédéral Finances*, 2020, disponible à l'adresse suivante : www.eservices.minfin.fgov.be/myminfin-web/pages/public (consultée le 17 avril 2022).

« Les cryptomonnaies », *Service Public Fédéral Finances*, 2022, disponible à l'adresse suivante : www.eservices.minfin.fgov.be/myminfin-web/pages/public (consultée le 2 avril 2022).

NOTES D'ANALYSE

Pignel Marion, « La technologie blockchain : une opportunité pour l'économie sociale ? », *Pour la Solidarité*, 2019, 23 p.

RAPPORT D'INFORMATION

Person Pierre, « Monnaies, banques et finance : vers une nouvelle ère crypto », Rapport d'information de l'Assemblée Nationale Française, 8 juin 2022, p.204.

ÉMISSION

« Perri Scope du jeudi 20 mai 2021 », *LCI*, disponible à l'adresse suivante : www.tf1info.fr/replay-lci/video-perri-scope-du-jeudi-20-mai-2021-2186600.html (consultée le 2 mai 2022).

ANNEXES

ANNEXE 1 : CADRE NORMATIF AYANT TRAIT À LA BLOCKCHAIN[133]

RÉGLEMENTATION EUROPÉENNE

Résolutions du Parlement européen

20.05.2021 – Résolution du Parlement européen sur le thème « Façonner l'avenir numérique de l'Europe : supprimer les obstacles au bon fonctionnement du marché unique numérique et améliorer l'utilisation de l'IA pour les consommateurs européens ».

25.11.2020 – Résolution du Parlement européen sur la sécurité des produits dans le marché unique.

13.12.2018 – Résolution du Parlement européen sur la chaîne de blocs : une politique commerciale tournée vers l'avenir.

03.10.2018 – Résolution du Parlement européen sur les technologies des registres distribués et les chaînes de blocs : renforcer la confiance par la désintermédiation.

17.05.2017 – Résolution du Parlement européen sur la technologie financière : influence de la technologie sur l'avenir du secteur financier.

Règlements de l'Union européenne

13.07.2021 – Règlement (UE) 2021/1173 du Conseil établissant l'entreprise commune pour le calcul à haute performance européen et abrogeant le règlement (UE) 2018/1488.

29.04.2021 – Règlement (UE) 2021/694 du Parlement Européen et du Conseil établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240.

24.03.2021 – Règlement (UE) 2021/523 du Parlement européen et du Conseil établissant le programme InvestEU et modifiant le règlement (UE) 2015/1017.

BLOCKCHAIN ET RGPD

Rapport de l'Observatoire-Forum des chaînes de blocs de l'UE publié le 16.10.2018.

CONTRATS INTELLIGENTS

Article 1101 du Code civil.

PROJETS ET AVIS EUROPÉENS

16.03.2022 – Proposition de règlement du Parlement Européen et du Conseil modifiant le règlement (UE) nº 909/2014 en ce qui concerne la discipline en matière de règlement, la fourniture transfrontière de services, la coopération en matière de surveillance, la fourniture de services accessoires de type bancaire et les exigences applicables aux dépositaires centraux de titres de pays tiers.

04.01.2022 – Appel à témoignages de l'Autorité européenne des marchés financiers (AEMF) sur la technologie des registres distribués.

15.06.2021 – Résumé de l'avis du contrôleur européen de la protection des données sur la proposition d'un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués.

30.04.2021 – Avis du Comité économique et social européen sur la proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937 et sur la proposition de règlement du Parlement européen et du Conseil sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués.

28.04.2021 – Avis de la Banque Centrale Européenne sur une proposition de règlement du Parlement européen et du Conseil concernant un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués.

24.09.2020 – Proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs et modifiant la directive (UE) 2019/1937 | Markets in Crypto-Assets (MiCA).

24.09.2020 – Proposition de règlement du Parlement européen et du Conseil sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués.

24.09.2020 – Proposition de directive du Parlement européen et du Conseil modifiant les directives 2006/43/CE, 2009/65/CE, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 et EU/2016/2341.

*133 SPF Finances, « La blockchain », **Service Public Fédéral Finances**, 2022, disponible à l'adresse suivante : www.eservices.minfin.fgov.be/myminfin-web/pages/public (consultée le 17 avril 2022).*

11.02.2020 – Avis du Comité économique et social européen sur « Les chaînes de blocs et le marché unique européen : et ensuite ? ».

18.10.2019 – Avis du Comité économique et social européen sur « La technologie des chaînes de blocs et des registres distribués : une infrastructure idéale pour l'économie sociale ».

23.10.2018 – Proposition de règlement du Parlement européen et du Conseil établissant le programme pour une Europe numérique pour la période 2021-2027.

Pan-European blockchain regulatory sandbox

Une sandbox (littéralement « bac à sable ») est un groupe de réflexion qui réunit des régulateurs, des entreprises et des experts en technologie pour tester des solutions innovantes et identifier les obstacles qui surviennent lors de leur déploiement. L'EBP prévoit de développer, en collaboration avec la Comission européenne, une sandbox régulatrice paneuropéenne au sujet de la portabilité des données, les espaces de données B2B, les contrats intelligents et l'identité digitale dans les domaines de la santé, de l'environnement, de la mobilité, etc. La sandbox devrait être opérationnelle en 2021-2022.

European Fund and Asset Management Association (EFAMA)

L'EFAMA a l'intention de lancer un projet pilote « Blockchain pour la fiscalité » et de découvrir comment la technologie du registre distribué (DLT) peut être utilisée pour fournir un modèle de réduction des retenues à la source et, en utilisant l'infrastructure actuelle du marché, apporter confiance et transparence à tous les participants du marché, y compris les autorités fiscales.

DECODE

DECODE est un projet de la Commission européenne qui explore et pilote de nouvelles technologies donnant aux gens plus de contrôle sur la façon dont ils stockent, gèrent et utilisent leurs données personnelles générées en ligne. DECODE utilisera la technologie blockchain pour créer des outils qui donneront aux gens la propriété des données qu'ils génèrent.

ANNEXE 2 : CADRE NORMATIF AYANT ATTRAIT AUX CRYPTOMONNAIES[134]

LÉGISLATIONS ET RÉGLEMENTATIONS

17.04.2019 – Directive (UE) 2019/713 du Parlement européen et du Conseil concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil | 5ème directive AML.

→ Délai de la transposition en droit interne : 31 mai 2021.

30.05.2018 – Directive (UE) 2018/843 du parlement européen et du conseil modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE.

→ Transposition en droit belge : 1er mai 2022 / Virtual Asset Service Provider (VASP).

- 08.02.2022 – Arrêté royal relatif au statut et au contrôle des prestataires de services d'échange entre monnaies virtuelles et monnaies légales et des prestataires de services de portefeuilles de conservation.

- 01.02.2022 – Loi modifiant la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces afin d'introduire des dispositions relatives au statut et au contrôle des prestataires de services d'échange entre monnaies virtuelles et monnaies légales et des prestataires de services de portefeuilles de conservation.

30.07.2018 – Arrêté royal relatif aux modalités de fonctionnement du registre UBO.

18.09.2018 – Loi relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces.

11.07.2018 – Loi relative aux offres au public d'instruments de placement et aux admissions d'instruments de placement à la négociation sur des marchés réglementés.

18.12.2016 – Loi organisant la reconnaissance et l'encadrement du crowdfunding et portant des dispositions diverses en matière de finances.

03.04.2014 – Règlement de l'Autorité des services et marchés financiers concernant l'interdiction de commercialisation de certains produits financiers auprès des clients de détail | Approuvé par l'arrêté royal du 24.04.2014.

*134 SPF Finances, « Les cryptomonnaies », **Service Public Fédéral Finances**, 2022, disponible à l'adresse suivante : www.eservices.minfin.fgov.be/myminfin-web/pages/public (consultée le 2 avril 2022).*

PROJETS ET AVIS EUROPÉENS

Banque centrale européenne (BCE)

14.07.2021 – L'Eurosystème lance un projet d'euro numérique.

19.01.2021 – Une déclaration commune (disponible uniquement en anglais) a été rédigée par la Commission européenne et la BCE sur leur coopération en matière d'euro numérique.

13.01.2021 – La Banque nationale de Belgique (BNB) a organisé un webinaire sur l'euro numérique intitulé « Numérisation de l'économie : en route vers l'euro numérique ? ».

01.10.2020 – La BCE a publié un rapport et un podcast (disponibles uniquement en anglais) sur l'euro numérique.

01.09.2020 – « Digital euro experimentation scope and key learnings ».

01.09.2020 – « Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area ».

Parlement européen et Conseil de l'Union européen

20.07.2021 – Proposition de règlement du Parlement européen et du Conseil sur les informations accompagnant les transferts de fonds et de certains crypto-actifs.

20.07.2021 – Proposition de règlement du Parlement européen et du Conseil instituant l'Autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme et modifiant les règlements (UE) nº 1093/2010, (UE) nº 1094/2010 et (UE) nº 1095/2010.

20.07.2021 – Proposition de règlement du Parlement européen et du Conseil relative aux mécanismes à mettre en place par les États membres pour prévenir l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et abrogeant la directive (UE) 2015/849.

20.07.2021 – Proposition de règlement du Parlement européen et du Conseil relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme.

20.07.2021 – Proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2019/1153 du Parlement européen et du Conseil en ce qui concerne l'accès des autorités compétentes aux registres centralisés des comptes bancaires par l'intermédiaire du point d'accès unique.

16.12.2020 – Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148.

Commission européenne

24.09.2020 – Proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs et modifiant la directive (UE) 2019/1937 | Markets in Crypto-Assets (MICA).

13.05.2020 – Communication sur un plan d'action pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme.

08.03.2018 – Communication « Plan d'action pour les technologies financières : pour un secteur financier européen plus compétitif et plus innovant »

Parlement européen

07.04.2020 – « Crypto-assets - Key developments, regulatory concerns and responses ».

26.05.2016 – Résolution (d'initiative) - « Les monnaies virtuelles ».

Comité économique et social européen

28.07.2017 – Avis (d'initiative) sur la « Numérisation et les modèles économiques innovants dans le secteur financier européen, conséquences sur l'emploi et sur la clientèle ».

ÉTATS-UNIS

09.03.2022 – Le président Biden signe un décret exécutif visant à garantir le développement responsable des actifs numériques.

→ Ce décret vise 7 objectifs :

1. Protéger les consommateurs, les investisseurs et les entreprises des États-Unis ;
2. Protéger la stabilité financière des États-Unis et du monde et réduire le risque systémique ;
3. Atténuer les risques de financement illicite et de sécurité nationale posés par l'utilisation illicite des actifs numériques ;
4. Promouvoir le leadership des États-Unis en matière de technologie et de compétitivité économique pour renforcer le leadership des États-Unis dans le système financier mondial ;
5. Promouvoir un accès équitable à des services financiers sûrs et abordables ;
6. Soutenir les progrès technologiques et assurer un développement et une utilisation responsables des actifs numériques ;
7. Explorer une monnaie numérique de banque centrale américaine (CBDC).

Editeur responsable : Daniel Bacquelaine,
Centre Jean Gol
Avenue de la Toison d'Or, 84-86
1060 Bruxelles

Retrouvez toutes nos études sur **cjg.be** *ou demandez-nous gratuitement un exemplaire par téléphone ou par mail*

Av de la Toison d'Or 84-86 1060 Bruxelles • 02.500.50.40 • info@cjg.be • centrejeangol • @CentreJeanGol • @CentreJeanGol

Centre Jean Gol

Mise en page : Maurane Ballez