Avril 2023

Finance « décentralisée » ou « désintermédiée » : quelle réponse réglementaire ?

Document de réflexion

AUTEURS
Olivier Fliche, Julien Uri, Mathieu Vileyn
Pôle Fintech-Innovation

ACPR
BANQUE DE FRANCE

Résumé

La **finance dite « décentralisée » ou *DeFi* désigne un ensemble de services sur crypto-actifs, comparables à des services financiers** et effectués **sans l'intervention d'un intermédiaire**. S'appuyant sur le principe de décentralisation popularisé par les technologies *blockchain*, elle s'est développée dans le sillage des innovations liées aux crypto-actifs, notamment la généralisation d'automates exécuteurs de clauses (ou *smart contracts*). **La transparence et l'immuabilité du code informatique devant remplacer la confiance entre les acteurs, la finance décentralisée est aussi, et peut-être avant tout, une finance désintermédiée**. Elle fait l'objet d'un intérêt marqué, dans le débat public comme de la part des superviseurs, autant pour ce qu'elle est aujourd'hui que pour ce qu'elle pourrait préfigurer demain : « tokénisation » de la finance, apport des technologies blockchain à l'activité de nombreux secteurs économiques.

Ce document de réflexion décrit succinctement l'écosystème de la *DeFi*, ses cas d'usage principaux, ses promesses, mais aussi ses limites. Parmi celles-ci, le document pointe **le haut niveau de concentration qui caractérise l'écosystème de la *DeFi*, ainsi que la gouvernance parfois très centralisée de ses applications**, premier facteur de risque à prendre en compte. À cet égard, il semble que le terme de « finance décentralisée » représente mal la réalité de la *DeFi* et qu'il est plus approprié de parler de « finance désintermédiée ».

Plus largement, le document propose une description des risques spécifiques de cette finance désintermédiée, en distinguant schématiquement les trois grandes strates qui la composent : l'infrastructure blockchain, la couche applicative des « services », et les dispositifs permettant l'accès des utilisateurs à ces services. **Une partie des risques de la finance désintermédiée sont étroitement liés aux caractéristiques des technologies qui en font aussi l'intérêt**. Ainsi, les solutions recherchées pour améliorer les performances des *blockchains* – leur « passage à l'échelle » – sont aussi celles qui peuvent fragiliser les mécanismes de consensus (solutions de *layer 1*) ou créer de nouveaux problèmes de sécurité (solutions de *layer 2*). De même, au niveau de la couche applicative, la transparence du code informatique, la composabilité des automates exécuteurs de clauses, leur dépendance aux « oracles » : tous ces avantages de la finance désintermédiée sont aussi des facteurs de sa vulnérabilité. **L'accès des utilisateurs à ces services soulève quant à lui des questions plus traditionnelles pour un contrôleur du secteur financier** : la grande volatilité, la complexité des produits, leur accès peu ou pas encadré exposent les utilisateurs à des risques élevés de perte en capital et peuvent menacer la stabilité interne de l'écosystème, à défaut de représenter – à ce jour – une menace pour la stabilité du système financier.

Face à ces risques, ce document de réflexion avance un certain nombre de pistes de réglementation, parfois complémentaires, parfois alternatives. L'idée principale qui y est développée est que **la réglementation de la finance désintermédiée ne peut se borner à répliquer les dispositifs encadrant actuellement la finance traditionnelle**. Elle doit tenir compte, au contraire, des spécificités de la *DeFi*. En outre, elle ne devrait pas s'envisager comme un bloc monolithique, mais pourrait plutôt prendre la forme d'une hybridation entre les réglementations financières traditionnelles et des réglementations inspirées d'autres secteurs économiques.

Parmi les propositions émises, un premier ensemble vise à **renforcer la sécurité des infrastructures** blockchains. Le document explore à cette fin deux grandes modalités d'organisation possible : dans un premier schéma, l'infrastructure continuerait à reposer sur des blockchains publiques mais, pour pouvoir être utilisées, celles-ci feraient l'objet d'une « homologation » via des standards minimaux de sécurité (certification du code informatique, nombre minimal de validateurs, plafond à la

concentration des capacités de validation). Dans un second schéma, les fonctions financières seraient basculées sur des blockchains privées, afin de garantir une gouvernance et un niveau de sécurité appropriés ; celles-ci seraient alors gérées par des acteurs de confiance, privés ou publics, au risque toutefois de limiter les capacités d'innovation de la finance désintermédiée.

S'agissant de la couche applicative, le document propose de **renforcer la sécurité des automates exécuteurs de clauses (*smart contracts*) via un mécanisme de certification**, portant sur la sécurité du code informatique, la nature du service ou encore la gouvernance. Celui-ci serait soit encouragé, soit rendu obligatoire par l'interdiction d'interagir avec un *smart contract* non certifié. Réalisée par des évaluateurs spécialisés procédant par audit humain, méthodes formelles ou une combinaison de ces méthodes, la certification comprendrait notamment une brique d'analyse de composition logicielle : la certification d'un *smart contract* nécessiterait ainsi la certification préalable de l'ensemble des composants appelés. **La certification répondrait en outre à trois règles fondamentales** : elle devrait **pouvoir être retirée à tout moment** ; elle ne serait accordée que **pour une durée limitée**, afin de prendre en compte l'évolution des savoirs et des techniques de sécurité informatique ; elle devrait **être réitérée à chaque changement significatif du code informatique**. Enfin, dans l'hypothèse où, dans le futur, les automates exécuteurs de clauses embarqueraient directement dans leur code un certain nombre d'obligations réglementaires, la certification pourrait inclure la vérification de la bonne traduction des dispositions de droit en langage informatique.

Enfin, le document propose de **mieux encadrer la fourniture de services et l'accès des utilisateurs à ces services**. Sur le premier volet, le document explore la possibilité de créer des statuts pour certains fournisseurs de services, en opérant une « recentralisation » : **les acteurs exerçant le contrôle effectif sur un service sensible pourraient devoir se constituer en société**, soumise au contrôle ; une alternative consisterait à assujettir directement les acteurs exerçant un contrôle effectif sur le service. L'attribution d'un **statut juridique aux « organisations autonomes décentralisées »** (DAO), qui permettrait – quand cela est nécessaire – un assujettissement à contrôle, paraît également une piste prometteuse : sur ce point, le document de réflexion renvoie aux travaux en cours du Haut comité juridique de la Place financière de Paris (HCJP).

Sur le second volet, le document envisage **un cadre de contrôle renforcé des intermédiaires facilitant l'accès des utilisateurs aux services de la *DeFi***. Seuls quelques utilisateurs disposent en effet des compétences pour interagir directement avec des applications de finance désintermédiée ; si l'accès de ces utilisateurs experts peut difficilement être réglementé, l'important est d'encadrer celui du plus grand nombre. À ce titre, **les intermédiaires peuvent jouer un rôle essentiel dans la prévention des risques**, en évitant aux investisseurs – notamment individuels – d'interagir avec des protocoles frauduleux ou dangereux (devoir de vigilance), ou de prendre des risques excessifs (devoir de conseil). En retour, la prise de risque des intermédiaires doit elle-même être encadrée par les autorités de contrôle, afin de limiter faillites et effets de contagion. Pour ce faire, le document propose en premier lieu **d'étendre explicitement les dispositions du règlement européen MiCA aux intermédiaires de la *DeFi***. Pour ne pas créer d'inégalité de traitement, cette extension s'appliquerait à tous les acteurs qui facilitent l'accès des utilisateurs à des services de *DeFi* ; les éventuelles interfaces « décentralisées » devraient également être incluses dans un tel cadre. En second lieu, il est proposé que **l'accès aux produits financiers dépende des compétences financières des clients et de leur appétence au risque**, ces deux notions devant faire l'objet d'une évaluation objective.

Ce document de réflexion entend **nourrir les réflexions en cours, notamment au niveau européen**, dans le prolongement du règlement MiCA, qui prévoit, dans les 18 mois suivant son entrée en vigueur, la rédaction d'un rapport qui évaluera, notamment, l'intérêt et les modalités d'une réglementation européenne de la finance désintermédiée.

Table des matières

Mots clés : blockchain, crypto-actifs, DAO, *DeFi*, finance, oracle, règlementation, *smart contracts*.

Codes JEL : G15, G23, G28, O33, O38

Introduction

La finance « décentralisée » ou « désintermédiée » – généralement désignée par la contraction anglaise « *DeFi* » (pour « *decentralised finance* ») – est apparue dans le débat public à la faveur de son développement rapide, au cours des années 2020-2021. Malgré le net recul qu'elle a connu à partir de mai 2022, comme l'ensemble de l'écosystème lié aux crypto-actifs, après l'effondrement du système Terra-Luna et ses effets en cascade, la *DeFi* continue d'être un sujet important à l'ordre du jour des organisations et groupes de travail internationaux. En effet, au-delà de sa taille – relativement modeste, même au plus haut de sa valorisation – la *DeFi* suscite l'intérêt par les innovations technologiques sur lesquelles elle est bâtie (*blockchain* publique, *smart contracts*) et par sa promesse fondamentale : remplacer la confiance entre les acteurs – comme les institutions financières – par du code informatique tenant lieu de règle commune. **L'intérêt pour la *DeFi* tient ainsi autant à ce qu'elle est aujourd'hui qu'à ce qu'elle pourrait préfigurer demain** : « tokénisation » de la finance, apport des technologies blockchain à l'activité de nombreux secteurs économiques.

L'intérêt du superviseur financier pour la *DeFi* tient évidemment aussi aux risques qu'elle présente : il s'agit alors d'identifier, au-delà de sa forme novatrice, quels sont les risques spécifiques, et éventuellement systémiques, portés par cet écosystème. Du point de vue de la **stabilité financière**, la *DeFi* ne semble pas avoir aujourd'hui la capacité à déstabiliser le système financier dans son ensemble, du fait de sa taille réduite et de ses interconnexions limitées avec la finance traditionnelle. Le superviseur doit cependant anticiper sur les risques et intégrer à sa réflexion ce qui, à l'avenir, pourrait constituer des vecteurs de contagion de la finance traditionnelle.

Mais c'est surtout en matière de **protection de la clientèle** que la *DeFi* présente à l'heure actuelle des lacunes significatives. Au-delà des actifs sur lesquels portent les services qu'elle propose (les crypto-actifs), à la volatilité importante, les risques spécifiques de la *DeFi* proviennent de son infrastructure technologique novatrice, de ses modes de gouvernance, de certaines de ses logiques financières ou encore de ses modalités d'accès. Scruter ces risques oblige donc à examiner l'ensemble du dispositif technique constituant la *DeFi*.

Pour encadrer ces risques, ce document de réflexion propose des **pistes de réglementation**, en raisonnant sur **les trois grandes strates constituant la *DeFi*** : l'infrastructure blockchain, la couche applicative des « services », et les dispositifs permettant l'accès des utilisateurs à ces services. L'idée maîtresse du document de réflexion est que la réglementation de la *DeFi* **ne doit pas s'envisager comme un bloc monolithique**, mais qu'elle pourrait prendre la forme d'une hybridation entre les réglementations financières traditionnelles et des réglementations inspirées d'autres secteurs économiques.

Ce document de réflexion a été rédigé par le Pôle Fintech-Innovation de l'Autorité de contrôle prudentiel et de résolution (ACPR), après une série d'entretiens auprès d'acteurs de l'écosystème français, complétée par une veille documentaire et des échanges avec le monde universitaire. Il s'est aussi enrichi des réflexions menées à l'échelle internationale par de nombreuses instances, comme le Conseil européen du risque systémique, le Conseil de stabilité financière, l'Organisation de coopération pour le développement économique (OCDE) ou la Banque des règlements internationaux (BRI).

Ce document n'a pas vocation à donner une vision exhaustive de l'ensemble des sujets liés à la *DeFi* ou des positions prises par l'ensemble des acteurs, ni à exprimer une position officielle de l'ACPR. Son objectif est de développer une première analyse sur les pistes d'encadrement de la *DeFi*, en vue de les discuter avec les parties prenantes, notamment la profession, à l'occasion d'une consultation publique.

L'ACPR entend ainsi **nourrir les réflexions en cours, notamment au niveau européen**, dans le prolongement du règlement MiCA, qui prévoit, dans les 18 mois suivant son entrée en vigueur, la rédaction d'un rapport sur l'assujettissement de la *DeFi* à la réglementation européenne.

I. Finance « décentralisée » ou « désintermédiée » : définition, cas d'usage et structure schématique

1-1. La finance « décentralisée » ou « désintermédiée » : une notion aux contours imprécis

La « finance décentralisée » ou *DeFi* désigne un ensemble de services sur crypto-actifs, comparables à des services financiers et effectués sans l'intervention d'un intermédiaire.

Elle généralise le principe de **décentralisation technique** popularisé par les technologies *blockchain*[1] et, de fait, s'est développée dans le sillage des innovations liées aux **crypto-actifs**, notamment la généralisation d'automates exécuteurs de clauses (ou ***smart contracts***) et l'émergence de crypto-actifs réputés stables, les « ***stablecoins*** ».

Un **faisceau de critères** peut donc être retenu pour caractériser la *DeFi*, même si aucun d'eux n'est suffisant pour qualifier un cas d'usage et que, réciproquement, de nombreux services de *DeFi* ne cumulent pas tous ces critères :

- une **architecture reposant sur des blockchains publiques** : le caractère public de la blockchain est un premier gage de décentralisation, en évitant l'intervention d'une autorité ou d'un tiers de confiance ; dans une blockchain privée, à l'inverse, une autorité décide du principe et des modalités de la participation ;
- des **protocoles fondés sur des *smart contracts***, c'est-à-dire des programmes informatiques dont l'exécution intervient automatiquement lors de la survenue d'évènements déclencheurs (*triggers*) ;
- une **gouvernance décentralisée**, c'est-à-dire reposant sur une communauté – parfois organisée autour d'une « **organisation autonome décentralisée** » (*decentralised autonomous organisation*, **DAO**[2]) –, sans autorité centrale ni de partie détenant des droits d'administrateur, sans non plus qu'un utilisateur ou un groupe d'utilisateurs ne détienne le contrôle effectif du protocole ; souvent, ce critère n'est pas respecté en pratique (*cf. infra*) ;
- **l'absence de dépositaire** (*non-custodial*) : dans un schéma décentralisé, les utilisateurs sont censés détenir eux-mêmes leurs fonds en crypto-actifs – c'est-à-dire en fait les clés privées permettant d'y accéder sur la blockchain –, et non les détenir via des intermédiaires.

Bien des projets présentent un caractère mixte. En outre, la décentralisation peut être **variable dans le temps**, le long du cycle de développement des protocoles. Les premières étapes d'un projet sont en effet généralement très centralisées : en phase de développement du logiciel, l'équipe principale de développeurs, souvent financée par des investisseurs en capital-risque (qui obtiennent en retour des jetons de gouvernance du protocole), détient les clés d'administration du protocole. C'est cette équipe qui élabore en général les principales règles de fonctionnement du protocole (frais, modalités de vote…), qui sont incorporées dans le code du programme. Le protocole est ensuite déployé sur le marché, et commence à fonctionner sur la base des règles encodées. Dans certains cas, les développeurs conservent des clés d'administrateurs pendant les premiers stades de la mise en service (phase de test), afin de pouvoir corriger d'éventuels dysfonctionnements le plus rapidement possible

[1] Se reporter au glossaire en annexe pour une définition des termes techniques.

[2] Une DAO est une composante usuelle (mais pas systématique) des protocoles *DeFi*, visant à en organiser la gouvernance ; elle est définie habituellement par la communauté des détenteurs de jetons de gouvernance, les *smart contracts* qui régissent ses règles de fonctionnement et les actifs qu'elle contrôle (*treasury* du protocole).

(avec la possibilité d'arrêter le système). Souvent, l'équipe de développement se rassemble dans une fondation ou dans une association.

La logique de décentralisation veut que, par la suite, la gouvernance soit transférée à une communauté, souvent organisée autour d'une DAO (exemples : MakerDAO, Compound, Uniswap). Il arrive cependant parfois que les développeurs ou fondateurs d'un projet conservent des clés d'administrateurs même après la phase de test, ce qui expose le protocole à des risques de manipulation, en particulier lorsque l'information n'est pas portée à la connaissance des utilisateurs (*cf.* le point 2-1 sur les risques liés à la gouvernance).

Encadré 1 : Les difficultés sémantiques de la DeFi : quand les termes usuels décrivent mal les réalités

- ***DeFi*** : ***finance décentralisée… ou désintermédiée ?*** Le terme usuel met l'accent sur la notion de décentralisation, qui peut faire référence au mode de gouvernance des applications, mais désigne également une propriété de l'infrastructure blockchain, registre partagé dans laquelle chaque nœud du réseau détient tout ou partie de l'information. S'agissant de la gouvernance, la promesse de décentralisation n'est pas toujours tenue (*cf.* partie 2-1) ; aussi, l'accent pourrait plus légitimement être mis sur le caractère désintermédié de ces activités financières et l'usage du terme « finance désintermédiée » encouragé. Sans prétendre trancher ce débat, ce document recourt le plus souvent à la contraction anglaise « *DeFi* », qui s'est largement imposée dans la littérature consacrée au sujet, y compris en français.

- ***Smart contract*** **ou automate exécuteur de clauses** : le terme « *smart contract* » apparaît peu approprié pour désigner ces programmes informatiques, qui ne sont pas « intelligents », dans le sens où ne modifient pas leur comportement au fil du temps, mais se bornent au contraire à exécuter un code lorsque sont remplies des conditions prédéfinies. Les « *smart contracts* » ne constituent pas forcément non plus des contrats, au sens juridique du terme. Malgré cela, le vocable anglais s'est largement répandu dans la littérature (même en français), et on l'utilise donc parfois dans ce rapport en lieu et place de son équivalent français.

- ***Stablecoin*** : crypto-actif ayant pour objectif de maintenir une valeur stable par référence à une monnaie officielle (ou un panier de ces monnaies), à d'autres droits ou actifs du monde réel, ou encore par référence à d'autres crypto-actifs. Le terme peut donc apparaître comme trompeur, puisque la stabilité est un objectif et non une garantie ; nombre de *stablecoins* ont ainsi connu des « décrochages » temporaires ou définitifs par rapport à leur valeur de référence.

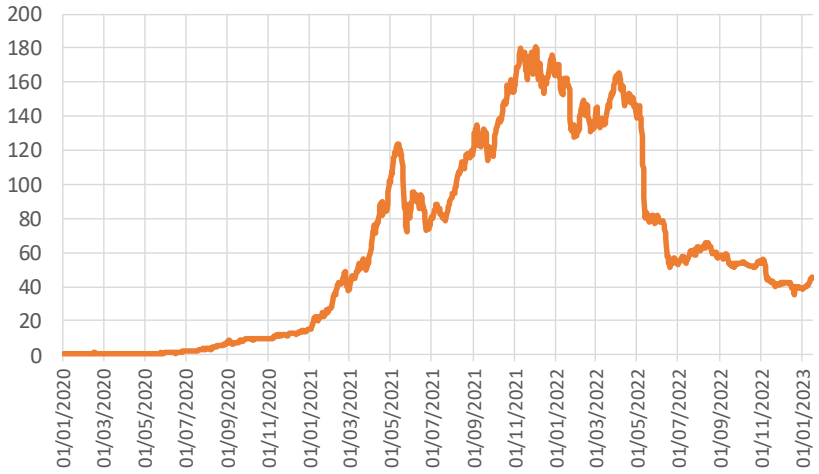
1-2. Le développement de la *DeFi*

Le premier service significatif de la *DeFi* combinant un *stablecoin*, une gouvernance décentralisée et des protocoles de prêts-emprunts, est apparu en 2017 (MakerDAO), suivi de développements limités jusqu'en 2020 (Bancor, Uniswap v1, Synthetix, Compound, REN, Kyber, 0x). L'année 2020 marque une rupture, avec « l'été de la *DeFi* » et la popularisation des programmes de récompense ainsi que des jetons de gouvernance (Compound, Yearn Finance, SushiSwap, Uniswap v2).

Entre l'été 2020 et le début de l'année 2022, la *DeFi* connait une **croissance soutenue**. Ainsi, même si cette métrique n'est pas entièrement satisfaisante[3], le montant total des crypto-actifs déposés dans les protocoles (*total value locked* ou TVL) atteint 170 G$ à la fin 2021[4], contre 2 G$ en juin 2020, soit un an et demi auparavant (*cf.* graphique 1). A la même date, la capitalisation de marché des principaux *tokens DeFi* atteignait environ 150 G$[5] (contre 6 G$ fin juin 2020), pour près de 5 millions de portefeuilles numériques utilisés[6] (contre environ 200 000 fin juin 2020).

Au cours de l'année 2022, en revanche, la valeur de marché de l'écosystème *DeFi* est en **net recul**, en particulier à partir du mois de mai (chute de Terra-Luna, *cf. infra*). À la fin 2022, la taille de la *DeFi* a ainsi été divisée par plus de 4 par rapport au pic de la fin 2021, la TVL revenant à environ 40 G$ (*cf.* graphique 1).

Graphique 1 : Montant total des actifs déposés (TVL) dans les protocoles *DeFi*, en milliards d'USD



Source : DeFi Llama

La dynamique de croissance de la *DeFi* en 2020-2021, s'explique notamment par le recyclage de profits liés au développement des crypto-actifs, en particulier avec l'augmentation du prix du Bitcoin[7]. Ce développement spectaculaire a également été favorisé par l'environnement macroéconomique, en particulier le faible niveau des taux d'intérêt, assurant un accès aisé à la liquidité et poussant à la prise de risque. La disponibilité accrue des développeurs pendant les confinements liés au Covid-19, puis dans un nouveau contexte d'organisation du travail, a également constitué un adjuvant.

A l'inverse, à partir de 2022, les investisseurs ont réagi au resserrement monétaire mondial, ainsi qu'au contexte économique et géopolitique plus incertain, en réduisant leur exposition aux actifs les plus

[3] Même s'il s'agit de la meilleure approximation à ce jour, la TVL constitue une mesure biaisée, notamment en raison des phénomènes de réinvestissement des jetons via les protocoles de prêts-emprunts collatéralisés : un utilisateur disposant de cryptos A peut décider de les déposer en collatéral pour obtenir un prêt de cryptos B, dont une partie pourra à son tour être déposée en collatéral pour obtenir des cryptos C. L'agrégation des TVL dans les différents protocoles conduirait ici à additionner les détentions de A, B et C, alors que les actifs B et C ne sont que le résultat de l'effet de levier exercé par l'utilisateur à partir de sa détention de A. Pour cette raison, la comptabilisation utilisée ici (TVL « nette ») exclut notamment les jetons empruntés ou déposés en *staking* ou en *liquid staking* (*cf. infra* sur ces notions).

[4] Source DefiLlama - DeFi Dashboard

[5] Source : Coingecko

[6] Source : DeFi users over time (dune.com)

[7] OCDE, *Why decentralized finance matters and the policy implications*, janvier 2022.

risqués. La chute de l'écosystème Terra-Luna et la faillite de plusieurs acteurs[8] (Celsius Network, Three Arrows Capital, Voyager Digital, BlockFi, FTX), qui se sont traduits par des doutes croissants sur l'écosystème des crypto-actifs, ont renforcé ce mouvement de baisse. Ainsi, après avoir profité de la dynamique des crypto-actifs en 2020-2021, la *DeFi* a souffert de leurs difficultés en 2022.

Il faut par ailleurs noter que, même au plus haut de sa capitalisation (vers la fin 2021), la taille de l'écosystème *DeFi* est **demeurée relativement faible** comparée à celle du marché des crypto-actifs (2 500 G$[9] à la fin 2021 : la *DeFi* représentait donc moins de 10 % de cet ensemble), et plus encore au regard de la finance traditionnelle.

1-3. Les cas d'usage de la *DeFi*

Dans la pratique, les cas d'usage se concentrent aujourd'hui sur un petit nombre d'activités restreintes. Les activités spéculatives dominent largement, et les utilisations au service de l'économie réelle, comme par exemple le financement des entreprises, restent peu développées. Les cas d'usage principaux sont les suivants :

- **Le prêt-emprunt collatéralisé *(lending)*** : il s'agit de la principale activité, en TVL « nette »[10], au sein de la *DeFi*. Elle permet de miser à la hausse ou à la baisse sur l'évolution de la valeur de crypto-actifs. Ce système est très proche de l'activité de pension livrée (*repurchase agreement* ou *repo)* en finance traditionnelle, puisque le prêt est garanti par un dépôt de collatéral, qui permet au prêteur (un autre utilisateur ou plus souvent un « pool de liquidité », *cf. infra*) de se couvrir contre la volatilité inhérente aux crypto-actifs et contre le risque de défaut de l'emprunteur. Ce collatéral est immédiatement mis en liquidation dès que sa valeur descend en dessous d'un seuil défini au préalable (sur la liquidation automatisée, voir le point 2-4-2).

- **L'échange et l'achat-vente de jetons (*swap*)** : les échanges ont lieu sur des plateformes d'échange décentralisées[11] (*decentralised exchanges* ou DEX). À l'origine, le système opérait grâce à l'utilisation d'un système de livre d'ordres, similaire à celui utilisé en finance traditionnelle. Dans de nombreux protocoles, les modèles de livre d'ordre ont progressivement été remplacés par les *Automated Market Makers* (AMM), autre grande innovation de la *DeFi* : l'échange ne se fait plus directement en pair-à-pair, mais vis-à-vis d'un « pool de liquidités ». Cette réserve est constituée de l'ensemble des jetons apportés (déposés) par les utilisateurs, ce qui permet de réaliser un achat ou une vente sans nécessairement disposer d'un ordre réciproque. La fourniture de « liquidité » dans le pool est encouragée en rémunérant les apporteurs de jetons avec des jetons de gouvernance de l'application[12].

- **Les protocoles de *staking* et de *liquid staking*** : le *staking* ou « mise sous séquestre de jetons », est lié à la validation des transactions sur les blockchains à « preuve d'enjeu » (*proof of stake* ou PoS) : dans ce système, la validation d'un bloc nécessite en effet d'immobiliser des jetons de

[8] Dont on pourra noter qu'ils sont tous des acteurs « centralisés ».
[9] Source : Crypto Market Cap Charts | CoinGecko
[10] D'après l'OCDE, elle représentait 53 % de la valeur totale de l'écosystème *DeFi* en juin 2021.
[11] Exemples de protocoles d'achat-vente : Uniswap v3, Curve.
[12] Exemples de protocoles de prêt : Aave, Compound.

gouvernance[13] de la blockchain, comme garantie du processus de validation, en « misant » sur le réseau (d'où le nom de « preuve d'enjeu »)[14]. Au départ, le *staking* était uniquement réalisé par des validateurs, ce qui nécessitait un engagement financier important de leur part. Certaines blockchains ont rapidement eu recours au système de « preuve d'enjeu déléguée »[15], où les validateurs confient leurs jetons à des délégués, charge à ceux-ci de sécuriser la blockchain. La validation de blocs étant rémunérée par l'octroi de nouveaux jetons de gouvernance, les utilisateurs qui confient leurs jetons en *staking* touchent une partie de cette rémunération (déduction faite de la commission du délégué).

Le système s'est progressivement développé vers le *liquid staking* : les utilisateurs désirant faire du *staking* déposent leurs jetons dans un pool de liquidités, et reçoivent en échange une sorte de certificat de dépôt (sous la forme d'un *wrapped token*), qui pourra lui-même être échangé, déposé en collatéral etc. De son côté, le protocole utilise les crypto-actifs déposés pour faire du *staking*, en reversant une commission aux délégués effectivement chargés de valider les transactions[16].

- **Les protocoles de *yield farming (*ou *liquidity mining)*** : ils donnent la possibilité aux utilisateurs de bloquer leurs crypto-actifs dans un *smart contract* – qui peut ensuite les utiliser –, en échange d'un rendement. Contrepartie des mécanismes d'emprunt, ils participent au bon fonctionnement des services décentralisés. Le *yield farming* peut être rapproché du *staking*, même si ce dernier concerne uniquement les jetons de gouvernance des blockchains.

- **Les prêts-emprunts sans collatéral (*flash loans*)** : les utilisateurs peuvent emprunter des cryptos-actifs sans garantie, à condition de rembourser le prêt au sein de la même transaction de la blockchain. Ce mécanisme repose sur des développements informatiques permettant le regroupement de transactions au sein d'une unique transaction agrégeant l'ensemble. Les utilisateurs peuvent ainsi réaliser des bénéfices en profitant des possibilités d'arbitrage entre différents crypto-actifs, ainsi que des disparités de prix de ces actifs entre les différentes plate-forme d'échange décentralisées. Les *flash loans* sont également utilisés pour la liquidation des positions : via cette technique, les liquidateurs peuvent vendre le collatéral afin de rembourser la dette avant que celle-ci ne cesse d'être couverte par le collatéral.

- **Les produits dérivés sur actifs financiers classiques** : un crypto-actif est émis pour représenter virtuellement la valeur d'un actif financier réel, détenu en collatéral, dont il suit le cours. Un crypto-actif peut ainsi répliquer la valeur des actions d'une grande entreprise. Ce fonctionnement est proche des *stablecoins* indexés sur la valeur d'une devise ou sur d'autres actifs (par exemple l'or).

- **Les produits dérivés sur crypto-actifs** : l'écosystème *DeFi* propose l'ensemble des produits dérivés traditionnels (contrats à terme, options) avec un sous-jacent en crypto-actif, qui sont échangés sur des plateformes centralisées ou décentralisées. Un type de produit est spécifique à l'univers des crypto-actifs : les contrats à terme perpétuels (*perpetual futures*)[17], qui constituent un équivalent

[13] Ces jetons sont parfois appelés « jetons de protocole », pour les différencier des jetons de gouvernance des applications *DeFi*.

[14] Le principal mécanisme concurrent, la « preuve de travail » (*proof of work* ou PoW), sur lequel fonctionne par exemple Bitcoin, consiste pour les mineurs à effectuer des calculs cryptographiques extrêmement pointus, nécessitant un matériel perfectionné… et une importante consommation d'électricité.

[15] *Delegated Proof of Stake* utilisée par exemple par Tezos, Lisk, ou EOS.

[16] Le marché du *staking-as-a-service* est à l'heure actuelle largement dominé par le protocole Lido.

[17] Un contrat à terme (*future*) est un engagement à la livraison d'un actif sous-jacent à une date future, à des conditions définies à l'avance. Les contrats à terme perpétuels n'ont pas de date d'expiration ; ils permettent donc de maintenir des positions ouvertes aussi longtemps qu'on le souhaite, sans besoin de changer de contrat.

aux *contracts for difference* (CFD)[18] de la finance traditionnelle (voir notamment les parties 2-4-2 et 3-3-2 sur ce point).

- **Les protocoles d'assurance décentralisés** : certains de ces protocoles visent à couvrir des risques propres aux activités de *DeFi*[19], tandis que d'autres consistent en des services d'assurance paramétrique sur des biens et services réels[20].
- **Les protocoles de financement participatif** : de nombreux projets de financement participatif (*crowdfunding*) choisissent une forme de gouvernance décentralisée et s'hébergent sur blockchain, avec la promesse d'une plus grande transparence.
- **Les marchés prédictifs** : une plateforme met en relation deux parieurs aux prédictions opposées.
- **Les loteries « sans perdant »** : elles reposent sur la mise en commun de crypto-actifs, placés sur divers protocoles de *staking*. L'utilisateur achète des tickets qui lui donnent quotidiennement la possibilité de remporter les intérêts récoltés. Il peut, à tout moment, ré-échanger ses tickets contre sa mise de départ[21]. Il s'agit donc de sacrifier des intérêts minimes contre l'éventualité d'un gain important.

Encadré 2 : Modalités d'accès à la *DeFi* pour les investisseurs

Les investissements dans les protocoles *DeFi* s'effectuent exclusivement en crypto-actifs. Les investisseurs doivent donc préalablement détenir des crypto-actifs, ou en acquérir contre de la monnaie officielle[22] auprès d'**intermédiaires centralisés** (*« crypto on-ramp »*) : **les plateformes d'échanges de crypto-actifs**. Une fois les crypto-actifs acquis, **ils peuvent être investis de trois manières** dans la *DeFi*.

La **première manière**, totalement désintermédiée, consiste à interagir directement avec les applications *DeFi* ; elle nécessite donc des compétences de programmation informatique. Pour des utilisateurs dépourvus de compétences de programmation, c'est-à-dire le plus grand nombre, une **deuxième manière** d'investir consiste à recourir à des **interfaces web** permettant l'accès en « clique-bouton » aux plateformes décentralisées. Ces interfaces peuvent être conçues par les développeurs des applications décentralisées auxquelles elles offrent l'accès, ou par des acteurs indépendants.

Un **troisième mode d'accès** consiste à recourir à des **intermédiaires centralisés**, réalisant des investissements dans l'écosystème *DeFi* pour le compte de leurs clients. Cette dernière méthode d'investissement est parfois appelée « *CeDeFi »* (finance décentralisée intermédiée). Ces plateformes, dont des exemples en France sont Binance ou Coinhouse[23], jouent donc un rôle clé d'intermédiaire en facilitant l'accès aux services de la *DeFi*.

[18] Les CFD sont des instruments financiers spéculatifs pariant sur des variations à la hausse ou à la baisse d'un actif sous-jacent (un indice, une action, etc.) sans détention effective de cet actif. La transaction entre l'acheteur et le vendeur se fait sur la différence entre la valeur actuelle du sous-jacent et sa valeur au moment de la vente. Les CFD sont généralement proposés avec un effet de levier, c'est-à-dire un multiplicateur des gains et des pertes.
[19] Exemple : Unslashed Finance.
[20] Exemple : Etherisc.
[21] Fonctionnement du protocole PoolTogether
[22] Monnaie émanant des États et garantie par eux (parfois également désignée sous le vocable « monnaie fiat »).
[23] Binance France et Coinhouse sont enregistrés comme prestataires de service sur actifs numériques (PSAN) auprès de l'Autorité des Marchés Financiers (AMF), avec l'avis conforme de l'ACPR.

1-4. La participation croissante des acteurs institutionnels

Les rendements offerts et la possibilité de s'engager dans des opérations à fort effet de levier sur des crypto-actifs ont attiré un certain nombre d'investisseurs institutionnels (fonds d'investissement notamment) dans la *DeFi* en 2020-2021. Cela a conduit à la création **d'applications dédiées aux besoins des investisseurs institutionnels**[24], dont la principale spécificité est de comporter des procédures de vérification de l'identité des participants (« *Know your customer* » ou KYC). Ces applications sont donc **permissionnées**, c'est-à-dire que leur accès est restreint aux participants autorisés. En contrepartie de ces vérifications, et après étude de leur solvabilité, ces applications proposent aux acteurs autorisés d'emprunter sans collatéral, comme en finance traditionnelle.

L'évolution du prix du « gaz » sur la blockchain Ethereum, c'est-à-dire les frais à régler[25] pour l'enregistrement des transactions sur la blockchain (*gas fees*), constitue un autre indice de la participation croissante des acteurs institutionnels. Le prix du gaz évolue en fonction de l'état de l'offre (validateurs disponibles pour enregistrer les transactions) et de la demande (transactions à valider). En outre, plus une transaction est complexe (taille du *smart contract* à exécuter, appels éventuels à d'autres *smart contracts*, nature des calculs, besoin de données etc.) et plus elle doit être validée rapidement, plus elle est chère.

Avec l'engouement pour la *DeFi*, les frais de transaction ont connu une augmentation significative sur Ethereum au cours de l'année 2021, où ils ont presque continuellement dépassé les 10 USD par transaction au cours du premier semestre – et ont parfois atteint 70 USD lors d'épisodes spéculatifs – avant de redescendre autour de 5 USD au cours du second semestre. De tels tarifs découragent clairement les transactions de petit montant, et ne demeurent abordables que pour des transactions de montant élevé, qui sont généralement le fait d'acteurs institutionnels.

1-5. Un écosystème marqué par une importante concentration, à tous les niveaux

Paradoxalement, l'une des caractéristiques notables du marché *DeFi* est son degré élevé de concentration. C'est d'abord le cas au niveau des **blockchains** qui servent d'infrastructure aux applications *DeFi* : à fin 2022, la blockchain Ethereum concentrait à elle seule 60 % de la TVL nette de la *DeFi* – une part quasi-identique à celle de fin 2021[26] –, tandis que plus de 80 % de la TVL nette de l'écosystème se concentre sur 3 blockchains à fin 2022[27]. En outre, les capacités de validation des transactions sur blockchains peuvent elles-mêmes être très concentrées[28].

Cette concentration se retrouve également au niveau des **applications** *DeFi*. Bien que des milliers de protocoles aient été développés, seuls quelques dizaines concentrent en pratique l'essentiel des fonds

[24] Par exemple Aave Arc (version du protocole Aave dédiée aux institutionnels) ou encore Atlendis.
[25] Les frais sont réglés en Ether (ETH), le crypto-actif natif de la blockchain Ethereum (qui constitue également son jeton de gouvernance).
[26] La blockchain Terra a gagné en importance au cours des premiers mois de l'année 2022, représentant jusqu'à 15 % de la TVL, avant son effondrement en mai 2022.
[27] Outre Ethereum, les blockchains Tron et Binance Smart Chain représentent respectivement 11 et 10 % de la TVL nette à cette date.
[28] Avant le passage à une validation en preuve d'enjeu, cinq entités concentraient 65 % des capacités de minage d'Ethereum (*Les Échos*, 30 août 2022). En preuve d'enjeu, les validateurs sont plus nombreux, mais le risque de concentration ne disparaît pas, notamment si ces derniers sont réunis au sein de *pools* de validateurs par des plateformes centralisées (ex : Coinbase).

et des usages. Ainsi, à fin 2021, les 3 premières applications *DeFi* représentaient ensemble 33 % de la TVL nette totale[29], les 7 premières 50 % du total, et les 36 premières 80 % du total. Ce mouvement de concentration a même eu tendance à s'accentuer au cours de l'année 2022, avec la baisse de la valeur de l'écosystème : 16 protocoles concentrent ainsi 70 % de la TVL nette à fin 2022, contre 21 à fin 2021[30] (*cf.* tableau 1). Enfin, la détention des **jetons de gouvernance des applications** peut elle-même être très concentrée (voir notamment la partie 2-1 sur ce sujet).

Tableau 1. Mesure de la concentration des applications *DeFi* à fin 2021 et 2022

Part de la TVL nette totale	Nombre de protocoles	
	A fin 2021	A fin 2022
33%	3	3
50%	7	6
60%	11	9
70%	21	16
80%	36	34
90%	65	83

Source : DeFi Llama
Lecture : À fin 2021, la TVL nette cumulée des 7 premiers protocoles représentait au moins 50 % du total ; à fin 2022, les 6 plus importants protocoles pesaient ensemble pour au moins 50 % du marché.

1-6. Présentation schématique des acteurs et des « composants » de la *DeFi*

En termes d'architecture, la *DeFi* est composée de différentes strates (*cf.* schéma ci-dessous). L'**infrastructure blockchain** en constitue la base, comprenant notamment un registre distribué sur un ensemble de nœuds, qui s'accordent sur son contenu via des algorithmes de consensus. La blockchain permet l'exécution des *smart contracts*. L'infrastructure constitue la « couche de règlement » (*settlement layer*) de la *DeFi*. Pour faire face aux problèmes de performance des blockchains, des solutions dites de « surcouche » (*layer 2*) permettent de traiter une partie des transactions hors chaîne (*cf.* partie 2-2), en n'enregistrant que le résultat dans la chaîne principale (*layer 1*). Des **ponts** (***bridges***) permettent de connecter les blockchains entre elles.

Les **applications décentralisées** (*dApps*) ou **protocoles *DeFi*** sont à proprement parler des empilements de logiciels – les automates exécuteurs de clauses ou *smart contracts* – construits sur l'infrastructure blockchain, répondant à des cas d'usage spécifiques. Le fait que les couches s'appuient les unes sur les autres, ajouté au caractère généralement *open source* du code des applications, permet de créer une architecture ouverte, favorisant la **composabilité**[31] **:** un automate peut facilement appeler d'autres automates pour en utiliser les propriétés ; des applications existantes peuvent être combinées pour en créer de nouvelles. **La facilité à composer et combiner des éléments modulaires est très favorable**

[29] Rappelons que ne sont pas comptabilisées ici les activités aboutissant à des doubles comptes (cf. *supra*).
[30] En revanche, le seuil de 90 % est atteint avec 83 protocoles à fin 2022, contre 65 à fin 2021, ce qui traduit une certaine diversification au milieu de la distribution.
[31] Il convient d'ailleurs de noter que la concentration des services de *DeFi* sur une même couche de règlement (avec la domination du réseau Ethereum) s'explique principalement par le fait qu'une infrastructure commune permet de profiter à plein des propriétés de composabilité (en s'appuyant sur les objets déjà construits sur l'infrastructure).

à la création d'activités et de produits innovants ; elle constitue l'une des innovations majeures de la *DeFi*, dont elle amplifie les effets de réseau[32]. Dans le même temps, le recyclage d'objets logiciels ajoute à la complexité d'un écosystème déjà foisonnant, et accroît les risques opérationnels (*cf.* partie 2).

À côté des applications décentralisées, des **applications centralisées**[33] peuvent se connecter à l'infrastructure blockchain, via des API[34], afin de proposer des services : plateformes d'échange centralisées[35] (*centralised exchanges* ou CEX), analyse de données, oracles etc. En pratique, les CEX constituent souvent un point d'entrée vers la *DeFi* pour les utilisateurs (*cf.* l'encadré 2), notamment en leur offrant des services de conservation des actifs (*custodian wallets*).

Enfin, la couche supérieure de la *DeFi* est constituée d'**interfaces** permettant de faire le lien avec les utilisateurs, pour leur permettre d'interagir plus facilement avec les applications centralisées ou décentralisées. Ces interfaces peuvent aussi jouer un rôle d'**agrégateur** : en se connectant simultanément à plusieurs applications et protocoles, elles permettent aux utilisateurs d'effectuer des tâches qui se révèleraient autrement plus complexes sans leur assistance (par exemple : comparer le rendement d'un prêt entre plusieurs applications concurrentes).

La plupart des utilisateurs ont également recours à un ***wallet*** (« portefeuille crypto ») pour interagir avec les applications *DeFi*. Ce *wallet* est une interface contenant une clé publique pour recevoir des crypto-actifs, et une clé privée pour y accéder. Les crypto-actifs ne sont pas stockés sur le *wallet* (ils demeurent toujours sur la blockchain) ; contrairement à ce que son nom laisse entendre, le *wallet* constitue donc davantage un porte-clés qu'un portefeuille. Le *wallet* peut être hébergé (*custodial*), c'est-à-dire qu'un tiers détient la clé privée et donc *in fine* le contrôle sur les crypto-actifs. Avec un *wallet* non hébergé (*non-custodial*), au contraire, l'utilisateur exerce directement le contrôle sur ses fonds. Enfin, certains portefeuilles sont logiciels et connectés à internet (*hot wallets*), ce qui les rend plus faciles d'utilisation, tandis que d'autres sont des portefeuilles matériels, c'est-à-dire des dispositifs physiques hors ligne (*cold wallets*), ce qui est de nature à réduire les possibilités d'attaque.

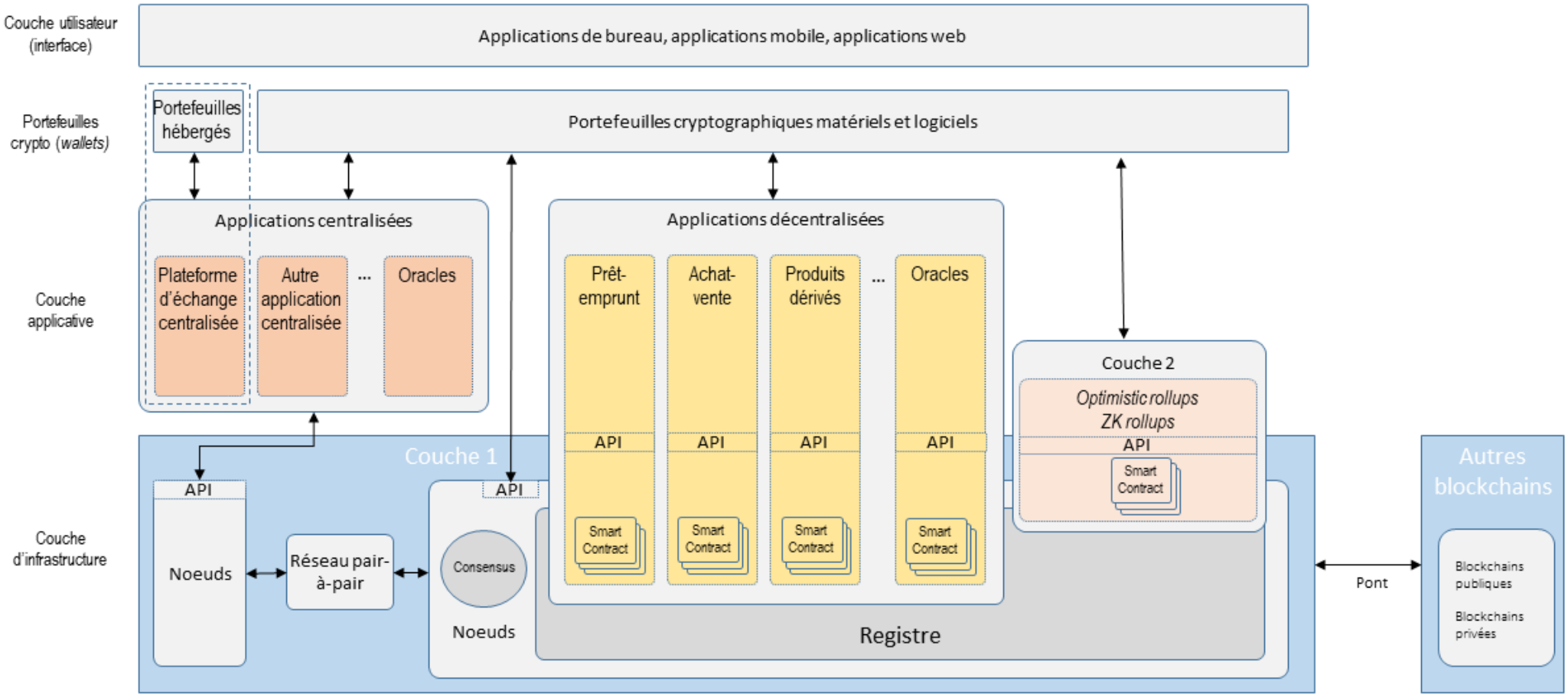
[32] Mécanisme d'externalité, ici positif, par lequel la valeur des services croît à mesure que la participation au réseau augmente.

[33] Comme leur nom l'indique, les applications centralisées ne sont pas à proprement parler de la *DeFi*. Elles jouent toutefois un rôle essentiel dans cet écosystème, constituant sa première source de financement et son principal point d'entrée pour les utilisateurs. L'OCDE estime ainsi que les applications centralisées sont le « lien vital » (« *lifeline* ») de la *DeFi* (OCDE, *Lessons from the crypto winter*, décembre 2022).

[34] *Application programming interface* (interface de programmation d'application), c'est-à-dire une interface logicielle permettant de « connecter » un logiciel ou un service à un autre logiciel ou service, afin d'échanger des données et des fonctionnalités.

[35] Exemples : Binance, Coinbase.

Schéma : L'architecture applicative de la *DeFi*



II. Les risques liés à la DeFi

2-1. Les risques liés à la gouvernance décentralisée

Qu'il s'agisse des blockchains ou des applications construites sur ces infrastructures, la **gouvernance décentralisée** présente d'importants risques : des utilisateurs détenant la gouvernance *de fait* d'un protocole peuvent prendre des décisions néfastes aux détenteurs minoritaires. Ce problème est d'autant plus prégnant dans l'univers *DeFi* que de nombreux protocoles présentent une **gouvernance faussement décentralisée**.

Tout d'abord, les **jetons de gouvernance sont parfois concentrés dans les mains de quelques acteurs**. Cela peut être lié au fait que les jetons de gouvernance peuvent être échangés comme d'autres crypto-actifs, ce qui permet à des utilisateurs importants (« *whales* ») d'accumuler de larges parts des jetons. Les prêts instantanés (*flash loans*) peuvent d'ailleurs être utilisés pour conduire des attaques contre un protocole, en empruntant de vastes quantités de jetons de gouvernance pour une durée courte, mais suffisante pour voter une décision nocive aux autres utilisateurs.

La concentration des jetons peut également provenir de ce que les **fondateurs, développeurs ou financeurs d'un protocole ont conservé pour eux une majorité des jetons de gouvernance** : ainsi, en février 2020, lorsque le protocole Compound a lancé son jeton de gouvernance (le COMP), près de 50 % des *tokens* ont été attribués aux développeurs et aux financeurs du projet[36] ; plusieurs années après, la gouvernance du protocole reste dominée par un petit nombre d'acteurs[37]. C'est d'autant plus vrai que de nombreux détenteurs de jetons de gouvernance ne prennent généralement pas part aux différents votes, soit parce qu'ils connaissent mal les procédures ou ne sont pas informés de la tenue d'un vote, soit parce qu'ils anticipent qu'ils parviendront difficilement à peser sur la décision face aux *whales*[38]. Il faut d'ailleurs noter que la logique de pseudonymat qui règne dans l'écosystème *DeFi* empêche la transparence sur la concentration des jetons de gouvernance, puisqu'un même utilisateur peut disposer de plusieurs adresses (voir aussi le point 2-4-4 sur la question du pseudonymat).

Il faut ensuite souligner que le fonctionnement de nombreux protocoles de blockchains ou d'applications *DeFi* **ne repose pas intégralement – et parfois : pas essentiellement – sur le vote** des détenteurs de jetons de gouvernance. L'adoption d'un changement dans les protocoles est ainsi souvent soumis à l'accord préalable de certaines parties, tandis que des entités peuvent disposer de droits de véto[39]. Dans la même veine, les fondateurs ou développeurs peuvent avoir conservé les **clés d'administrateurs** d'un protocole *DeFi*, et ainsi disposer de la capacité à modifier ses règles de fonctionnement sans l'accord des instances de gouvernance décentralisée. Si la pratique peut sembler légitime au lancement d'un protocole, afin de pouvoir rectifier rapidement d'éventuels

[36] Sur les 10 millions de jetons émis, 4,9 millions ont ainsi été distribués en interne : 2,3 millions aux actionnaires de l'entreprise Compound Labs, 2,2 millions aux fondateurs et membres de l'équipe de développement, et 0,4 million aux futurs membres de l'équipe.

[37] Au 20 janvier 2023, 50 % des droits de vote étaient ainsi partagés entre 9 acteurs (source : site internet du protocole).

[38] Sur ce point, voir OCDE, *Why Decentralised Finance (DeFi) Matters and the Policy Implications,* janvier 2022, p. 35

[39] Par exemple, l'adoption d'un changement dans le fonctionnement d'Ethereum est soumise à l'avis conforme des développeurs du protocole, et nécessite également l'accord de nombreuses parties prenantes (voir : Gouvernance d'Ethereum | ethereum.org)

dysfonctionnements, elle entre rapidement en contradiction avec les promesses de la gouvernance décentralisée, notamment lorsque les autres utilisateurs ne sont pas informés de cette situation.

Un exemple classique des risques liés à la mauvaise gouvernance est la manœuvre dite de « ***rug pull*** », une situation dans laquelle l'émetteur d'un crypto-actif s'enfuit avec les fonds des investisseurs. De fait, un nouveau jeton peut être émis sur une blockchain pour un coût modique ; grâce à un apport de liquidité, le jeton peut ensuite être introduit sur des plates-formes d'échange décentralisées (DEX) ; des campagnes marketing sur les réseaux sociaux, parfois à l'aide d'influenceurs populaires, ainsi que des distributions gratuites de jetons (*airdrops*), peuvent ensuite être organisées pour en faire monter le prix ; lorsque le prix atteint un niveau suffisamment élevé et que la liquidité est importante, les fondateurs ou développeurs du projet vendent en masse les jetons qu'ils ont conservés, et disparaissent avec ces fonds et la réserve[40] ; les autres investisseurs se retrouvent alors avec de grandes quantités de jetons dont la valeur est nulle.

2-2. Les risques liés aux infrastructures

2-2-1. Le problème du passage à l'échelle et ses conséquences en matière d'infrastructure

Certaines blockchains font face à des épisodes de **congestion du réseau** en raison d'un nombre important de transactions requérant une puissance de calcul élevée. Cette congestion fait échouer certaines transactions, impacte les retraits en crypto-actifs ou empêche la mise à jour de certaines cotations. La congestion est la conséquence des difficultés qu'ont les blockchains à **passer à l'échelle** (*scalability*), c'est-à-dire à traiter un plus grand nombre de transactions à la seconde sans perte d'efficacité[41]. Le caractère décentralisé de la validation des transactions sur blockchain implique en effet des contraintes d'énergie et de stockage – donc des coûts – pour chaque nœud validateur. L'arbitrage entre décentralisation, sécurité et capacité à passer à l'échelle a été désigné sous le vocable de « trilemme de la blockchain »[42]. Ce problème pourrait devenir crucial si les opérations de *DeFi* avaient vocation à jouer un rôle significatif, en complément ou en substitution de la finance traditionnelle, dans la mesure où le nombre de transactions deviendrait alors considérable.

a. Les solutions de « *layer 1* » augmentent le risque de corruption des blockchains

Face au problème de congestion du réseau, des **solutions internes à la blockchain**, dites solutions de ***layer 1***, ont d'abord émergé. Elles peuvent en premier lieu consister à augmenter la puissance de validation. Mais, en raison du peu de machines disponibles et du coût de la validation, ceci tend à réduire concomitamment le nombre de nœuds validateurs, et donc la sécurité du réseau et sa

[40] Face à ce problème, la plupart des clés d'administration des protocoles proposant un dépôt de fonds sont sécurisées par des *timelocks* (verrouillage des fonds pendant un certain temps) ou, plus souvent, par des mécanismes de signature multiples (*multisig*) : les fonds du protocole ne peuvent alors être débloqués qu'avec la signature de plusieurs personnes (souvent une dizaine). Ce système de *multisig* n'est cependant pas sans risque, puisque les personnes en question peuvent se connaître (il peut notamment s'agir de l'équipe des développeurs du protocole), et donc s'entendre à des fins malveillantes.

[41] Ethereum ne peut traiter aujourd'hui qu'entre 10 et 15 transactions par seconde (autour de 7 pour Bitcoin), quand un réseau comme Visa traite jusqu'à 24 000 transactions par seconde.

[42] Le développement de nouvelles générations de blockchains et de solutions de surcouche pourrait toutefois permettre de surmonter ce trilemme (*cf. infra*).

décentralisation (*cf. infra*). Une autre solution, le partitionnement (*sharding*), consiste à fragmenter une blockchain en plusieurs blockchains plus petites et plus flexibles, appelées fragments (*shards*). Les nœuds de validation ne stockent plus alors qu'une partie de l'information, même si celle-ci peut toujours être partagée ; leur travail s'en trouve donc accéléré.

L'inconvénient commun de ces solutions est de rendre les blockchains plus facilement corruptibles, notamment via des « attaques des 51 % » (*cf. infra*). Le passage à l'échelle via les solutions de *layer 1* se réalise donc **au détriment de la sécurité et de la décentralisation**.

b. Les solutions de « *layer 2* » peuvent accentuer le manque d'interopérabilité entre blockchains et poser des problèmes de sécurité

Un deuxième axe pour favoriser le passage à l'échelle consiste à recourir à des « **surcouches** » ou ***layer 2***, situées **en dehors de la blockchain principale** (considérée comme la *layer 1*) dont on cherche à accroître l'efficacité. Le principe est que les transactions aient lieu en dehors de la blockchain principale, et que seul leur résultat soit reporté sur celle-ci, ce qui limite le besoin d'enregistrer de nouveaux blocs. Un certain nombre de techniques permettent de mettre en œuvre ce principe (*state channels*[43], *nested blockchains*[44], *sidechains*[45]…) ; les plus répandues aujourd'hui sont les « ***rollups*** ». Un *rollup* exécute les transactions passées sur son réseau, « enroule » ces transactions en une seule opération (d'où son nom), et compresse l'information, en envoyant uniquement les données strictement nécessaires à la vérification des transactions sur la blockchain.

Deux grands types de *rollups* existent actuellement, selon la manière d'envisager la validation des transactions reportées sur la blockchain principale. Les ***optimistic rollups***[46], d'abord, partent du principe que les transactions sont valides jusqu'à preuve du contraire (d'où leur nom). Concrètement, les lots de transactions sont envoyés sur la blockchain par un opérateur ; s'ouvre alors une période de 7 jours durant laquelle n'importe quel nœud du réseau blockchain peut en contester la validité ; si une transaction frauduleuse est repérée, un retour en arrière est effectué ; le nœud ayant contesté la validité est alors récompensé, tandis que l'opérateur ayant soumis le lot de transaction est puni (via la destruction d'une partie des crypto-actifs qu'il a préalablement déposés en collatéral). Une fois la période de 7 jours écoulée, le lot de transactions est définitivement inscrit sur la blockchain principale. L'*optimistic rollup* nécessite donc qu'il y ait au moins un validateur honnête sur le réseau, faute de quoi l'opérateur[47] du *rollup* peut produire des blocs frauduleux en vue de dérober des crypto-actifs. En outre, le délai nécessaire à l'inscription définitive des transactions induit un temps de latence conséquent pour les utilisateurs.

[43] Elles permettent des transactions de pair-à-pair, entre utilisateurs connus les uns des autres, sans intervention d'un tiers de validation (exemple : Lightning Network sur Bitcoin ou Raiden Network sur Ethereum).
[44] Système de poupées gigognes de différentes blockchains avec une sous-traitance d'opération d'une blockchain plus fondamentale à la suivante (exemple : Plasma sur Ethereum).
[45] Blockchains adjacentes fonctionnant sur une infrastructure et des mécanismes de consensus entièrement indépendants de ceux de la chaîne principale. Elles communiquent toutefois directement avec cette dernière : contrairement aux *state channels*, les transactions ne sont donc pas privées, mais affichées publiquement sur la blockchain (exemple : Polygon pour Ethereum).
[46] Exemples sur Ethereum : Arbitrum, Optimism.
[47] Les *optimistic rollups* sont aujourd'hui opérés par des entités centralisées.

Un deuxième modèle est celui des ***Zero-knowledge rollups*** (ou *ZK-rollups*)[48]. Dans ce modèle, à chaque fois qu'un opérateur place un lot de transactions sur la blockchain, il dépose également une preuve cryptographique de leur validité, dite « preuve à divulgation nulle de connaissance » (*zero-knowledge proof*), car elle prouve la véracité d'une proposition sans délivrer d'autre information, ce qui génère notamment d'importantes économies d'information[49]. Ce modèle permet en outre à n'importe quel acteur de reporter les transactions sur la blockchain principale. Il est toutefois en cours de développement et ne fait pas l'objet d'une adoption généralisée. Surtout, le calcul des preuves nécessite une puissance de calcul conséquente ; en pratique, ces preuves ne sont donc produites aujourd'hui que par quelques acteurs, ce qui génère un risque.

Le **développement rapide**[50] des solutions de *layer 2* tend à transformer les blockchains *layer 1* en simples couches de « tenue de compte », les transactions se déroulant de manière croissante sur les « surcouches ». Cependant, il tend aussi à **amplifier le manque de connectivité ou d'interopérabilité**[51] **entre blockchains**, qui constitue un problème majeur : en effet, chaque blockchain fonctionne aujourd'hui isolément[52]. En outre, aucune de ces solutions n'offre le même niveau de sécurité que les blockchains principales, le résultat n'étant pas garanti jusqu'à ce que les transactions soient enregistrées sur la *layer 1*. Enfin, on peut se demander si certaines des solutions de *layer 2* ne créent pas un obstacle à la transparence de l'information sur la blockchain principale.

Le développement de solutions internes aux blockchains ou recourant à des surcouches peuvent donc conduire à limiter la sécurité de l'infrastructure ou à accroître certaines de ses fragilités, ce qui devrait attirer l'attention du régulateur.

2-2-2. Ces développements pourraient accroître les vulnérabilités de l'infrastructure blockchain[53]

La robustesse d'un protocole *DeFi* se mesure à sa capacité à n'être ni piraté ni détourné de son utilisation première. En raison de son caractère récent et de son immaturité, la *DeFi* est particulièrement propice à des vulnérabilités dites *zero day* : des abus de protocole auxquels personne n'avait eu à faire face auparavant. Parmi ces faiblesses, on peut citer :

- **Les attaques sur le réseau de la blockchain** (*network layer*) : lorsqu'un nœud se connecte à la blockchain, il est mis en relation avec d'autres nœuds à travers un réseau pair-à-pair pour partager des informations sur les évolutions de la blockchain. Il est relativement facile de créer

[48] Exemples sur Ethereum : Starkware, zkSync.
[49] La taille de la preuve étant logarithmique à la taille des opérations.
[50] Notons que ces solutions peuvent elles-mêmes être touchées par des problèmes de congestion, du fait de leur succès. Il semble que ce phénomène touche particulièrement les surcouches les plus généralistes, et moins les *layer 2* à usage restreint, comme par exemple le Lightning Network de Bitcoin qui se contente de proposer des transactions pair-à-pair.
[51] Ce défi de l'interopérabilité s'étend aussi au format de données fournies par les oracles et utilisées par les blockchains, qui n'est pas encore standardisé
[52] Même si certains projets récents tendent à laisser penser que des avancées pourraient avoir lieu sur cette question : Polkadot, Cosmos ou Avalanche par exemple.
[53] On peut noter, plus largement, que les infrastructures blockchain, pour garantir la sécurité des transactions qui s'y déroulent, reposent crucialement sur les techniques de cryptographie par clé publique, qui pourraient être à terme menacées par le développement de l'informatique quantique. Sur ce sujet, on pourra notamment se reporter au rapport d'expérimentation publié par la Banque de France en novembre 2022.

des nouveaux nœuds. Un utilisateur malveillant peut créer des faux nœuds, qui sont ensuite mis en relation avec un nœud légitime ciblé, qui se trouve alors isolé du reste du « véritable » réseau. Le nœud ciblé peut ainsi être éclipsé : les blocs qu'il valide ne sont jamais ajoutés à la blockchain, tandis que les crypto-actifs qu'il reçoit peuvent faire l'objet d'une double dépense.

- **Les attaques sur les mécanismes de consensus** (*consensus layer*) **ou de gouvernance** (*governance layer*) : ces attaques tirent parti de la vulnérabilité que peut représenter une gouvernance concentrée entre les mains de quelques acteurs. C'est notamment le cas lorsque la gouvernance est faussement décentralisée – lorsque les fondateurs ont par exemple gardé pour eux une majorité de jetons de gouvernance –, ou encore en situation de stress[54]. Les blockchains sont en particulier très vulnérables aux attaques dites « des 51 % » qui se produisent lorsqu'un groupe d'utilisateurs malveillant dispose de plus de 50 % des capacités de validation. Cette majorité permet au groupe d'altérer la blockchain en validant des blocs falsifiés[55] ou en bloquant les adresses de certains utilisateurs. Les blockchains les plus petites sont les plus vulnérables à ce type d'attaques, car disposer de la majorité du potentiel de validation (puissance de calcul ou jetons de validation) est extrêmement coûteux sur les plus grosses blockchains[56].

- **Les attaques sur les ponts** (*bridges)* entre blockchains : ces ponts concentrent un bon nombre d'attaques significatives intervenues récemment[57]. Pour les *bridges* centralisés, il s'agit le plus souvent de prise de contrôle des signatures nécessaires à la validation, en particulier lorsque ces signatures sont relativement concentrées dans les mains d'un même acteur. Pour les *bridges* décentralisés, il s'agit souvent de failles dans les *smart contracts*. La vulnérabilité des structures de *bridge*, quelle que soit leur forme, a d'ailleurs conduit beaucoup d'acteurs à privilégier des solutions de *layer 2* plutôt que des systèmes multi-chaînes.

2-3. Les risques liés à la couche applicative

Une bonne partie des risques liés aux services de *DeFi* provient du **code informatique des automates exécuteurs de clauses** (*smart contracts*), que ce code comporte des failles volontaires (programme frauduleux) ou involontaires (programme écrit sans intention malveillante, mais présentant des défauts pouvant être utilisés par des attaquants). Les principaux risques en la matière sont l'attaque de « réentrée » (*reetrancy attack*)[58] qui permet de siphonner les fonds disponibles, ou encore les

[54] Ainsi, lorsque le jeton Luna a perdu 98 % de sa valeur, en mai 2022, un petit groupe d'acteurs malveillants avait l'opportunité de racheter une majorité des jetons de gouvernance de la blockchain Terra et, en déléguant ensemble leur pouvoir de décision à un validateur complice, de prendre le contrôle de l'infrastructure. Pour empêcher ce scénario, la blockchain avait dû être mise en pause par ses administrateurs (les principaux validateurs s'étant mis d'accord pour stopper temporairement la validation de nouveaux blocs).

[55] Le risque principal est alors la possibilité de « double dépense », qui permet de récupérer des crypto-actifs déjà dépensés en faisant passer un premier bloc avant celui validant définitivement la transaction.

[56] À noter que la blockchain Ethereum Classic a été plusieurs fois victime de ce type d'attaque en 2019 et 2020.

[57] Par exemple Wormhole (Solana) en février 2022, ou Ronin Network en mars 2022.

[58] Possibilité d'utiliser certaines fonctions des *smart contracts* de manière récursive, c'est-à-dire plusieurs fois à un rythme très rapide ; typiquement, l'opération permet d'effectuer de nombreux retraits de fonds sur un compte avant que la fonction de mise à jour du solde du compte ne puisse s'exécuter.

attaques par dépassement ou « soupassement » d'entier[59] ainsi que les manipulations possibles par les validateurs[60]. À cet égard, le fait que le code des *smart contracts* soit public fait de ces automates une cible exposée à tous : la surface d'attaque est donc accrue, même si l'on peut arguer que cette caractéristique les rend, à l'usage, plus résistants que des algorithmes privés.

Il est à noter que la vulnérabilité de la couche applicative de la *DeFi* est accrue par l'une de ses caractéristiques les plus intéressantes, c'est-à-dire la **composabilité** de ses éléments : un *smart contract* défectueux peut être appelé par d'autres *smart contracts* ; ses vulnérabilités peuvent ainsi se propager à un grand nombre d'applications, sans que les utilisateurs n'en aient conscience.

La question de la **fiabilité des données**, moins explorée, contribue également aux risques pour l'utilisateur. La bonne transmission de l'information est en effet la condition d'un fonctionnement efficient des marchés, dans la *DeFi* comme dans la finance traditionnelle. Une spécificité de la *DeFi* est en revanche qu'un certain nombre d'opérations sont automatiquement exécutées lorsque certaines clauses sont remplies. Or il s'agit d'une tâche redoutablement complexe, l'alimentation de données devant s'effectuer en quasi temps réel, et ce pour une grande variété de données (reflétant la grande variété des sous-jacents sur lesquels peuvent porter les automates exécuteurs de clauses : cours de crypto-actifs ou d'actifs traditionnels bien sûr, mais aussi météo, flux logistiques etc.).

Cette complexité souligne le rôle critique des fournisseurs de données – les **oracles** – qui importent les flux d'information exogènes dans les blockchains (rappelons que celles-ci ne peuvent pas accéder à des bases de données externes). Ces oracles peuvent être classiquement des entités centralisées, mais également des applications décentralisées, dans leur gouvernance comme dans leur manière de collecter l'information : des volontaires sont appelés à envoyer des données ; l'oracle synthétise les informations fournies via une moyenne (généralement pondérée) ; les fournisseurs d'information sont ensuite rémunérés en fonction de leur proximité à cette moyenne, considérée comme la donnée juste.

Le rôle crucial des oracles met en lumière les risques qui peuvent découler d'erreurs ou de fraudes de leur part : exécution ou non-exécution erronée de clauses automatisées, voire manipulation des prix de marché. Ces erreurs sont d'autant plus problématiques que les transactions effectuées sur une blockchain sont presque toujours irréversibles.

2-4. Les risques liés aux services et aux usages

2-4-1. La *DeFi* fait peser des risques particuliers sur la clientèle de détail

L'écosystème *DeFi* a attiré, en 2020-2021, un nombre significatif de particuliers, séduits par l'effet de mode et la peur de « ne pas en être » (*fear of missing out* – « FOMO »), ainsi que par la promesse de

[59] Un dépassement d'entier (*integer overflow*) survient lorsqu'une opération mathématique produit une valeur numérique supérieure à celle représentable dans l'espace de stockage disponible (par exemple, en 32 bits, la valeur maximum représentable est 2^{32}-1). De la même manière, le « soupassement » (*integer underflow*) se produit en cas d'obtention d'un résultat non nul inférieur à la plus petite valeur non nulle susceptible d'être représentée. Ces erreurs informatiques peuvent être exploitées par des attaquants pour neutraliser des procédures de vérification, par exemple celle assurant qu'un compte dispose d'un montant minimum avant de valider un retrait.

[60] Par exemple en exploitant la *transaction ordering dependence*, c'est-à-dire en altérant l'ordre d'exécution des transactions. Ceci donne la possibilité à un validateur de modifier le prix d'une transaction pendant qu'elle est traitée, en validant préalablement une autre transaction à un prix différent (possiblement manipulé).

rendements élevés. Par exemple, en février 2021, la fourniture de liquidité en Tether au sein du protocole de prêt Compound était associée à un taux d'intérêt de 11 %[61]. En outre, les plus-values réalisées au sein de la *DeFi* apparaissent corrélées au nombre de participants : cela peut refléter une évolution de la valeur fondamentale de l'écosystème, bénéficiant de l'accroissement de la liquidité et de la profondeur du marché, mais cela peut également relever de logiques pyramidales de type Ponzi.

De fait, les particuliers entrés sur ce marché ont été confrontés à des **risques élevés de perte en capital**, en raison de la volatilité du cours des crypto-actifs, des risques liés à la gouvernance des protocoles (*cf.* partie 2-1), de la complexité des produits proposés, et de la prolifération des escroqueries, vols et piratages. Or ces utilisateurs n'ont pas toujours eu pleinement conscience du niveau de risque des placements qu'ils avaient souscrit. Les interfaces web conçues pour faciliter l'accès aux protocoles *DeFi* peuvent en effet contribuer à donner aux utilisateurs un **faux sentiment de compréhension** de mécanismes financiers pourtant complexes. De même, la transparence du code peut donner un faux sentiment de maîtrise à des utilisateurs qui n'ont pourtant aucune compétence en programmation, ou même à des programmeurs informatiques dénués de compétences financières.

Le problème est renforcé par la facilité à coder des **produits extrêmement complexes**, grâce notamment à la composabilité des automates exécuteurs de clauses sur la blockchain. L'écosystème *DeFi* se caractérise ainsi par la prolifération de dérivés sur crypto-actifs, sous diverses formes, qui permettent notamment de s'endetter avec un effet de levier considérable (*cf. infra*). Ce faisant, des particuliers peuvent participer, sans vérification aucune de leurs connaissances financières, à des contrats à haut risque, habituellement réservés à des professionnels aguerris dans l'univers de la finance traditionnelle.

2-4-2. L'écosystème *DeFi* présente des fragilités systémiques, renforcées par certains mécanismes comme la liquidation automatisée

a. La fragilité systémique de la *DeFi*

La fragilité systémique de la *DeFi* tient d'abord à la **volatilité du prix des cryptos-actifs** qui y sont échangés. Ce phénomène peut d'ailleurs toucher des actifs présentés comme sûrs et stables par leurs promoteurs, comme l'a montré l'effondrement du système Terra-Luna en mai 2022. De plus, **l'écosystème *DeFi* exerce une rétroaction sur le marché des crypto-actifs, tendant à renforcer sa volatilité** : d'une part, en contribuant à la création de nombreux jetons (souvent en contrepartie du fonctionnement des protocoles *DeFi*), dont la valeur fondamentale est difficile à estimer, et qui font souvent l'objet de mouvements spéculatifs de grande ampleur ; d'autre part, en accentuant l'effet de levier des acteurs, ce qui renforce l'amplitude des chocs sur les prix, et donc les risques en cas de cycle baissier (*cf. infra*).

La fragilité provient ensuite de **l'endogénéité de nombreux placements**, notamment en raison de l'importance des activités de prêts-emprunts, et de la **concentration du marché *DeFi*** dans les mains de quelques acteurs : un petit nombre de protocoles concentrent ainsi l'essentiel de la valeur de l'écosystème (*cf.* partie 1) tandis que certains détenteurs massifs de jetons de gouvernance (*whales*) exercent la gouvernance de fait de nombreux protocoles (*cf.* point 2-2-1).

[61] Taux annuel effectif global. Source : Banque centrale européenne (BCE), Decentralised finance – a new unregulated non-bank system?

Enfin, la fragilité est liée à l'important **effet de levier** de nombreux emprunteurs. Certes, les prêts dans l'écosystème *DeFi* sont généralement « sur-collatéralisés », c'est-à-dire que la garantie déposée auprès du prêteur (souvent un « pool de liquidité ») a une valeur supérieure au montant emprunté[62]. Cette **sur-collatéralisation** est la conséquence de l'**absence de confiance** entre les parties à l'échange, d'une part, et de la **volatilité** du cours des crypto-actifs d'autre part. Un emprunteur qui souhaite éviter le risque d'une liquidation de sa position doit en permanence vérifier la valeur du collatéral qu'il a déposé et, lorsque celle-ci diminue, bloquer davantage de jetons. Ce système correspond aux « appels de marge » des chambres de compensation sur le marché traditionnel des *repos* ou des *swaps*. Il présente l'avantage de limiter l'effet de levier des emprunteurs, toutes choses égales par ailleurs.

Pourtant, **plusieurs mécanismes mettent à mal ce schéma** et expliquent que le niveau des dettes soit souvent élevé dans l'univers de la *DeFi*. Tout d'abord, la corrélation observée entre la valeur des crypto-actifs et la vigueur du marché *DeFi* (*cf. supra*) peut conduire à une augmentation de l'effet de levier (exprimé par rapport à la valeur de départ des positions) : la hausse de la valeur des jetons augmente la valeur du collatéral, ce qui permet en retour d'emprunter davantage. Ensuite, le développement de **l'échange décentralisé de produits dérivés** – en particulier les contrats à terme perpétuels (*perpetual futures*)[63] qui ne nécessitent pas l'emprunt effectif des crypto-actifs sous-jacents[64] – permet aux utilisateurs d'atteindre des effets de levier considérables, de l'ordre de x25[65] début 2023 sur la plateforme dYdX, ou de x50 sur la plateforme GMX[66].

Même dans le cas des emprunts plus classiques, il faut noter que la **sur-collatéralisation ne constitue nullement une règle gravée dans le marbre**, et ce d'autant plus qu'elle est **peu efficace en capital** : sous l'effet de la concurrence, des applications de prêt pourraient à l'avenir proposer des taux de collatéralisation inférieurs à 100 % ; elles seraient alors probablement assorties de mécanismes d'évaluation de la solvabilité, éventuellement eux-mêmes décentralisés. En tout état de cause, **la collatéralisation ne constitue pas une ligne de défense à toute épreuve, en particulier lorsque la valeur de tous les crypto-actifs diminue simultanément**. Cette fragilité tend même à être exacerbée par les mécanismes de liquidation automatisée des positions qui sont aujourd'hui la règle dans l'écosystème *DeFi*.

b. Les mécanismes de liquidation automatisée des contrats peuvent paradoxalement accroître la fragilité du système

Dans toutes les applications de prêt de la *DeFi* (prêts classiques de crypto-actifs, prêts via l'échange de dérivés comme les *perpetual futures* etc.), la position de l'emprunteur est liquidée lorsque la valeur de son collatéral diminue en-dessous d'un certain seuil. Les liquidations sont effectuées avec l'aide d'un

[62] Le niveau de sur-collatéralisation dépend généralement de la nature du collatéral déposé. Ainsi, en janvier 2023, sur Aave, la sur-collatéralisation est de 133 % pour des « *stablecoins* » comme l'USDC ou le DAI, de 166 % à 250 % pour d'autres crypto-actifs, et peut atteindre 600 % pour des crypto-actifs considérés comme de qualité médiocre.

[63] Voir aussi la partie 1-3 sur ces contrats.

[64] D'autres techniques similaires existent, comme l'achat de jetons à effet de levier (*leveraged tokens*), qui encapsulent l'exposition souhaitée.

[65] L'effet de levier s'exprime en multiples de l'actif réellement détenu par l'emprunteur. Ainsi un effet de levier x25 signifie qu'un emprunteur disposant de l'équivalent de 100 euros en crypto-actifs s'endette à hauteur de 2 500 euros. Plus l'effet de levier est important, plus le gain est important en cas de succès, mais plus les pertes sont élevées en cas d'échec.

[66] Les niveaux indiqués ici évoluent en fonction du temps ; ils ont pu atteindre x100 en 2021.

tiers appelé « liquidateur » – généralement un robot –, qui rembourse au prêteur les crypto-actifs prêtés et procède à la liquidation du collatéral en prélevant une commission : l'emprunteur subit donc une perte en capital à la suite de l'opération (et il supporte seul l'ensemble de la perte). **Cette liquidation est quasi-automatique**, c'est-à-dire qu'elle est encodée dans le *smart contract* du prêt : dès lors que la valeur du collatéral diminue en dessous d'un seuil prédéterminé, la position est liquidée[67].

La liquidation des positions constitue au premier regard un système protecteur pour le prêteur et pour l'emprunteur. Elle permet en effet au prêteur de ne subir aucune perte en capital ; tout juste subira-t-il un coût d'opportunité si le prêt n'a pas généré de revenus en raison de la liquidation. Pour l'emprunteur, c'est l'assurance de subir une perte limitée : par construction, la perte maximum ne peut excéder la valeur du collatéral engagé. Ainsi, la souscription d'un prêt à effet de levier important n'augmente pas le niveau maximum de capital susceptible d'être perdu par l'utilisateur, mais la probabilité de perdre ce capital et la vitesse à laquelle celui-ci risque d'être perdu.

Le système de liquidation automatique comporte pourtant un **risque d'effondrement général du système**. La diminution de la valeur d'un jeton peut enclencher la liquidation d'un certain nombre de positions garanties par celui-ci ; la liquidation automatique des positions conduit en retour à des ventes massives du jeton en question, ce qui amoindrit encore sa valeur[68]. Cela tend à provoquer de nouvelles liquidations puis, par effet de contagion, la baisse de la valeur d'autres crypto-actifs, pouvant résulter *in fine* en un effondrement général se traduisant par des pertes massives (y compris pour les prêteurs).

Le risque est d'autant plus aigu que des comportements de **liquidation agressive** sont fréquemment observés : puisqu'ils empochent une commission à chaque liquidation, les liquidateurs peuvent être tentés de les provoquer, notamment en spéculant à la baisse sur la valeur de certains crypto-actifs. Lorsque leur taille est suffisamment importante, ces acteurs disposent ainsi de la capacité à réaliser des manipulations de marché déclenchant des liquidations. Ceci est d'autant plus vrai que lorsque la valeur d'un crypto-actif diminue très rapidement, les utilisateurs n'ont pas toujours le temps (ou les moyens) de re-collatéraliser leurs positions.

2-4-3. Le rôle particulier joué par les « *stablecoins* » et les risques liés ont fait l'objet d'une première réponse réglementaire

Les **« *stablecoins* »[69] sont aujourd'hui indispensables au fonctionnement de la *DeFi*** en raison des deux rôles qu'ils jouent dans cet écosystème. **Premièrement ils sont les actifs de règlement des transactions** : les *stablecoins* sont en particulier largement utilisés comme collatéral des emprunts de crypto-actifs. De fait, les autres crypto-actifs, du fait de la volatilité de leur cours, peuvent difficilement prétendre jouer ce rôle. **Deuxièmement, ils constituent le point de contact principal de la *DeFi* avec le monde réel**. Ainsi, de nombreux utilisateurs conservent leurs avoirs sous la forme de *stablecoins*, afin de se prémunir contre la volatilité des cours des crypto-actifs sans avoir pour autant à repasser

[67] Plus précisément, la position est « ouverte à la liquidation » par le *smart contract* ; la liquidation n'advient que si un liquidateur intervient. Cela dit, bon nombre de liquidateurs sont en pratique des robots, ce qui confère au mécanisme un fort degré d'automaticité.
[68] De même, en finance traditionnelle, l'activité de repo est soumise au risque de « *fire sales* ».
[69] Parfois aussi désignés sous le vocable « unité de compte à faible volatilité ». Voir aussi l'encadré 1 sur les difficultés sémantiques sur le vocable « *stablecoin* ».

par une conversion en monnaie officielle (mais en gardant la possibilité de procéder à tout moment à cette conversion). Dans le sens inverse, les principaux émetteurs de *stablecoins*, qui ont investi une partie de leurs réserves dans des billets de trésorerie et d'autres actifs de court terme aux États-Unis, sont devenus des acteurs importants de ce marché en 2021[70]. Pour ces deux raisons, les *stablecoins* constituent un élément critique de l'écosystème *DeFi* : au sein de l'écosystème, la perte de parité (*depeg*) d'un *stablecoin* (par rapport à la devise à laquelle il entend s'indexer) a la capacité de déstabiliser de nombreuses applications, comme l'ont montré les effets en chaîne de l'effondrement du système Terra-Luna ; en dehors de l'écosystème, les *stablecoins* constituent le principal vecteur potentiel de transmission des chocs de la *DeFi* vers la finance traditionnelle.

Les plus importants *stablecoins* sont aujourd'hui émis par des **entités centralisées** (Tether pour l'USDT, Circle pour l'USDC, Binance pour le BUSD), en contrepartie de dépôts de collatéral en monnaie officielle. Mais certaines **applications *DeFi*** émettent elles aussi des actifs ayant pour objectif de répliquer la valeur d'une monnaie officielle. Deux modèles principaux existent : les ***stablecoins* décentralisés collatéralisés**, tout d'abord, sont émis en contrepartie d'un collatéral en crypto-actifs déposé par les utilisateurs (là où les *stablecoins* centralisés sont émis en contrepartie d'un collatéral en monnaie officielle) ; l'exemple le plus connu en la matière est le DAI de MakerDAO. Les ***stablecoins* décentralisés « algorithmiques »**, quant à eux, entendent atteindre l'objectif de stabilité via une adaptation dynamique de l'offre de jetons : selon le niveau de la demande, le protocole émet de nouveaux jetons pour accroître l'offre ou, au contraire, rachète des jetons pour les détruire. Ces actions sont régies par des règles préalablement inscrites dans les algorithmes du protocole. L'exemple le plus connu de *stablecoin* décentralisé « algorithmique » était l'UST de Terra.

Le **règlement européen sur les marchés de crypto-actifs, dit MiCA**[71], **constitue une première réponse réglementaire** sur la question des *stablecoins*. Le règlement définit trois catégories de crypto-actifs ; parmi-celles-ci, les *Electronic money tokens* (EMT), correspondent aux crypto-actifs ayant pour objectif de maintenir une valeur stable en se référant à une monnaie officielle, tandis que les *Asset-referenced tokens* (ART) cherchent à atteindre cet objectif en se référant à un panier de devises ou à d'autres types de droits ou d'actifs (l'or par exemple)[72]. Le règlement MiCA prévoit en particulier que les EMT sont i) convertibles au pair, à tout moment, par rapport à leur devise de référence et ii) émis par des entités dont l'intégralité de la réserve est constituée d'actifs sûrs et liquides du monde réel. Cette seconde condition constitue en effet la seule garantie possible pour que l'émetteur ait à tout moment la capacité de rembourser ses clients, même en cas de panique (*run*).

Toutefois, le règlement MiCA ne s'applique pas aux services fournis de manière entièrement décentralisée[73] sans aucun intermédiaire, et en particulier pas aux protocoles émettant un crypto-actif prétendument stable, ni aux services qui utilisent des EMT pour leur fonctionnement. Il **faudrait probablement combler ce vide** en posant la règle suivante : **dès lors qu'un service décentralisé**

[70] Tether (émetteur de l'USDT) a ainsi pu détenir jusqu'à 30 milliards de dollars en billets de trésorerie (*commercial paper*) aux États-Unis au cours de l'année 2021, ce qui en faisait le 7ème plus gros investisseur mondial sur ce marché, selon JP Morgan. En 2022, Tether a annoncé avoir basculé une partie de ses réserves en bons du Trésor américain, un marché plus profond et donc moins sujet aux tensions sur la liquidité. Sur ce sujet, on pourra plus généralement se reporter à Barthélémy, Gardin et Nguyen, *Stablecoins and the Financing of the Real Economy* (Banque de France, Working paper, février 2023).

[71] Le règlement MiCA (« *Markets in crypto-assets regulation* ») entrera en vigueur en 2023, et en application au second semestre de 2024.

[72] MiCA distingue, outre les EMT et les ART, les « autres crypto-actifs ».

[73] Le règlement prévoit néanmoins l'établissement d'un rapport sur l'assujettissement de la *DeFi* à la réglementation européenne dans les 18 mois suivant l'entrée en vigueur du texte.

prétend créer ou utiliser un crypto-actif ayant pour référence une monnaie officielle, ce crypto-actif doit obligatoirement être un EMT au sens de MiCA (ou un actif équivalent). L'appellation *stablecoin* constitue en effet une promesse de stabilité et de sécurité pour les utilisateurs. Son utilisation doit donc être strictement encadrée, afin de protéger la clientèle et afin de limiter les effets de contagion possibles vers le monde réel.

2-4-4. Les risques de blanchiment de capitaux et de financement du terrorisme dans l'écosystème *DeFi*

L'absence d'identification des utilisateurs (procédure « *Know your customer* » ou KYC) et de contrôle de l'origine des fonds engendre logiquement des risques de blanchiment de capitaux et de financement du terrorisme (BC-FT) dans l'écosystème *DeFi*. En effet, sur les blockchains publiques qui servent d'infrastructure à la *DeFi*, la règle est le **pseudonymat** : les utilisateurs sont identifiés par leur adresse sur la blockchain (et/ou un pseudonyme), et pas par leur nom. En outre, les applications *DeFi* fonctionnent pour la plupart sans contrôle d'accès : la participation nécessite uniquement la connexion à un *wallet (cf.* partie 1-6*)*, et une partie de ces portefeuilles peuvent être ouverts par les clients sans vérification d'identité ni contrôle de l'origine des fonds déposés.

Notons toutefois que **le pseudonymat n'est pas l'anonymat** : les actions de chaque adresse sont enregistrées dans la blockchain et, dans la mesure où des blockchains publiques[74] sont utilisées, ces actions sont traçables publiquement, ce qui n'est généralement pas le cas dans l'univers de la finance traditionnelle. Certaines adresses peuvent ainsi être identifiées comme malveillantes ou suspectes par la communauté des utilisateurs. De fait, une forme d'auto-régulation est déjà à l'œuvre dans l'écosystème *DeFi*, qui s'exerce essentiellement par le partage de listes d'adresses d'utilisateurs et de services malveillants (*black lists*), cet échange s'opérant essentiellement via les réseaux sociaux. Sur la base de ces informations, ainsi que des liens qui peuvent être retracés entre adresses sur la blockchain, des entreprises spécialisées[75] proposent des services d'analyse de risque des adresses blockchains ou des protocoles *DeFi*. Cette traçabilité est néanmoins limitée par la facilité à créer de nouvelles adresses. De plus, elle est compliquée par différentes techniques (mixeurs[76], *chain-hopping*[77], actifs à anonymat renforcé). Selon le Groupe d'action financière (GAFI), les actifs numériques ont permis l'essor considérable de certains pans de la criminalité, notamment les rançongiciels[78] (les rançons étant presque systématiquement payées en actifs numériques).

[74] On peut noter, à rebours, que le développement des surcouches (*layer 2*, cf. *supra*) tend à réduire la transparence de l'information.
[75] Exemples : ScoreChain, Chainalysis.
[76] Les plates-formes de mixage mettent en commun les actifs de différents utilisateurs dans un même « *pool* », qui redistribue ensuite le montant déposé à chaque membre, de manière à rendre les fonds plus difficile à tracer.
[77] Fait de passer d'une infrastructure à une autre, ou d'un actif numérique à un autre, souvent en succession rapide, dans le but d'échapper aux tentatives de traçage.
[78] GAFI, Countering Ransomware Financing, Mars 2023.

III. Les pistes d'encadrement réglementaire

Lorsqu'une activité financière reposant sur des innovations technologiques apparaît, les régulateurs tentent d'abord de déterminer dans quelle mesure l'activité doit être considérée comme une novation, et si elle présente des risques spécifiques. En effet, la réglementation financière, technologiquement neutre, doit essentiellement s'articuler autour des risques, ce que résume la formule « même activité, mêmes risques, mêmes règles ».

La *DeFi*, appuyée sur des infrastructures blockchains, présente des caractéristiques qui la rendent **difficilement assimilable à la finance « traditionnelle »**. En particulier, la finance classique repose crucialement sur un certain nombre d'**intermédiaires** (banques, assurances, chambres de compensation etc.), accomplissant les opérations-clés et gérant les risques, sur lesquels pèse logiquement l'essentiel de la réglementation. Or le concept même de *DeFi* consiste en principe à bâtir une finance sans intermédiaires ou tiers de confiance (même s'il a pu être constaté dans les parties 1 et 2 que cette promesse n'est pas toujours tenue), ce qui engendre en retour des risques spécifiques. Face à cette novation, deux écueils doivent être évités.

Le **premier écueil consiste à vouloir répliquer intégralement et uniquement le cadre réglementaire existant**, sans prendre en compte les spécificités de la *DeFi* (et donc son intérêt potentiel). Cette tentation conduit à **restreindre la réflexion à l'identification d'intermédiaires** à qui appliquer des obligations – et il y a dans les faits des intermédiaires dans la *DeFi*, quoi que pas nécessairement à tous les niveaux. La démarche peut donc avoir ses limites : c'est pourquoi ce rapport se propose **d'explorer également d'autres types de solutions**, en s'inspirant notamment de **réglementations non financières**, comme celles qui régissent la sécurité des produits dans l'Union européenne (UE). Dans celles-ci, un certain nombre d'obligations pèsent directement sur les **produits**, se traduisant par la construction de chaînes d'obligations pour tous les acteurs intervenant dans leur fabrication et leur distribution, pouvant en particulier conduire à des mécanismes de substitution lorsque l'un de ces acteurs est situé hors de l'Union. C'est ainsi qu'un système de certification des automates exécuteurs de clauses est ici proposé, qui s'appliquerait au produit lui-même, sans qu'il soit nécessaire de définir un responsable direct de cette obligation. Si personne ne souhaite faire certifier un produit, il ne pourra tout simplement pas être distribué. Cela permet de définir un ensemble de produits jugés « sûrs », qui seront les seuls à pouvoir être proposés par les intermédiaires assurant l'accès du plus grand nombre aux services *DeFi*.

Un écueil inverse consiste à penser que, face au caractère décentralisé de la *DeFi* et à l'absence d'inscription territoriale[79] de ses protocoles, **la réglementation est forcément impuissante**. C'est, en premier lieu, prendre pour argent comptant l'ensemble des promesses de la *DeFi* ; dans la réalité, **la décentralisation est loin d'être toujours au rendez-vous** dans l'écosystème *DeFi*, tandis que certains acteurs centralisés y exercent des rôles-clés. C'est, en second lieu, **sous-estimer la capacité de régulation des pouvoirs publics** : que quelques individus dotés de compétences pointues puissent

[79] Ce document n'entend pas sous-estimer les problèmes liés à l'extra-territorialité des services *DeFi*, qui posent notamment la question de la capacité à réguler les acteurs de manière effective. S'agissant des intermédiaires, les problèmes d'extra-territorialité se posent de la même manière dans la *DeFi* qu'en finance traditionnelle. Il pourra d'ailleurs être noté que les intermédiaires fournisseurs de services ne cherchent pas toujours à s'implanter dans les territoires les moins-disants d'un point de vue réglementaire, car ils ont besoin de susciter la confiance des clients. Mais ces enjeux peuvent également concerner les nœuds de l'infrastructure blockchain (en particulier aux nœuds validateurs des transactions, *cf.* partie 3-1), ou encore les gestionnaires d'applications. Pour autant, les pistes proposées dans ce document semblent de nature à réduire les problèmes posés par l'éventuelle extra-territorialité des différents acteurs.

parvenir à accéder aux services *DeFi* ne constitue pas l'enjeu principal (de même que la régulation d'internet n'est pas rendue inutile par l'existence d'un *dark web*). L'enjeu principal est l'accès à la *DeFi* du grand public, d'une part, et des acteurs institutionnels, d'autre part. Ainsi, dans l'exemple de la certification obligatoire des automates exécuteurs de clauses : si la grande majorité des utilisateurs individuels est en pratique empêchée d'accéder aux protocoles non labellisés, et si les entreprises savent qu'elles encourent des amendes et une atteinte à leur réputation en cas d'infraction, la mesure est bien susceptible de produire des effets concrets.

3-1. Assurer une sécurité minimale de l'infrastructure

Un développement de la *DeFi* dans le futur supposerait de renforcer la sécurité et la résilience de l'infrastructure blockchain. Ceci peut se traduire par deux grands types de scenarii de régulation, selon le degré de criticité de l'infrastructure et le degré d'engagement des autorités publiques.

Schéma de régulation A : une infrastructure reposant sur des blockchains publiques, mais faisant l'objet d'un encadrement voire d'une surveillance

Dans un système assis sur des blockchains publiques, ce n'est pas la confiance entre les acteurs mais des règles du jeu automatisées qui doivent garantir la solidité de l'infrastructure. Ce mode d'organisation présente pour principal avantage d'être ouvert et accessible à tous : chacun peut décider de participer au réseau, voire en devenir un nœud validateur. En outre, les fournisseurs de services peuvent construire leur projet sur une infrastructure existante, qu'ils n'ont pas besoin de gérer ou de maintenir.

Toutefois, les blockchains publiques devraient être encadrées par un certain nombre de **standards minimaux**[80], concernant la conception du code informatique de l'infrastructure (risque de panne), les règles de gouvernance (voir le point 2-1 sur cette question), le nombre effectif de validateurs et leur concentration (*cf. infra*). S'agissant du **risque de panne**, les standards de sécurité pourraient notamment prévoir que le code sous-jacent fasse l'objet d'une certification a priori, soit par des audits humains, soit par des méthodes formelles (*cf.* le point 3-2 sur la certification du code informatique des applications *DeFi*, qui peut trouver largement à s'appliquer à l'infrastructure blockchain).

Le risque de prise de contrôle d'un réseau par un groupe d'attaquants (« attaque des 51 % ») étant d'autant plus élevé que le nombre de nœuds est faible, une réponse logique pourrait consister à fixer des règles quant au **nombre minimal de validateurs** d'une blockchain publique. Cela peut toutefois poser un **problème de concurrence** : si les transactions – ou les transactions au-delà d'un certain volume – devenaient interdites sur les blockchains trop petites, il serait difficile pour ces dernières de grandir et d'atteindre la taille minimale requise. Plus exactement, il faut noter que ce problème de concurrence existe déjà, comme dans toute industrie à effet de réseau : la fixation de règles ne ferait donc que l'accentuer.

Les autorités publiques devraient en tout cas prêter une attention soutenue au **degré de concentration des capacités de validation** sur les blockchains publiques, dès lors que l'infrastructure considérée atteint un certain niveau de criticité – et ce quelle que soit l'infrastructure en question : blockchains *layer 1*, mais aussi *rollups*, *sidechains*, *nested chains*, *shards* etc. Il faudrait ainsi surveiller à tout

[80] Pour ne pas contraindre excessivement les projets émergents, cet encadrement pourrait être proportionné à la taille (nombre de nœuds, valeur manipulée…) de chaque blockchain.

moment l'état de concentration des capacités de validation (détenteurs de jetons de protocole et validateurs délégués), et **fixer des plafonds** à cette concentration afin de garantir la sécurité des blockchains. Notons qu'afin d'éviter les phénomènes de contrôle indirect, une telle mesure supposerait la levée du pseudonymat, afin de pouvoir regrouper les différentes adresses d'un même individu ou d'une même entreprise ; elle supposerait également une connaissance exhaustive des détenteurs du capital de chaque entreprise possédant des jetons de gouvernance.

Si toutefois les seuils d'alerte étaient dépassés sur une blockchain publique, divers mécanismes d'intervention devraient être imaginés, afin d'éviter une utilisation frauduleuse de l'infrastructure. La première étape pourrait consister en une **communication avancée**, notamment en direction des gestionnaires d'application et des utilisateurs. Un indicateur d'alerte pourrait aussi être présent sur les interfaces de chacun des services s'appuyant sur cette infrastructure. Ces avertissements permettraient aux utilisateurs de la blockchain visée de retirer leurs actifs, pour les déplacer sur d'autres blockchains. En revanche, **un arrêt de l'infrastructure ne peut pas toujours être mis en œuvre** : s'agissant d'une blockchain publique, celui-ci suppose un large accord des nœuds validateurs. Pour les crypto-actifs bloqués dans des contrats, on pourrait en revanche envisager que les autorités ordonnent, au-delà d'un certain niveau d'alerte, une résolution (rupture immédiate des contrats en cours, remboursement des fonds). Il faudrait alors que la réglementation des automates exécuteurs de clauses prévoie de tels mécanismes (*cf.* le point 3-2). Enfin, les autorités publiques pourraient opérer un **nœud d'archive** sur les blockchains publiques : ce nœud ne participerait pas à la validation, mais contribuerait à la récupération de l'information si la chaîne cessait de fonctionner à la suite d'une attaque ou d'une panne.

Schéma de régulation B : une infrastructure reposant sur des blockchains privées

Une autre manière de répondre au défi de sécurité et d'efficacité posé par les blockchains publiques serait de basculer les fonctions purement financières sur des **blockchains privées**[81].

Contrairement aux blockchains publiques, le fonctionnement des blockchains privées repose en effet sur des **acteurs de confiance**, bien identifiés et agréés par la gouvernance de l'infrastructure, ce qui présente deux avantages principaux. D'abord du point de vue de l'efficacité : disposant de moins de nœuds et de mécanismes de consensus plus simples, ces infrastructures peuvent traiter les transactions plus rapidement. Elles mettent aussi à jour plus rapidement leurs règles de fonctionnement (sécurité, algorithme de consensus, montée de version technique etc.) car le processus décisionnel est plus rapide et moins étendu que pour des blockchains publiques.

Les blockchains privées ont ensuite un **avantage en termes de sécurité** : en filtrant les membres autorisés à participer au réseau, elles limitent la présence d'utilisateurs malveillants. Le risque d'une prise de contrôle hostile est ainsi presque éliminé, là où la corruption d'une blockchain publique par une attaque des 51 % est toujours possible.

Le défaut d'une architecture reposant sur des blockchains privées est qu'elle **limite** la composabilité et donc **la capacité d'innovation**. Il faut cependant noter que la cohabitation efficace de blockchains

[81] Une blockchain privée est ici entendue au sens d'une blockchain sur laquelle l'accès n'est ouvert qu'aux utilisateurs autorisés. Chaque nouveau membre doit ainsi être coopté par les membres déjà existants, et dispose de droits d'accès différenciés à la donnée partagée. En outre, seuls certains membres du réseau peuvent avoir le rôle de validateur. Sur les blockchains publiques, certaines applications peuvent être « permissionnées », c'est-à-dire restreintes à certains utilisateurs présélectionnés ; en revanche, la validation des blocs reste du ressort des validateurs de l'ensemble du réseau.

privées et de blockchains publiques n'a rien d'impossible, dès lors qu'est résolue la question de la sécurisation des points de connexion.

Les blockchains privées pourraient être **opérées par différents types d'acteurs de confiance**. Il pourrait en premier lieu s'agir **d'acteurs privés** reconnus ou agréés par la puissance publique. Des banques ou des consortiums bancaires pourraient par exemple opérer de telles blockchains, mais on pourrait également imaginer que des jeunes pousses innovantes (fintechs) fassent de l'administration de blockchains leur cœur de métier. Des acteurs non financiers pourraient également opérer des infrastructures blockchain, comme des opérateurs télécom, des entreprises de services du numérique (ESN), ou encore des acteurs industriels[82] qui développeraient une expertise de cette technologie via des besoins métier spécifiques (logistique…).

Des blockchains privées opérées par des acteurs privés pourraient être soumises à un **cadre de surveillance**, à l'image de celui qui existe aujourd'hui dans la zone euro pour les systèmes de paiement de détail (*cf.* l'encadré 3). Le respect d'un certain nombre de règles ferait ainsi l'objet d'un suivi en continu, avec des obligations de *reporting* pour les administrateurs des blockchains, suivies de recommandations et d'avertissements publics[83]. Notons que, dans un tel schéma de surveillance, les administrateurs des blockchains doivent être situés sur le territoire national ou européen.

Encadré 3 : Le cadre PISA (*Payment instruments, schemes and arrangements*)

Fin 2021, l'Eurosystème a publié un cadre de surveillance des paiements électroniques dit « PISA », qui entrera en vigueur à la fin de l'année 2023. Le bon fonctionnement des systèmes de paiement fait en effet partie des missions confiées à l'Eurosystème.
Ce cadre instaure un ensemble de principes de surveillance, fondés sur des normes internationales, pour évaluer la sécurité et l'efficacité des instruments, des systèmes et des dispositifs de paiement électronique :

- Les instruments de paiement électronique sont entendus largement et englobent les virements, les prélèvements, les cartes de paiement, les virements en monnaie électronique et les jetons de paiement électronique (par exemple, les cryptos-actifs utilisés dans le cadre d'un système de *stablecoin*).
- Un système est un ensemble de règles formelles, normalisées et communes permettant le transfert de valeur entre utilisateurs finaux au moyen d'instruments de paiement électroniques. Il est géré par un organe de gouvernance.
- Un accord est un ensemble de fonctionnalités opérationnelles qui aident les utilisateurs finaux de plusieurs prestataires de services de paiement à utiliser des instruments de paiement électroniques. L'accord est géré par un organe de gouvernance qui, entre autres, arrête les règles ou les modalités pertinentes.

Le cadre PISA s'adresse aux organes de gouvernance des dispositifs qui ont atteint un niveau d'importance considérable pour la zone euro. Il repose sur une méthodologie d'évaluation du respect des principes de surveillance définis par l'Eurosystème. Toutes les entreprises supervisées seront donc invitées à soumettre des auto-évaluations et des documents de référence, qui formeront la base d'un dialogue continu entre elles et le superviseur.

[82] En France, des acteurs industriels fournissent d'ores et déjà l'infrastructure technique pour l'hébergement des nœuds de certains réseaux blockchains. L'opération d'une blockchain à un stade industriel suppose en effet de fonctionner sur des infrastructures physiques d'une qualité minimale, afin de pouvoir garantir en continu un certain niveau de service.
[83] La Commission européenne a proposé dans un premier temps que les acteurs de la *DeFi* respectent un cadre de surveillance de ce type sur une base volontaire (Commission européenne, juin 2022, *Decentralized finance : Information frictions and public policies*).

Une autre possibilité serait que des **établissements publics opèrent directement l'infrastructure blockchain**. Cela pourrait notamment se justifier si une importante partie de la finance devenait « tokénisée ». Ces établissements publics seraient plus logiquement européens que nationaux ; il pourrait s'agir d'une entité européenne créée spécialement à cet effet, ou encore de partenariats entre acteurs publics dans l'hypothèse d'une blockchain souveraine européenne[84] dont l'utilisation dépasserait les seules questions financières ; il pourrait enfin s'agir des banques centrales de l'Eurosystème. Dans la finance traditionnelle, c'est ainsi que l'Eurosystème est aujourd'hui l'opérateur des systèmes Target 2 (paiements interbancaires) et Target 2 Securities (règlement-livraison de titres). Un tel schéma pourrait être d'autant plus pertinent que des monnaies numériques de banque centrale (MNBC) de gros pourraient également voir le jour dans le futur : les banques centrales pourraient alors être gestionnaires de systèmes intégrés fournissant la liquidité aux acteurs financiers et conservant leurs portefeuilles numériques.

3-2. Proposer un encadrement adapté à la nature algorithmique des services

3-2-1. Les limites des solutions actuelles de certification

Tout d'abord, le **caractère public du code**[85] des automates exécuteurs de clauses est parfois considéré comme une parade efficace contre les risques de piratage (principe de sécurité par transparence). Il permet en effet à des communautés de développeurs de repérer et de signaler les programmes frauduleux ou vulnérables. Ces échanges ont toutefois lieu sur des forums spécialisés et ne parviennent pas forcément à la connaissance des utilisateurs moins avertis. En outre, le caractère public du code ne permet pas toujours de repérer à temps les défauts d'un programme informatique, comme l'a montré la faille majeure *Log4Shell* sur un logiciel pourtant *open source*. La publication du code peut même avoir pour défaut de permettre à des attaquants de découvrir des vulnérabilités. Enfin, il faut noter que la possibilité d'examiner le code informatique ne garantit pas la compréhension des mécanismes financiers à l'œuvre dans un *smart contract*.

Face à ces vulnérabilités, un système couramment utilisé par les développeurs consiste à **faire tester leurs protocoles par la communauté** des développeurs et des utilisateurs avertis, afin d'identifier des failles. Ils ont recours pour cela au système de *bounty reward* (ou *bug bounty*), qui récompense les personnes qui parviennent à révéler des défauts de conception.

Une version plus encadrée de cette pratique consiste à faire réaliser un **audit du code** des *smart contracts*[86]. Cet audit est réalisé par des acteurs spécialisés dans la sécurité informatique, par exemple des cabinets de conseil. Mais la demande de certification est très forte, ce qui peut conduire à une pénurie de personnel compétent dans le domaine[87]. En outre, l'audit de code n'est une tâche aisée : une étude récente de l'université Cornell[88] a ainsi révélé que seuls 15 à 55 % des développeurs (selon

[84] À ce sujet, voir par exemple le projet européen EBSI

[85] Il faut noter que le code de certains smart contracts n'est que partiellement public.

[86] L'OCDE a fait une proposition du même type (*Why Decentralised Finance (DeFi) Matters and the Policy Implications*, janvier 2022*)*

[87] Cela peut pousser de nouveaux acteurs, dont l'expérience n'est pas forcément éprouvée, à proposer des services d'audit.

[88] Tanusree Sharma, Zhixuan Zhou, Andrew Miller, Yang Wang (université d'Illinois), Exploring Security Practices of Smart Contract Developers, avril 2022.

le niveau d'expérience) parvenaient à identifier les failles d'un *smart contract* à l'issue d'un audit approfondi.

Une autre solution consiste à soumettre le code des automates exécuteurs de clauses à des mécanismes de **preuve formelle**. Ces méthodes analysent la sémantique des programmes, c'est-à-dire la description mathématique formelle du sens d'un programme donné par son code source. L'idée générale consiste à vérifier que le programme sous revue effectue bien les actions pour lesquelles il a été conçu, ou qu'il ne permet pas d'effectuer un certain nombre d'actions recensées comme dangereuses.

Le potentiel des méthodes formelles provient de leur **caractère automatisable**, qui permet théoriquement un passage à l'échelle quasiment infini, contrairement à l'audit humain. Toutefois, leur utilisation n'est pour l'heure guère répandue[89], notamment en raison de leur coût[90]. Outre le faible nombre de spécialistes, les méthodes formelles supposent en général que les automates exécuteurs de clauses aient été écrits dans un **langage de programmation compatible**, ce qui est loin d'être toujours le cas. Elles font également l'objet d'une critique plus fondamentale : si elles permettent de vérifier le respect par un programme d'un ensemble de spécifications, encore faut-il pouvoir vérifier la validité desdites spécifications[91].

Si elles ne constituent pas des solutions miraculeuses, **les méthodes de preuve formelle et d'audit humain présentent**, on le voit, **des qualités complémentaires** ; leur combinaison constitue donc une piste prometteuse. Par ailleurs, il faut noter que la vérification ou l'amélioration du code présentent un intérêt pour les développeurs de *smart contracts*, pour les utilisateurs, ainsi que pour les administrateurs de blockchain ; cet alignement d'intérêt est susceptible de conduire à la formation de communautés unissant leurs efforts pour la détection de vulnérabilités.

3-2-2. La certification du code informatique des applications *DeFi*

Compte tenu des nombreuses attaques enregistrées sur les automates exécuteurs de clauses, et afin de réduire les risques technologiques et de contrepartie, une piste logique de réglementation consisterait à définir le **périmètre des protocoles jugés « sûrs »** (au moins pour un état donné des connaissances techniques). Cet ensemble correspondrait aux automates exécuteurs de clauses dont le code informatique a fait l'objet d'une **certification**. Il faut immédiatement noter que le dispositif décrit ci-après ne s'appliquerait qu'aux automates exécuteurs de clauses ne posant pas de problème dans leur principe ; un *smart contract* rendant un service jugé dangereux ne devrait pas pouvoir être labellisé.

[89] Parmi les cas d'utilisation, Nomadic Labs (développeur de la blockchain Tezos) a par exemple créé Mi-Cho-Coq, un cadre de vérification formelle des *smart contracts*.

[90] Les méthodes formelles ont jusqu'ici principalement été utilisées pour le développement d'algorithmes dans des domaines mettant en jeu la sécurité des personnes, par exemple dans les transports.

[91] Ce problème a été mis en lumière par une faille de sécurité sur la plateforme d'échange Dexter (blockchain Tezos). Nomadic Labs avait annoncé le succès de sa vérification formelle, mais les spécifications testées comportaient elles-mêmes des vulnérabilités.

a. En quoi consisterait la certification du code ?

La certification d'un code informatique consiste à parcourir le code source d'un programme pour vérifier qu'il effectue bien les tâches pour lesquelles il a été conçu, et qu'il les effectue en adéquation avec un certain nombre de standards de sécurité (*cf.* point b ci-après sur la fixation des standards). Elle n'est pas forcément binaire, et peut notamment comporter plusieurs niveaux de sécurité[92], à l'image du visa de sécurité de l'ANSSI qui existe actuellement. Elle est en tout cas réalisée par des **évaluateurs spécialisés**, qui procèdent par audit humain, méthodes formelles, ou une combinaison des deux. Dans sa dimension la plus large, **elle comprend trois dimensions principales** : l'**analyse statique** permet d'identifier les erreurs formelles de programmation ou de conception ; l'**analyse dynamique** s'attache au suivi de l'exécution du programme ; enfin, l'**analyse de composition logicielle** (*software composition analysis* ou SCA) permet d'établir l'inventaire des dépendances externes du programme sous revue, c'est-à-dire à des librairies tierces ou à des composants *open source*.

Dans l'écosystème *DeFi*, la brique d'analyse de composition logicielle prend une importance particulière. Il est en effet très fréquent qu'un *smart contract* en appelle une série d'autres, pour utiliser leurs fonctionnalités. Cette architecture modulaire, où les automates exécuteurs de clauses sont « empilés » les uns sur les autres, constitue une caractéristique de l'écosystème *DeFi*, et appelle à la fixation d'une règle simple : **la certification d'un *smart contract* nécessite la certification préalable de l'ensemble des composants appelés[93]**.

Comme tout mécanisme d'autorisation, la certification possède un **cycle de vie**, ce qui conduit à énoncer **trois règles générales**. Premièrement, elle doit pouvoir être **retirée à tout moment**, par exemple lors de la découverte d'une nouvelle faille de sécurité. Deuxièmement, elle doit être accordée pour une **durée limitée**, afin de prendre en compte l'évolution des techniques de sécurité informatique. Troisièmement, si la certification correspond à un état donné des connaissances informatiques, elle correspond aussi à un **état donné du programme sous revue**. Les automates exécuteurs de clauses sont normalement immuables dans la blockchain. En pratique, toutefois, il est possible de les faire évoluer – par exemple pour corriger des vulnérabilités – sans nécessairement créer un nouveau programme : ceci peut se faire par des mécanismes d'appel (via des *proxies*), ou en utilisant des *smart contracts* paramétrables. Ceci ne constitue pas un problème spécifique à la *DeFi* : toute base de code auditée peut contenir des paramètres de configuration et tend à faire l'objet de mises à jour régulières, risquant de rendre les certifications obsolètes. Une solution possible à ce problème classique est de définir ce qui constitue un **changement significatif de code**, et d'imposer **l'obligation d'une nouvelle certification** dès lors qu'une mise à jour remplit ces critères.

Il est à noter que, si la *DeFi* devenait à l'avenir davantage régulée, les automates exécuteurs de clauses pourraient directement embarquer dans leur code un certain nombre d'obligations réglementaires[94]. Ceci constituerait une manière efficace d'assurer le respect de la réglementation à tout moment[95]. La

[92] L'idée d'une échelle de sécurité figure également dans la loi Lafon du 3 mars 2022, qui crée un « cyberscore » permettant aux internautes de connaître le niveau de sécurisation de leurs données sur les sites internet et réseaux sociaux qu'ils fréquentent.

[93] Cette condition est nécessaire mais pas suffisante : l'assemblage de *smart contracts* certifiés ne garantit pas le bon fonctionnement de l'ensemble. On se reportera par exemple au cas de Chainlink lors de l'arrêt de Luna, discuté en partie 3-2-3.

[94] Rafael Auer (2022), *Embedded Supervision: How to Build Regulation into Decentralised Finance*, CESifo Working Paper Series 9771.

[95] L'Autorité monétaire de Singapour (MAS) a ainsi proposé l'idée de « protocoles *DeFi* de qualité institutionnelle », intégrant des garanties réglementaires dans leur conception (communiqué de presse de mai 2022 : *MAS Partners the Industry to Pilot Use Cases in Digital Assets*).

certification du code pourrait alors inclure la vérification de la bonne traduction des dispositions de droit en langage informatique.

b. Qui aurait la responsabilité d'établir les standards de sécurité ?

Dans un premier schéma, les standards de sécurité seraient **fixés par les acteurs de marché eux-mêmes**. Dans ce type de configuration, les standards adoptés tendent à être proches des réalités de marché, ce qui garantit leur acceptabilité et facilite leur mise en œuvre. Cela suppose toutefois que les acteurs privés, en général concurrents, parviennent à s'accorder sur des normes communes. De leur côté, les autorités publiques peuvent encourager l'adoption de ces standards.

Dans un second schéma, les **autorités publiques fixent elles-mêmes les standards**[96]. Ceci a normalement l'avantage d'assurer que les standards choisis répondent à des objectifs d'intérêt général, et permet de trancher les désaccords entre acteurs ou segments du marché. En pratique, les standards fixés par les autorités publiques font généralement l'objet de concertations avec les acteurs de marché, afin d'assurer leur viabilité.

Il est à noter qu'un tel schéma ne donne pas nécessairement aux autorités publiques la tâche de certifier elles-mêmes le respect de ces normes : l'organisation consistant à confier la certification des produits à un ensemble de laboratoires privés, exerçant leur activité sous le contrôle d'une autorité publique de surveillance[97], est largement répandu dans le domaine de la sécurité des produits (*cf.* l'encadré 4 sur le règlement IA).

c. Quelles conséquences en cas d'absence de certification ?

Là encore, deux grandes possibilités peuvent être imaginées. Dans un premier cas, **l'absence de certification serait seulement découragée**. Afin de rassurer leurs clients face aux possibilités de vol ou de fraude, une partie des intermédiaires (PSAN) choisiraient de ne travailler qu'avec des protocoles certifiés ; gage de sérieux, la certification constituerait ainsi un argument commercial. Pour la rendre visible, la certification pourrait être référencée sur chaque protocole ou sur chaque blockchain ; des techniques plus élaborées pourraient aussi permettre d'intégrer les informations relatives à la certification dans le *smart contract* lui-même. De leur côté, les autorités publiques mettraient en avant dans leur communication, notamment auprès du grand public, l'utilité de la certification comme mécanisme de prévention des risques pour la clientèle. Si les pratiques des acteurs les plus vertueux sont progressivement adoptées par l'ensemble du marché, la certification peut devenir *de facto* quasiment obligatoire. Dans ce schéma de régulation incitatif, il est toutefois possible que les pratiques vertueuses ne se diffusent pas, pour des raisons de coût.

Une seconde possibilité consisterait à **interdire d'interagir avec des automates exécuteurs de clauses non certifiés**, soit que la certification n'ait pas été demandée, soit qu'elle ne puisse pas être obtenue. Cette interdiction vaudrait pour les individus comme pour les entreprises, qu'il s'agisse de plates-formes d'échange, de PSAN, d'investisseurs institutionnels, de banques ou de sociétés non financières. Pour les entités régulées, elle ferait l'objet d'une surveillance par les superviseurs financiers. Toute interaction avérée serait sanctionnée (amendes, interdictions futures…).

[96] Ces standards pourraient d'ailleurs ne pas se limiter aux aspects techniques, en incluant par exemple des considérations de bonne gouvernance.

[97] L'Agence nationale de la sécurité des systèmes d'information (ANSSI) agrée déjà des professionnels de la sécurité informatique sur le même principe.

Il faut remarquer que dans ce schéma d'interdiction, la loi ferait porter **certaines obligations à l'objet « *smart contract* », en tant que produit** – sur le modèle du règlement IA (*cf.* l'encadré 4) –, quand bien même la responsabilité pénale ou civile du développeur (individu, unité légale…) ne pourrait être engagée, soit du fait de l'impossibilité d'identifier ce développeur, soit du fait de l'impossibilité de lui imposer des sanctions (question de territorialité).

Encadré 4 : Le projet de règlement européen sur l'intelligence artificielle (IA)

En avril 2021, la Commission européenne a proposé un projet de règlement visant à assurer que les systèmes d'IA utilisés dans l'UE soient sûrs, transparents, éthiques, impartiaux et demeurent sous contrôle humain. Dans la lignée du RGPD, le règlement se concentre sur les effets potentiels sur les personnes physiques et les atteintes à leurs droits fondamentaux.
Le projet de texte est en partie inspiré des réglementations européennes portant sur la sécurité des produits (jouets, véhicules automobiles etc.). Ainsi, si certaines obligations créées par le texte portent sur des acteurs (fournisseurs, utilisateurs, importateurs etc.), d'autres portent directement sur les produits développés ou commercialisés (ici les systèmes d'IA). Cette organisation peut constituer une source d'inspiration pour la *DeFi*, dont une partie des produits n'est pas fournie par un individu ou une entité juridique identifiée.
En outre, pour certifier la conformité des systèmes d'IA aux exigences du règlement, le projet de texte prévoit d'avoir recours, dans certains secteurs, à des évaluateurs tiers, agréés par les autorités publiques de surveillance sectorielle. Il s'agit là encore d'une organisation classique en matière de sécurité des produits, qui permet de démultiplier les capacités de contrôle, tout en créant une filière économique de l'évaluation. Ce schéma de contrôle est peu usité dans les activités financières, mais existe déjà dans le champ de la sécurité informatique (certification de sécurité de l'ANSSI), et pourrait inspirer l'architecture de supervision de la *DeFi*.

d. Qui doit payer la certification ?

La certification du code informatique par des organismes spécialisés représente un certain coût, ce qui pose inévitablement la question de savoir quels acteurs doivent l'assumer. Deux modèles principaux peuvent ici être imaginés, présentant chacun des avantages et des inconvénients. Tout d'abord, les frais liés à la certification d'un *smart contract* pourraient être **assumés par le développeur ou le gestionnaire** du programme, c'est-à-dire le fournisseur du service informatique. Il y aurait une incitation économique claire à payer ce coût : permettre au produit d'être plus largement utilisé, ce qui peut s'avérer directement ou indirectement rémunérateur. Toutefois, lorsque les développeurs sont des personnes physiques, le coût d'une certification pourra leur sembler disproportionné[98]. Notons que les fournisseurs de *smart contracts* auront souvent, par la suite, la possibilité de refacturer tout ou partie du coût de certification aux utilisateurs, sous la forme d'un prélèvement à chaque utilisation du service.

Une autre possibilité consisterait à **faire payer directement les frais de certification par les utilisateurs** des automates exécuteurs de clauses, c'est-à-dire pour l'essentiel les plates-formes jouant le rôle d'intermédiaire (*cf.* le point 3-3-2). Cette solution correspondrait elle aussi à une logique économique : le service serait payé par les agents qui en ont besoin. En outre, cette solution serait plus parcimonieuse, puisqu'elle conduirait à ne certifier que les automates exécuteurs de clauses dont l'utilisation est intéressante pour au moins un acteur. Enfin, les intermédiaires sont des sociétés

[98] Le problème paraît moins significatif lorsque, comme c'est souvent le cas, le développement des *smart contracts* est plutôt piloté par une fondation ou une entité commerciale, comme par exemple la société Aave Limited pour les automates du protocole Aave.

commerciales, donc des acteurs ayant la capacité de payer des frais de certification. En revanche, un tel système présente **deux défauts** : en premier lieu, il peut conduire à une préférence pour les *smart contracts* « anciens », déjà certifiés, au détriment des nouveaux, ce qui risque de décourager l'innovation, et éventuellement d'utiliser des programmes moins sûrs (sous l'hypothèse que les « nouveaux » *smart contracts* sont plus sûrs que les anciens, même certifiés). En second lieu, ce système tend à engendrer des phénomènes de passagers clandestins, faisant peser soit un risque de blocage de la certification (si chaque intermédiaire attend que les autres paient la certification pour utiliser gratuitement les produits), soit un risque d'injustice dans la répartition des coûts entre les intermédiaires[99].

Une autre manière de faire contribuer les utilisateurs en évitant les défauts évoqués ci-dessus consisterait à **financer la certification par une taxe sur les transactions** réalisées par les automates exécuteurs de clauses (c'est-à-dire un prélèvement en crypto-actifs sur chaque ordre passé). Cette taxe viendrait alimenter un fonds commun à l'écosystème, ce qui permettrait aux développeurs de nouveaux projets de ne pas être bloqués par le montant des frais de certification (les créateurs prendraient toujours à leur charge une partie des coûts, afin de décourager les abus).

3-2-3. La fourniture de données dans l'écosystème *DeFi*

En premier lieu, il apparaît nécessaire d'**évaluer les risques du modèle des oracles décentralisés**. Sur le plan du principe, notons tout d'abord que la donnée la plus juste n'est pas toujours la moyenne pondérée des informations fournies ; la fourniture de données suppose une expertise. Surtout, l'oracle décentralisé présente un risque de collusion de la part de ses fournisseurs d'information, dès lors qu'une donnée n'est fournie que par un nombre limité de nœuds de l'oracle. Il en va de même lorsque le poids accordé à un fournisseur d'information dépend de sa « fiabilité » passée : un acteur disposant d'un fort poids du fait des n premières informations fournies peut avoir intérêt à manipuler l'information la (n+1)ème fois. De plus, du fait de leur caractère très automatisé, les oracles décentralisés présentent d'importants risques opérationnels. Ainsi Chainlink, qui fournissait le prix du LUNA, a cessé de fonctionner lorsque l'écosystème Terra a été suspendu[100], renvoyant une cote de 0,10 USD (inscrite en dur), alors même que la cote réelle plongeait à 0,01 puis à 0. Des utilisateurs ayant remarqué l'écart entre le prix réel et le prix envoyé par Chainlink dans certaines plateformes, comme Blizz Finance, en ont profité pour acheter de vastes montants de LUNA à 0,01 USD et les utiliser comme collatéral, valorisé à 0,10 USD, dans l'emprunt d'autres crypto-actifs.

Une solution face à ce problème pourrait reposer sur **un système de certification** des oracles décentralisés, proche de celui décrit dans la section précédente, mais qui porterait un **accent particulier sur le mécanisme de consensus** amenant au résultat final (pondération des différentes sources par exemple). **Introduire un coupe-circuit** sur la fourniture de données constitue également un élément intéressant, mais qui devrait alors s'accompagner d'un mécanisme d'arrêt des applications utilisant l'oracle.

Un autre moyen d'injecter des données dans l'écosystème *DeFi* est de recourir à des **entités centralisées**. Ceux-ci ne sont toutefois pas immunisés contre les risques opérationnels, ni contre les

[99] Ce problème n'est pas entièrement nouveau : le règlement MiCA prévoit par exemple qu'une plate-forme souhaitant commercialiser un crypto-actif émis hors de l'UE doit en rédiger elle-même le livre blanc ; les autres plateformes peuvent alors utiliser ce livre blanc pour commercialiser à leur tour le crypto-actif ; les plateformes peuvent convenir d'arrangements contractuels entre elles pour faire face à ce problème de passager clandestin.
[100] En raison d'un coupe-circuit inscrit dans son code, en cas de fortes turbulences sur les prix.

risques de manipulation de marché. Dans la finance traditionnelle, le mode de régulation consiste pour l'essentiel en la « **discipline de marché** » : une erreur ou une défaillance sont sanctionnées par une moindre confiance des clients, ce qui conduit à des pertes financières voire à la faillite. Ce modèle repose toutefois sur l'existence de fournisseurs de données bien implantés, disposant d'une expertise et de moyens importants dédiés au contrôle qualité. En outre, le défaut de ce type de régulation est qu'il conduit à des sanctions a posteriori, ce qui n'empêche pas forcément la défaillance de se produire, et éventuellement d'entraîner des conséquences graves. Il s'agit d'un point particulièrement crucial pour l'écosystème *DeFi* : la fourniture d'informations déclenche automatiquement l'exécution de contrats, dont le résultat est final sur la blockchain.

On pourrait donc considérer que le modèle de régulation de la finance traditionnelle n'est pas adapté aux risques spécifiques de la *DeFi*. Ceci plaiderait pour l'instauration d'un **cadre de surveillance des fournisseurs de données (centralisés ou décentralisés)** par les autorités publiques[101]. Ce cadre pourrait être progressif, et réglementer la production de données financières **en fonction de leurs seuils d'utilisation** par les automates exécuteurs de clauses, sur le modèle du règlement européen sur les indices de référence[102] (règlement « Benchmark ») de 2016, qui avait constitué une réponse aux manipulations avérées d'indices de marché comme le Libor. Aux termes de ce règlement, les entités responsables de la fourniture d'indices financiers de référence doivent être agréées ou enregistrées par les autorités publiques de surveillance des marchés, selon le niveau de criticité des indices fournis (évalués en fonction de la valeur des contrats qui s'y réfèrent), et sont surveillées par celles-ci. Le règlement instaure des règles concernant les dispositifs de gouvernance, les dispositifs de contrôle interne ou encore la prévention des conflits d'intérêt, qui pourraient être étendues au marché de la fourniture de données dans l'écosystème *DeFi*.

3-3. Règlementer la fourniture et l'accès aux services

3-3-1. La création de statuts pour certains fournisseurs de services

Le mécanisme de certification ou d'interdiction des automates exécuteurs de clauses peut comporter des limites. En effet, **pour certains services sensibles** – tant au plan des risques pesant sur la clientèle que des risques systémiques – **il peut être nécessaire d'imposer des contraintes** ou d'exiger des mesures correctrices *ex-post*, **qui ne peuvent être anticipées lors de la conception des algorithmes**. Dans ce cas, une piste alternative ou complémentaire à la certification des *smart contracts* consiste à **identifier les acteurs responsables** de la fourniture de ces services *DeFi* et **en capacité d'exercer sur ces services le contrôle minimal** requis pour leur correction ou leur arrêt[103].

Cette **« recentralisation » partielle des services considérés comme sensibles** pourrait s'accomplir selon différentes modalités. Il pourrait d'abord être envisagé **d'imposer aux acteurs exerçant un contrôle effectif** sur le service sensible, tels les détenteurs significatifs des jetons de gouvernance

[101] La Commission européenne propose ainsi de créer un cadre juridique spécifique pour le fonctionnement des oracles, afin d'améliorer leur efficacité et la confiance des utilisateurs (*Decentralized Finance: information frictions and public policies*, juin 2022).

[102] Règlement européen 2016/1011 concernant les indices utilisés comme indices de référence dans le cadre d'instruments et de contrats financiers ou pour mesurer la performance de fonds d'investissement

[103] Dans certains cas, il pourrait s'agir d'un fondateur qui ne détient pas de jetons de gouvernance en quantité significative mais dispose d'un pouvoir d'influence sur la communauté.

d'une application *DeFi* ou les détenteurs des clés d'administrateur d'un protocole, **de se constituer en société**, soumise au contrôle, ou de faciliter la reconnaissance par le juge de « sociétés créées de fait »[104], à la demande des autorités. Une alternative peut consister à **assujettir directement les acteurs exerçant un contrôle effectif[105] sur le service[106].**

L'exigence de créer une entité responsable du service *DeFi* pourrait aussi être l'occasion de **conférer aux DAO un statut juridique** permettant, entre autres, leur assujettissement à contrôle. Sur ce sujet, on renverra aux travaux en cours du HCJP (*cf.* l'encadré 5).

Ainsi, sans remettre en cause la décentralisation du fonctionnement de la *DeFi*, les participants à sa gouvernance décentralisée seraient soumis à une réglementation inspirée de la finance traditionnelle.

Encadré 5 : Les travaux du HCJP sur la *DeFi*

Le Haut comité juridique de la Place financière de Paris (HCJP) est composé d'avocats, d'universitaires et de personnalités qualifiées ; il inclut notamment des représentants de l'Autorité des marchés financiers, de la Banque de France et de l'ACPR. Il réalise des analyses juridiques qu'il rend publiques. En 2022, il a ainsi été saisi d'une réflexion sur les questions que pose la *DeFi* en droit français. Cette réflexion portera notamment sur le statut juridique des DAO. Le HCJP devrait rendre ses conclusions au début du troisième trimestre 2023. Son rapport, tout comme le présent document de réflexion, permettra d'alimenter les réflexions en cours sur la *DeFi* au niveau européen.

3-3-2. L'encadrement de l'accès à la *DeFi* pour protéger la clientèle

Il est techniquement difficile pour un utilisateur non programmeur d'interagir directement avec un *smart contract*. De ce fait, l'essentiel des interactions du grand public avec les protocoles *DeFi* se font actuellement[107] – et continueront probablement à se faire dans le futur – via des **intermédiaires**. Ces intermédiaires sont aujourd'hui de **deux grands types : des fournisseurs (centralisés) de services sur crypto-actifs, et des interfaces web (*front-end*) de protocoles décentralisés**. En France, les fournisseurs centralisés de services sont notamment les acteurs actuellement enregistrés sous le

[104] En droit français, la « société créée de fait » désigne la situation dans laquelle deux personnes ou plus se sont comportées en fait comme des associés, sans avoir exprimé la volonté de former une société (cette catégorie ne doit pas être confondue avec la « société de fait », qui a été immatriculée mais dont la création a ensuite été annulée par une décision de justice). L'article 1873 du Code civil précise que son régime juridique est celui des sociétés en participation. La « société créée de fait » n'a ainsi pas la personnalité morale, mais cette qualification – établie par le juge – donne des droits et des devoirs aux individus considérés comme des associés de la société, qui sont notamment tenus responsables personnellement et solidairement vis-à-vis des tiers.

[105] Un type de raisonnement similaire a été tenu par le GAFI en 2021 : une application *DeFi* n'est pas en tant que telle un fournisseur de services sur actifs numériques (VASP en anglais), car les normes du GAFI ne s'appliquent pas aux logiciels ou aux technologies sous-jacentes. Cependant, les créateurs, les propriétaires, les opérateurs ou d'autres personnes détenant le contrôle ou une influence suffisante dans les dispositifs *DeFi* peuvent constituer des VASP au sens du GAFI, même si ces dispositifs semblent décentralisés. C'est le cas même si d'autres parties jouent un rôle dans le service, ou si des éléments du processus sont automatisés.

[106] Plusieurs institutions ont fait des propositions de ce type : l'OCDE en janvier 2022 (*Why Decentralised Finance (DeFi) Matters and the Policy Implications),* la BCE en avril 2022 (*Decentralised finance – a new unregulated non-bank system?)* et le FMI en septembre 2022 (*Regulating the Crypto Ecosystem - The Case of Unbacked Crypto-Assets*).

[107] Il a ainsi pu être estimé que seules 2 % des adresses sur Ethereum interagissaient directement avec des protocoles *DeFi*.

statut de **prestataire de services sur actifs numériques (PSAN)**, en vertu du dispositif issu de la loi PACTE de 2019. En revanche, les interfaces web, qui permettent d'interagir avec des protocoles décentralisés sans communiquer via du code informatique, ne font actuellement l'objet d'aucune réglementation particulière[108].

Un encadrement plus strict de l'accès aux services *DeFi* en vue de réduire les nombreux risques qu'ils présentent, en particulier pour les investisseurs individuels, passerait donc logiquement par un **cadre de supervision renforcé des intermédiaires fournisseurs d'accès[109]**. Pour bien fonctionner, un tel cadre devrait avoir deux grands volets. Tout d'abord, les intermédiaires doivent éviter aux investisseurs (notamment individuels) d'interagir avec des protocoles frauduleux ou dangereux (**devoir de vigilance**) ou de prendre des risques excessifs (**devoir de conseil**). Ensuite, la prise de risque des intermédiaires doit être elle-même encadrée par le superviseur, afin de limiter les faillites et leurs effets de contagion qui ont notamment pu être observés en 2022 (voir notamment l'encadré 6 sur les risques liés à la « *DeFi* intermédiée »). À cet égard il conviendrait de mieux identifier les **liens et les interdépendances** entre les différents fournisseurs (centralisés) de services sur crypto-actifs, en particulier lorsque ceux-ci sont contrôlés par les mêmes personnes ou groupes de personnes (voir l'encadré 6 sur le sujet des « conglomérats crypto »). Ceci permettrait de prévenir les conflits d'intérêt entre ces acteurs, mais aussi de réduire le risque systémique[110].

Encadré 6 : Les risques spécifiques liés à la *DeFi* intermédiée (*CeDeFi*) et aux « conglomérats crypto »

Les faillites récentes d'intermédiaires fournissant des services de prêt et d'échange en crypto-actifs (Celsius Network, FTX et Alameda Research) ont mis en lumière des fragilités résultant d'un excès de prise de risques (notamment via un levier excessif), d'un excès de transformation financière, ou tout simplement de fraude. Dans le cas de FTX, les prises de risque excessives sont en particulier liées aux interdépendances frauduleuses de la plateforme avec son entreprise sœur Alameda Research : les crypto-actifs déposés par des tiers auprès de FTX étaient ensuite prêtés à Alameda Research afin que celle-ci puisse rémunérer ses propres investisseurs et ses dirigeants.

Pour proposer des rémunérations élevées afin d'attirer les dépôts, des acteurs comme FTX ne se sont pas contentés pas d'assurer la conservation des crypto-actifs, mais se sont engagés dans des stratégies d'investissement risquées. Alors que ces acteurs exercent finalement des activités proches de la finance traditionnelle, ils ne sont pour l'heure pas assujettis à des exigences prudentielles, ni de contrôle interne ou de gestion des risques. En cas de difficulté, ces acteurs peuvent donc soudainement interrompre leurs services et geler les fonds des clients.

Plus largement, au-delà des questions de fraude ou de gouvernance, le modèle des « conglomérats crypto » semble présenter des fragilités financières : l'intégration verticale de diverses fonctions peut

[108] Dans le cas d'interfaces web décentralisées, il serait nécessaire d'appliquer le raisonnement décrit dans le point 3-3-1 aux personnes responsables de fait de cette interface.

[109] Entre les pistes évoquées au 3-3-1 (encadrement des fournisseurs de services sensibles) et au 3-3-2 (encadrement des intermédiaires fournisseurs d'accès), un équilibre est à rechercher, qui tienne compte des rapports de force et des capacités effectives de ces différents acteurs. En l'état actuel, il apparaît prioritaire de mettre l'accent sur la réglementation des fournisseurs d'accès. La mise en œuvre peut toutefois poser des problèmes de proportionnalité pour les intermédiaires de taille modeste.

[110] À ce titre, la faillite de FTX a conduit le Conseil de stabilité financière (*Financial Stability Board* en anglais) à programmer des travaux de recherches en 2023 sur les crypto-conglomérats (désignés sous le vocable : « *multifunction crypto-asset intermediaries* »).

en particulier faciliter l'accumulation (peu transparente) d'effets de levier et de déséquilibres de liquidité, générant un risque systémique.

Le **règlement européen MiCA** devrait renforcer le dispositif de supervision des intermédiaires (*cf.* l'encadré 7), désormais désignés sous le vocable **« prestataires de services sur crypto-actifs » (PSCA)**[111]. Toutefois, le règlement excluant de son champ les services entièrement décentralisés, il n'est pour l'heure pas certain qu'il s'applique à des prestataires de services qui fourniraient exclusivement des services sur des crypto-actifs issus de la *DeFi*. **Il conviendrait donc, en premier lieu, d'étendre explicitement aux intermédiaires de la *DeFi* la réglementation de MiCA relative aux PSCA[112]**.

A minima, la règlementation pourrait exiger de la part de chaque intermédiaire la publication d'un livre blanc exposant les caractéristiques de tous les crypto-actifs sur lesquels un service est fourni[113], ainsi que la mise en place d'un dispositif de KYC. Dans tous les cas, pour ne pas créer d'inégalité de traitement, **cette extension devrait s'appliquer à tous les acteurs** qui facilitent l'accès des utilisateurs à des services *DeFi* : tous ceux-ci doivent être encadrés par un régime commun, dépendant uniquement de la nature des services fournis (et éventuellement de leur volume), et non pas du dispositif technique utilisé pour la fourniture. Cela signifierait notamment que les **interfaces web seraient elles aussi soumises à l'obligation de réaliser les procédures standards d'enrôlement des clients (KYC)** avant de fournir un accès aux services décentralisés. Plus généralement, tous les fournisseurs d'accès à la *DeFi* obéiraient à des règles de bonne conduite – interdisant par exemple de manipuler les fonds en crypto-actifs des clients à leur insu –, et seraient soumis à des exigences prudentielles, afin de limiter les risques de faillite.

En second lieu, s'il n'est pas possible – et peut-être pas souhaitable – de garantir l'absence de pertes financières pour les utilisateurs de services *DeFi*, la réglementation devrait toutefois avoir pour objectif de **limiter la prise de risque des utilisateurs**, en particulier les moins avertis. De ce point de vue, en plus des exigences prévues par MiCA, **il paraît indispensable que l'accès aux produits financiers dépende des compétences financières des clients et de leur appétence au risque**. En outre, la compétence financière ne doit pas être évaluée subjectivement par les utilisateurs eux-mêmes, mais objectivement par le biais de questionnaires, sur le modèle de ceux visant à établir le profil des investisseurs, prévus par la directive MIF2[114]. Ainsi, les intermédiaires devraient réserver la possibilité de souscrire des produits complexes – comme par exemple des emprunts à fort effet de levier via des contrats sur des *perpetual futures* –, à des utilisateurs déjà très aguerris, voire à des professionnels. Enfin, même pour ces derniers, la réglementation devrait fixer un effet de levier maximum, à l'image des règles édictées en 2018 par l'Autorité européenne des marchés financiers (AEMF), qui prévoient un levier maximum de x30 dans l'échange de CFD.

[111] *Crypto-asset service provider* (CASP) en anglais.

[112] L'OCDE a formulé une proposition proche (*Why Decentralised Finance (DeFi) Matters and the Policy Implications,* janvier 2022*).*

[113] Les exigences du livre blanc tel que prévu par MiCA pourraient être adaptées pour prendre en considération les caractéristiques de la *DeFi*.

[114] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers.

Encadré 7 : Les obligations des prestataires de service sur crypto-actifs dans le règlement MiCA

Le règlement MiCA prévoit que la fourniture de services sur crypto-actifs soit régie par des exigences permettant de rendre l'accès à ces services plus sûrs et plus transparent pour les utilisateurs. Les services concernés sont les suivants :

- la conservation et l'administration de crypto-actifs pour compte de tiers ;
- la gestion de plateformes de négociation ;
- l'échange de crypto-actifs contre des monnaies ayant cours légal ou d'autres crypto-actifs ;
- l'exécution d'ordres sur crypto-actifs pour le compte de tiers ;
- le placement de crypto-actifs ;
- la fourniture de services de transfert sur crypto-actifs pour le compte de tiers ;
- la réception et transmission d'ordres sur crypto-actifs ;
- la fourniture de conseils sur les cryptos-actifs ;
- la gestion d'un portefeuille de cryptos-actifs.

L'agrément de **prestataire de services sur crypto-actifs (PSCA)** sera obligatoire (alors qu'il est optionnel en droit français, dans le régime issu de la loi Pacte) pour fournir ces services en France (et sur le territoire de UE). Ces prestataires obéiront à des règles de bonne conduite, et devront en particulier agir de manière honnête, loyale, professionnelle et dans l'intérêt de leurs clients. De plus, les informations fournies aux clients devront être claires et non trompeuses ; elles porteront notamment sur les risques associés aux transactions en crypto-actifs, ainsi que sur les coûts associés aux différents services fournis.

Enfin, outre des exigences spécifiques à certaines activités, l'agrément des PSCA sera conditionné au respect d'un cadre général, prévoyant notamment :

- des exigences prudentielles ;
- des exigences de gouvernance (honorabilité et compétence des dirigeants et actionnaires) ;
- des règles relatives à la conservation des crypto-actifs et des fonds des clients ;
- des règles relatives au traitement des réclamations des clients ;
- des règles en matière de conflits d'intérêts ;
- des règles couvrant l'externalisation de services ;
- des règles prévoyant une liquidation ordonnée ;
- des règles relatives à la publication d'informations sur l'impact environnemental des crypto-actifs ;
- des règles relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Glossaire

API (*application programming interface* ou interface de programmation d'application) : interface logicielle permettant de « connecter » un logiciel ou un service à un autre logiciel ou service, afin d'échanger des données et des fonctionnalités.

Application : programme ou ensemble logiciel directement utilisé pour réaliser une tâche.

Blockchain ou *distributed ledger technology (DLT)* : s'entend dans la réglementation financière française comme un dispositif d'enregistrement électronique partagé. Il s'agit d'un registre électronique qui conserve les données des transactions et qui est partagé et synchronisé entre un ensemble de nœuds du réseau d'utilisateurs, fonctionnant au moyen d'un mécanisme de consensus. Les conditions d'accès au réseau et d'utilisation du registre déterminent si cette blockchain est publique, c'est-à-dire ouverte à tous, ou privée, c'est-à-dire réservée à certains utilisateurs.

> Mécanisme de consensus : ensemble des règles et procédures par lesquelles un accord est conclu entre les nœuds du réseau blockchain pour valider une transaction.
>
> Nœud du réseau : machine faisant partie d'un réseau pair à pair (voir ce terme), et qui contient une réplique intégrale ou partielle des enregistrements de toutes les transactions effectuées sur un registre distribué.
>
> Protocoles de validation des blocs : la validation de nouveaux blocs repose sur un algorithme de consensus (*cf*. ci-dessus). La méthode historique pour aboutir à ce type de consensus est la « preuve de travail » (*proof of work*). Cette méthode utilise un problème mathématique dont la solution permet de vérifier que le « mineur » a bien réalisé un travail ; la résolution de la preuve nécessite une puissance de calcul informatique élevée, nécessitant un matériel perfectionné (et générant une importante consommation d'électricité). Au contraire, la « preuve d'enjeu » ou « preuve de participation » (*proof of stake*) demande à l'utilisateur de prouver la possession d'une certaine quantité de crypto-actif pour prétendre valider des blocs supplémentaires

Crypto-actif : une représentation numérique d'une valeur ou d'un droit qui peut être transférée et stockée électroniquement au moyen d'une blockchain. Certains crypto-actifs sont désignés par le terme « jeton » (*token*).

> *Stablecoin* : crypto-actif ayant pour objectif de maintenir une valeur stable par référence à une monnaie officielle (ou un panier de ces monnaies), à d'autres droits ou actifs du monde réel, ou encore par référence à d'autres crypto-actifs. Les *stablecoins* peuvent être émis et gérés par des entités centralisées – c'est le cas des plus importants d'entre eux actuellement. Ils peuvent aussi être émis par des applications *DeFi* ; leurs règles d'émission sont alors inscrites dans des *smart contracts* et leur gestion assurée par ces automates. Deux modèles de *stablecoins* décentralisés existent : des *stablecoins* collatéralisés, émis en contrepartie des dépôts (comme pour les *stablecoins* centralisés) ; des *stablecoins* « algorithmiques », reposant sur l'adaptation dynamique de l'offre de jetons.
>
> *Depeg* : perte de parité d'un « stablecoin » avec l'actif dont il a pour objectif de répliquer la valeur (monnaie officielle, crypto-actif etc.).

Clé : paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature). Une clé de chiffrement peut être symétrique (la même clé sert à chiffrer et à déchiffrer) ou asymétrique : c'est ce second cas qui est

utilisé dans les blockchains. On recourt alors à deux clés différentes : la clé publique est utilisée pour le chiffrement, tandis que la clé privée, qui permet le déchiffrement, est gardée secrète.

Cryptographie : discipline s'attachant à protéger des messages, en assurant leur confidentialité, leur authenticité et leur intégrité, en s'aidant souvent de *clés*. Elle vise à rendre les informations inintelligibles à d'autres personnes que leur destinataire.

KYC (*Know your customer*) ou connaissance du client : nom donné au processus permettant de vérifier l'identité des clients d'une entreprise. Le terme est également utilisé pour faire référence à la réglementation bancaire qui régit ces activités. Les processus *KYC* sont utilisés pour s'assurer de l'identité et de la probité des clients, et ont notamment pour but de prévenir l'usurpation d'identité, la fraude fiscale, la corruption, le blanchiment d'argent et le financement du terrorisme.

Oracle : entité transportant des informations du monde physique vers des *smart contracts*. Il fait le lien entre le monde physique et une blockchain, et permet aux *smart contracts* de ne pas être limités aux informations internes à la blockchain.

Organisation autonome décentralisée (DAO) : composante usuelle (mais pas systématique) des protocoles *DeFi*, visant à en organiser la gouvernance ; elle est définie habituellement par la communauté des détenteurs de jetons de gouvernance, les *smart contracts* qui régissent ses règles de fonctionnement et les actifs qu'elle contrôle (*treasury* du protocole).

Pont ou *bridge* : protocoles connectant deux blockchains, leur permettant d'interagir entre elles. Par défaut, la majorité des blockchains existent dans des environnements isolés, possédant leurs propres règles, mécanismes de gouvernance, actifs natifs et données, qui sont incompatibles avec les autres blockchains. Ces ponts peuvent être centralisés (opérés par un tiers, à qui les utilisateurs doivent alors accorder leur confiance) ou décentralisés, c'est-à-dire reposant sur un *smart contract*.

Réseau pair à pair : modèle d'échange où chaque entité du réseau est à la fois client et serveur, contrairement au modèle client-serveur. Les termes « pair », « nœud » et « utilisateur » sont généralement utilisés pour désigner les entités composant un tel système. Un système pair à pair peut être partiellement centralisé (une partie de l'échange passe par un serveur central intermédiaire) ou totalement décentralisé (les connexions se font entre participants sans infrastructure particulière).

Rollup : solution de *layer 2* la plus répandue aujourd'hui, consistant à exécuter des transactions hors chaîne, à « enrouler » ces transactions en une seule opération (d'où son nom), et à compresser l'information, en envoyant uniquement les données strictement nécessaires à l'inscription définitive des transactions sur la blockchain. Deux grands modèles de *rollups* existent aujourd'hui, selon la manière d'assurer la validité des transactions reportées sur la blockchain : les *optimistic rollups* considèrent les transactions valides jusqu'à preuve du contraire, et reposent ainsi sur un délai de latence de 7 jours, permettant aux nœuds du réseau de détecter d'éventuelles transactions frauduleuses ; les *zero-knowledge rollups*, quant à eux, déposent sur la blockchain une preuve cryptographique de la validité des transactions, appelée « preuve à divulgation nulle de connaissance » (*zero-knowledge proof*).

Smart contract (automate exécuteur de clause) : protocole informatique qui facilite, vérifie et exécute des transactions. Ces programmes informatiques ne sont pas « intelligents », dans le sens où ils ne modifient pas leur comportement au fil du temps, mais se bornent au contraire à exécuter un code lorsque sont remplies des conditions prédéfinies. Les *smart contracts* ne constituent pas toujours non plus des contrats, au sens juridique du terme.

Solutions de *Layer 1* : solutions de passage à l'échelle des blockchains, consistant à augmenter la puissance de validation (au détriment de la sécurité du réseau et/ou de sa décentralisation), ou encore

à fragmenter une blockchain en plusieurs blockchains plus petites et plus flexibles, appelées fragments (*shards*). Avec ce partitionnement (*sharding*), les nœuds de validation ne stockent plus alors qu'une partie de l'information, même si celle-ci peut toujours être partagée ; leur travail s'en trouve donc accéléré.

Solutions de *Layer 2* (surcouches) : solution de passage à l'échelle des blockchains (alternatives aux solutions dites de *layer 1*), dont le principe est de traiter une partie des transactions hors chaîne, en n'enregistrant que le minimum d'informations dans la chaîne principale (considérée comme le *layer 1*). Ces solutions comprennent notamment les *rollups* (voir ce terme).

Wallet (portefeuille) : interface contenant une clé publique pour recevoir des crypto-actifs, et une clé privée pour y accéder. Les crypto-actifs ne sont pas stockés sur le *wallet* (ils demeurent toujours sur la blockchain) ; contrairement à ce que son nom laisse entendre, le *wallet* constitue donc davantage un porte-clés qu'un portefeuille. Le *wallet* peut être hébergé (*custodial*), c'est-à-dire qu'un tiers détient la clé privée et donc *in fine* le contrôle sur les crypto-actifs. Avec un *wallet* non hébergé (*non-custodial*), au contraire, l'utilisateur exerce directement le contrôle sur ses fonds. Enfin, certains portefeuilles sont logiciels et connectés à internet (*hot wallets*), ce qui les rend plus faciles d'utilisation, tandis que d'autres sont des portefeuilles matériels, c'est-à-dire des dispositifs physiques hors ligne (*cold wallets*), ce qui est de nature à réduire les possibilités d'attaque.

Bibliographie sommaire

Rafael Auer, *Embedded Supervision: How to Build Regulation into Decentralised Finance*, CESifo Working Paper Series 9771, 2022.

Autorité monétaire de Singapour (MAS), *MAS partners the Industry to Pilot Use Cases in Digital Assets*, mai 2022.

Banque centrale européenne (BCE), *Decentralised finance – a new unregulated non-bank system?*, Macroprudential Bulletin, avril 2022.

Banque de France, Rapport d'expérimentation, Solution de sécurisation post-quantique des échanges de données, Le Lab, octobre 2022.

Banque des règlements internationaux (BRI/BIS) : *DeFi risks and the decentralisation illusion*, BIS Quarterly Review, décembre 2021.

Jean Barthélémy, Paul Gardin et Benoît Nguyen, *Stablecoins and the Financing of the Real Economy*, Working papers de la Banque de France, février 2023.

Commission Européenne, Proposition de règlement européen sur les marchés de crypto-actifs (MiCA), 2020.

Commission européenne, *Decentralized finance : Information frictions and public policies*, juin 2022.

Conseil de stabilité financière, *The Financial Stability Risks of Decentralised Finance*, février 2023.

Ethereum.org, Introduction à la gouvernance d'Ethereum, consulté en janvier 2023.

Fonds monétaire international (FMI), *Regulating the Crypto Ecosystem - The Case of Unbacked Crypto-Assets*, septembre 2022.

Groupe d'action financière (GAFI), *Updated Guidance for a risk-based approach - Virtual assets and virtual asset service providers,* octobre 2021.

GAFI, Countering Ransomware Financing, mars 2023.

Organisation de coopération et de développement économiques (OCDE), *Regulatory Approaches to the Tokenisation of Assets*, OECD Blockchain Policy Series, janvier 2021.

OCDE, *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, janvier 2022.

OCDE, *Lessons from the crypto winter: DeFi versus CeFi*, OECD Business and Finance Policy Papers, décembre 2022.

Tanusree Sharma, Zhixuan Zhou, Andrew Miller, Yang Wang (université d'Illinois), *Exploring Security Practices of Smart Contract Developers*, avril 2022.

Questionnaire de consultation

Les réponses sont à envoyer à l'adresse fintech-innovation@acpr.banque-france.fr **avant le 19 mai 2023.**

Partie 1 du document – La *DeFi* : définition, cas d'usage et structure schématique

Q1 : Avez-vous des commentaires sur la définition de la *DeFi* retenue dans le document ? Le document rend-il correctement compte du niveau effectif de décentralisation des services ?

Q2 : À vos yeux, quels cas d'usage de la *DeFi* sont appelés à se développer à l'avenir ? Peuvent-ils servir l'économie réelle ?

Q3 : Que pensez-vous des phénomènes de concentration décrits dans la partie 1-5 du document ?

Q4 : Avez-vous des commentaires à formuler ou des compléments à apporter sur la présentation schématique de la *DeFi* figurant en partie 1-6 ?

Partie 2 du document – Les risques liés à la *DeFi*

Q5 : Avez-vous des remarques sur la description des risques liés à la gouvernance décentralisée (partie 2-1 du document) ?

Q6 : Pensez-vous que les solutions de *layer 1* peuvent accroître les problèmes de sécurité de l'infrastructure blockchain ? Et pour les solutions de *layer 2* ? Selon vous, existe-t-il de ce point de vue d'importantes différences selon les solutions de *layer 2* considérées ?

Q7 : L'utilisation de *rollups* ou de solutions similaires est-elle selon vous de nature à réduire la transparence de l'information pour un observateur ?

Q8 : Avez-vous des remarques quant à la description des risques liés à la couche applicative de la *DeFi* (partie 2-3) ?

Q9 : Avez-vous des commentaires à formuler au sujet du recensement des risques de la *DeFi* pour la clientèle particulière (partie 2-4-1) ?

Q10 : Avez-vous des remarques ou des compléments à apporter sur la description (partie 2-4-2) des fragilités systémiques de l'écosystème *DeFi* (endogénéité des placements, importants effets de levier, rôle des mécanismes de liquidation automatisée des positions) ?

Q11 : Êtes-vous d'accord avec la proposition s'agissant de la réglementation à appliquer aux *stablecoins* émis par des protocoles *DeFi* ? (*Cf.* partie 2-4-3 : « *dès lors qu'un service décentralisé prétend créer ou utiliser un crypto-actif ayant pour référence une monnaie officielle, ce crypto-actif doit obligatoirement être un EMT au sens de MiCA (ou un actif équivalent)* »)

☐Oui

☐Non

Pour quelles raisons ?

Q12 : Avez-vous des remarques à formuler quant à la description des risques que la *DeFi* peut faire peser dans la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) (partie 2-4-4) ?

Q13 : Voyez-vous d'autres risques à prendre en considération, qui ne seraient pas évoqués (ou insuffisamment) dans le document ?

Partie 3 du document – Les pistes d'encadrement réglementaire

Partie 3-1 – Assurer une sécurité minimale de l'infrastructure

Q14 : Les blockchains publiques devraient-elles faire l'objet d'un encadrement ou de standards minimaux de sécurité (cf. partie 3-1, schéma de régulation A) ?

☐Oui

☐Non

Si oui, de quelle façon ? Sinon, pourquoi ?

Q15 : Les autorités publiques devraient-elles superviser la concentration des capacités de validation sur les blockchains publiques ? Si oui, par le biais de quelles actions ?

☐Surveiller la concentration en temps réel

☐Fixer des plafonds à cette concentration

☐Communiquer publiquement en cas de dépassement de certains seuils de concentration

☐Engager d'autres actions (préciser lesquelles)

Q16 : Partagez-vous l'analyse qui est faite dans le document quant aux avantages et inconvénients des blockchains privées (partie 3-1, schéma de régulation B) ? Les blockchains privées opérées par des opérateurs privés devraient-elles, le cas échéant, être soumises à un cadre de surveillance ?

☐Oui

☐Non

Pourquoi ?

Q17 : Des acteurs publics devraient-ils gérer directement les blockchains servant d'infrastructure à la *DeFi* ?

☐Oui

☐Non

Pourquoi ?

Q18 : Avez-vous d'autres pistes de réglementation à proposer dans le but d'assurer une sécurité minimale de l'infrastructure blockchain ?

☐Oui

☐Non

Si oui, lesquelles ?

Partie 3-2 – Proposer un encadrement adapté à la nature algorithmique des services

Q19 : Un mécanisme de certification constitue-t-il une solution efficace pour définir un périmètre de *smart contracts* « sûrs » (pour un état donné des connaissances) ? Des solutions alternatives permettraient-elles d'aboutir au même résultat ?

Q20 : Partagez-vous la description qui est faite (partie 3-2-1) des différentes techniques d'audit du code informatique des automates exécuteurs de clauses (*smart contracts)*, y compris de leurs avantages et de leurs inconvénients respectifs ?

Q21 : Identifiez-vous des exemples de *smart contracts* qui ne devraient pas pouvoir être certifiés du fait de la nature même des services qu'ils rendent ?

☐Oui

☐Non

Si oui, lesquels ?

Q22 : Que pensez-vous des règles proposées dans le document (partie 3-2-2, point a) quant à la manière de certifier les *smart contracts* (certification préalable des composants appelés, cycle de vie de la certification) ?

Q23 : Les *smart contracts* devraient-ils embarquer dans leur code un certain nombre d'exigences réglementaires à l'avenir ?

☐Oui

☐Non

Pourquoi ?

Q24 : Qui devrait établir les standards de sécurité des *smart contracts* (cf. partie 3-2-2, point b) et pourquoi ?

Q25 : L'interaction avec des *smart contracts* non certifiés devrait-elle être découragée ou interdite (cf. partie 3-2-2, point c) ?

☐Découragée

☐Interdite

☐Ni découragée ni interdite

Pourquoi ?

Q26 : Qui devrait supporter le coût de la certification des *smart contracts* (cf. partie 3-2-2, point d) et pourquoi ?

Q27 : Avez-vous des remarques quant à la description des risques inhérents au modèle des oracles décentralisés ? Ces risques peuvent-ils être limités par un système de certification adapté aux spécificités de ces applications (cf. partie 3-2-3) ? Avez-vous des remarques ou des propositions alternatives d'encadrement de l'activité des oracles ?

Q28 : Avez-vous d'autres pistes de réglementation à proposer en vue de réduire les risques liés à la couche applicative de la *DeFi* ?

☐Oui

☐Non

Si oui, lesquelles ?

Partie 3-3 – L'encadrement de la fourniture et de l'accès aux services

Q29 : Pensez-vous qu'il puisse dans certains cas être nécessaire de « recentraliser » certaines activités sensibles (partie 3-3-1) ?

☐Oui

☐Non

Si oui, lesquelles ? Si non, pourquoi ?

Q30 : Que pensez-vous des propositions formulées quant aux manières d'atteindre cet objectif (obligations de se constituer en société, assujettissement des acteurs exerçant un contrôle effectif, statut juridique pour les DAO) ? Avez-vous des suggestions à faire sur le statut juridique à conférer aux DAO ?

Q31 : Partagez-vous la description des risques liés à la « *CeDeFi* », d'une part, et aux « conglomérats crypto » d'autre part (encadré 6) ?

Q32 : Quelles exigences devraient s'appliquer aux intermédiaires facilitant l'accès à la *DeFi* ?

☐Des obligations d'information

☐Des obligations de conseils et de vigilance

☐Des exigences concernant la publication de livre blanc

☐Des exigences de KYC

☐Un cadre complet inspiré de MiCA

☐Autre

Pourquoi ?

Q33 : Faudrait-il appliquer les mêmes règles à l'ensemble des intermédiaires de la *DeFi* (y compris, le cas échéant, à des interfaces web décentralisées) ?

☐Oui

☐Non

Pourquoi ?

Q34 : L'accès aux produits financiers doit-il être conditionné aux compétences financières des clients et à leur appétence au risque ?

☐Oui

☐Non

Pourquoi ?

Q35 : Avez-vous d'autres pistes de réglementation à proposer concernant l'encadrement de la fourniture et de l'accès aux services ?

☐Oui

☐Non

Si oui, lesquelles ?

Pistes de réglementation – aspects transversaux

Q36 : Comment tenir compte des impératifs de proportionnalité (pour les acteurs de taille modeste) dans les différentes pistes réglementaires avancées par le document (ou proposées par vos soins) ?

Q37 : Quelles pistes de réglementation – qu'elles soient ou non proposées dans le document – pourraient permettre de surmonter les problèmes liés à la possible extra-territorialité des acteurs (d'un point de vue national ou européen) ?

Q38 : Qui devrait, dans chaque cas, contrôler la mise en œuvre des différentes pistes réglementaires (qu'elles soient avancées dans ce document ou proposées par vos soins) ? Avec quels moyens ?