

FINANCE DÉCENTRALISÉE (DEFI), PROTOCOLES D'ÉCHANGE ET GOUVERNANCE :

VUE D'ENSEMBLE, TENDANCES OBSERVÉES
ET POINTS DE DISCUSSION RÉGLEMENTAIRES

Papier de discussion AMF

Sommaire

Introduction

I) Qu'est-ce que la finance décentralisée ?

- 1) Des protocoles automatisés, décentralisés et désintermédiés
- 2) Les contrats intelligents (*smart contracts*)
- 3) Les applications décentralisées (*DApps*)

II) Le marché de la DeFi : activités et produits

- 1) Vue d'ensemble et tendances observées
- 2) Une diversité d'activités et de produits

III) Les Echanges Décentralisés (DEX) et les Teneurs de Marché Automatisés (AMM)

- 1) Description et vue d'ensemble
- 2) Similitudes et différences avec les plateformes d'échange centralisées
- 3) Différences entre les modèles d'échanges décentralisés (DEX) et les teneurs de marché automatisés (AMM)
- 4) Risques engendrés par les protocoles d'échange DeFi

IV) Gouvernance de protocoles : organisations autonomes décentralisées (DAO) et jetons de gouvernance

- 1) Les organisations autonomes décentralisées (DAO)
- 2) Les jetons de gouvernance
- 3) Risques liés aux DAO de protocoles et à la gouvernance des protocoles DeFi
 - 3.1 Risques liés à l'incertitude légale des DAO et au modèle économique
 - 3.2 Risques de « pseudonymat » et de gouvernance
 - 3.3 Niveau de décentralisation et de degré de contrôle

Conclusion

Introduction

La technologie *blockchain* est, depuis plusieurs années, un catalyseur d'innovations financières. Elle est à l'origine d'activités et de produits souvent inédits fournis aux acteurs économiques, et de la création de structures de marché et de gouvernance se posant en alternative aux modèles traditionnels.

Dans ce contexte, la finance décentralisée (*Decentralised Finance*, ou DeFi) se présente comme un phénomène de rupture, portant la promesse d'un modèle complémentaire aux services financiers traditionnels. Elle est un nouveau mode opératoire par lequel des activités sur crypto-actifs sont fournies. Elle suscite un intérêt croissant des législateurs et autorités de contrôle afin d'identifier les opportunités et les risques proposés par ses différents modèles.

L'une des caractéristiques de la DeFi repose sur l'utilisation d'une infrastructure *blockchain* qui se veut décentralisée, désintermédiée et automatisée. Selon ces principes, les fonctions traditionnellement fournies par des entités centralisées sont désormais remplacées par l'utilisation de programmes automatisés, sous la forme de protocoles, et de « contrats intelligents » (ou *smart contracts*), accessibles en théorie à tout utilisateur et sans intermédiaire. Au-delà des nouvelles opportunités d'innovation que cet écosystème peut apporter, la DeFi soulève des enjeux parfois difficiles à appréhender et engendre des risques spécifiques à ces mécanismes. En particulier, certains de ces risques ont pu être observés lors de la défaillance du protocole de DeFi Terra / Luna en mai 2022 qui a eu pour conséquences de produire des pertes massives pour ses investisseurs et ses utilisateurs, interrogeant quant à la nécessité de réguler ce secteur.

Ce papier de discussion vise à définir ce qui constitue l'écosystème de la finance décentralisée et les tendances relevées de son marché, en explorant certaines thématiques spécifiques dont les protocoles d'échange décentralisés et les enjeux de gouvernance, tout en soulevant certaines problématiques et des points de discussion réglementaires.

Les opinions exprimées dans ce papier ne tiennent pas lieu de position officielle de l'AMF sur la finance décentralisée mais visent à engager le dialogue avec l'écosystème, acteurs publics et privés, afin de permettre l'émergence d'une approche réglementaire équilibrée.

Au regard des points soulevés dans ce papier, les acteurs sont invités à apporter leur contribution à la réflexion – sous format libre – avant le 30 septembre 2023 à l'adresse innovation@amf-france.org.

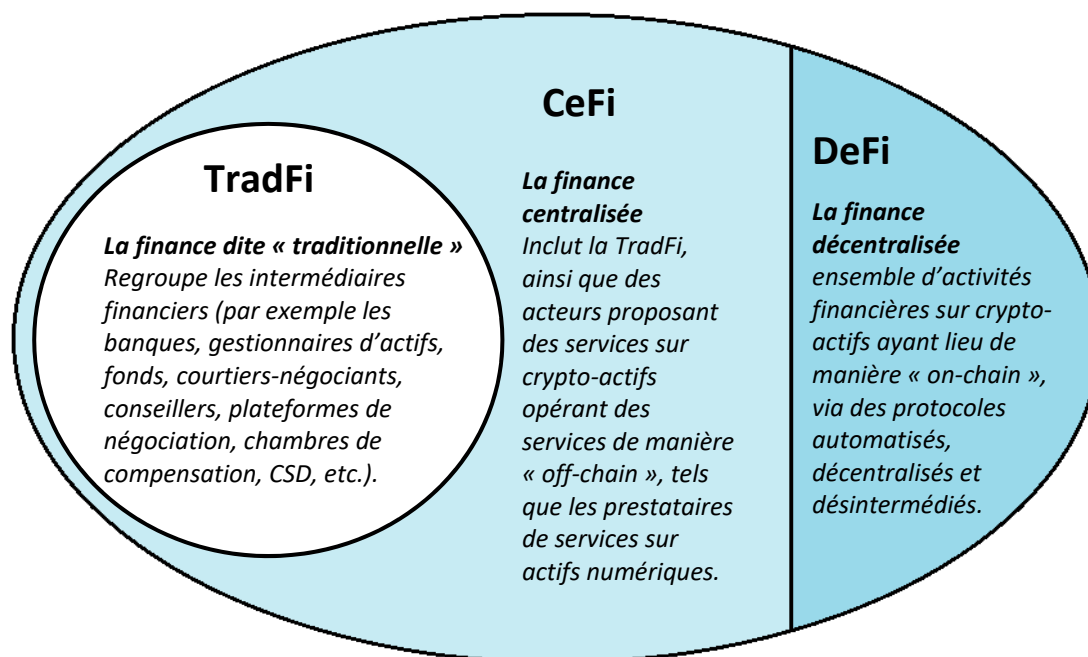
I) Qu'est-ce que la finance décentralisée ?

1. Des protocoles automatisés, décentralisés et désintermédiés

Développé à la suite du lancement de la *blockchain* Ethereum, le concept de finance décentralisée est apparu en 2017 avec l'émergence des premiers protocoles. Depuis lors, cet écosystème s'est développé rapidement avec comme but affiché d'être une alternative aux services financiers traditionnels (*traditional finance*, ou TradFi)¹, reproduisant certaines activités existantes et en introduisant des nouvelles. La DeFi porte la promesse d'une fourniture d'activités totalement automatisées, décentralisées et désintermédiées, sans – théoriquement – besoin d'intervention humaine. Reposant exclusivement sur l'utilisation de protocoles *blockchain*² et de crypto-actifs, elle définit également de nouveaux modèles de gouvernance en permettant aux utilisateurs de participer directement à la gestion des protocoles en interagissant sur la *blockchain* (*on-chain*).

Par conséquent, le terme DeFi s'inscrit par définition en opposition à des modèles existants, la TradFi ou bien plus globalement la « CeFi », la finance centralisée qui peut être « traditionnelle », ou proposer des services sur crypto-actifs mais réalisés via des systèmes hors *blockchain* (*off-chain*).

Graphique I: Distinction entre TradFi, CeFi et DeFi



¹ Lien : "ethereum.org/en/defi"

² Voir la notion de protocole, encadré n°1.

Encadré n° 1 – Qu'est-ce qu'un protocole ?

Un protocole est un ensemble de règles informatiques permettant à des ordinateurs de formater, de traiter et de transmettre des données. Il s'agit d'un langage informatique commun permettant aux différents ordinateurs de communiquer de manière standardisée. Collectivement, ces ordinateurs forment ensuite les nœuds d'un réseau (chaque nœud pouvant opérer, ou « exécuter » les ordres du protocole).

Ainsi, par exemple, le protocole de transfert hypertexte (http) permet de générer des informations sur des pages web. Certaines applications (comme par exemple des navigateurs internet) peuvent exécuter le protocole, générant ainsi les pages web et les informations qu'elles contiennent.

Les fonctions fournies par les protocoles peuvent être plus ou moins complexes selon le nombre de tâches à effectuer (par exemple, identification de canaux de communication, formatage de données, routage et transmission de messages, etc.). Les protocoles peuvent ainsi être superposés en différentes couches de manière stratifiée (layers) qui effectuent plusieurs tâches, où chaque nouvelle couche dépend du fonctionnement de la couche sous-jacente.

Le protocole http, par exemple, est établi au-dessus du protocole TCP / IP (Transmission Control Protocol / Internet Protocol), qui permet de lier entre eux les périphériques d'un réseau, formant ainsi la base du réseau bien connu qu'est internet.

De manière générale, la désignation d'un protocole se fera selon la fonction qu'il exerce. On parlera ainsi de « protocoles blockchain » pour les protocoles permettant le séquençage de transactions sous forme de blocs au sein d'un registre distribué sur les nœuds d'un réseau, de « protocoles DeFi » pour les protocoles permettant des activités de finance décentralisée, ou de « protocoles d'échange décentralisé » en référence aux protocoles DeFi permettant cette activité spécifique (voir section III).

L'infrastructure technologique sur laquelle repose la DeFi provient majoritairement de la *blockchain* Ethereum. De manière similaire aux protocoles informatiques traditionnels décrits dans l'encadré n°1 ci-dessus, les protocoles *blockchain* peuvent opérer de manière stratifiée. Par exemple, la *blockchain* Ethereum constitue un protocole de niveau 1 (*layer 1*), permettant de régler et d'homologuer les transactions sous la forme d'une séquence de « blocs ». Au-dessus de cette première strate, une deuxième couche (*layer 2*) peut ensuite être développée. Plusieurs protocoles fournissent ainsi une fonction d'optimisation (ou de *scaling*), visant à rendre plus efficace le fonctionnement du protocole Ethereum, notamment vis-à-vis de la fréquence à laquelle les transactions peuvent être enregistrées³. Enfin, au-dessus de ces deux premières couches, plusieurs autres protocoles ou programmes informatiques (*smart contracts* et *DApps*, voir sections 1.2 et 1.3 ci-dessous) peuvent être développés et intégrés. Collectivement, ces couches forment l'écosystème de la finance décentralisée.

Tandis que la fonction d'automatisation de la DeFi provient du fonctionnement des protocoles qui la constituent, la notion de décentralisation repose quant à elle sur l'architecture distribuée des nœuds d'un réseau au sein d'un protocole *blockchain* dans lequel un nœud ne peut décider seul du traitement des opérations enregistrées. Dans la pratique, on constate que les protocoles DeFi peuvent connaître divers degrés de décentralisation, selon la manière dont ils ont été conçus (voir ci-dessous), ou en raison du contrôle exercé par certaines personnes sur leur gouvernance (voir section IV).

Si l'émergence de la DeFi est principalement associée à la *blockchain* Ethereum, d'autres *blockchains* comme Solana, Cardano, Polkadot ou Hyperledger disposent de fonctionnalités similaires. En fonction de la manière dont elles ont été conçues, une différence majeure réside cependant dans la capacité d'accès par les utilisateurs à ces *blockchains*. Par exemple, alors que l'accès à Ethereum n'est pas restreint (définissant ainsi une *blockchain* de type « publique » ou « non permissionnée »), d'autres (comme Hyperledger) ne permettent qu'à certains participants d'y accéder (constituant ainsi un réseau dit « privé » ou « permissionné »).

³ Lien : "<https://ethereum.org/en/layer-2>"

Point de discussion n°1 – Protocoles blockchain permissionnés et non permissionnés

Un aspect à prendre en compte dans l'élaboration d'un cadre réglementaire pour la DeFi est de considérer la nature et le degré d'accès des protocoles blockchain aux utilisateurs. Bien qu'une blockchain permissionnée accorde un rôle décisionnaire à certaines entités ou nœuds sur le réseau (et qu'elles engendrent par conséquent un certain degré de centralisation), on peut aussi considérer que le fonctionnement d'un protocole via des nœuds distribués sur un réseau demeure décentralisé par nature.

Ainsi un critère permettant de déterminer ou non si une activité relève de la DeFi serait d'évaluer la nature permissionnée ou non d'une blockchain, en incluant une analyse de son « degré » de permissivité. Les critères à prendre en compte pourraient notamment être le nombre d'entités, d'individus ou d'utilisateurs pouvant contrôler l'activité sur le réseau.

Au-delà des questions liées au libre accès des *blockchains*, un dénominateur commun des protocoles DeFi est leur capacité à intégrer certaines fonctionnalités, au premier rang desquelles celle des contrats intelligents (*smart contracts*).

2. Les « contrats intelligents » (*smart contracts*)

Au-delà des protocoles décrits précédemment, les « *smart contracts* »⁴ constituent un aspect central de la DeFi. Un *smart contract* peut être défini comme un programme ou un code informatique inscrit sur la *blockchain* visant d'une certaine manière à répliquer les fonctionnalités d'un contrat traditionnel, exécutant des transactions sur la base de certains critères, puis transmettant l'information à la *blockchain* pour l'enregistrer de manière permanente. Ces conditions d'exécution peuvent être par exemple le franchissement de certains seuils de valeur du cours d'un crypto-actif ou l'atteinte d'un ratio. Un *smart contract* fonctionne de manière automatisée et autonome, il est considéré comme « auto-exécutant ». Ainsi l'opération d'un *smart contract* est continue dans le temps et ne nécessite pas d'intervention humaine pour en assurer le fonctionnement (il ne nécessite pas de serveur centralisé ni d'équipe dédiée à son opération), lui conférant un caractère immuable ou irréversible une fois les critères d'exécution remplis.

Après l'initiation d'une demande de transaction ordonnée via un *smart contract*, les paramètres de la transaction sont transmis puis vérifiés par les nœuds de la *blockchain*. Une telle demande peut être initiée via n'importe quel nœud, qui la diffuse à l'ensemble du réseau ; les autres nœuds pourront alors lire la transaction et vérifieront qu'elle est bien exécutée selon les critères définis dans le code du *smart contract*. Si la transaction est exécutée avec succès, la *blockchain* est alors mise à jour avec l'enregistrement de la transaction. Un *smart contract* peut également rejeter une transaction si les critères ne sont pas validés, auquel cas aucune transaction n'est inscrite sur la *blockchain*.

Également, le code des *smart contracts* peut être modifié et adapté pour intégrer certaines fonctionnalités spécifiques. Certains types de *smart contract* prévoient par exemple le concept d'un *hash timelock*⁵ (ou délai d'attente pour le hachage), un mécanisme permettant d'exiger d'un acheteur qu'il confirme sa capacité de paiement avant l'échéance déterminée d'une transaction. Une fois que l'acheteur confirme qu'il est bien en capacité de régler le paiement, la transaction et le transfert des crypto-actifs sont exécutés, et les actifs sont transférés de manière simultanée⁶, rendant l'ensemble du processus quasi instantané, permettant un règlement dit « atomique » (*atomic settlement*). L'intégration d'une telle fonctionnalité permet également d'annuler les transactions lorsque le paiement n'est pas confirmé à une échéance prédéterminée.

⁴ Les développeurs ont intégré la fonctionnalité de *smart contract* à la *blockchain* Ethereum, [concept initialement développé dans les années 1990](#).

⁵ Lien : "[Corporate Finance Institute.com - hashed timelock contract](#)"

⁶ Lien : "[imf.org - DeFi's promise and-pitfalls](#)"

La fonction d'un *smart contract* est donc d'exécuter diverses tâches, processus ou transactions via un code informatique préprogrammé. En eux-mêmes, les *smart contracts* ne constituent donc pas un accord juridiquement contraignant entre deux parties. Des démarches juridiques distinctes doivent être entreprises pour lier les parties prenantes à l'exécution du *smart contract* afin que celui-ci puisse être contraignant juridiquement.

Malgré le caractère immuable des transactions qu'il génère, le code des *smart contracts* peut être modifié. Lorsqu'une modification du code a lieu, le protocole sur lequel le *smart contract* opère doit être bifurqué (*forked*), du fait de la nature continue et autonome du *smart contract*. Après un tel événement, les deux versions du *smart contract* continuent à fonctionner en parallèle et indépendamment l'une de l'autre. Les versions précédentes d'un *smart contract* peuvent continuer d'être utilisées tant que des interfaces (ou applications) y fournissent un accès (voir section I.3 sur les *DApps* ci-dessous). La possibilité de modifier le code d'un *smart contract* appartient aux développeurs informatiques des protocoles qui peuvent mettre en place ces modifications, et les utilisateurs du protocole peuvent être impliqués dans le processus, s'ils ont un droit de regard et de prise de décision sur les modifications proposées (voir section IV).

Point de discussion n°2 – *Smart contracts*

Le premier enjeu réglementaire relatif aux *smart contracts* réside en la détermination de leur base juridique. Même s'ils visent d'une certaine manière à répliquer la fonction d'un contrat traditionnel, leur code n'est pas nécessairement directement traduisible dans un langage non informatique, et a fortiori ne permet pas une transcription juridique des termes dont il est composé. Également, la responsabilité légale des parties prenantes participant à la création, au développement ou à l'utilisation d'un *smart contract*, n'est pas clairement établie. Il conviendrait dès lors d'évaluer si la responsabilité d'individus responsables de son code ou celle des individus qui l'utilisent pourrait être engagée.

Les *smart contracts* étant capables d'exécuter des transactions selon des règles prédéterminées, il est possible théoriquement qu'ils intègrent des règles répondant à des exigences réglementaires. Cependant, la nature autonome et continue de leur fonctionnement peut contraster avec les aspects interventionnistes requis pour qu'une supervision soit établie (par exemple, pour forcer l'arrêt ou la reprise des opérations en cas de détection d'une irrégularité). Ainsi, une législation visant à encadrer les *smart contracts* pourrait exiger qu'ils soient conçus pour inclure des règles permettant un mécanisme d'interruption et de redémarrage, ou plus généralement permettre la certification de la conformité de leur code par rapport aux exigences réglementaires applicables.

La mise en place de telles mesures devra s'appuyer sur une analyse technique visant à vérifier si certains *smart contracts* déjà développés et opérationnels peuvent effectivement entrer dans ce cadre.

3. Les applications décentralisées (*DApps*)

Les applications décentralisées (*DApps*) sont des applications logicielles fournissant une interface permettant aux utilisateurs d'avoir accès aux fonctionnalités des *smart contracts*. De la même manière qu'une nouvelle couche (*layer*) au sein d'un protocole peut remplir une fonctionnalité différente (voir encadré n°1 ci-dessus), les *DApps* sont développées directement au-dessus de la couche des protocoles *blockchain*, facilitant ainsi l'accès à la fonctionnalité des *smart contracts* et leur utilisation par le public. Les *DApps* permettent en quelque sorte au public d'accéder à la structure décentralisée de la *blockchain*, ouvrant ainsi à ces utilisateurs la possibilité d'effectuer des transactions de pair-à-pair entre particuliers via le *smart contract* et les nœuds du réseau auquel elles fournissent un accès.

Les *DApps* sont donc des interfaces d'accès à la fonction des *smart contracts*, et les utilisateurs peuvent y soumettre une demande de transaction via l'interface qu'elles proposent. L'interface transmet ensuite le message au nœud du réseau auquel elle est reliée, qui le communique ensuite au *smart contract*. Une fois que les critères de validation de la transaction sont remplis, le *smart contract* exécute la transaction et la diffuse au reste de la *blockchain*.

Certains participants de l'écosystème DeFi ont tenté de définir le terme de *DApp*⁷ en se référant à la nature *open source*⁸ de leur code. Il s'agit ici d'une différence notable avec les applications logicielles utilisées en TradFi, qui sont pour la plupart développées sous une licence privée (*proprietary software*).

Point de discussion n°3 – Utilisation de code *open source*

De même que dans le cas des blockchain permissionnées vs. non permissionnées (voir point de discussion n°1 ci-dessus), un autre aspect à prendre en compte pour définir un cadre réglementaire adapté à la DeFi serait de considérer la nature *open source* ou non du code utilisé par ses applications et, en conséquence, la responsabilité légale liée au développement ou à l'utilisation d'un tel code. A ce jour, l'utilisation de code *open source* soulève un certain nombre de questions d'un point de vue juridique en raison de sa distribution libre sans conditions de licence, contrairement à un code développé sous licence privée.

La nature *open source* sur code des *DApps* leur confère certaines caractéristiques que n'ont pas les programmes développés sous licence privée⁹ :

1. **Transparence** : La conception *open source* des *DApps* les rend transparentes et théoriquement lisibles par tout utilisateur averti, qui peut ainsi identifier ses fonctionnalités ainsi que les données utilisées par les *smart contracts* associés.
2. **Auditabilité** : Du fait d'une telle transparence, le code peut être facilement audité, permettant d'identifier et d'évaluer ouvertement certains paramètres comme, selon l'activité proposée, les flux de transaction indiquant entre autre les montants et les volumes échangés, les montants collatéralisés etc.
3. « **Composabilité** »¹⁰ : Du fait qu'un code *open source* puisse être facilement partagé et modifié, les *DApps* peuvent être recombinaisonnées avec d'autres applications. Le code de certains *smart contracts* pouvant en effet faire référence à celui d'autres *smart contracts*, ces chaînes permettent en conséquence de rendre « composables » entre elles les applications qui les opèrent¹¹.

⁷ [Lien : "Github - The General Theory of Decentralized Applications, DApps"](#)

⁸ Un logiciel dit *open source* est un logiciel dont le code source est libre d'accès, réutilisable et modifiable. On parle également de « logiciel libre » pour désigner un logiciel ainsi conçu.

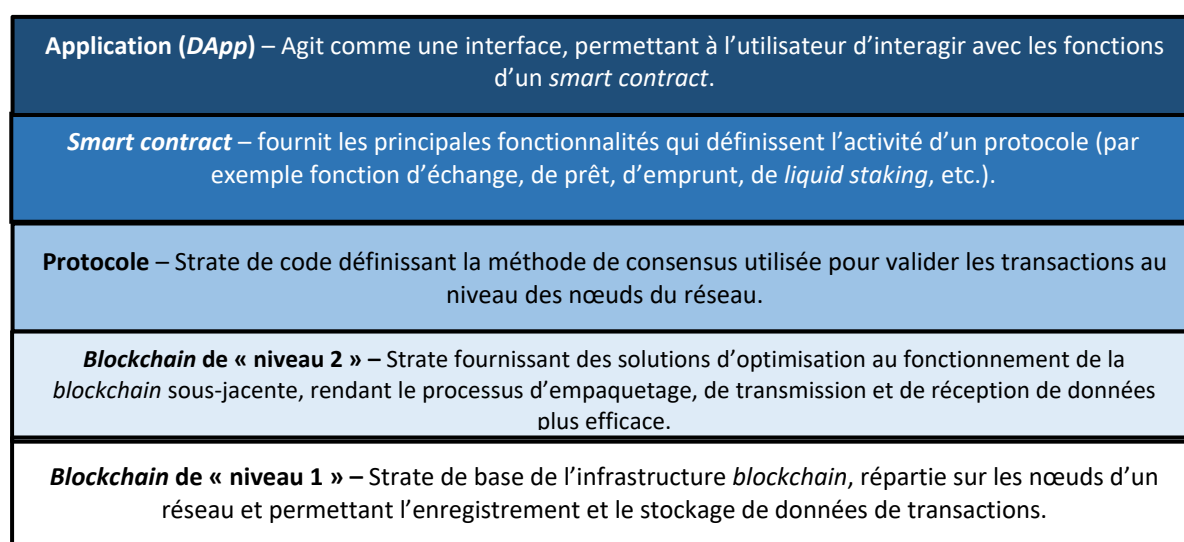
⁹ [Lien : "medium.com - DeFi Infrastructure 101 - Overview & Market Landscape"](#)

¹⁰ La « composabilité » est un principe de conception de système qui traite des interrelations des composants. Un système composable fournit des composants qui peuvent être assemblés dans diverses combinaisons pour répondre aux exigences spécifiques de l'utilisateur.

¹¹ [Lien : "imf.org - DeFi's promise and-pitfalls"](#)

Le diagramme ci-dessous résume les différentes couches qui composent le fonctionnement technologique de la DeFi :

Graphique 2 – Les couches technologiques de la DeFi¹²



II) Le marché de la DeFi : activités et produits

1. Vue d'ensemble et tendances observées

Selon les données relevées sur le marché, près de 2 000 protocoles DeFi auraient été dénombrés début 2023¹³, soit plus du double du nombre de protocoles (855) enregistrés début 2022. Parmi ces protocoles, environ 650 seraient des protocoles d'échange décentralisés (*Decentralised Exchanges* ou DEX) ou des teneurs de marché automatisés (*Automated Market Makers* ou AMM) (voir section III). Il existerait également plusieurs milliers de *DApps* donnant accès à ces protocoles. Une estimation globale du nombre exact de *DApps* est difficile à établir en raison du manque de cohérence entre diverses sources. Certaines sources indiquent qu'il y aurait plus de 3 500 *DApps*¹⁴ au total, tandis que le réseau *blockchain* Polygon indiquait fin octobre 2022 que plus de 53 000 *DApps* avaient été développées sur son réseau¹⁵.

Le volume d'activité de la DeFi se mesure grâce à l'indicateur de « valeur totale verrouillée » (*Total Value Locked* ou TVL) qui correspond à la valeur totale des actifs déposés dans des *smart contracts* de protocoles DeFi à un instant donné.

Fin janvier 2023¹⁶, la TVL des protocoles DeFi était évaluée approximativement à 80 Mds \$USD, en baisse par rapport à un maximum de près de 258 Mds \$USD fin 2021, à la suite de la chute de la valeur des crypto-actifs de près de 60 % au 1^{er} semestre 2022 (voir Graphique 4 ci-dessous).

Parmi les diverses activités des protocoles DeFi, les teneurs de marché automatisés (AMM), les échanges décentralisés (DEX) et les protocoles de prêt et d'emprunt (voir section II.2) totalisent à eux seuls près des deux tiers de la TVL totale.

¹² Source AMF.

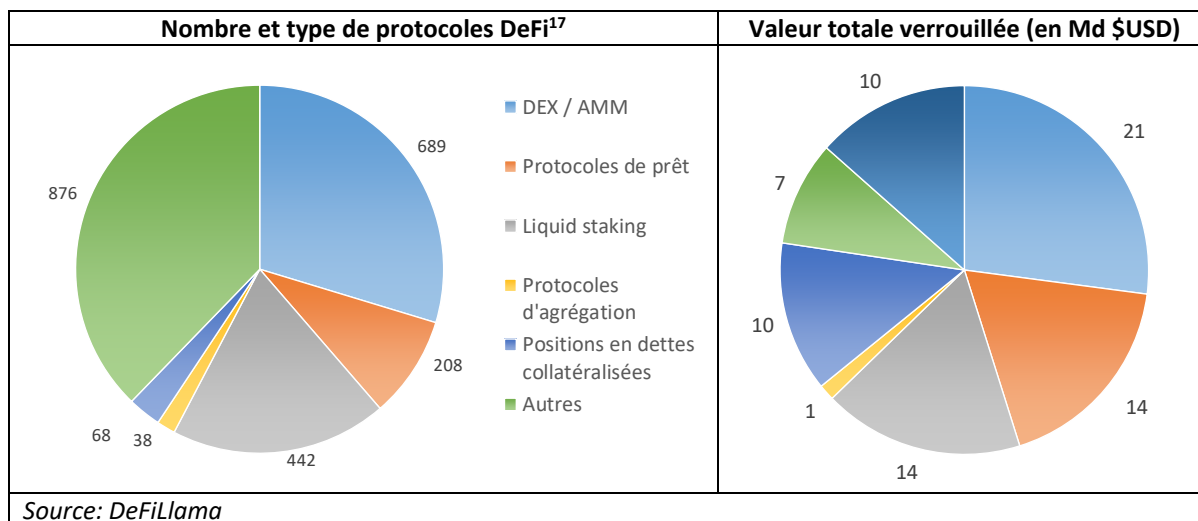
¹³ [Defillama.com](https://defillama.com)

¹⁴ Lien : "[Tap Global - What are DApps?](#)"

¹⁵ Lien : "[Polygon Labs - Polygon Crosses 53,000 DApps Mark in a Major Adoption Milestone](#)"

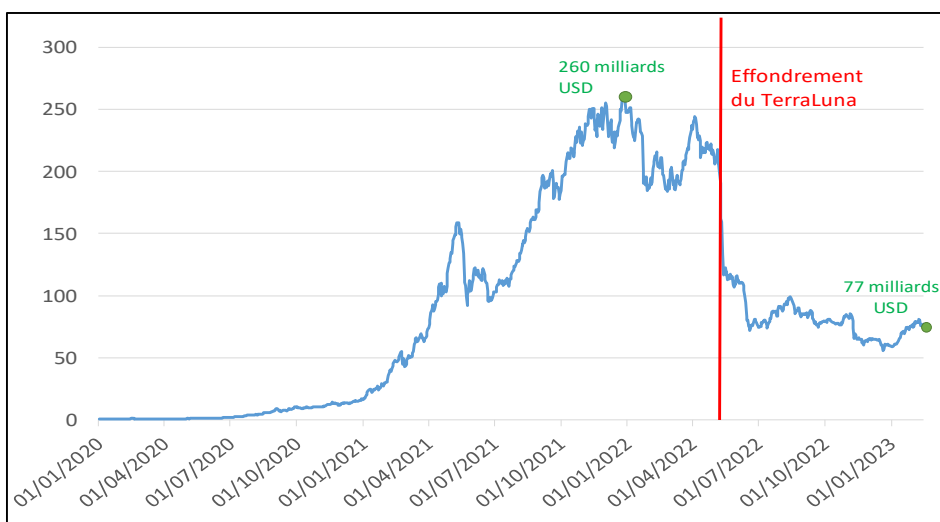
¹⁶ Données datant du 25 Janvier 2023. Sources: [DeFiLlama](https://defillama.com), [Stelareum](https://stclareum.com).

Figure 3 – Nombre total de protocoles DeFi et valeur totale verrouillée (TVL)



Le secteur de la DeFi a connu de fortes fluctuations ces dernières années. La phase initiale de son développement vit une croissance importante de la TVL, jusqu'à près de 260 Mds \$USD à début 2022, avant de connaître une chute de valeur au deuxième trimestre 2022. Les niveaux plus récents (environ 80 Mds \$USD à fin janvier 2023) avoisinaient un tiers de la valeur maximale enregistrée fin 2021. Cette décroissance constatée de la TVL est notamment expliquée par les conséquences de la crise Terra / Luna (voir encadré n°2 ci-dessous) et la baisse généralisée de la valorisation des crypto-actifs. Malgré cette baisse, on observe cependant sur la même période une croissance importante du nombre de *DApps* et de protocoles DeFi (comme expliqué ci-dessus).

Graphique 4 – Valeur totale verrouillée (TVL) en DeFi (en Md \$USD)¹⁸



¹⁷ Une position en dette collatéralisée est un protocole DeFi verrouillant des collatéraux dans un *smart contract* pour émettre des *stablecoins* en échange.

¹⁸ [Defillama.com](https://defillama.com)

Encadré n°2 – L’effondrement du protocole DeFi Terra / Luna

Résumé

En mai 2022, la valeur du « jeton stable » (*stablecoin*) Terra (UST) et celle du jeton Luna (LUNA), composantes essentielles du protocole DeFi Terra / Luna, ont chuté simultanément, menant à une diminution de près de 60 Mds \$USD de la valeur verrouillée au sein du protocole en l’espace de quelques jours¹⁹, et engendrant des répercussions majeures au sein des marchés crypto-actifs. Marquant la première crise d’importance significative de l’écosystème DeFi, l’effondrement de l’écosystème Terra / Luna et son ampleur soulèvent de nombreuses questions sur la fiabilité et la robustesse des protocoles DeFi, en particulier sur les risques posés par les *stablecoins* dits « algorithmiques »²⁰.

Le protocole Terra / Luna était un protocole DeFi²¹ dont le mécanisme reposait sur une relation algorithmique entre le *stablecoin* UST (qui prétendait maintenir une valeur stable par rapport au dollar américain (\$USD)) et le jeton Luna (LUNA), un crypto-actif natif du protocole. Contrairement à d’autres *stablecoins*, l’UST n’était pas collatéralisé et n’était donc pas directement adossé à une valeur en réserve. La quantité disponible d’UST était directement liée à la quantité de LUNA en circulation. Le jeton LUNA servait en quelque sorte de mécanisme de stabilisation, la quantité de LUNA disponible était ainsi ajustée en réponse aux variations de la valeur de l’UST permettant théoriquement d’absorber toute volatilité de l’UST par rapport au \$USD, son actif de référence. Ceci reposait sur une relation entre l’offre et la demande des deux jetons, la destruction (ou *burn*) de l’un entraînant la création (ou *mint*) de l’autre.

Par exemple, lorsque la valeur de l’UST chutait à 0,98 \$USD, des utilisateurs cherchant des opportunités d’arbitrage pouvaient acheter 100 UST pour 98 \$USD, les convertissant ensuite en l’équivalent de 100 \$USD de LUNA (l’algorithme du protocole maintenant une valeur stable où 1 UST valait 1 \$USD lors de toute conversion entre UST et LUNA). Une demande accrue d’UST par les arbitragistes augmentait ainsi la valeur de l’UST sur le marché tandis que le protocole Terra / Luna détruisait l’UST en échange de la création de LUNA, réduisant ainsi l’offre disponible et par conséquent, la valeur de l’UST. A son tour, ceci faisait disparaître l’opportunité d’arbitrage lorsque la valeur de l’UST atteignait de nouveau 1 \$USD. Le phénomène inverse se produisait lorsque la valeur de l’UST était supérieure à 1 \$USD.

Chronologie

Après son lancement initial en 2019, l’écosystème Terra / Luna suscita progressivement l’intérêt des investisseurs, faisant croître la demande en *stablecoin* UST et en jeton LUNA. La valorisation du jeton LUNA atteignit un montant maximal de 139 Mds \$USD en avril 2022²². Peu après, les 7 et 8 mai 2022, le vent tourna subitement lorsque des utilisateurs retirèrent une valeur de plus de 2 Mds \$USD en UST, menant à une chute de valeur du *stablecoin* qui perdit sa corrélation au dollar USD (atteignant 0,91 \$USD).

¹⁹ Lien : ["Forbes - What really happened to Luna crypto"](#)

²⁰ Lien : ["banking.senate.gov - The Financial Stability Oversight Council Annual Report to Congress"](#)

²¹ Malgré ces événements, le protocole Terra / Luna continue d’opérer à ce jour.

²² Lien : ["coinmarketcap.com - Terra Luna"](#)

Le 8 mai 2022, la Luna Foundation Guard, une organisation à but non lucratif établie en janvier 2022 par les fondateurs du protocole pour soutenir le développement de projets au sein de l'écosystème Terra / Luna²³, commença à puiser dans ses réserves en vendant plus de 80 000 bitcoins (évalués à près de 3 Mds \$USD au moment de la vente) afin d'acheter une valeur équivalente en LUNA, dans le but de faire remonter la valeur de l'actif et d'ainsi pallier la déstabilisation de l'UST²⁴. Cette vente massive mena à une baisse significative des prix des crypto-actifs sur le marché, obérant également la valeur du jeton LUNA, ne faisant qu'aggraver la situation. Les utilisateurs continuèrent à vendre des UST, ce qui entraîna de nouvelles créations de LUNA. Ainsi, alors que le 6 mai 2022 le prix de LUNA était d'environ 80 \$USD, il ne valait plus qu'1 \$USD une semaine plus tard, tandis que l'UST ne retrouva jamais sa valeur cible d'1 \$USD, s'établissant à moins de 0,50 \$USD le 9 mai, avant de tomber sous la barre des 0,15 \$USD le 16 mai.

Risques identifiés et enseignements

Fonctionnement des *stablecoins* algorithmiques – Considérant la place centrale des *stablecoins* au sein des protocoles DeFi (du fait de leur représentation de valeur fiduciaire sur la *blockchain*), le modèle du protocole Terra / Luna a montré qu'un mécanisme de stabilisation automatisé peut, sous certaines conditions de stress économique, causer des effets négatifs inattendus sur l'ensemble du protocole.

Complexité et manque de transparence du modèle – Le manque de compréhension des utilisateurs et investisseurs vis-à-vis de la nature complexe du mécanisme de stabilisation du protocole Terra / Luna fut aussi évoqué comme une des raisons de l'effondrement du protocole, comme un élément perturbateur supplémentaire ayant contribué à la panique des utilisateurs et des investisseurs.

Risque de panique (*run risk*) – La crise du protocole Terra / Luna a démontré que les protocoles DeFi n'étaient pas à l'abri des risques de panique qui ont pu être précédemment observés dans le secteur bancaire. Au cas d'espèce, cette panique a largement aggravé la situation et a eu un effet en cascade sur les deux crypto-actifs (Terra et Luna) échangés, ce qui a précipité l'effondrement du protocole.

Risques d'interconnexion et de contagion à l'écosystème DeFi – Bien que la chute de l'UST et du LUNA soit due au fonctionnement d'un protocole donné, l'événement entraîna un débordement vers d'autres protocoles DeFi qui permettaient également l'échange ou l'immobilisation contre rémunération d'UST (*staking*)²⁵. En prenant l'écosystème dans sa globalité, certaines sources ont même estimé l'impact global à près de 500 Mds \$USD de perte en valeur²⁶.

Manque de mécanisme de résolution – À ce stade, aucun mécanisme de résolution n'a été défini depuis la chute du protocole Terra / Luna et les utilisateurs n'ont pas été indemnisés, même partiellement. En octobre 2022, la Luna Foundation Guard indiquait qu'elle n'était toujours pas en mesure de fournir un calendrier relatif à la procédure de compensation des utilisateurs affectés²⁷.

²³ [Lien : "medium.com - Formation of the Luna Foundation Guard \(LFG\)"](https://medium.com/Formation-of-the-Luna-Foundation-Guard-(LFG))

²⁴ [Lien : "twitter.com - LFG | Luna Foundation Guard"](https://twitter.com/LFG_Luna_Foundation_Guard)

²⁵ [Lien : "cointelegraph.com - Terra contagion leads to 80%+ decline in DeFi protocols associated with UST"](https://cointelegraph.com/news/Terra-contagion-leads-to-80-plus-decline-in-DeFi-protocols-associated-with-UST)

²⁶ [Lien : "washingtonpost.com - Crypto's meltdown refocuses regulator attention on the industry"](https://www.washingtonpost.com/crypto/meltdown-refocuses-regulator-attention-on-the-industry/)

²⁷ [Lien : "twitter.com - LFG | Luna Foundation Guard"](https://twitter.com/LFG_Luna_Foundation_Guard)

2. Une diversité d'activités et de produits

Tel qu'indiqué précédemment, il existe de nombreux types de protocoles et d'applications DeFi qui remplissent diverses fonctions. Si certains fournissent des activités similaires à celles de la TradFi, d'autres présentent de nouvelles fonctionnalités et de nouveaux types de produits et souvent une combinaison de plusieurs activités. Sont présentés ci-après les principales activités et produits recensés dans l'écosystème DeFi.

- **Les échanges décentralisés (DEX) et les teneurs de marché automatisés (AMM)** sont des protocoles mettant en relation des utilisateurs cherchant à échanger leurs crypto-actifs. Bien qu'ils ressemblent à ce que proposent les plateformes de négociation en CeFi, la nouveauté du modèle proposé par les AMM et les DEX réside dans le fait que les opérations d'échange ont lieu sur les protocoles, directement sur la *blockchain* (soit *on-chain*), faisant usage de *smart contracts* qui gèrent les flux d'échange de manière automatisée, sans intervention humaine. Dans le cas des AMM, en particulier, le processus est rendu possible par l'existence de « pools de liquidité » qui fournissent la liquidité dans des paires de crypto-actifs proposées à la négociation (voir section III de la note qui aborde ces concepts plus précisément).
- **Les protocoles de prêt / emprunt** proposent des activités de prêts et emprunts de crypto-actifs, permettant aux déposants de déposer leurs crypto-actifs en échange de l'obtention d'un prêt d'un autre crypto-actifs, généralement sous la forme de jetons stables (ou *stablecoins*). Les protocoles exigent généralement que les prêts soient sur-collatéralisés afin de minimiser le risque d'exposition en cas de défaut. Lorsqu'un prêt n'est pas remboursé, les actifs garantis deviennent la propriété du prêteur. Il sera noté que cette exigence de sur-collatéralisation rend cette activité de prêt / emprunt significativement différente de celle qui est rencontrée en TradFi.

Par ailleurs, la technologie *blockchain* utilisée par les protocoles DeFi permet l'apparition de nouveaux types de produits, tels que les *flash loans*, des prêts non garantis, sous remboursement « immédiat ». Ce modèle est souvent utilisé par les utilisateurs dans un contexte de stratégies d'arbitrage, où l'emprunteur peut, par exemple, revendre sur une autre plateforme le principal du prêt souscrit pour en tirer profit, avant de procéder au remboursement du prêt à la valeur originale, le tout réalisé simultanément. En TradFi, bien que ceci puisse s'apparenter à un mécanisme de rachat dans le cadre d'une vente à découvert, la nature quasi-instantanée et entièrement automatisée de l'émission, de la vente et du remboursement du prêt (qui ont toutes lieu via une seule écriture sur la *blockchain*, ou « bloc ») sans passer par de multiples intermédiaires, confère un aspect novateur à cette activité.

- **Les protocoles de *staking* et de *liquid staking*** permettent aux utilisateurs de déposer leurs actifs en échange d'une rémunération (par exemple sous forme d'intérêts). La *blockchain* Ethereum par exemple permet aux utilisateurs de déposer des *Ethers*, qui (en tant que jetons natifs du protocole) sont utilisés pour valider les transactions via le mécanisme de preuve de participation (*Proof of Stake*)²⁸. Ce mécanisme permet de créer de nouveaux *Ethers* lorsque de nouveaux blocs sont créés sur la *blockchain* Ethereum, les distribuant sous forme de récompense aux validateurs, proportionnellement à leur mise²⁹.

Le *liquid staking* est un cas spécifique de *staking*, pour lequel la récompense en échange d'un dépôt d'actifs est un jeton dit « de liquidité », qui peut ensuite être utilisé comme monnaie d'échange sur un protocole donné. L'utilisateur doit par la suite rendre ses jetons afin de pouvoir retirer ses actifs.

- **Les protocoles d'agrégation** sont capables de lire l'activité de plusieurs protocoles DeFi, offrant de meilleures perspectives de liquidité ou de prix en agrégeant les données à disposition. Par exemple, certains protocoles peuvent fournir de meilleures solutions d'allocation de liquidité sur plusieurs protocoles d'échanges (DEX et AMM) ; d'autres permettent une meilleure efficacité dans le cas de protocoles de prêt ou d'emprunt, en réduisant les écarts de taux.

²⁸ A l'heure actuelle le montant minimal pouvant être immobilisé contre rémunération ("staké") sur *Ethereum* pour qu'un nœud puisse être considéré comme validateur de transactions sur la *blockchain* est de 32 *Ethers*.

²⁹ Lien : ["ethereum.org - How The Merge impacted ETH supply"](https://ethereum.org)

- **Les protocoles de marchés prédictifs** sont un outil permettant aux utilisateurs de souscrire à un contrat fournissant des opportunités de retour sur investissement sur la base de résultats d'événements futurs. Alors que cela peut sembler similaire à certains produits TradFi qui promettent un retour en fonction de la valeur future de certains actifs, les marchés prédictifs offrent une récompense sur la base d'événements et non sur la base de la valeur d'actifs sous-jacents. Ainsi, la nature économique de telles activités se rapprocherait davantage de celle de jeux de hasard ou de paris.
- Il est relevé également certaines activités ou produits proposés par des protocoles DeFi qui se rapprochent des activités TradFi existantes :
 - **Les protocoles de gestion d'actifs** permettent aux utilisateurs de développer des stratégies de gestion d'actifs, par exemple en termes d'opérations d'achat, de vente ou de transfert. Certains protocoles permettent par exemple de mettre en place différents types de stratégies de négociation (arbitrages, optimisation de temps de latence, etc.). A la différence de la gestion d'actifs en TradFi, le détenteur des actifs est également le décisionnaire vis-à-vis de la stratégie adoptée, tandis que le *smart contract* l'exécute.
 - **Les protocoles de négociation de marge (*margin trading*)** permettent d'échanger des actifs en utilisant des fonds empruntés auprès de tiers, donnant accès aux utilisateurs à davantage de sources de capital, de manière similaire à ce qui peut être observé sur certains marchés TradFi permettant la négociation à effet de levier, comme sur les marchés Forex.
 - De même qu'en TradFi, certains protocoles DeFi permettent de négocier des **produits dérivés ou synthétiques**, dont le prix est déterminé en référence à la valeur d'un actif sous-jacent, offrant ainsi une exposition indirecte à cet actif ou à son marché. Au sein de la DeFi, certains types de contrats sont particulièrement utilisés comme les contrats à terme perpétuels³⁰.
 - La DeFi offre également des **produits d'assurance** qui visent à assurer les utilisateurs contre des pertes potentielles. Alors que certains de ces produits cherchent à reproduire les fonctionnalités de produits d'assurance traditionnels, d'autres peuvent permettre d'assurer contre des pertes pouvant survenir en raison d'événements affectant spécifiquement les protocoles DeFi, ce qui peut inclure des pertes résultant de chutes de prix de jetons, d'attaques cyber ou de piratages de protocoles.

Point de discussion n°4 – Prise en compte des risques des activités DeFi

Le développement d'un cadre réglementaire pour la DeFi devrait prendre en compte les caractéristiques des différentes activités qui peuvent y être observées. A cet effet :

Lorsque les activités au sein de DeFi peuvent être considérées comme ayant des caractéristiques similaires à celles de la TradFi, les législateurs devraient avant tout déterminer si la réglementation applicable au secteur TradFi est transposable aux activités similaires de la DeFi.

Si les activités proposées par la DeFi présentent de nouvelles caractéristiques ou permettent de combiner plusieurs activités de type TradFi et DeFi, il convient d'examiner si une réglementation *ad hoc* permettrait une meilleure protection contre les risques encourus par les utilisateurs, du fait des spécificités des protocoles DeFi. Dans certains cas, certains aspects des activités proposées pourraient être encadrés par la réglementation existante, mais celle-ci pourrait également s'avérer inadaptée, voire impossible à mettre en œuvre dans certains cas.

³⁰ Lien : ["synthetix.io - Decentralized Perpetual Futures"](https://synthetix.io)

III) Les échanges décentralisés (DEX) et les teneurs de marché automatisés (AMM)

Cette section entend fournir une analyse plus approfondie des activités des protocoles d'échange décentralisés (*Decentralised Exchanges* ou DEX) et de teneurs de marché automatisés (*Automated Market Makers* ou AMM), dont les activités peuvent présenter certaines similitudes avec celles des plateformes d'échange centralisées. Elle fournit une explication des modèles de DEX et AMM identifiés sur ces marchés, met en évidence des similitudes et des différences avec les systèmes de négociation traditionnels et analyse les risques à prendre en considération dans ces activités.

1. Description et vue d'ensemble

Les AMM et DEX (collectivement les « protocoles d'échange DeFi ») visent à fournir une activité similaire à celle des plateformes de négociation centralisées, rassemblant des intérêts acheteurs et vendeurs, permettant aux utilisateurs d'échanger leurs actifs à des quantités et des prix définis.

La différence majeure réside dans le fait que ces protocoles d'échange DeFi ne gèrent pas des carnets d'ordres *off-chain* centralisés comme les plateformes centralisées le font. Le fonctionnement de ces carnets d'ordres est en effet remplacé par des *smart contracts* opérant sur les protocoles, lesquels contiennent les règles de code qui déterminent le format de la négociation entre participants. Dans un tel modèle, les prix des actifs sont déterminés via l'opération d'un algorithme automatisé (dont la formule est inscrite dans le code du *smart contract*), ce qui peut différer du processus de formation de prix observé sur les mécanismes de carnets d'ordres traditionnels.

Les *smart contracts* qui opèrent au sein des protocoles d'échange DeFi peuvent également exiger (dans le cas des AMM notamment, voir ci-dessous) que les actifs soient verrouillés dans des réserves de liquidités (*liquidity pools*), au sein desquelles des montants de crypto-actifs sont apportés par des fournisseurs de liquidités (*liquidity providers*), permettant ainsi au *smart contract* de déterminer à tout moment la quantité d'actifs disponibles dans la réserve. Les fournisseurs de liquidités sont quant à eux rémunérés par les frais de transaction produits par l'activité d'échange sur le protocole, proportionnellement à la liquidité qu'ils fournissent. En échange de cet apport de liquidité, ils sont rémunérés via des jetons représentant la part de liquidité apportée, ces jetons devant être restitués s'ils souhaitent retirer leurs fonds de la réserve.

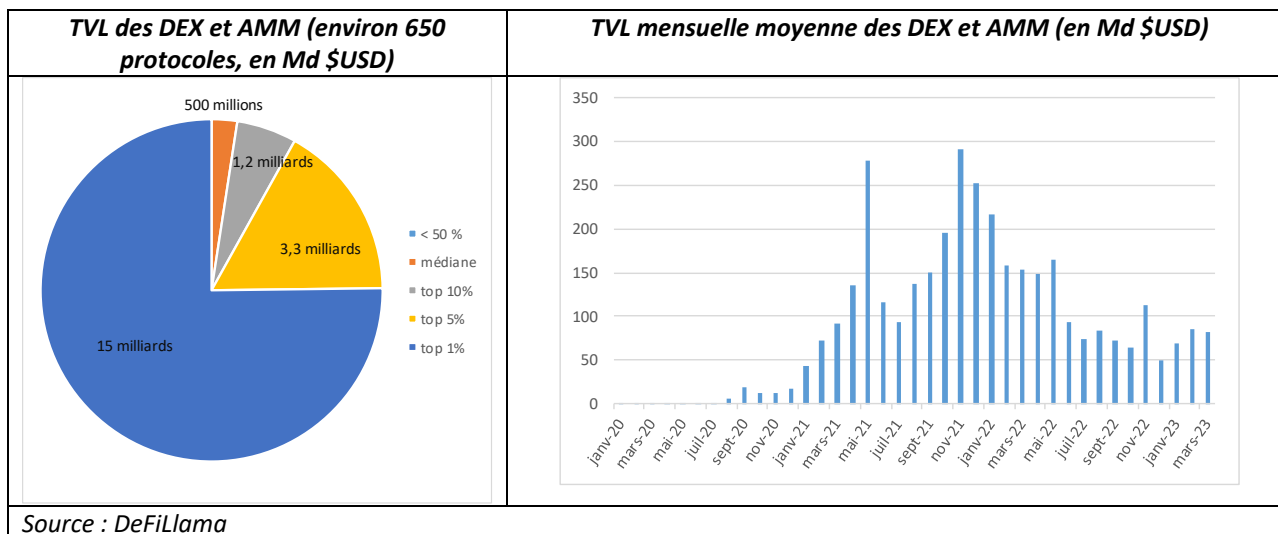
Dans ce modèle, la formule de formation de prix tient compte, d'une part, de la valeur des actifs au sein de la réserve (ce qui nécessite une source externe de prix (ou « oracle », voir ci-après) avant négociation) et, d'autre part, de la quantité d'actifs disponibles. Une fois les ordres de transaction soumis par les utilisateurs, la formule rééquilibre ensuite les prix des actifs en fonction de la valeur relative des actifs disponibles dans la réserve. Le mécanisme reproduit ainsi un scénario d'offre et de demande : un actif qui devient plus rare (si sa quantité disponible diminue au sein de la réserve) devient automatiquement plus cher.

Une des limites découlant de ce modèle est que les protocoles d'échange DeFi ont tendance à s'appuyer sur l'utilisation d'informations externes, notamment pour déterminer les prix initiaux, car l'évaluation de la valeur d'une réserve suppose une connaissance préalable de la valeur des actifs qui s'y trouvent. Une telle dépendance se caractérise par l'utilisation de flux de données externes (pouvant provenir d'autres protocoles DeFi, mais parfois aussi depuis des plateformes CeFi) intégrés au *smart contract* du protocole. En DeFi, de telles sources sont appelées « oracles », et soulèvent un certain nombre de questions au regard des risques qu'elles engendrent (voir section III. 4 ci-dessous).

Le marché des protocoles d'échange DeFi se caractérise par des niveaux de concentration importants. 650 protocoles ont été recensés, le top 1 % en terme de TVL (soit 6 protocoles) représentant près de 15 Mds \$USD et 75 % de la TVL totale pour ces activités (estimée à près de 20 Mds \$USD).

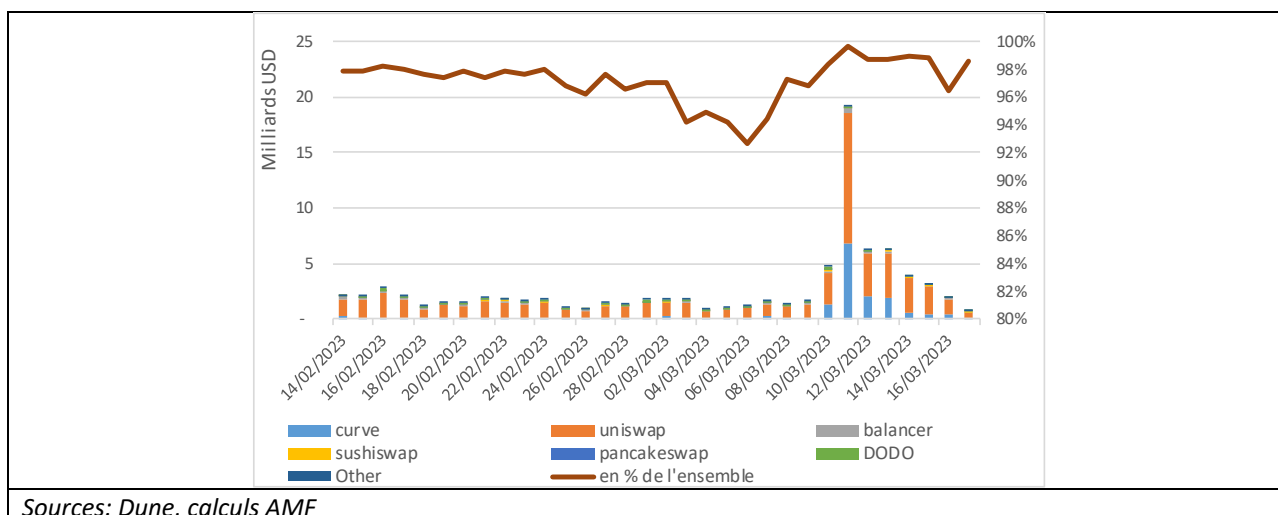
La TVL totale des protocoles d'échange DeFi a fortement diminué depuis fin 2021 (passant de près de 260 Mds \$USD à 200 Mds \$USD début 2022), et a continué à décroître depuis mai 2022 (chutant depuis à un peu moins de 80 Mds \$USD). Le volume mensuel moyen de transactions est actuellement estimé à environ 50 Mds \$USD, un montant trois fois moindre qu'au premier semestre 2022.

Graphique 5 – TVL totale et moyenne mensuelle au sein des protocoles d'échange DeFi



Le volume quotidien moyen enregistré par les protocoles d'échange DeFi s'est récemment stabilisé autour de 2 Mds \$USD alors qu'il fluctuait entre 3 et 5 Mds \$USD début 2022. Un pic notable de volume à hauteur de 19 Mds \$USD a été récemment observé le 11 mars 2023 en raison de l'incertitude récente entourant la perte de corrélation temporaire du *stablecoin* USDC par rapport au dollar. On notera que le volume quotidien moyen au sein des plateformes de négociation de crypto-actifs CeFi était de 52 Mds \$USD en mai 2023³¹. En comparaison, le volume moyen d'échange quotidien constaté sur la plateforme Euronext à elle seule sur la même période représentait 8 Mds \$USD toutes classes d'actifs confondues³².

Graphique 6 – Volume quotidien moyen des 6 protocoles d'échange DeFi principaux (en Md \$USD)



³¹ Lien : "[coingecko.com - Principales plateformes d'échange de crypto monnaies selon le Trust Score](https://www.coingecko.com/fr/principales-plateformes-d-echange-de-crypto-monnaies-selon-le-trust-score)"

³² Lien : "[euronext.com - Statistics](https://www.euronext.com/fr/statistiques)"

2. Similitudes et différences avec les plateformes d'échange centralisées

Les protocoles d'échange DeFi diffèrent des plateformes de négociation centralisées dans la mesure où ces dernières opèrent des modèles de négociation et de règlement qui ont lieu *off-chain*. Tel qu'indiqué ci-dessus, la différence majeure de fonctionnement des protocoles d'échange DeFi, réside dans l'utilisation de *smart contracts* qui permettent l'initiation, la négociation, le règlement et l'enregistrement automatisé des transactions en un seul cycle directement sur la *blockchain*.

Une autre différence majeure est que les protocoles d'échange DeFi permettent aux particuliers d'échanger entre eux de pair-à-pair sans intermédiaire, offrant une forme directe d'accès à un marché, tandis que les plateformes de négociation opèrent un modèle reposant sur une adhésion, où l'accès au marché est fourni via des intermédiaires inscrits auprès de la plateforme en tant que membres. De ce point de vue, les protocoles d'échange DeFi sont plus comparables aux plateformes d'échange de crypto-actifs CeFi, qui, bien qu'elles opèrent des modèles de carnet d'ordres *off-chain*, privilégient également un accès direct des utilisateurs entre eux sans recours à des intermédiaires.

Dans le cas des AMM, un autre facteur de différenciation par rapport aux plateformes centralisées est qu'ils permettent à tout participant de déposer des actifs dans une réserve, leur donnant ainsi la possibilité de devenir un fournisseur de liquidité et d'être rémunérés pour cela. De cette manière, les protocoles d'échange DeFi pourraient permettre un accès plus ouvert à la fourniture de liquidité et aux avantages que cela occasionne, tandis que les plateformes centralisées ont recours à des teneurs de marché ou à des fournisseurs de liquidité professionnels pour jouer ce rôle.

Enfin, en raison de leur nature décentralisée, les protocoles d'échange DeFi adoptent généralement la structure d'une DAO (voir section IV ci-dessous), ce qui permet aux utilisateurs de participer à la gouvernance du protocole. Sauf cas très particulier d'un utilisateur d'une plateforme de négociation CeFi qui en serait également actionnaire, ce modèle est plus rare pour les infrastructures centralisées, alors que les protocoles d'échange DeFi permettent à leurs utilisateurs de jouer un rôle actif dans la gouvernance du protocole (par exemple en votant sur des décisions relatives à la modification du code ou des fonctionnalités du *smart contract*).

Enfin, en TradFi, de nombreuses plateformes de négociation sont soumises à des exigences réglementaires (telles que la directive MiFID II dans l'Union européenne³³), les obligeant à disposer de règles de marché qui sont, sauf certaines exceptions, revues et approuvées par une autorité de marché.

Point de discussion n°5 – Règles de marché d'un protocole d'échange DeFi

Dans le cadre d'une réglementation des activités relatives aux protocoles d'échange DeFi, il pourrait être envisagé que les règles des smart contracts opérés par ces protocoles soient « traduites » dans un langage non technique, permettant leur lecture, leur revue et, le cas échéant, leur approbation par les organismes de régulation afin de garantir la bonne information des participants et le respect des règles édictées par ces protocoles.

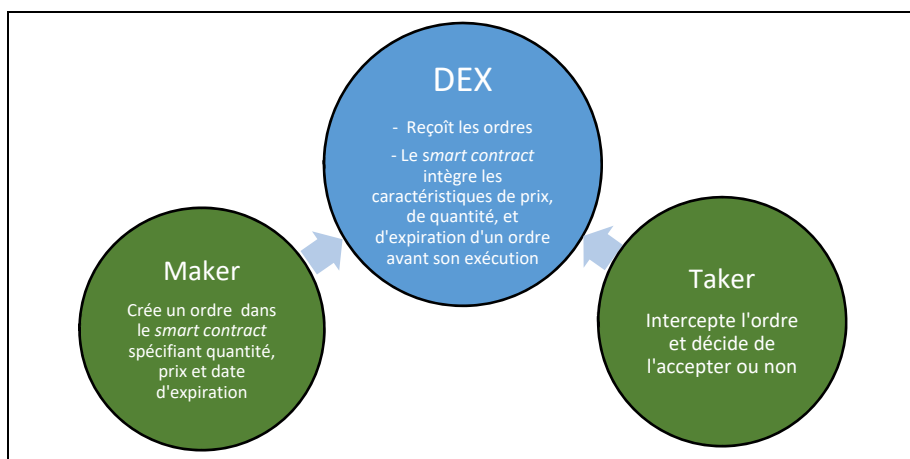
3. Différences entre les modèles d'échanges décentralisés (DEX) et les teneurs de marché automatisés (AMM)

Tel qu'indiqué ci-dessus, il existe deux principaux modèles de protocoles d'échange DeFi : les protocoles d'échange décentralisés (*Decentralised Exchanges* ou DEX) et les teneurs de marché automatisés (*Automated Market Makers* ou AMM). Leur principale différence réside dans la conception du *smart contract* qu'ils opèrent.

³³ Voir article 47 de MiFID II.

Les protocoles d'échange décentralisés³⁴ (DEX) opèrent un modèle de type carnet d'ordres *on-chain*, permettant à un participant teneur de marché (*market maker*) d'envoyer un ordre à un *smart contract*, en spécifiant l'actif à échanger, la valeur d'achat ou de vente souhaitée, ainsi qu'une date d'expiration pour la réalisation de la transaction. Le preneur (*market taker*) peut décider ou non de répondre à cet ordre via le même mécanisme. Bien que la technologie utilisée par ce genre de protocole vise à reproduire les fonctionnalités d'un carnet d'ordres traditionnel, elle présente certaines limites liées aux difficultés qu'un *smart contract* peut rencontrer dans le traitement d'un nombre potentiellement élevé de transactions, les messages informatiques devant être communiqués de manière simultanée à tous les nœuds du réseau, et non à une base de données centralisée. Ce processus peut donner lieu à des difficultés opérationnelles, et peut dans certains cas décourager l'apport de liquidité sur ce type de protocole. En conséquence, la faible liquidité qui en découle peut contribuer à la détérioration des écarts réels de cours entre acheteurs et vendeurs et occasionner des frais élevés de transaction. Pour cette raison, certains protocoles de type DEX offrent parfois une couche supplémentaire de code hors protocole (« *off-chain* ») permettant de fluidifier l'interaction entre l'interface (*DApp*) et le *smart contract* pour minorer ce risque.

Graphique 7 – Échange entre teneur (maker) et preneur (taker) sur un carnet d'ordres DEX

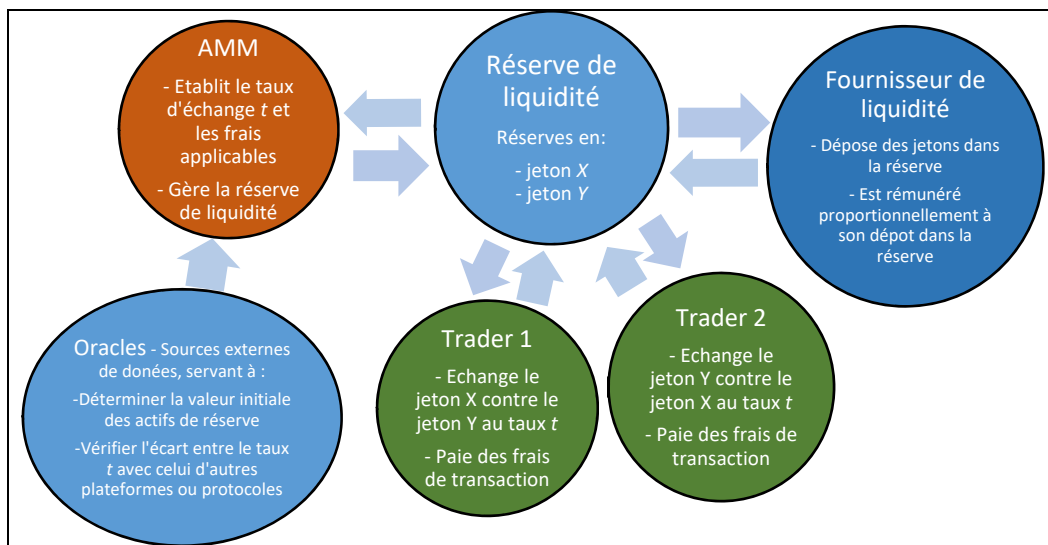


Concernant les **teneurs de marché automatisés (AMM)**, ils permettent également aux utilisateurs d'échanger *on-chain* des crypto-actifs mais à un taux déterminé via un algorithme fonctionnant sur la base d'un modèle d'offre et de demande. L'échange sur l'AMM est permis par l'existence de réserves qui fournissent la liquidité dans les paires proposées. La valeur initiale des actifs déposés dans la réserve est cependant prédéterminée par référence à des « oracles », une source externe de prix, permettant également au *smart contract* de s'assurer que les taux d'échange restent cohérents avec ceux sur d'autres marchés (voir section III. 4 pour plus de détails)³⁵.

³⁴ Également définis comme des DEX opérant un carnet d'ordres (« *Order-book based DEX* »).

³⁵ Bartoletti, M., Chiang, J. H. Y., & Lafuente, A. L. (2021). SoK: lending pools in decentralized finance. In *Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers 25* (pp. 553-578). Springer Berlin Heidelberg.

Graphique 8 – Échange sur un protocole de type AMM



Comme indiqué ci-dessus, le développement de protocoles de type DEX peut présenter certaines difficultés en raison des coûts importants occasionnés pour répliquer le modèle d'un carnet d'ordres sur la *blockchain*. En conséquence, les frais d'opération (*gas fees*) des *smart contracts* sur un protocole de type DEX tendent à être plus élevés que ceux qui sont généralement relevés sur les protocoles de type AMM. En raison des limites présentées par les DEX, les AMM sont donc plus répandus parmi les protocoles d'échange DeFi³⁶, et les deux dénominations (DEX ou AMM) sont parfois utilisées alternativement et à tort pour définir ces deux types de protocoles.

Ce manque de clarté peut contraster avec les activités observées en TradFi, où les rôles des intervenants et la fonction des plateformes sont plus clairement définis.

A noter que des organismes internationaux comme l'Organisation internationale des commissions de valeurs (OICV) et le Conseil de stabilité financière (FSB) ont indiqué à ce sujet que certains critères pourraient être utilisés afin de distinguer les AMM des DEX entre eux^{37, 38}, notamment qu'un DEX peut contenir un élément de carnet d'ordres *off-chain* (comme la couche supplémentaire de code hors protocole décrite ci-dessus), alors que les opérations d'un AMM sont considérées être entièrement *on-chain*.

Point de discussion n°6 – Définitions des DEX et des AMM

- L'intégration ou non d'un élément *off-chain* dans un protocole de DeFi apparaît essentielle pour en caractériser la nature. On constate dans certains cas que l'intégration d'un tel élément *off-chain* dans un protocole de DeFi rapproche ce modèle de celui d'une plateforme de négociation CeFi dans le sens où cet élément centralise l'opération. Pour concevoir la réglementation des plateformes de négociation DeFi, il apparaît dès lors essentiel de clarifier la distinction entre un protocole d'échange DeFi, qui opérerait uniquement *on-chain*, et un protocole qui intègre une composante *off-chain*.
- En considérant la manière dont un DEX et un AMM peuvent différer, il apparaît également nécessaire d'identifier la nature du mécanisme utilisé dans le cadre de la formation des prix. Par exemple, un élément pourrait être de comprendre si le protocole d'échange DeFi utilise un modèle de formation de prix qui se fonde sur la valorisation d'actifs au sein de réserves (*liquidity pools*), ou un processus de formation de prix fondé sur un modèle de carnet d'ordres *on-chain*.

³⁶ Parmi les 10 protocoles d'échanges DeFi enregistrant le plus grand volume de transactions au mois de mars 2023, le volume d'échange sur les AMM représente 98 % du total des volumes (source: DeFiLlama, calculs AMF).

³⁷ Lien : "iosco.org - IOSCO Decentralised Finance Report (March 2022)"

³⁸ Lien : "fsb.org - The Financial Stability Risks of Decentralised Finance (16 February 2023)"

4. Risques engendrés par les protocoles d'échange DeFi

Certains risques observés sur les protocoles d'échange DeFi sont comparables à ceux constatés au sein des plateformes de négociation centralisées, mais d'autres sont inédits ou émergents en raison de la nature spécifique des modèles de finance décentralisée. Cette section fournit un aperçu des principaux risques liés aux activités des protocoles d'échange DeFi. Il convient de noter que les risques globalement observés à l'échelle de DeFi ne sont donc pas détaillés ici.

<p>Risques lié aux marchés non réglementés et régulés</p>	<p>Les protocoles d'échange DeFi ne relevant d'aucune réglementation, ils sont par conséquent plus fortement exposés à un risque potentiellement élevé d'activités illicites, notamment en termes d'abus de marché, de risque de manipulation de cours ou de fraude, ou d'activité illicites de blanchiment d'argent.</p> <p>Par ailleurs, pour les utilisateurs (en particulier ceux qui ne sont pas experts en protocoles <i>blockchain</i>), les protocoles d'échange DeFi peuvent être complexes à comprendre et à appréhender. La technologie employée et le manque de clarté des codes informatiques peuvent être des facteurs aggravants d'erreurs et de placement incorrects et non désirés pour les utilisateurs. Cela peut augmenter les risques pris par les participants (notamment en terme de pertes potentielles), étant précisé que ces risques sont rarement communiqués par les plateformes.</p>
<p>Risques de liquidité et de négociation équitable et ordonnée</p>	<p>Un risque significatif de liquidité peut être observé sur certains protocoles d'échange DeFi, ce qui peut en conséquence engendrer des situations de négociation inéquitables et désordonnées sur ces marchés. Au sein de ces protocoles, la liquidité dépend en effet fortement du nombre de participants : un échange réalisé dans un volume important (au sein d'un AMM par exemple) peut avoir un impact immédiat et significatif sur le taux d'échange constaté et influencer l'exécution d'autres ordres au sein du <i>smart contract</i>.</p> <p>Par ailleurs, dans le cas d'un AMM, lorsqu'un apporteur de liquidité décide de retirer ses crypto-actifs de la réserve de liquidité, cela peut affecter directement la valeur relative des actifs déposés dans cette réserve, engendrant une irrégularité de prix qui peut se maintenir dans le temps en l'absence d'un apport supplémentaire de liquidité. Des phénomènes de panique (<i>bank run</i>) peuvent ainsi en résulter et amplifier l'ampleur des irrégularités. En conséquence, dans le cas où les valeurs de crypto-actifs au sein d'une réserve divergeraient durablement entre elles, les fournisseurs de liquidité peuvent subir des pertes importantes au regard des cours constatés sur d'autres marchés.</p>
<p>Risques liés au modèle de valorisation</p>	<p>Alors que les « oracles » peuvent être utilisés pour corriger des divergences potentielles de valorisation des crypto-actifs au sein des protocoles d'échange DeFi, leur utilisation soulève des questions quant à la solidité du modèle de valorisation proposé par ces protocoles. Par ailleurs, la source des données utilisées par certains « oracles » n'est pas toujours clairement communiquée et peut ainsi fausser les cours des actifs contenus dans les réserves de liquidité.</p>

<p>Risques de manipulation des prix et de front running</p>	<p>Le recours à des « oracles » peut conduire à une manipulation potentielle des prix dans les protocoles, les données issues du marché cible de « l’oracle » – hors protocole – pouvant elles-mêmes être altérées.</p> <p>Egalement, les utilisateurs d’un protocole d’échange DeFi peuvent être exposés à un risque de manipulation de prix en raison de l’exécution des transactions, qui nécessite une validation par les nœuds du réseau. Ainsi, au moment de la soumission d’un ordre de transaction, le délai de règlement de la transaction n’est pas connu par l’utilisateur et, lors de la transmission aux nœuds du réseau, la transaction devient publique sur la <i>blockchain</i> avant qu’elle ne soit réglée. Ce décalage ouvre la porte à de potentiels acteurs malveillants, qui peuvent, dans l’intervalle, soumettre leurs propres ordres de transaction pour tirer bénéfice d’un ordre déjà placé – mais pas encore réglé – ce qui pourrait avoir une influence significative sur le cours constaté dans le protocole³⁹.</p> <p>Les attaques de ce type menées par les acteurs malveillants sont communément surnommées <i>sandwich attacks</i>, car un ordre placé peut se retrouver entre des ordres placés par un acteur malveillant à cet effet⁴⁰.</p>
<p>Risque de glissement de valeur (<i>slippage risk</i>)</p>	<p>Le risque de glissement de valeur (<i>slippage risk</i>) est un risque relevé sur certains protocoles d’échange DeFi, qui résulte du décalage entre le moment où un ordre est placé au sein d’un <i>smart contract</i> et le moment de règlement sur la <i>blockchain</i>. Ce décalage peut entraîner des variations importantes entre le prix désiré par l’utilisateur et le prix effectif d’exécution et donc un risque de pertes importantes qui peuvent en résulter.</p> <p>En pratique, lorsqu’ils négocient sur un protocole d’échange DeFi, les participants peuvent être amenés à spécifier un niveau de « tolérance de glissement » maximal (<i>slippage tolerance</i>), soit la variation maximale de prix qu’ils sont prêts à accepter entre le placement et l’exécution. Cependant, de tels niveaux de tolérance ne sont pas toujours indiqués ou prévus.</p>
<p>Risques liés aux effets de levier</p>	<p>Des effets de levier importants peuvent exister sur les protocoles d’échange DeFi, en particulier lorsque ces derniers sont interconnectés avec des protocoles de prêt ou avec ceux offrant des produits dérivés. Bien que les activités de prêt sur les protocoles DeFi soient généralement sur-collatéralisées, les montants empruntés dans ces protocoles peuvent être réutilisés comme garantie dans des transactions sur des protocoles d’échange (incluant potentiellement des produits dérivés sur crypto-actifs), engendrant des fluctuations très importantes des positions et un risque de perte très significatif.</p> <p>Comme relevé par la Banque des règlements internationaux (BRI)⁴¹, contrairement aux opérations réalisées en TradFi, les opérations réalisées en DeFi ne bénéficient pas d’intermédiaires pouvant amortir les chocs et toute contagion résultant d’une activité de marché incluant de forts effets de levier peut ainsi potentiellement être fatale à un protocole d’échange DeFi.</p>
<p>Risques de gouvernance</p>	<p>Au regard des risques indiqués ci-dessus liés à la manipulation des prix et au <i>front-running</i>, la structure de gouvernance décentralisée peut engendrer des situations dans lesquelles des acteurs malveillants peuvent prendre le contrôle du protocole et réaliser des gains sur la base d’ordres de transactions observés par les utilisateurs du protocole avant que les transactions correspondantes ne soient enregistrées sur la <i>blockchain</i>.</p>

³⁹ Lien : "[bis.org - DeFi risks and the decentralisation illusion](#)"

⁴⁰ Lien : "[arxiv.org - SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance](#)"

⁴¹ Lien : "[bis.org - DeFi risks and the decentralisation illusion](#)"

IV) Gouvernance de protocoles : organisations autonomes décentralisées (DAO) et jetons de gouvernance

1. Les organisations autonomes décentralisées (DAO)

Le concept d'organisation autonome décentralisée (*Decentralised Autonomous Organisation* ou DAO) a été initié pour la première fois en 2014 par Vitalik Buterin, le fondateur du protocole Ethereum, qui l'a décrit comme une « *entité vivant sur internet et existant de manière autonome, mais s'appuyant également fortement sur des individus pour effectuer certaines tâches que l'automate ne peut accomplir* »⁴². Au contexte de la DeFi, les DAO représentent une forme d'organisation ayant pour fonction d'organiser la gouvernance d'un projet en réunissant les différentes parties prenantes d'un protocole (comme les utilisateurs, les développeurs ou les investisseurs). Sous cette structure, ces acteurs peuvent s'organiser pour effectuer des tâches en lien avec l'utilisation et le développement du protocole, y compris concernant les décisions relatives à sa gouvernance. Les caractéristiques et les règles de fonctionnement de ces DAO sont prévues au sein d'un *smart contract*.

Les DAO sont des organisations non définies juridiquement qui permettent de réunir une communauté de personnes, chacune disposant de droit de décision sur la gestion d'un protocole sous-jacent. Ces décisions sont prises sur la base de droits de vote matérialisés par la détention et l'exercice de jetons de gouvernance (voir section 2 ci-dessous). Alors qu'un protocole compte des utilisateurs qui participent à sa vie économique, une DAO est composée de membres qui participent à sa gouvernance. En pratique, on constate généralement que les utilisateurs d'un protocole sont très souvent également membres de la DAO qui l'organise, dans la mesure où les utilisateurs peuvent être rémunérés par le protocole en jetons de gouvernance, ouvrant un droit de vote dans le cadre de la DAO.

Les votes des membres d'une DAO servent à prendre des décisions importantes pour l'organisation d'un protocole et à déterminer ses orientations. Les membres d'une DAO peuvent ainsi voter sur des propositions concernant des questions de développement d'une nouvelle activité, l'intégration de nouveaux types de jetons, ainsi que sur tout type d'actes de gestion et de modifications des règles de gouvernance elles-mêmes.

Une DAO est organisée à l'image d'un protocole DeFi dans le sens où elle peut également être considérée comme décentralisée, ses règles sont inscrites sur la *blockchain* et ses membres sont répartis sur le réseau et participent individuellement à la gouvernance des protocoles, sans entité permettant une gestion centralisée. Le vote des membres est ainsi effectué directement *on-chain*, ce qui permet de garantir l'immuabilité et la transparence du processus de vote. Les résultats du vote sont enregistrés sur la *blockchain* et sont accessibles publiquement pour permettre à tous les membres de l'organisation de les vérifier.

Les développeurs d'un protocole DeFi ont un rôle clé dans une DAO. Ces développeurs sont souvent à l'origine de la création du protocole et de sa mise en place sur la *blockchain*. Ils sont généralement les membres fondateurs de la DAO associée et, par la suite, travaillent en étroite collaboration avec les membres de l'organisation pour proposer des améliorations et des mises à jour du protocole, lesquelles sont ensuite votées par la communauté. Les membres des DAO peuvent soumettre des propositions de changements, qui sont ensuite examinées et débattues entre les développeurs et les membres. Si une proposition est acceptée, les développeurs travaillent ensuite à l'implémentation du changement de code sur le protocole. Les développeurs jouent également un rôle crucial dans la sécurité et la stabilité du protocole. Ils sont responsables de l'identification et de la résolution de tout problème ou bug qui pourrait affecter la sécurité ou le bon fonctionnement du protocole, et en alertent le cas échéant les membres de la DAO en étant force de proposition.

Plus généralement, il sera noté qu'une DAO fait référence à une forme d'organisation plutôt qu'à un type d'activité économique, de nombreuses activités pouvant ainsi être gouvernées sous un modèle de DAO.

⁴² Lien : "[blog.ethereum.org - DAOs, DACs, DAs and More: An Incomplete Terminology Guide](https://blog.ethereum.org/2014/07/14/dacs-das-and-more-an-incomplete-terminology-guide/)"

Au-delà des DAO de protocoles DeFi, certaines DAO peuvent être créées à des fins d'investissement (des membres pouvant mettre leurs fonds en commun en vue d'investir dans des projets), à des fins philanthropiques ou caritatives (par exemple pour l'attribution de subventions ou dans un but d'animation d'activités non lucratives), et peuvent avoir un objet purement « social », en rassemblant des membres partageant des idées ou des vues communes. Fin 2022, selon certaines estimations, le nombre de DAO en activité dépasseraient les 5 000⁴³.

2. Les jetons de gouvernance

Dans le cas d'un protocole DeFi, les membres d'une DAO reçoivent généralement un jeton créé par le protocole sous-jacent. Ces jetons, qui représentent un droit lié à la gouvernance ou à la prise de décisions sur le fonctionnement d'un protocole, sont appelés « jetons de gouvernance ». Dans certains cas, ces jetons peuvent également représenter une rémunération pour les utilisateurs qui utilisent le protocole.

Les jetons de gouvernance peuvent être acquis à l'achat, via leur distribution initiale lors de la constitution du protocole, ou en échange de travaux ou de services rendus pour le protocole (les développeurs d'un protocole DeFi peuvent par exemple obtenir des jetons de gouvernance en échange de leur travail de développement informatique). Au cas particulier des protocoles d'échange DeFi, les jetons de gouvernance peuvent également être versés aux apporteurs de liquidités, servant de rémunération et incitant ainsi les utilisateurs à déposer leurs crypto-actifs dans les réserves de liquidités.

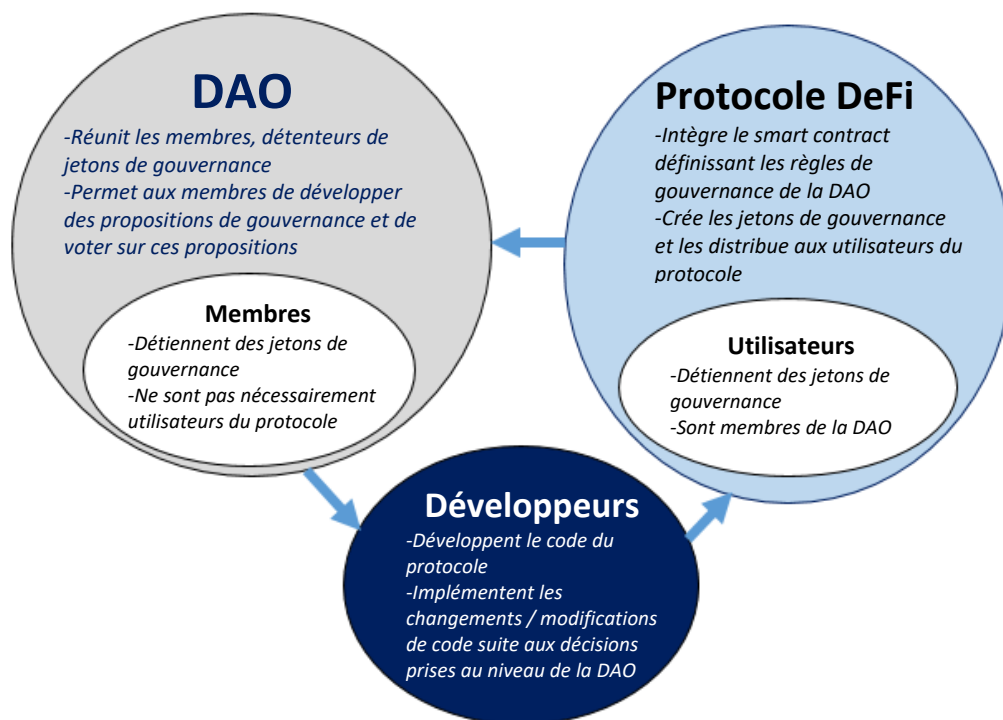
Au sein des DAO de protocole DeFi, ces jetons sont utilisés pour prendre part aux votes sur la gouvernance des protocoles⁴⁴. Selon les cas, les mécanismes de vote montrent quelques similarités et différences si on les compare aux actions émises par les entités juridiques traditionnelles. Par exemple, sur le modèle d'une assemblée générale, certaines DAO requièrent un quorum minimal pour qu'un vote soit pris en compte, ou présentent des conditions de majorité simple ou qualifiée pour que le vote soit effectif. D'autres conditions, comme le vote « quadratique » ou de « conviction », introduisent de nouvelles variables, en permettant une forme de pondération permettant aux plus petits détenteurs d'être reconnus de manière plus équitable face aux détenteurs disposant de positions importantes de vote, ou, dans d'autres cas, attribuant plus de valeur aux votes constants et inchangés dans le temps. Enfin, des mécanismes tels que la « multi-signature » ou des formes de vote par procuration permettent de déléguer son vote, soit à d'autres membres au sein de la DAO (par exemple à un collège de membres désignés), soit à des personnes ou organisations en dehors de la DAO.

Alors que les jetons de gouvernance sont spécifiquement émis pour permettre leur utilisation dans le cadre d'une DAO, ils peuvent aussi être librement échangés sur les protocoles d'échange DeFi ou CeFi, leur conférant un caractère spéculatif comme d'autres crypto-actifs. Ainsi, en théorie, quiconque peut acquérir des jetons de gouvernance et devenir membre d'une DAO et un détenteur peut se retrouver en situation d'influer sur la gouvernance d'un protocole sans en être utilisateur.

⁴³ Lien : ["bitkan.com - How many DAOs are there in the world?"](https://bitkan.com)

⁴⁴ Lien : ["medium.com - Voting Options in DAOs"](https://medium.com)

Graphique 9 – Relation entre une DAO, un protocole et les développeurs du protocole



3. Risques liés aux DAO de protocoles et à la gouvernance des protocoles DeFi

3.1. Risques liés à l'incertitude légale des DAO et au modèle économique

Une DAO est une organisation dont la forme juridique est, dans la plupart des juridictions⁴⁵, non définie. On constate en outre qu'une DAO peut parfois être associée à une « société sœur », elle-même structurée juridiquement en société anonyme ou en association. Via le mécanisme de jetons de gouvernance, cette société sœur peut parfois influencer fortement sur le contrôle de la DAO.

La responsabilité juridique de la structure et des différentes parties prenantes peut donc fortement varier suivant le mode organisationnel adopté. En outre, alors que certaines DAO fonctionnent comme des organisations à but non lucratif, d'autres peuvent être structurées dans une perspective de profits et percevoir les frais liés à l'activité du protocole qu'elles régissent, voire détenir en réserve des fonds dont elles peuvent disposer comme un acteur économique traditionnel. Les DAO impliquent donc diverses formes d'incitation économique pour leurs parties prenantes, ce qui engendre une variété de risques à considérer selon le mode de fonctionnement adopté. En conséquence, et en l'absence de clarifications juridiques, les membres de ces organisations ne disposent pas des moyens légaux traditionnels permettant de les protéger.

De plus, on notera que la localisation des membres d'une DAO, et *a fortiori* de la DAO elle-même, est difficile à percevoir en raison de l'organisation par nature décentralisée d'une telle structure. Du fait de leur anonymat (ou « pseudonymat », voir ci-dessous), les membres peuvent agir masqués et l'absence de rattachement territorial à une juridiction crée une source d'incertitude quant aux droits qui leur sont applicables.

⁴⁵ A ce jour, certaines juridictions ont travaillé au développement de cadres juridiques fournissant une définition légale des DAO, notamment aux Etats-Unis (au Delaware, en Utah, au Vermont et au Wyoming), ainsi qu'en Suisse, à Jersey, à Guernesey ou encore au Royaume-Uni.

Ceci pose une difficulté notable pour les législateurs qui souhaiteraient encadrer ces organisations afin d'apporter davantage de protection à leurs membres et permettre le développement de ces structures dans un cadre sécurisé.

En France, des travaux sont actuellement menés par le Haut comité juridique de Place (HCJP), qui étudie en détail les modes de structuration et de gouvernance des DAO et leurs différentes typologies, dans la perspective de clarifications quant au cadre juridique qui pourrait s'appliquer à ces structures.

3.2. Risques de « pseudonymat » et de gouvernance

L'identité des intervenants sur la *blockchain* étant par nature masquée par un pseudonyme, la difficulté d'identification des utilisateurs constitue un risque majeur de responsabilité des parties prenantes. Plus précisément, étant donné que la *blockchain* permet l'enregistrement de certains identifiants de données (tels que les adresses des portefeuilles ou les références des transactions), les données qu'elle capture sont considérées comme « pseudonymisées »⁴⁶, c'est-à-dire qu'on ne peut pas les rattacher directement à un individu déterminé. Ceci engendre des difficultés d'identification des responsables – notamment concernant l'évaluation de leur compétence et honorabilité –, de la provenance et la destination des fonds qui transitent dans les protocoles, et accroît ainsi le risque de blanchiment induit par l'échange de ces capitaux.

Exacerbé par cette situation de « pseudonymat », le risque de gouvernance lié à la structure de la DAO apparaît dès lors significatif, du fait de la difficulté d'identification des parties contrôlant la DAO, lesquelles peuvent se regrouper et agir de concert en masquant leurs intentions, augmentant de fait les risques de collusion et de conflits d'intérêts.

Enfin, le pseudonymat des intervenants peut rendre difficile, voire impossible, toute forme de poursuite par les autorités à leur encontre, ce qui pourrait inciter des acteurs malveillants à prendre une part active à l'organisation d'une DAO.

Il convient de noter cependant que le pseudonymat est une caractéristique intrinsèque aux protocoles *blockchain* non permissionnés. Dès lors qu'une *blockchain* est permissionnée (voir point de discussion n°1 ci-dessus), le protocole sous-jacent peut alors mettre en place des exigences spécifiques permettant de minorer les risques mentionnés.

3.3. Niveau de décentralisation et de degré de contrôle

Une difficulté relevée au sujet des DAO est d'évaluer le degré effectif de contrôle qu'exercent les acteurs sur leur gouvernance. Un acteur ou un groupe d'acteurs agissant de concert peuvent de fait contrôler une DAO et le protocole associé, ramenant ainsi l'organisation à un mode de gouvernance centralisé.

En fonction de la configuration d'une DAO et de l'implication des développeurs (qui peuvent, selon les cas, détenir une part significative des jetons de gouvernance), ce niveau de décentralisation peut fortement varier.

En pratique, le niveau de décentralisation varie fortement d'une DAO à une autre. Une étude montre des écarts de contrôle très importants, avec certaines structures où 90 % des votes sont détenus par 1 % des membres, tandis que d'autres affichent un degré de répartition plus équitables entre les utilisateurs⁴⁷.

⁴⁶ Lien : europa.eu - Decentralized finance: Information frictions and public policies : approaching the regulation and supervision of decentralized finance"

⁴⁷ Lien : blog.chainalysis.com - Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated"

Point de discussion n°7 – Niveau de décentralisation et degré de contrôle

Le niveau de décentralisation réel de la gouvernance d'une DAO est un aspect clé à prendre en compte pour déterminer le contrôle effectif exercé sur la gouvernance d'une DAO et donc sur son protocole DeFi sous-jacent.

En particulier, l'estimation du niveau de détention de jetons de gouvernance par les développeurs en charge du code et de la gestion des protocoles se révèle être un enjeu clé pour déterminer si un protocole est effectivement contrôlé, et, dès lors, si ce protocole est de facto contrôlé par un individu ou un groupe d'individus. Dans certains cas, il ne peut être exclu que ce contrôle soit exercé par des personnes tierces, sans lien direct avec l'utilisation et la gestion effective du protocole.

A l'image des organisations et entités traditionnelles, le contrôle d'une DAO peut reposer sur des éléments factuels et induire une situation de contrôle « de fait » s'il existe un individu ou un groupe d'individus avec un niveau élevé de détention (sans majorité) et que les autres détenteurs sont disséminés ; ou une situation de contrôle « de droit » si un individu ou un groupe d'individus détiennent au moins la majorité des jetons de gouvernance.

Conclusion

A travers la publication de ce papier, l'Autorité des marchés financiers (AMF) souhaite partager ses premières réflexions sur le sujet de la finance décentralisée, notamment en définissant ce qui constitue l'écosystème de la finance décentralisée et les tendances constatées de son marché, en explorant certaines thématiques spécifiques dont les protocoles d'échange décentralisés et les enjeux de gouvernance, et en soulevant certaines problématiques réglementaires et des points de discussion.

L'émergence de ces mécanismes et la chute de l'écosystème Terra / Luna en mai 2022 soulèvent des questions quant à la maturité et la viabilité de certains protocoles DeFi. Une telle crise a mis en lumière un manque de clarté dans ces processus et le besoin d'un encadrement qui aurait pu permettre une meilleure information et protection des utilisateurs, tout en assurant un développement sécurisé et propice à l'innovation.

La finance décentralisée est encore à un stade précoce de son développement, mais évolue aussi de manière rapide. Par conséquent, la mise en place d'un cadre réglementaire devra être réalisé de manière progressive et proportionnée, tenant compte d'une part des innovations apportées par les activités de la DeFi et leur mode d'organisation et, de l'autre, des risques encourus par ses utilisateurs.

Dans la définition d'un cadre réglementaire, l'approche générale « même activité, même risque, même réglementation » devrait être appliquée sans ambiguïté, en prenant en compte les aspects émergents induits par ces activités nouvelles. La DeFi présente notamment un certain nombre de risques – au-delà de ceux détaillés dans ce papier –, sur lesquels les régulateurs devront se prononcer, notamment concernant la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) ou la connaissance du client (KYC), qui découlent principalement des problématiques de pseudonymat mentionnées en section IV.

L'AMF soutient par ailleurs le développement d'une approche réglementaire coordonnée de la DeFi, compte tenu notamment de la nature transfrontière de ses activités, afin de permettre l'émergence d'un « terrain de jeu égal » (*level playing field*) propice au développement de l'innovation et à la protection des investisseurs.

Dans ce contexte, les prochaines années s'avèreront cruciales pour la DeFi, avec un double enjeu : construire des mécanismes sécurisés et transparents pour permettre le développement de l'écosystème et assurer une meilleure protection des investisseurs.

En France, l'Autorité de contrôle prudentiel et de résolution (ACPR) a publié un papier de consultation développant des pistes de réflexion réglementaire pour la DeFi⁴⁸. Au niveau européen, la Commission européenne devra établir, après l'entrée en vigueur du règlement sur les Marchés de crypto-actifs (MiCA), une évaluation du développement de la finance décentralisée et du traitement réglementaire adéquat des systèmes de crypto-actifs décentralisés. Aussi, les travaux des organismes internationaux (OICV-IOSCO⁴⁹ et FSB⁵⁰) permettront de clarifier les enjeux de la régulation de la DeFi en y apportant des pistes réglementaires.

L'AMF s'associe d'ores et déjà à ces initiatives et entend accroître ses échanges avec les parties prenantes, publiques et privées, afin de permettre l'émergence d'un cadre réglementaire équilibré propice au développement de la finance décentralisée.

⁴⁸ [Lien : "ACPR - Finance « décentralisée » ou « désintermédiée » : quelle réponse réglementaire ?"](#)

⁴⁹ [Lien : "iosco.org - IOSCO Decentralised Finance Report \(March 2022\)"](https://iosco.org)

⁵⁰ [Lien : "fsb.org - The Financial Stability Risks of Decentralised Finance \(16 February 2023\)"](#)