NEXIALOG CONSULTING

DeFi 101

LE GUIDE DE LA FINANCE DÉCENTRALISÉE

2024

GINESTE PIERRE
JACQUET ANTOINE
NEKMOUCHE REDA

Finance Innovation

TABLE DES MATIERES

INTRODUCTION

La finance décentralisée, ou DeFi, est une évolution technologique émergente qui se développe sur la base des infrastructures de blockchains publiques. Elle vise à répliquer le fonctionnement du système financier traditionnel au sein d'un environnement décentralisé, donc sans tiers de confiance, ouvert et automatisé à l'aide des fameux « smart contracts ».

Son potentiel disruptif est majeur et laisse entrevoir la possibilité d'une finance désintermédiée, démocratisée et ouverte sur le monde, substituant le code à la confiance entre humains et institutions et améliorant grandement l'efficacité globale de notre système financier.

Cette vision utopique est néanmoins encore lointaine, et de nombreux risques et obstacles, tant endogènes qu'exogènes, peuvent entraver le développement de cet écosystème naissant.

Ce document se penche sur l'univers fascinant de la DeFi, en explorant ses composantes clés : les différentes couches technologiques sur lesquelles il repose ainsi que les stablecoins et les protocoles d'échange et de prêts décentralisés.

Il aborde ensuite les différentes innovations en termes de produits dérivés et structurés qui y sont développés, ainsi que les surcouches d'agrégation, véritables brokers et portfolio managers de la DeFi.

S'ensuit un tour d'horizon des différents risques qu'il comporte, ainsi que des réglementations naissantes qui l'entourent.

Enfin, le document se penche sur les multiples initiatives lancées par des acteurs institutionnels de la finance traditionnelle pour tenter de s'approprier les bénéfices technologiques induits par cette innovation, ou bien d'y prendre part directement, permettant d'envisager à l'avenir une hybridation des deux mondes.

Nous avons fait le choix de centrer cette étude sur l'écosystème développé sur la blockchain Ethereum, la plus importante en termes d'utilisation et de valeur échangée, et sur laquelle ont été conçues la majorité des innovations majeures de la DeFi. Nous avons également tenté de sélectionner majoritairement les protocoles les plus décentralisés, au sens d'absence de tiers de confiance, sur lesquels les utilisateurs gardent le contrôle de leurs fonds et qui limitent drastiquement toute intervention humaine dans leur fonctionnement.

Le mot de Cyril Armange,
Directeur Général adjoint de Finance Innovation

Un emballement, une énième bulle spéculative ? Quoiqu'on en dise, c'est la plus visible des disruptions : la « DeFi », ou finance décentralisée représente une modernisation majeure et ouvre un nouvel horizon au secteur de la finance. Stricto sensu, la finance décentralisée est héritière des caractéristiques propres aux propriétés des blockchains :

- La DeFi est un système nativement numérique et fonctionne sans organe de contrôle grâce à la technologie de la blockchain et des smart contracts. Les opérations sont donc effectuées de pair-à-pair ;
- Un système financier résilient du fait de sa nature décentralisée et distribuée ;
- Un système public et ouvert à tous. Ce système financier est ouvert à tous, aussi bien en termes d'usage, de consultation que de participation à sa construction.
- Interopérable : la finance décentralisée se compose de nombreux protocoles informatiques qui ont vocation à fonctionner ensemble via l'utilisation de « bridges ». (Un bridge est un protocole informatique permettant de rendre interopérable deux blockchains différentes afin de permettre la circulation de tokens entre celles-ci).
- Programmable : via l'utilisation des smart contracts, la volonté des parties est exécutée automatiquement lorsque les conditions déterminées par les cocontractants sont remplies.

La finance décentralisée se distingue donc du système financier traditionnel car nativement numérique (les services financiers sont basés sur les mathématiques et la programmation), fonctionnant sur des infrastructures décentralisées (Dapps) et ouvert à tous (y compris aux populations exclues du système financier traditionnel) aussi bien en termes d'usage, de consultation que de participation à sa construction. Dès lors, la confiance dans les tiers (banques, assurances) disparaît au profit de la confiance dans la fiabilité et la sécurité d'un protocole informatique décentralisé, infalsifiable et immuable.

Très rapidement, la finance décentralisée fut, également, appréhendée comme une réponse innovante pour renforcer l'inclusion financière, celle-ci étant le pendant direct de l'inclusion sociale. Si le taux de bancarisation moyen est estimé à plus de 80% en Europe, ce taux est largement inférieur dans de nombreuses zones géographiques.

Le phénomène d'exclusion bancaire est engendré par l'exclusion sociale et la pauvreté d'autant qu'il en résulte. Très souvent, les populations subissent le coût trop élevé des services financiers, un éloignement géographique important des établissements bancaires, et le manque de documents officiels. La finance décentralisée adresse ces problématiques en permettant aux particuliers d'avoir accès à des services financiers 24h/24, en restant souverains de leurs fonds.

Toute personne ayant un accès à Internet peut prétendre accéder à ces services : aucune barrière à l'entrée (conditions de ressources ou de nationalité) ne peut être imposée.

L'accès à la finance décentralisée est toutefois conditionné à la création d'un portefeuille de crypto-actifs (en anglais wallet) par l'utilisateur. Un wallet est à la crypto-monnaie ce qu'un compte bancaire est à la monnaie fiduciaire.

Les acteurs institutionnels s'emparent du sujet avec la volonté d'expérimenter, d'inventer, d'innover et de créer de nouveaux produits financiers et les usages financiers de demain; usages qui étaient encore impensés et/ou impossibles jusqu'à présent.

Néanmoins, l'innovation reste du côté des start-ups et des développeurs indépendants. Tous ces protocoles et ces services sur blockchains peuvent se combiner, s'enrichir mutuellement afin de répondre à des besoins spécifiques : échange d'actifs numériques, usage d'actifs numériques stables, prêts, produits dérivés, etc.

Risques et Complexités

A l'image de toute innovation, la finance décentralisée est vectrice de risques nouveaux. Premièrement, le risque est technologique : les smart contracts ne sont pas exempts de failles de sécurité. En présence d'une faille dans un protocole décentralisé, un agent malveillant pourrait parvenir à siphonner les fonds.

Par ailleurs, le risque est structurel : les protocoles décentralisés peuvent présenter un risque d'instabilité, trouvant leur origine dans une gouvernance désorganisée ou des réserves de liquidités trop peu importantes. Dernièrement, le risque est financier : la volatilité du marché des crypto-actifs ainsi que le recours aux effets de leviers sont susceptibles d'engendrer d'importants risques de perte en capitaux pour les utilisateurs.

Si cet écosystème prometteur constitue une alternative aux produits du secteur bancaire et financier traditionnel, son adoption massive dépendra de la vulgarisation auprès du grand public des technologies complexes qui le composent.

Sur le papier, il suffit, en effet, de posséder des cryptos et un smartphone pour se lancer. Pourtant, le jargon (DEX, Dapps, Oracles, Smart Contracts…) et l'univers de la DeFi nécessitent un temps d'adaptation. De même, les interfaces demeurent techniques, même si quelques acteurs proposent aujourd'hui des surcouches user friendly.

Ecosystème naissant

L'émergence de la finance décentralisée a introduit une nouvelle ère dans l'industrie financière, autorités de régulation et banques changent de mentalité, en offrant une alternative accessible, transparente et décentralisée pour les transactions financières. Tokens, crypto-actifs, et protocoles décentralisés sont bel et bien en train de changer la donne. La finance de demain se construit sous nos yeux …et elle sera bâtie sur des blockchains mais surtout sur les nombreux talents et avantages comparatifs dont la France dispose.

La finance décentralisée se distingue donc du système financier traditionnel car nativement numérique, fonctionnant sur des infrastructures décentralisées et ouvert à tous aussi bien en termes d'usage, de consultation que de participation à sa construction.

1 BASE TECHNOLOGIQUE DE LA DeFi

La finance décentralisée repose sur différentes couches technologiques dont l'ensemble est souvent qualifié de "DeFi Stack"

Une blockchain et son crypto-actif natif :

Une blockchain est un registre, assimilable à une base de données, partagé simultanément à ses utilisateurs. Ces derniers ont la possibilité d'y inscrire des données selon des règles spécifiques fixées par un protocole informatique pair-à-pair sécurisé via des méthodes cryptographiques. Il existe des blockchains publiques, ouvertes à tous, et des blockchains privées dont l'accès peut être restreint. Dans le cas d'une blockchain publique, cette base de données est transparente, pseudonyme (chaque utilisateur possède une ou plusieurs clés publiques) et infalsifiable. Elle a de plus la particularité de fonctionner sans organe central de contrôle. Ce registre distribué sert de « grand livre comptable » pour l'enregistrement de transactions. La première et plus célèbre des blockchains est Bitcoin. Cependant, de nombreux réseaux « concurrents » ont été développés, offrant des fonctionnalités supplémentaires tels que les contrats intelligents « smart contracts », qui ont servi de base au développement de la finance décentralisée.

Nous faisons le choix dans cette note de nous focaliser sur la blockchain Ethereum sur laquelle sont bâtis les principaux protocoles DeFi. Cependant, de nombreuses alternatives existent (Avalanche, Polkadot, etc…) ainsi que des surcouches d'Ethereum (layers 2 tels que Arbitrum, Polygon ou Optimism) destinées à augmenter la rapidité des transactions et en réduire les frais qui peuvent régulièrement exploser en cas d'engorgement de la blockchain. Des « bridges » peuvent être utilisés pour transférer des crypto-actifs ou tokens (jetons numériques) entre différentes blockchains.

Le crypto-actif natif d'Ethereum est l'Ether (ETH) ; ce dernier est utilisé pour payer les opérations réalisées sur la blockchain. De nombreux tokens peuvent directement être émis et échangés sur la blockchain, qu'ils soient fongibles (ERC-20) ou non-fongibles (ERC-721).

L'utilisateur de la blockchain garde un contrôle exclusif de ses fonds à partir de sa clé privée. Différentes solutions/portefeuilles (software, hardware, MPC…) existent pour la gestion des clés privées et le suivi des transactions. Certains portefeuilles sont dits « custodial », la clé privée permettant la signature des transactions est alors gérée par un tiers de confiance, comme c'est le cas sur les plateformes d'échanges dites centralisées (CeFi). Les portefeuilles peuvent être connectés à Internet (Hot Wallet) ou bien peuvent être gérés hors connexion via une clé (Cold Wallet).

Ethereum permet la création de smart contracts, des programmes exécutables directement sur la blockchain. Ces contrats permettent de déclencher des transactions conditionnelles prédéfinies lorsqu'un utilisateur interagit avec eux.

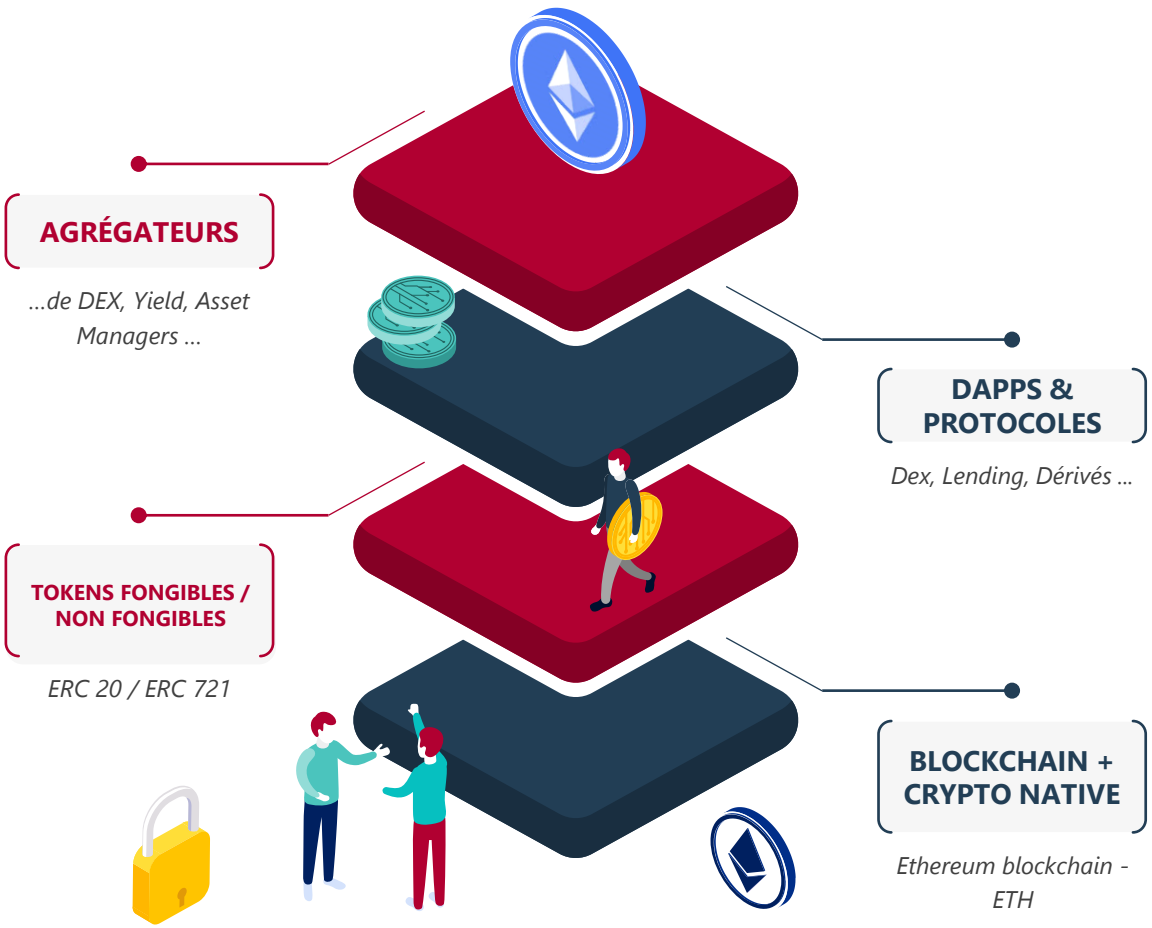
Les Protocoles / Dapps :

Les **Dapps** (Decentralized Applications) sont des programmes permettant d'interagir avec des protocoles construits sur la base de smart contracts, généralement accessibles à partir d'une interface web classique. Les protocoles possèdent souvent un token natif allouant des droits de vote à leur détenteur. Ces droits de vote vont servir à prendre des décisions entre autres en termes de paramétrage, d'évolution du code ou d'utilisation des ressources du protocole, permettant d'en faire un DAO (Decentralized Autonomous Organization), un DAO étant une entité dont les règles sont définies et appliquées à travers des smart contracts.

Dans le cadre de la DeFi, les protocoles vont servir par exemple à échanger des tokens, les prêter, ou structurer des produits financiers, comme nous le verrons plus loin dans cette étude.

Les agrégateurs :

Différents protocoles permettent d'interagir simultanément avec plusieurs autres protocoles de la couche "inférieure". Nommés "agrégateurs", ils vont servir par exemple à convertir un token en un autre jeton en passant par plusieurs protocoles d'échanges pour obtenir un prix optimal ou de la liquidité supplémentaire. Ces protocoles constituent une illustration parfaite de la « composabilité » de la finance décentralisée, permise par leur développement sur un socle commun aux règles prédéfinies (blockchain). La DeFi peut être visualisée comme un ensemble de lego imbriqués



FOCUS SUR LES LAYERS 2

Un layer 2 (L2) est une couche technologique supplémentaire construite au-dessus d'une blockchain existante afin de répondre à certaines problématiques rencontrées par les blockchains.

Dans le cas d'Ethereum par exemple, les limitations rencontrées par les utilisateurs sont le coût élevé des transactions et leur temps d'exécution relativement lent (problème similaire à la blockchain Bitcoin). Les L2 vont venir se greffer aux blockchains pour désengorger le trafic et réduire le coût des transactions.

Parmi les principaux L2, la technologie adoptée est celle du roll-up qui permet d'exécuter un certain nombre de transactions sur le réseau du layer 2 puis de publier le résultat de ces transactions en une seule opération sur le réseau de la blockchain principale. On distingue les "optimistic roll-ups" des "zero knowledge (zk) rollups" qui se différencient par leur mécanisme de validation des transactions.

La figure 1 présente les principaux L2 d'Ethereum classés par TVL. On notera qu'Arbitrum, Base (Coinbase) et Optimism représentent à eux trois plus de 70% de la TVL totale des L2 d'Ethereum.

#	NAME	RISKS	TYPE	STAGE	PURPOSE	TOTAL	MKT SHARE
1	Arbitrum One		Optimistic Rollup	STAGE 1	Universal	$17.00B ▲ 2.35%	39.64%
2	Base		Optimistic Rollup	STAGE 0	Universal	$7.27B ▲ 1.17%	16.96%
3	OP Mainnet		Optimistic Rollup	STAGE 1	Universal	$6.44B ▼ 1.05%	15.03%
4	Blast		Optimistic Rollup	STAGE 0	Universal, DeFi	$2.90B ▼ 4.37%	6.76%
5	ZKsync Era		ZK Rollup	STAGE 0	Universal	$1.27B ▼ 19.26%	2.97%

Figure 1 : Principaux Layer 2 d'Ethereum classés par TVL
(Source : L2Beat, juin 2024)

La popularité croissante des L2 d'Ethereum s'est matérialisée par une TVL qui a quasiment doublé depuis le début de l'année 2024, se situant aujourd'hui autour de 43 Mds $ pour l'ensemble des L2 d'Ethereum (près de 60 L2 à ce jour). L'évolution de cette TVL est présentée sur la figure 2 :

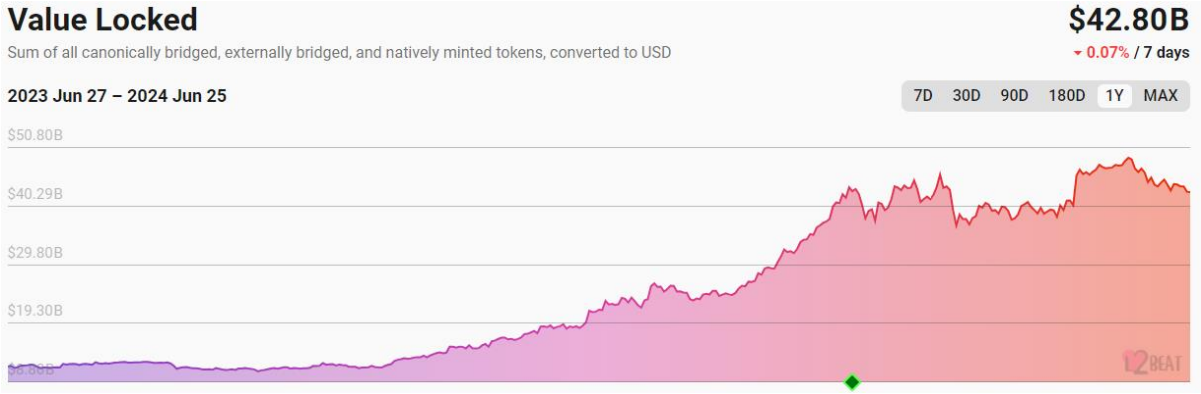


Figure 2 : Evolution de la TVL des L2 d'Ethereum (Source : L2Beat)

En permettant d'augmenter considérablement le nombre de transactions par seconde, l'utilisation des L2 a permis l'explosion des applications et des cas d'utilisation sur les blockchains, en particulier dans l'écosystème de la DeFi. La figure 3 compare l'évolution du nombre de transactions par seconde (tps) sur la blockchain Ethereum (courbe bleue) et celle des tps sur l'ensemble des L2 d'Ethereum (courbe multicolore). Au moment de l'écriture de ce guide, les L2 d'Ethereum permettent ainsi d'effectuer plus de 20 fois plus de transactions que sur la blockchain principale.

Puisque le résultat de toutes les transactions effectuées sur les L2 finit par être publié sur la blockchain principale, cette différence de transactions peut également s'interpréter comme un facteur d'échelle ou le nombre de transactions que les L2 ont permis de publier en plus sur le mainnet (couche principale) d'Ethereum.

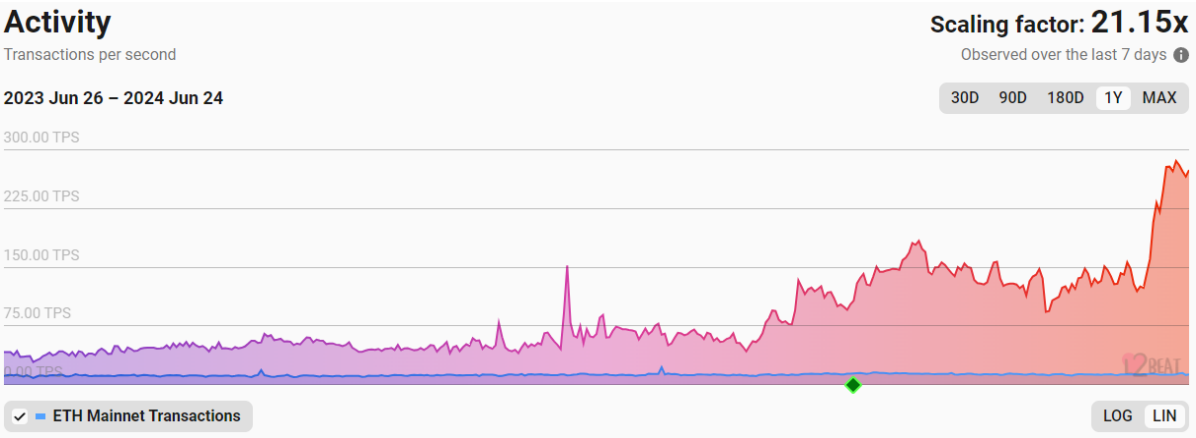


Figure 3 : Evolution du "scaling factor" des L2 d'Ethereum depuis un an (Source : L2Beat)

INTERVIEW

LÉOPOLD WENGER

CFO

COMETH

Léopold Wenger est directeur financier et chargé de la conformité chez Cometh. Issu de la filière expertise-comptable, il a débuté sa carrière en audit chez Deloitte, où il a été Ambassadeur Digital France, déployant des outils de data mining pour améliorer la détection de fraudes.

Par la suite, il a rejoint Chaintrust, contribuant au développement d'un robot d'automatisation de saisie comptable basé sur l'intelligence artificielle.

Depuis deux ans, Léopold élabore la stratégie financière et de conformité de Cometh. Pionnier dans le web3, Cometh offre des solutions d'onboarding uniques et navigue avec succès entre innovation et régulations (JONUM, MiCA, DORA).

> *« Les Layers2 permettent d'assurer la promesse selon laquelle les utilisateurs bénéficient des vertus de la blockchain tout en héritant d'une familiarité d'usage qui est celle du Web2 traditionnel. »*

En quoi les layers 2 et 3 sont-ils nécessaires pour mener à une adoption de masse de la DeFi et plus largement du Web3 ?

Quand on parle d'adoption de masse, on fait référence à la capacité pour une infrastructure web d'accueillir un nombre substantiel d'utilisateurs avec une expérience qui leur est familière (rapide, intuitive et peu coûteuse).

L'introduction de la blockchain dans l'espace Internet est réputée augmenter la sécurité et la vélocité des transferts de valeur. Ethereum est le standard qui remplit le plus cette promesse aujourd'hui au travers des centaines de chaînes EVM.

En parallèle, l'usage des SmartAccount (wallet basé sur des smart contracts) ainsi que des relayeurs de transactions sont devenus un nouveau paradigme d'onboarding qui s'impose aux éditeurs pour accroître leur attractivité en déplaçant le coût de l'onboarding de l'utilisateur vers l'éditeur. Contraints de devoir supporter des frais de réseaux; les développeurs de projets Web3 se sont naturellement tournés vers des infrastructures des centaines de fois moins chères et plus rapide en termes d'exécution. C'est ainsi qu'est né le développement des Layer 2 (Arbitrum, Base, Optimism ...) voire des Layers 3 (Nova, Muster, ...). Certains acteurs vont même jusqu'à déployer leur propre layer 2 ou 3 pour un usage propre, on parle alors d'AppChain.

INTERVIEW

LÉOPOLD WENGER

Avantages côté éditeurs d'applications

- Réduction drastique des coûts de fonctionnement
- Réduction des délais de transactions des opérations onchain
- Meilleure expérience d'onboarding et donc moins de déperdition d'utilisateurs
- Compatibilité avec des standards de développement comme le Rust sur Arbitrum offrant plus de possibilités sur l'édition de smart contract

In fine, l'amélioration des performances côté blockchain grâce aux L2/L3 réduit les coûts d'acquisition pour les projets ainsi que les coûts de fonctionnement. Cette perspective de rentabilité plus accessible pour les projets Web3 incite inévitablement l'adoption dans la sphère industrielle de la technologie.

Avantages côté utilisateurs

- Peu onéreux, voire presque gratuit
- Abstraction des frictions liées à l'onboarding
- Instantanéité (jusqu'à 10 fois plus rapide que le mainnet)

En définitive, côté utilisateur, les Layers2 permettent d'assurer la promesse selon laquelle ces derniers bénéficient des vertus de la blockchain (pleine possession de leurs actifs, rapports transparents avec l'éditeur d'application, sécurisation des transferts ...) tout en héritant d'une familiarité d'usage qui est celle du Web2 traditionnel.

Quels sont les principaux challenges auxquels doit faire face le CFO d'une société intervenant dans le web 3, notamment en matière de gestion des risques ?

L'arrivée d'un projet Web3 au sein d'une entreprise implique nécessairement des impacts côté finance.

De manière générale, la circulation de crypto-actifs au sein de l'entreprise se structure de la manière suivante :

- Marketing : gestion de la communauté (pilotage de la collection NFT, versement de récompenses ...)
- Développeurs : paiement de frais de transactions et développement de smart contracts
- Finance : sécurisation du patrimoine de l'entreprise

Inévitablement, il incombe à la finance de posséder une vue d'ensemble sur les actifs numériques de l'entreprise, que ce soit dans un souci de reporting pour le reste de l'entreprise ou simplement de gestion du patrimoine.

Le CFO se retrouve confronté à une toute nouvelle mission qui en définitive ne s'éloigne pas vraiment de ce qu'on connaît de la finance traditionnelle.

INTERVIEW

LÉOPOLD WENGER

La blockchain ayant un sous-jacent très technique, la mise en place de procédures internes se fait généralement de concert avec le CTO afin d'arbitrer sur :

- Le standard de wallet à utiliser
- Le(s) réseau(x) blockchain sur le(s)quel(s) s'établir
- Les modalités de transferts
- Les protocoles avec lesquels interagir
- Les cryptos auxquels l'entreprises peut s'exposer
- Les modalités d'archivage de l'information et de reporting

Les choix du CTO, combinés à celui du CFO doivent aboutir à une configuration résiliente face aux principaux risques propres à la « trésorerie » crypto :

- Le risque informationnel : s'assurer que l'information relayée en interne représente une image fidèle du patrimoine crypto de l'entreprise
- Le risque cyber : s'assurer qu'il n'existe pas de possibilité pour un acteur malveillant externe de profiter d'une faille cyber pour détourner le patrimoine de l'entreprise
- Le risque de perte de contrôle : s'assurer que l'ensemble des personnes bénéficiant de moyens d'accès aux actifs de l'entreprises ne peuvent pas en faire un mauvais usage par malveillance ou négligence
- Le risque de résilience : s'assurer qu'en cas d'indisponibilité des personnes clefs, les actifs sont toujours accessibles à la personne morale

A noter que l'introduction des SmartAccount apporte un niveau de sécurité et de confort pour l'entreprise. Grâce à la modularité de ce standard de wallet, il est possible d'écrire directement sur la blockchain des règles de contrôles internes (multi-signature, adresses interdites, droits d'administrations limités par des seuils ...) qui ont force exécutoire sur les transactions de l'entreprise.

Quelles sont les interactions entre DeFi et gaming Web3 ? Se dirige-t-on vers une hybridation ou a contrario un cloisonnement des deux secteurs ?

Avant même de parler de Web3, on a toujours parlé d'économie dans le monde du jeux vidéo.

L'intégration de la blockchain comme moteur de jeu permet effectivement la création d'un vase communicant entre la Finance Décentralisée et le Gaming.

Les items principaux du jeu deviennent des NFT, les valeurs qui transitent (soft & hard currencies) deviennent des tokens transférables (erc-20) etc.

INTERVIEW

LÉOPOLD WENGER

Cette configuration ouvre un champ des possibles :

- Mimer au sein du jeu des mécanismes de DeFi (staking, crafting, Lending ...) sans pour autant s'ouvrir au marché

et/ou

- Exposer les valeurs du jeu à des valeurs extérieures présentent sur la DeFi (par exemple staker ses items du jeu sur des protocoles DeFi et obtenir des rendements, créer des pools de liquidités via un Dex à l'entrée du jeu pour que les currencies du jeu s'obtiennent par contrepartie d'Ether ou d'USDC).

Même si l'hybridation des deux mondes est réalisable dans l'univers du gaming, elle tend surtout à être intégrée dans des démarches marketing visant à révolutionner des expériences d'achats mêlant gamification et incentive pour l'utilisateur comme le propose Sweat.

A noter qu'en parallèle, un nouveau cadre réglementaire est venu apporter des précisions sur les modalités de fourniture de ce type de divertissement monétisable, au carrefour du divertissement classique (gaming) et du jeu d'argent (sacrifice financier dans l'espérance d'un gain).

Ce cadre intitulé JONUM - Jeux à Objets Numériques Monétisables vise à protéger les personnes vulnérables (addicts, mineurs, ...). Outre la supervision des activités par un régulateur (l'ANJ), il prévoir notamment :

- Le contrôle de l'âge des joueurs
- L'encadrement des communications commerciales
- La limitation des récompenses à une certaine part du chiffre d'affaires
- La mise en place de dispositifs de luttes contre l'addiction
- La mise en place de dispositifs de LCB-FT (Lutte Contre le Blanchiment de capitaux et le Financement du Terrorisme)
- Des enregistrements auprès de l'ANJ (Autorité Nationale des Jeux)

En définitive, même si la technique permet d'aller sur la voie de l'hyper-financiarisation du divertissement avec le Web3, le contexte légal et les restrictions qu'il apporte présument plutôt d'un cloisonnement des deux secteurs.

> *Inévitablement, il incombe à la finance d'avoir une vue d'ensemble sur les actifs numériques de l'entreprise, que ce soit dans un souci de reporting pour le reste de l'entreprise ou simplement de gestion du patrimoine.*

2 STABLECOINS

Capitalisation : **162 Md$** Evolution : **+27% 1 an | +49% 3 ans**

Volume quotidien : **44 Md$**

Parts de marché du leader **USDT : 69%**

Sources : coinmarketcap.com, coingecko.com, defillama.com (données à fin juin 2024)

Un stablecoin est un crypto-actif qui vise à répliquer la valeur faciale d'un actif de référence, une monnaie fiduciaire dans la majorité des cas.

Ces tokens servent de pont entre la finance « traditionnelle » et le marché des crypto-actifs et permettent également aux différents acteurs du marché de se couvrir contre la volatilité extrêmement élevée lorsqu'ils le souhaitent, sans repasser directement en monnaie fiduciaire. Ils sont devenus un rouage essentiel de l'écosystème, et alors que lors de la « bulle » de 2017, la plupart des crypto-actifs cotaient principalement en bitcoin (BTC), la majorité d'entre eux peuvent à présent directement être échangés contre des stablecoins, et ce sont sur ces paires de crypto-actifs que réside la majorité de la liquidité.

Cependant, sous ce terme coexistent plusieurs types de stablecoins qui utilisent des mécanismes de stabilisation très différents :

2.1. STABLECOINS COLLATÉRALISÉS PAR L'ACTIF DE RÉFÉRENCE

L'émetteur du stablecoin dit détenir une unité de l'actif de référence pour chaque unité émise sur la blockchain. Ainsi, la stabilité du prix est assurée par le fait qu'un utilisateur peut échanger son stablecoin contre l'actif de référence auprès de l'entité émettrice, qui détruira le token une fois l'échange réalisé. Sur le marché, tout écart de prix entre le token et l'actif de référence sera arbitré, ce qui permet de maintenir la parité.

La majorité des stablecoins est adossée à des monnaies fiduciaires (principalement l'USD), mais certains sont adossés à des matières premières comme l'or, ou encore des paniers de devises.

Les principaux émetteurs de stablecoins sont des institutions en lien avec des plateformes d'échanges de crypto-actifs, comme Centre, un consortium fondé par les entreprises Circle et Coinbase, qui émet le token USDC ou encore Archblock, l'émetteur initial du TUSD (racheté depuis par le conglomérat Techteryx). Les fonds en USD sont détenus auprès d'institutions régulées aux Etats-Unis et les réserves sont auditées par des acteurs indépendants (Grant Thornton pour l'USDC par exemple).

D'autres acteurs tels que les émetteurs de l'USDT, le premier stablecoin créé en 2014, et le plus important sur le marché en termes de capitalisation, opèrent au sein de juridictions moins régulées et sont soupçonnés de ne pas adosser totalement leurs émissions de tokens à la devise de référence.

Les stablecoins collatéralisés par l'actif de référence, malgré leur rôle prépondérant dans l'écosystème de la DeFi, sont dépendants de la finance traditionnelle et de ses règlementations. La question de l'appartenance des crypto-actifs à la catégorie des valeurs mobilières, notamment, est au centre des attentions. Aux Etats-Unis, toute valeur mobilière doit être validée et enregistrée auprès de la SEC, l'autorité régulatrice des marchés financiers américains. Cette dernière a ainsi ordonné en février 2023 l'arrêt de l'émission de BUSD, jugeant que ce stablecoin s'apparentait à une valeur mobilière. Le BUSD, stablecoin adossé au dollar et assurant la liquidité sur la plateforme Binance, était alors le troisième stablecoin par capitalisation. Pour le moment, seul le BUSD a été visé par la SEC mais celle-ci semble avoir pour objectif de continuer à mener des actions dans ce sens. Binance s'est depuis rabattu sur le TUSD pour assurer la stabilité de sa plateforme d'échange.

Bien que le mécanisme de collatéralisation via des institutions de la finance traditionnelle (« off-chain », c.à.d. hors blockchain) soit contraire au principe de décentralisation qui constitue l'essence de l'esprit du marché des crypto-actifs, c'est ce type de stablecoin qui est aujourd'hui le plus largement utilisé. (voir Figure 4 ci-dessous)

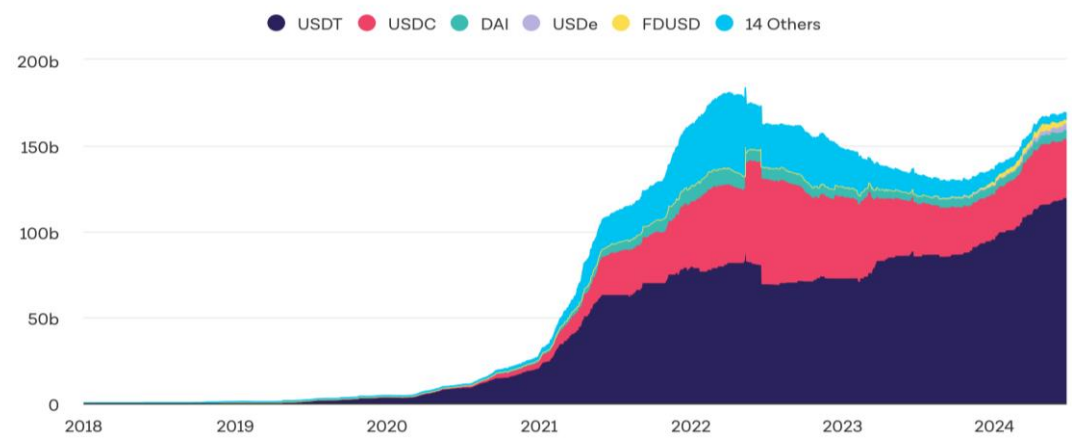


Figure 4 : Offre totale de stablecoins sur Ethereum (Source : theblock.co)

Cependant, d'autres types de stablecoins, aux mécanismes de stabilisation plus complexes, parviennent à fonctionner de manière décentralisée (« on-chain », c.à.d. reposant uniquement sur des smart contracts intégrés sur une blockchain).

2.2. STABLECOINS COLLATÉRALISÉS PAR DES CRYPTO-ACTIFS

Ce type de stablecoin assure sa parité avec l'actif de référence grâce à un système de collatéralisation par un panier « pool » de crypto-actifs, appelé CDP (Collateralized Debt Position) Le plus important et ancien stablecoin de ce type en termes de capitalisation est le DAI, émis par le protocole Maker, sur la blockchain Ethereum.

2.2.1. DAI DE MAKERDAO

Emission de DAI

Un utilisateur peut générer de nouveaux DAIs en verrouillant ses crypto-actifs dans un smart contract spécifique (Vault) sur le protocole maker. L'utilisateur pourra ensuite s'il le désire récupérer son collatéral en restituant les DAIs au protocole et moyennant des frais de stabilité, payés en DAI. Ce mécanisme s'apparente à une opération de prêt-emprunt.

Collatéralisation

Etant donné la volatilité de la valeur du collatéral, une sur-collatéralisation est requise et définie selon le profil de risque de la cryptomonnaie utilisée. A partir de ces profils de risque, un ratio de liquidation est déterminé pour chaque vault : ce ratio correspond à un seuil de collatéral/dette minimum qui ne doit pas être franchi à la baisse, sous peine de liquidation automatique.

Mécanisme de liquidation

Si ce mécanisme de liquidation s'enclenche, le collatéral est vendu à travers un système d'enchères interne contre des DAI. Les DAI récoltés servent à couvrir les dettes du vault (montant de DAI généré) et à payer une pénalité de liquidation. Tout collatéral résiduel est restitué au vault.

Deuxième ligne de défense

Si les DAI récoltés ne couvrent pas la totalité des dettes, un deuxième mécanisme de compensation s'enclenche alors : le déficit résiduel est converti en dette de protocole, couverte par le stock de DAI récolté grâce aux frais de stabilité et pénalités de liquidation, au sein du « maker buffer ».

3ème ligne de défense

Enfin, si le « maker buffer » ne suffit pas à couvrir le déficit, le protocole déclenche un mécanisme de recapitalisation, en générant de nouveaux MKR (token de gouvernance du protocole) et en les vendant via un mécanisme d'enchère contre des DAI, qui sont ensuite intégrés dans le « maker buffer ».

Afin de limiter le nombre de MKR en circulation, la taille du « maker buffer » est limitée. Ainsi, si le montant des frais récoltés devient supérieur à cette limite, un mécanisme de vente aux enchères des DAI composant le surplus est activé, ces DAI étant échangés exclusivement contre des MKR qui seront ensuite détruits.

4ème ligne de défense

En dernier recours, en cas de hack ou de mouvement de marché extrêmement violent, un « emergency shutdown » peut être initié par un vote des détenteurs de Maker et de DAI. Dans ce cas de figure, le collatéral des vaults est libéré et les détenteurs de DAI et de vaults sont automatiquement remboursés à hauteur des fonds disponibles.

Les « oracles »

Afin de fonctionner correctement, le protocole nécessite d'être alimenté continuellement en données de marchées relatives aux actifs détenus en tant que collatéral dans les vaults. Un module s'assure de recueillir ces données auprès de différents fournisseurs décentralisés, appelés communément « oracles ».

Le « DAO »

La gouvernance du protocole est décentralisée (Decentralized autonomous organization). Ce sont les détenteurs de Maker qui proposent et décident par vote des différentes évolutions des paramètres du protocole : nouveaux types de collatéral et paramètres de risques associés, taux d'intérêt du DAI, sélection des oracles, « emergency shutdown », évolutions plus structurantes du protocole.

Nous venons de synthétiser de manière simplifiée et non exhaustive le fonctionnement du protocole Maker. Cet exercice permet d'offrir un aperçu de la complexité des mécanismes et du mille-feuille de gestion des risques qui permet d'assurer la résilience du protocole et son fonctionnement continue depuis plusieurs années.

A noter qu'une grande partie du collatéral posté pour la création de DAI a longtemps été constitué d'USDC, un stablecoin non décentralisé car collatéralisé directement par de la monnaie fiduciaire détenue par une société émettrice. Ainsi, MakerDAO était fortement critiqué pour sa dépendance indirecte à des institutions centralisées. La proportion d'USDC à l'actif du « bilan » de MakerDAO a cependant été fortement réduite depuis quelques années.

MakerDAO a par ailleurs pris la décision stratégique d'inclure les actifs du monde réel ou « real-world assets » (RWA) dans son collatéral. Le DAO a ainsi prêté au début de l'année 2023 l'équivalent de 7M $ à la Société Générale (par l'intermédiaire de SG-FORGE, sa filiale dédiée aux actifs digitaux) en échange d'un collatéral de 40M $ sous la forme d'OFH tokens (obligations de financement de l'habitat) notées AAA. MakerDAO avait accordé un prêt similaire à la banque américaine Huntingdon Valley Bank en 2022, ce qui avait marqué un tournant historique, à savoir la première transaction entre une banque de la finance traditionnelle et un protocole de la finance décentralisée. Les RWAs constituent aujourd'hui près d'un tiers du collatéral de DAI.

INTERVIEW

PABLO VEYRAT

Co-Founder & Core Contributor
Angle Protocol

Pablo Veyrat est cofondateur du protocole Angle, qui propose des stablecoins décentralisés.

Il a remporté récemment le prix de "Jeune talent Web3 de l'année.

> *Angle cherche à se démarquer en étendant les cas d'utilisation d'un stablecoin, notamment via la distribution de rendements.*

Quels sont les cas d'utilisation principaux d'un stablecoin décentralisé ?

Les cas d'utilisation les plus connus sont les paiements et transferts de fonds. Cependant, les stablecoins permettent également de se protéger contre la volatilité du marché sans avoir à convertir ses cryptos contre des monnaies fiduciaires. Ils servent également à accéder à d'autres services de la Finance Décentralisée, pour emprunter, prêter ou chercher du rendement sur d'autres protocoles. Enfin, pour les stablecoins comme Angle, un mécanisme inhérent de distribution de rendements peut être intégré directement sur le protocole et en faire un véritable véhicule d'investissement.

On assiste à l'émergence de nombreux stablecoins. Comment se démarquer dans ce marché qui devient très concurrentiel ?

Angle cherche à se démarquer en étendant les cas d'utilisation d'un stablecoin, notamment via la distribution de rendement. Angle investi dans différents actifs, comme des fonds Blackrock tokenisés par le protocole Backed. Un rendement attractif proposé aux utilisateurs est essentiel afin de se démarquer de la concurrence. Outre son stablecoin Euro EURA, Angle a développé récemment un stablecoin Dollar USDA, afin d'étendre sa gamme et d'atteindre un marché offrant plus de profondeur. A terme, l'ambition est de continuer à élargir l'offre en Stablecoin et devenir une véritable plateforme Forex.

Quels sont les principaux risques auxquels un protocole comme Angle est exposé ? Et quels sont les dispositifs mis en place pour les couvrir ?

Outre les risques d'attaques cyber inhérents à l'écosystème DeFi, les principaux risques auxquels Angle est exposé sont les risques réglementaire et de liquidité. Un stablecoin décentralisé fonctionne comme une banque, et une gestion robuste des réserves est nécessaire. Le principal challenge auquel doit faire face le protocole est l'optimisation de son bilan sous contrainte de liquidités. Angle maintient à tout instant au moins 30% d'actifs liquides dans ses réserves, afin d'assurer une capacité suffisante pour répondre aux retraits sans compromettre la stabilité du protocole. En termes de conformité réglementaire, Angle bénéficie actuellement d'une exemption sous MICA, en tant que protocole décentralisé. Il faut néanmoins suivre avec attention l'évolution du cadre réglementaire qui pourrait devenir moins favorable dans les mois à venir.

2.3. STABLECOINS ALGORITHMIQUES

Les stablecoins algorithmiques tentent de repousser les limites de la décentralisation en se passant en partie voire totalement de collatéral, éliminant ainsi toute dépendance à une institution tierce. De nombreuses expérimentations sont lancées chaque année, utilisant différents types de mécanismes avec plus ou moins de succès. Nous allons ici uniquement analyser les principaux projets représentatifs, qui peuvent être divisés en trois sous-catégories :

2.3.1. REBASE STABLECOINS : AMPL

Le modèle de stabilisation de ces types de stablecoin repose sur un mécanisme de « rebasage » de l'offre de tokens en circulation : pour contrer une hausse de prix au-dessus du prix de l'actif de référence, le protocole augmente le nombre de token en circulation en les attribuant directement aux adresses détentrices. Ces tokens supplémentaires vont faire immédiatement baisser le prix dans les pools de liquidité des échanges décentralisés.

L'ajustement sur les échanges centralisés se fera assez rapidement car une opportunité d'arbitrage sera alors présente. A l'inverse, si le prix du token baisse en dessous du niveau cible, l'offre en circulation sera automatiquement réduite.

Malgré une volatilité élevée par rapport aux autres types de stablecoin, le AMPL (principal rebase stablecoin) parvient à graviter autour de son prix cible depuis maintenant plus de quatre ans.

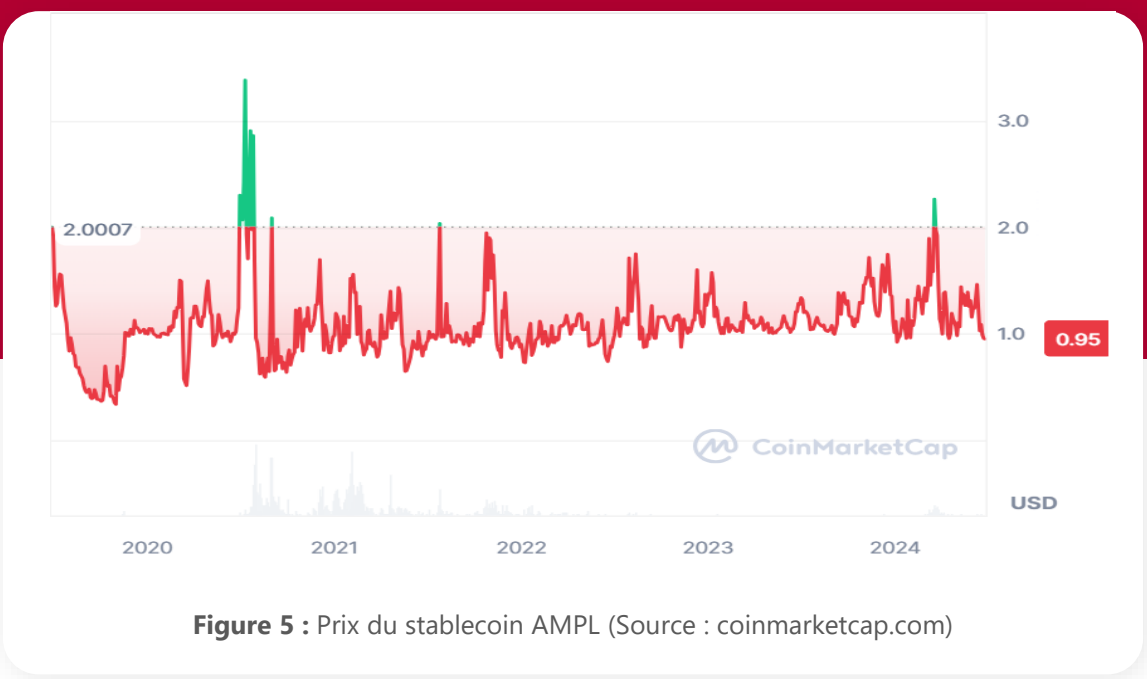


Figure 5 : Prix du stablecoin AMPL (Source : coinmarketcap.com)

2.3.2. SEIGNIORAGE STABLECOINS 

Ce modèle est composé d'un système multi-tokens, l'un étant le stablecoin censé répliquer l'actif de référence, le ou les autres servant de mécanisme de stabilisation pour ledit stablecoin.

Focus sur UST de la blockchain Terra Luna :

Le stablecoin le plus dramatiquement célèbre représentant cette catégorie est l'UST de la blockchain Terra Luna. L'UST (adossé au dollar) et le LUNA, le token natif de la blockchain, ont suscité progressivement l'intérêt des investisseurs entre 2019 et 2022. La valorisation du LUNA atteignit 139 Mds $ en avril 2022, peu avant l'effondrement de l'écosystème Terra Luna commencé le 7 mai 2022 et qui mena à la diminution de près de 60 Mds $ de la valeur verrouillée au sein du protocole en quelques jours

Le LUNA servait à payer les frais de transaction sur le réseau et permettait également de générer des UST via un mécanisme de « Burn », les utilisateurs pouvaient à tout moment détruire l'équivalent de 1$ de LUNA pour générer 1 UST. Réciproquement, ils pouvaient échanger à tout moment 1 UST contre l'équivalent de 1$ de LUNA.

Ainsi, lorsque l'UST n'était plus totalement adossé au dollar, une opportunité d'arbitrage apparaissait et les acteurs du marché, en l'exploitant, rétablissaient l'adossement cible :

- Si l'UST tombait sous les 1$, il était possible d'acheter des UST, de les échanger contre 1$ de LUNA et ainsi obtenir des LUNA en dessous de leur prix de marché, en réalisant ainsi un gain immédiat.
- Si l'UST passait au-dessus des 1$, il était possible d'acheter pour 1$ de Luna et immédiatement générer 1 UST qu'il était possible de revendre à plus de 1$.

En mai 2022, trois évènements majeurs ont cependant entraîné subitement la chute de cet écosystème. Le 7 mai 2022, une série de transactions de montants significatifs est initiée sur le protocole DeFi Curve, dégradant la liquidité sur ce dernier. Une réaction en chaîne se produit alors et d'importantes sortie de fonds interviennent entre le 7 et le 9 mai sur Anchor, une des premières plateformes DeFi à avoir été construites au-dessus de la blockchain Terra, qui proposait des rendements allant jusqu'à près de 20% sur l'UST. En parallèle, la Luna Foundation Guard, créée par les fondateurs du protocole, pris la décision d'effectuer un rachat massif de LUNA (l'équivalent de 3Mds $) en vendant près de 80 000 bitcoins afin de faire remonter les cours du LUNA et ainsi de stabiliser l'UST. Cette vente massive provoqua un violent mouvement baissier sur les marchés crypto et entraîna encore plus bas la valeur du LUNA. Une semaine plus tard, l'UST ne valait plus que 0.15$.

Figure 6 : Evolution du prix du LUNA et de l'UST (Source : coindesk.com**)**

On notera qu'un nombre significatif de projets appartenant à cette catégorie de seigniorage stablecoins ont échoué malgré des débuts très prometteurs. Hormis l'UST dont la capitalisation maximale a approché 19 Mds $, le FEI a également vu son projet s'arrêter en 2022 alors que sa capitalisation avait atteint 2,4 Mds $ au plus haut. On citera également l'effondrement en 2021 du Basis Cash qui fut la première tentative de création d'un modèle de stablecoin de Do Kwon, le fondateur de Terra Luna.

2.3.3. FRACTIONAL ALGORITHMIC STABLECOINS : FRAX

Les stablecoins algorithmiques « fractionnés » utilisent à la fois le mécanisme de collatéralisation vu au-dessus avec l'exemple du DAI, et le système de seigniorage vu avec l'exemple de l'UST.

Par exemple, le FRAX, dans sa première version, fonctionnait sur un ratio initial d'environ 75% d'USDC et 25% de FXS (le token utilisé, à l'instar du Luna, pour générer de nouveau FRAX, mais également pour la gouvernance du protocole). Le ratio variait en fonction du prix du FRAX : lorsque ce dernier dépasse les 1$, le protocole abaisse le ratio de collatéralisation, et l'augmente à l'inverse lorsque le cours descend sous les 1$.

Le protocole a également développé un nouveau stablecoin, le FPI (Frax Price Index), qui réplique un panier de bien de consommations (CPI : Consumer Price Index).

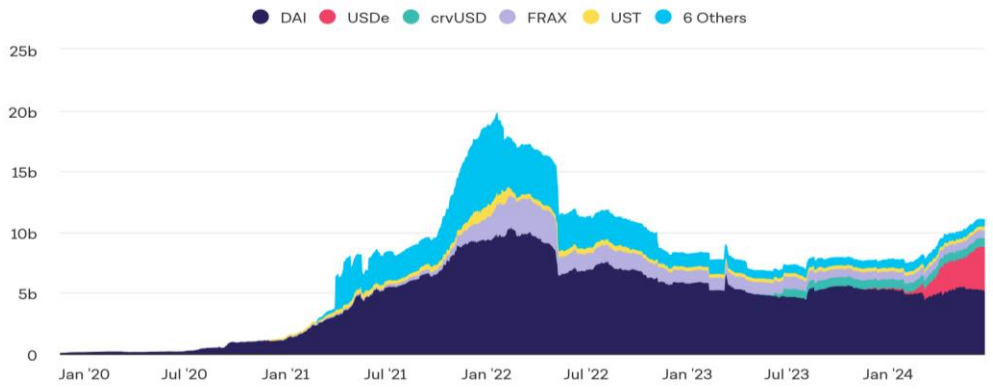


Figure 7 : Offre de stablecoins collatéralisés par des crypto-actifs et stablecoins algorithmiques sur Ethereum
(Source : theblock.co)

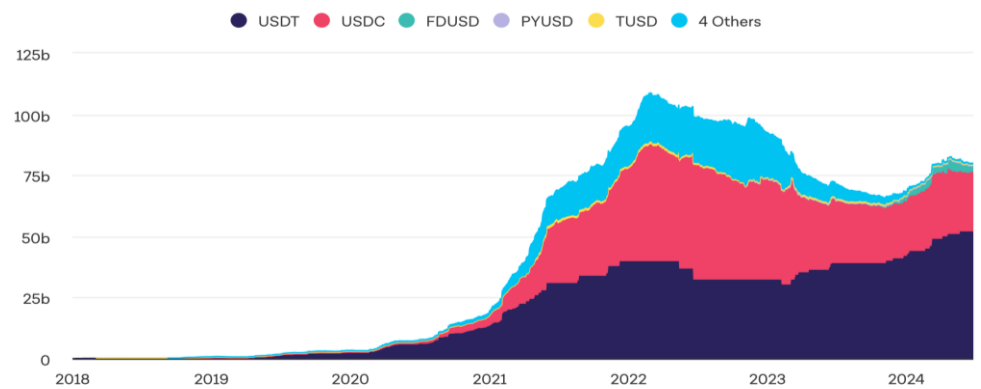


Figure 8 : Offre de stablecoins collatéralisés par des devises FIAT sur Ethereum
(Source : theblock.co)

2.4. CBDCs

Le marché des stablecoins poursuit son développement protéiforme et parfois chaotique ; et il semble difficile de revenir en arrière au vu de la révolution qu'il engendre : un système monétaire global permettant des transactions quasi-instantanées 24 heures sur 24 et 7 jours sur 7. Jusqu'à présent principalement utilisés pour le trading ou les échanges au sein de l'écosystème crypto, l'usage des stablecoins commence à s'étendre vers les règlements internationaux (BtoB et particuliers) ainsi qu'au sein des économies locales.

Les grandes entreprises de la tech américaine ont bien saisi l'enjeu d'un tel marché, et après la tentative de Meta avec le lancement avorté du Libra, c'est Paypal qui a annoncé récemment la création de son stablecoin, PYUSD, adossé au dollar et collatéralisé en devise et obligations du trésor américain. En offrant à tous ses utilisateurs la possibilité de payer et de transférer des fonds plus rapidement, PayPal vient ancrer un peu plus les crypto-actifs et les stablecoins en particulier dans notre quotidien.

Ce marché n'a pas non plus échappé à la vigilance des banquiers centraux. Devant les nombreux avantages de l'utilisation des blockchains (traçabilité, rapidité etc.) et la menace de voir un jour les stablecoins concurrencer les monnaies fiduciaires, les banques centrales du monde entier ont commencé à se pencher sur la création de leurs propres monnaies digitales : les CBDC (Central Bank Digital Currency). En reposant sur une technologie similaire à celle des blockchains, les CBDC surpasseraient ainsi en efficacité le système traditionnel de virement. De plus, en reposant sur les banques centrales, les CBDC ne seraient pas exposés au risque de crédit que supportent les dépôts dans les banques commerciales. Les détracteurs des CBDC estiment que le rôle joué par les banques centrales dans l'émission de cette monnaie constituerait un renforcement de la centralisation du système monétaire. Ce qui séparerait encore plus l'écosystème de la DeFi (et des crypto-actifs en général) du système financier traditionnel.

Parmi la pléthore d'initiatives de créations de CBDC, il convient de distinguer les CBDC de détail, adressées aux particuliers, et les CBDC de gros, vouées à être utilisées par les institutionnels.

Les CBDC de détail permettraient aux paiements d'être plus rapides et plus sécurisées. Elles permettraient également de faciliter l'accès aux services financiers pour les personnes n'ayant pas de comptes bancaires traditionnels.

Les CBDC institutionnelles (de gros) sont quant à elles destinées à rendre plus efficaces les transactions opérées entre les banques centrales et les autres institutions financières.

Selon une enquête de la BIS (banque des règlements internationaux) menée en 2022, sur les 86 banques centrales étudiées (94% du PIB mondial), 93% des banques centrales travaillent sur un projet de CBDC de détail. La BIS prévoit ainsi près de 15 CBDC en circulation d'ici 2030.

Actuellement il y a 4 CBDC de détail en circulation : aux Bahamas, dans les Caraïbes orientales, en Jamaïque et au Nigéria. La Chine, l'Inde et la Russie ont quant à elles un projet pilote de CBDC de détail abouti alors que les Etats-Unis, la Norvège, ou encore le Japon sont en phase de POC. Il est à noter que les initiatives de l'UE sur les CBDC de détail sont encore au stade de recherches. Les initiatives concernant les CBDC institutionnelles ne sont pas aussi avancées que pour les CBDC de détail et pour l'instant aucun projet n'a abouti.

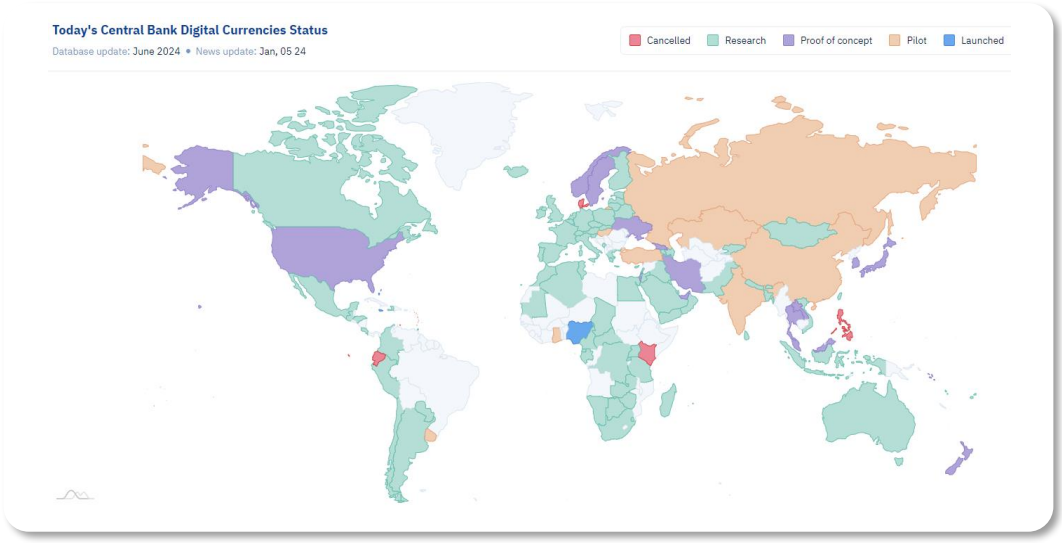


Figure 9 : Etat d'avancement des projets de CBDC de détail à l'échelle mondiale (Source : CBDCTracker)

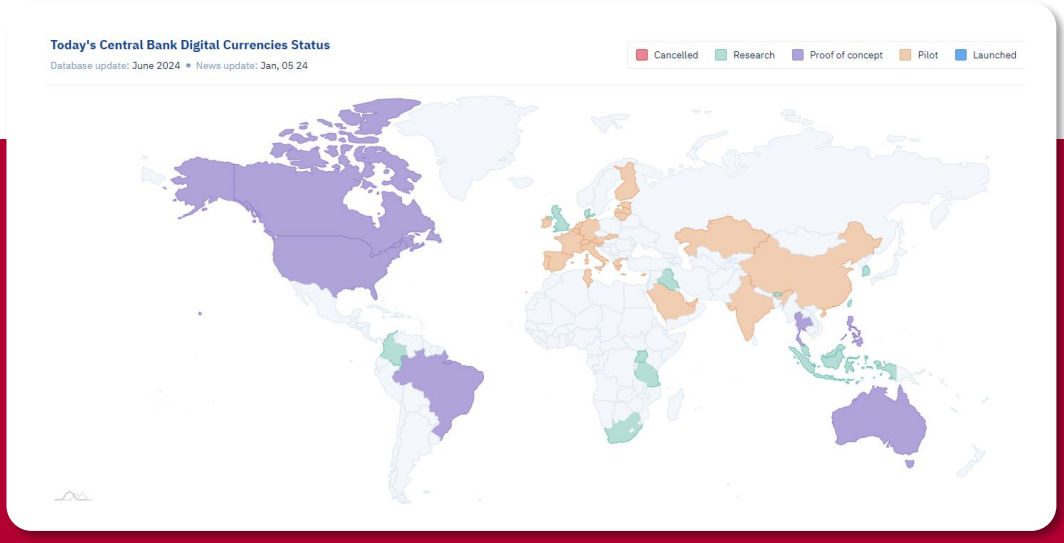


Figure 10 : Etat d'avancement des projets de CBDC de gros à l'échelle mondiale (Source : CBDCTracker)

INTERVIEW

trakx

YANN LE FLOCH

Digital Asset Banker

TRAKX

Yann le Floch est un ancien banquier d'affaires, développeur de produits financiers et entrepreneur dans l'écosystème blockchain et les monnaies numériques institutionnelles. Il conseille et finance des startups du secteur, et collabore avec les acteurs institutionnels (banques, fonds, industries..) et gouvernements (Europe, Asie, Venezuela).

« Les CBDCs peuvent modifier en profondeur sur le moyen-long terme le système monétaire mondial, si la potentialité technique de ces outils est utilisée pleinement.»

Vous avez contribué à différents projets de création de CBDCs, notamment pour les BRICS. Pensez-vous que les CBDCs auront un impact majeur sur l'organisation du système monétaire mondial ?

Les CBDCs peuvent modifier en profondeur sur le moyen-long terme le système monétaire mondial, si la potentialité technique de ces outils est utilisée pleinement. Toutefois, il est à noter que les usages qui en sont et seront donnés, et l'esprit de ces usages est vraiment la clé de ces outils technologiques.

L'âme de ces monnaies dépendra des porteurs d'âmes qui les réalisent et réaliseront, et avec quelle volonté et quelle intention. La voûte d'une harmonie monétaire est l'enjeux, et un équilibre de partage des pouvoirs et des richesses, au-delà la coexistence de philosophies économiques différentes et complémentaires.

Cette thématique est désormais marginalement technique, et avant tout politique, sur l'âme des alchimistes qui guideront la création de ces outils. Mais sans ambiguïté, les armes monétaires amèneront le meilleur et la paix et des équilibres, ou des extrémismes quels que soient les terreaux philosophiques associés, de l'extrême égalitarisme, à l'extrême unipolarité philosophique, y compris à l'extrême finance.

L'impact des CBDCs de droit public ou de droit privé sera pour sûr majeur et il ne s'agit probablement que du début d'un processus de transformation profond des systèmes monétaires.

INTERVIEW

YANN LE FLOCH

Les CBDCs seront-elles en concurrence directe avec les stablecoins décentralisés ? Ces derniers auront-ils un avenir dans un monde dominé par les monnaies de banque centrale ?

Toutes les monnaies digitales, de nature de droit privé, ou de nature de droit public, peuvent présenter des vertus humaines, sociétales, économiques, et financières. Les CBDCs sont aujourd'hui vus comme des outils des banques centrales historiques associés in fine aux réserves d'Or de grands réseaux financiers, de même le Bitcoin est une structure via sa fondation et ses réseaux d'influence, des structures privés, d'usage publique. Et d'ailleurs cette perspective s'inscrit sur l'ensemble du spectre des crypto-monnaies. Personne n'aurait l'audace de considérer aujourd'hui que l'Internet décentralisé historique est aujourd'hui un espace public dans la propriété et les choix stratégiques, dans l'usage si en effet, mais la liberté d'usage peut parfois s'avérer une liberté contrôlée voire une chaîne de liberté. Pour les monnaies digitales, de droit de banque centrale historique, ou de droit de structures privées entrepreneuriales, l'enjeux pourrait être le même que pour l'Internet. L'écosystème des dites cryptomonnaies se "gafamisent", et la promesse de départ est déviée de ses fondamentaux et objectifs, d'ailleurs Edward Snowden a pu l'exprimer selon ce prisme d'analyse. En clair, je ne pense pas que les monnaies qui seront utilisées dans 30 ans existent toutes aujourd'hui, l'avenir est à construire, et selon les principes philosophiques qui animent nos âmes. Donc la saine concurrence va s'opérer entre équilibres marketing, politiques, géopolitiques, techniques, de droit naturel, et de droit public comme privé. L'avenir s'avère se dessiner à la concurrence, où chacun peut exprimer ses préférences d'usage.

L'ACPR, dans une étude publiée en 2023, a jugé plus opportun d'utiliser le terme "désintermédiée" en lieu et place de "décentralisée" pour décrire la DeFi. Cette requalification est-elle pertinente selon vous ?

L'ACPR a parfaitement raison dans cette nuance, qui est en réalité un point fondamental. Les systèmes technologiques dits DeFi présentent tous des administrateurs ultimes avec des clés systèmes qui rendent ces structures décentralisées dans l'usage, mais très centralisées à certains égards. La centralisation de la DeFi est tellement concentrée et invisible, qu'il serait presque impossible de la voir ou la deviner parfois, en particulier dans les usages, mais elle est présente et cryptique.

Ainsi le tiers de confiance existe toujours, qu'il soit humain, technologique, institutionnel, ou quelques techs ou investisseurs discrets. La décentralisation ultime n'existe pas, y compris pour Bitcoin, la structure la plus décentralisée techniquement, car in fine la définition des valeurs de marché se fait de manière centralisée par beaucoup de places de marché CeFi.

Ainsi la requalification de l'ACPR est parfaitement cohérente, et est à saluer par souci de vérité dans l'esprit des fondamentaux.

3 PROTOCOLES D'ÉCHANGE DÉCENTRALISÉS (DEX)

TVL (Total Value Locked) : **19,8 Md$** Evolution : **+35% 1 an**

Volume quotidien : **4,7 Md$**

Parts de marché du leader Uniswap **: 28%**

Sources : coinmarketcap.com, coingecko.com, defillama.com (données à fin juin 2024)

Les protocoles d'échanges décentralisées (DEX) permettent d'acheter ou vendre des cryptomonnaies sans avoir recours à un tiers de confiance, en opposition avec les CEX (Centralized Exchanges comme Coinbase et Binance pour citer les plus importants) sur lesquels on doit déposer ses actifs et qui proposent un carnet d'ordre qui permet au prix de se former, à l'instar des places financières traditionnelles.

Les CEX ont attisé la méfiance des acteurs du marché des cryptomonnaies au fil des années, en raison des faillites et escroqueries récurrentes subies, de la chute de Mt Gox en 2013 à celle d'FTX en fin 2022. De plus, leur fonctionnement va à l'encontre de l'esprit de décentralisation et de développement open source qui prévaut dans l'écosystème et qui a pour ambition de se passer de tout tiers de confiance et intermédiaire.

Mais comment, sans autorité centralisatrice, permettre d'offrir de la liquidité et former un prix ? Et le tout sans que les utilisateurs aient à déléguer le contrôle de leurs fonds ?

Une première génération de DEX a tenté de répliquer le système existant en proposant un carnet d'ordre « on chain » (Etherdelta par exemple) mais cette solution s'est avérée coûteuse en frais de transaction et ressources.

A partir de 2018, une nouvelle génération de DEX a émergée, qui reposent sur un système appelé AMM (Automated Market Making).

Ce système n'utilise pas de carnet d'ordre ni de système de matching d'ordres. Le prix est déterminé de manière algorithmique en fonction de l'offre de liquidité présente sur les deux crypto-monnaies dont l'échange est proposé. L'un des premiers et le plus important de ces DEX est UniSwap, lancé en novembre 2018. Trois versions de ce DEX ont été déployées depuis sa création et le code de sa 4ème version a été dévoilé en juin 2023. A l'instar d'un grand nombre de DEX créés par la suite, UniSwap utilise un mécanisme de « constant function » market making.

3.1. UNISWAP

FONCTIONNEMENT

- Un LP (Liquidity Provider) place les deux cryptomonnaies dont l'échange est proposé dans un smart contract représentant un « pool » de liquidité.
- Les utilisateurs du DEX vont ensuite pouvoir procéder à un achat ou une vente en déposant leur cryptomonnaie dans le pool de liquidité et en retirant un certain montant de l'autre cryptomonnaie.
- Le cours d'échange est déterminé lors de la transaction par la fonction suivante (simplifiée en enlevant les frais de transaction) :

$$x * y = k$$

  - x et y sont les réserves respectives, en quantité, des deux cryptomonnaies **A** et **B**
  - k est une constante
  - Cette fonction est représentée par une hyperbole : le prix de chaque trade va être basé sur le déplacement sur la courbe induit par la transaction. Si un utilisateur souhaite acheter de la cryptomonnaie **B**, en l'échangeant contre de la cryptomonnaie **A**, il va diminuer le nombre d'unités de **B** et augmenter le nombre d'unités de **A** dans le pool de liquidité.

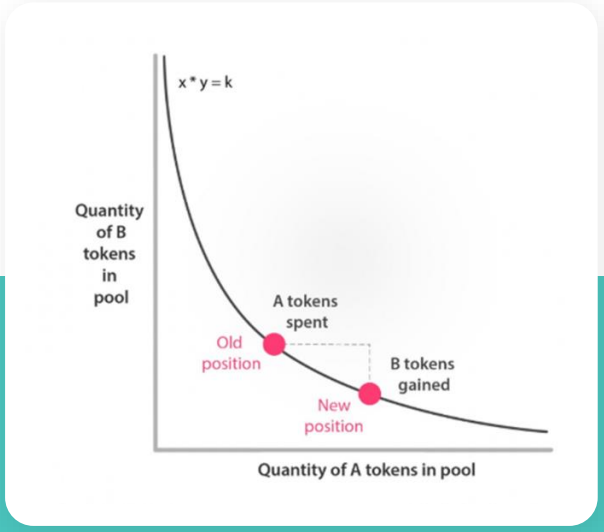


Figure 10 : Fonctionnement d'un AMM (Automated Market Maker)

- Plus la quantité est importante en proportion de la liquidité présente dans le pool, plus le déplacement va l'être et donc plus le prix de la cryptomonnaie achetée va augmenter relativement à la cryptomonnaie vendue. Il faut visualiser la pente de la courbe à chaque point comme le taux d'échange marginal entre les deux crypto-actifs.
- Exemple : si un pool de liquidité ETH / DAI est composé de 1ETH et 100DAI, on aura : $\boldsymbol{k = 1 * 100 = 100}$ **.** Si un utilisateur du DEX veut acheter 0.5ETH (et donc les retirer du pool), il va devoir apporter 100 DAI afin de maintenir $\boldsymbol{k}$ constante ($\boldsymbol{0.5 * 200 = 100}$). Cet exemple est un cas extrême car la transaction aurait lieu sur un pool très illiquide et donc entraînerait un « slippage » du prix très important (de 100 DAI / ETH initialement à 200 DAI / ETH lors de la transaction).
- Si à la suite de la transaction, le prix s'éloigne trop du prix disponible sur les autres plateformes d'échange, du fait du déséquilibre entre les deux actifs dans le pool de liquidité, un arbitrage va alors être réalisable, ce qui va permettre de rétablir l'équilibre et donc le prix.

- Afin d'attirer de la liquidité, les utilisateurs du protocole doivent payer des frais de transaction (0.3% sur UniSwap V1 et V2, entre 0.05% et 1% à partir de la V3) pour rémunérer les apporteurs de liquidité, proportionnellement à leur contribution aux réserves du pool. Ils reçoivent également de la crypto-monnaie native du protocole, leur donnant des droits de gouvernance.

Le risque principal pour les apporteurs de liquidité est appelé IL « Impermanent Loss » :

- Lorsqu'un utilisateur apporte de la liquidité sur le smart contract, il reçoit en échange une certaine quantité d'un liquidity token, représentant sa contribution dans le pool et lui permettant à tout moment de retirer les crypto-actifs qu'il a apportés, et entretemps de profiter des frais de transaction générés par les échanges effectués sur le pool. S'il apporte par exemple 1 ETH et 100 DAI dans un pool de liquidité comportant 99 ETH et 9 900 DAI, il recevra l'équivalent de 1% des liquidity tokens du pool.
- Supposons que le prix de l'ETH varie par rapport au DAI et soit à présent de 1 ETH pour 120 DAI, à la suite de transactions d'achats d'ETH dans le pool. Il y aura à ce moment 91.2871 ETH et 10954.4511 DAI dans le pool.
- Si l'utilisateur souhaite récupérer la liquidité qu'il a apporté, il échangera ses liquidity tokens contre 1% du pool, soit 0.91287ETH et 109.544511 DAI. SI nous convertissons ces ETH en DAI, il récupèrera l'équivalent de $\boldsymbol{0.91287 * 120 + 109.544511 = 219.089}$ **DAI**. Si au lieu de placer ses crypto-actifs dans le pool, il les avait conservés, il aurait cependant l'équivalent de $\boldsymbol{1 * 120 + 100 = 220}$ **DAI**. SI nous faisons abstraction des frais de transaction qu'il a pu gagner dans l'opération, cette dernière présente donc un coût d'opportunité de **0.911 DAI**.

C'est ce coût ou perte que l'on appelle l'impermanent loss ou divergence loss.

Il est « impermanent » car tant que l'utilisateur n'a pas sorti ses crypto-actifs du pool, la perte n'est pas avérée, le taux de change entre les deux crypto-monnaies pouvant entretemps revenir à son niveau d'origine. Apporter de la liquidité dans un pool revient donc à être « short » volatilité et « long » corrélation. En effet, moins le prix des crypto-actifs contenus dans le pool est corrélé, plus leur prix relatif est amené à varier ; et plus la volatilité du prix de ces crypto-actifs est importante, plus des mouvements importants sont probables et donc le risque d'impermanent loss considérable.

L'impermanent loss peut être représenté par l'équation suivante :

$$\textit{Impermanent loss} = 2\frac{\sqrt{m}}{1+m} - 1 \text{ avec } m = \frac{\textit{taux de change } (t)}{\textit{taux de change } (t-1)}$$

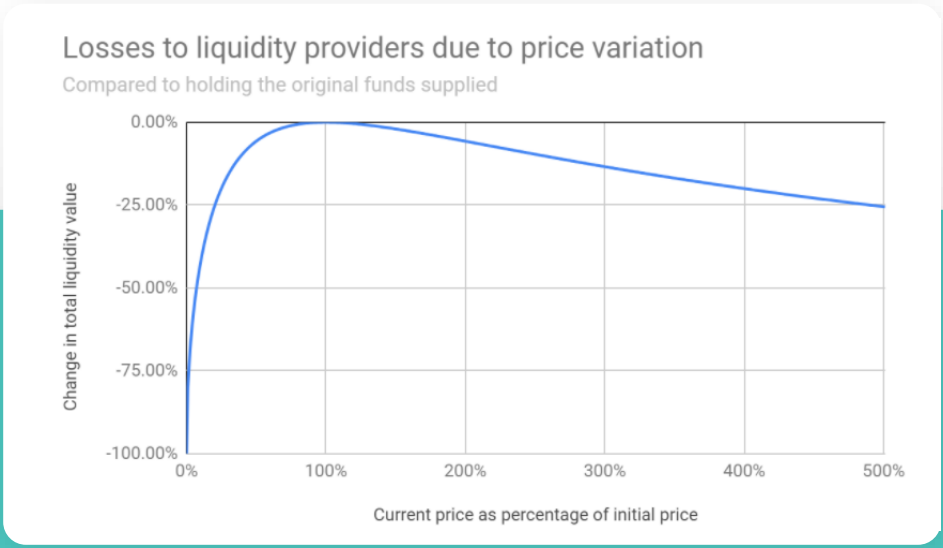


Figure 11 : Impermanent loss (Source **:** uniswap.org)

EVOLUTION

01 Les mécanismes et concepts décrits précédemment sont l'essence du fonctionnement de la première version du protocole d'UniSwap et constituent également les fondations des deux versions suivantes du protocole.

02 La V2, lancée en 2020, permet de créer des pools de liquidité avec des paires formées par n'importe quels tokens ERC-20 sans passer par l'ETH comme c'était le cas avec la V1. Des oracles de prix, services décentralisés fournissant le prix d'un actif sur la blockchain (voir encadré plus loin), sont également utilisés pour la première fois dans la V2 afin de combattre les manipulations de prix sur l'échange.

03 La V3 a été lancée quant à elle en 2021 et implémente le concept de liquidité concentrée. Dans la V1 et la V2, la liquidité était répartie de manière homogène sur toute la plage de prix possible pour l'équation « x*y = k ». Dans la V3, les LPs peuvent concentrer leur liquidité sur une plage déterminée (la plage dans laquelle l'actif a le plus de chances d'être échangé) afin d'améliorer l'efficience du capital (rapport entre le volume de transactions dans un pool et la taille du pool) et augmenter le volume de transactions et donc les commissions collectées. De plus la concentration de liquidités autour de prix pertinents permet de réduire le slippage.

Cette dernière version du protocole est considérée par beaucoup comme l'un des protocoles AMM les plus performants. Des études montrent en effet que la liquidité des paires les plus populaires (comme ETH/USD ou ETH/BTC) est plus grande sur ce protocole que sur les plus importants échanges centralisés comme Coinbase ou Binance.

04 Enfin, la V4 du protocole a été dévoilée en juin 2023 et a pour objectif de faire baisser les gas fees et d'améliorer l'efficacité des pools en faisant exister ces derniers dans un seul smart contract (architecture singleton) au lieu d'avoir un smart contract par pool. Les utilisateurs de la V4 pourront également personnaliser leurs stratégies en utilisant des hooks : des fonctions spécifiques comme le TWAMM (Time Weighted Automated Market Maker) qui permettra aux traders voulant exécuter des volumes importants de diviser ces volumes en plus petits blocs et de les exécuter de manière automatisée au cours du temps afin de minimiser le slippage.

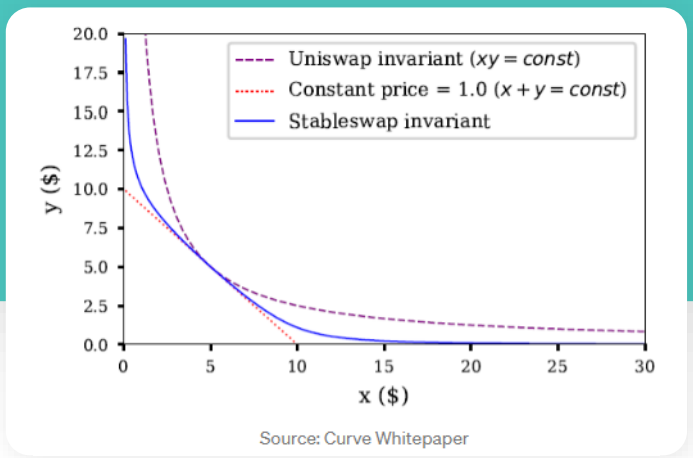
De nombreux protocoles ont copié ou tenté d'améliorer le fonctionnement d'UniSwap. Rappelons ici que le code est open source dans l'univers de la DeFi, ce qui induit une vitesse d'innovation impressionnante dans le secteur. Des clones d'UniSwap développés sur des chaînes concurrentes d'Ethereum, tels que Pancakeswap ou Sushiswap ont connu un succès important. Mais le protocole qui concurrence actuellement le plus UniSwap en termes de liquidité proposée est Curve, fondé au début de l'année 2020, et dont nous allons analyser le fonctionnement.

3.2. CURVE

Curve proposait initialement d'échanger exclusivement des stablecoins (par exemple DAI vs USDC) puis a diversifié son offre en proposant entre autres le BTC et l'ETH. Malgré cette diversification, Curve reste une plateforme d'échange optimisée pour les stablecoins. Etant donné que ces derniers présentent par nature un fort niveau de corrélation et une faible volatilité, car répliquant le même actif sous-jacent, le risque d'impermanent loss que nous avons analysé plus haut est fortement réduit. De plus, le slippage a pu également être réduit par l'utilisation d'un mécanisme sensiblement différent du « constant product » market making d'UniSwap.

Curve utilise une fonction hybride entre « constant sum » lorsque le pool de liquidité est équilibré, et « constant product », lorsqu'il est en déséquilibre (*voir Figure 12 page suivante*). Ce mécanisme permet de réduire fortement le slippage ce qui rend le protocole très compétitif.

Figure 12 : Fonction hybride « constant sum » et « constant product »



Source: Curve Whitepaper

Un autre aspect intéressant du protocole est qu'en plus des frais de transaction, les apporteurs de liquidité sont rémunérés avec des tokens de gouvernance, les CRV. Dans le but d'éviter que ces tokens soient revendus immédiatement une fois obtenus, le protocole a mis en place un système de récompense si l'utilisateur les bloque dans un smart contract pour une durée comprise entre 1 an et 4 ans. L'utilisateur reçoit un certain nombre de veCRV (Vote Escrowed Curve) en échange de ses CRV bloqués. Ces veCRV permettent de recevoir 50% des frais de transaction de tous les pools de Curve, mais également de « booster » ses revenus sur les pools de liquidité où l'utilisateur va déposer des crypto-actifs.

CURVE WARS

En supplément des avantages cités précédemment, les veCRV donnent des droits de votes pour déterminer la quantité de récompenses en CRV à attribuer par pool de liquidité. Curve étant l'un des DEX le plus important du marché, un protocole émettant un stablecoin aura intérêt à se procurer un maximum de veCRV s'il veut attirer de la liquidité sur un pool permettant son échange, car il pourra voter pour en augmenter le rendement.

Cependant, les protocoles voulant promouvoir leurs crypto-actifs ne sont pas les seuls intéressés par ces droits de votes. Des protocoles d'agrégation tels que Convex, se sont greffés sur Curve et permettent à leurs utilisateurs d'unir leurs droits de vote pour booster leurs revenus dans les pools de liquidité. Convex possède une quantité tellement importante de veCRV et donc de droits de votes, qu'à présent les protocoles souhaitant influer sur les pools de liquidité de Curve préfèrent passer par Convex en achetant du CVX, le token de gouvernance de Convex, ou bien en louant les droits de vote des détenteurs de CVX. Une « Bribing Economy » soit économie du soudoiement s'est même développée, des protocoles se spécialisant sur l'optimisation des « pots-de-vin » et le contrôle de Convex et Curve.

Par sa position dominante sur le marché et sa « tokenomics » particulièrement réussie, Curve a donc permis à tout un écosystème de se développer autour de son protocole, et est devenu l'un des principaux champs de bataille de l'univers DeFi pour le contrôle de la liquidité.

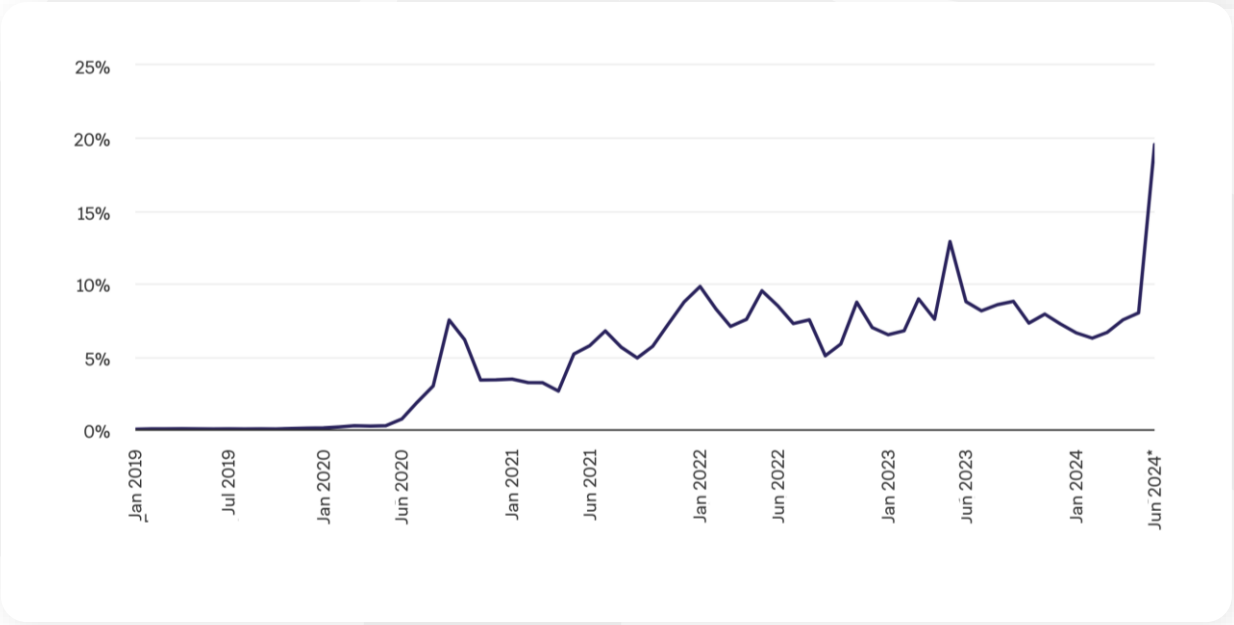


Figure 13 : Evolution du volume traité sur les échanges décentralisés (DEX) par rapport aux échanges centralisés (CEX) (Source : Theblock.co)

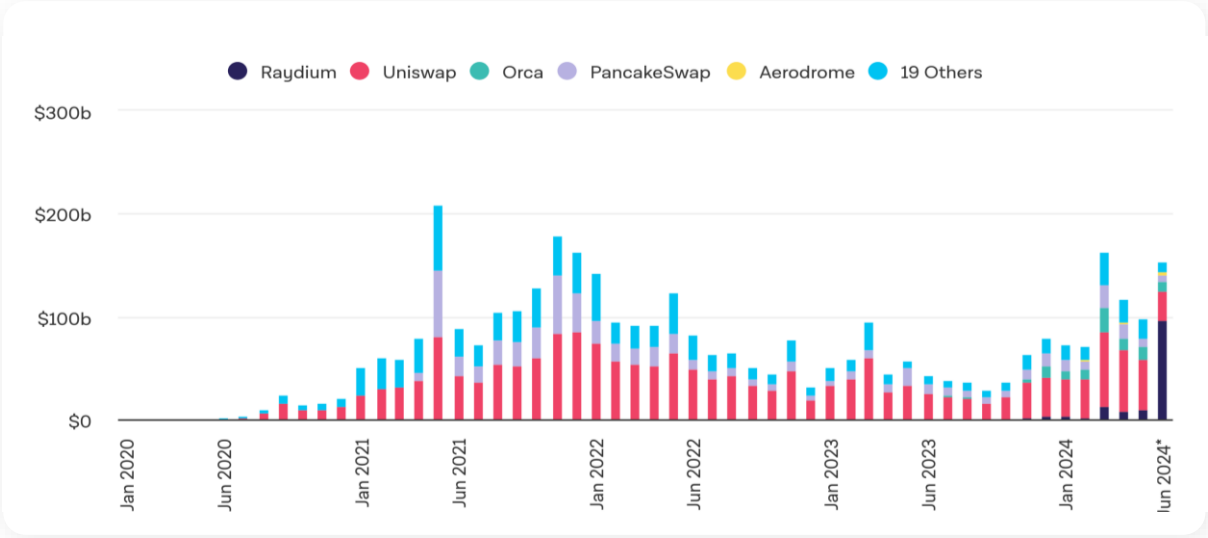


Figure 14 : Evolution du volume traité sur les échanges décentralisés (DEX) par rapport aux échanges centralisés (CEX) (Source : Theblock.co)

INTERVIEW

LOUIS BERTUCCI

Head of Center for Digital and Decentralized Finance (C2DF)

INSTITUT LOUIS BACHELIER

Louis Bertucci est chercheur à l'Institut Louis Bachelier (Paris, France). Il a obtenu un doctorat en économie financière de l'Université Paris-Dauphine en 2019. Depuis 2017, son travail est presque entièrement axé sur l'analyse fondamentale des protocoles blockchain.

Ses intérêts se portent sur les protocoles de consensus, la finance décentralisée et d'autres sujets connexes. À l'Institut Louis Bachelier, il est responsable du Centre pour la Finance Numérique et Décentralisée (C2DF) et le coordinateur scientifique du Programme FaIR : Finance and Insurance Reloaded.

Il enseigne également l'économie de la blockchain à Paris-Dauphine depuis 2020, et intervient fréquemment sur la blockchain et la DeFi lors de programmes de formation professionnelle en Europe.

« L'idée principale que nous portons avec le C2DF est qu'il existe 40 ans de recherche en finance quantitative et qu'il faut absolument utiliser ces enseignements pour développer la DeFi et plus largement le système financier de demain. »

Quelles sont les dernières évolutions technologiques marquantes au niveau des protocoles décentralisés d'échanges et de prêts ?

Que ce soit sur les protocoles d'échanges ou de prêts décentralisés, la tendance est à la séparation des rôles. Historiquement les protocoles DeFi s'occupaient eux-mêmes de l'ensemble des fonctions de l'échange ou du prêt. De la définition des prix, de la liquidité, des paramètres de risque, et l'ensemble des autres fonctions n'étaient que très peu personnalisables. Bien que les développeurs de ces protocoles soient bien placés pour proposer des protocoles efficients, ils ne peuvent pas convenir à toutes les utilisations. Que ce soit avec l'annonce d'Uniswap V4 avec les « hooks » (pas encore live) ou encore Morpho Blue avec MetaMorpho et les «vaults » (live depuis Janvier 2024), la tendance est à la personnalisation. Les protocoles eux-mêmes prennent en charge les fonctions les plus importantes : sécurité des actifs, règlement-livraison, fonction de dépositaire, mais offrent la possibilité que des tiers personnalisent la gestion du risque ou de la liquidité par exemple. Même si le protocole d'ancienne génération Aave reste encore le plus important en termes de volumes. Morpho blue a fait un très bon démarrage, en rassemblant plus d'un milliard de dollars de TVL en 5 mois. Les prochains mois nous diront si cette tendance se confirme.

INTERVIEW

LOUIS BERTUCCI

Aujourd'hui, de nombreuses solutions coexistent. Devant la domination croissante de protocoles comme Uniswap, tend-on vers une concentration du marché ou bien de nouveaux protocoles innovants pourraient continuer d'émerger ?

Par nature, les barrières à l'entrée dans le monde de la DeFi sont assez faibles, et le coût de changement de protocole (pour un utilisateur) est relativement faible à cause de l'interopérabilité. Économiquement c'est une situation qui est censée favoriser l'émergence d'acteurs innovants.

Il y a cependant des effets d'échelle en particulier au niveau de la liquidité des protocoles qui pourraient contrebalancer cette émergence. Tout se jouera au niveau de la concurrence, tant que les acteurs importants comme Uniswap continueront d'innover il sera plus compliqué pour des nouveaux acteurs de se faire une place dans l'écosystème. Cependant il ne faut pas oublier que l'innovation est extrêmement rapide dans la DeFi donc nous ne sommes pas à l'abri de renversements de part de marché.

Vous avez créé le C2DF (Center for digital and decentralized finance) au sein de l'Institut Louis Bachelier. Quelle est l'ambition de ce centre de recherche ?

La plupart des protocoles DeFi sont développés par des ingénieurs, et des entrepreneurs qui ne viennent pas nécessairement du monde de la finance. L'idée principale que nous portons avec le C2DF est qu'il existe 40 ans de recherche en finance quantitative et qu'il faut absolument utiliser ces enseignements pour développer la DeFi et plus largement le système financier de demain. Bien que l'infrastructure soit complètement différente, une blockchain vis-à-vis d'un ensemble d'intermédiaires, les principales fonctions financières comme l'échange d'actifs et le prêt ne sont pas du tout nouvelles, et sont même intrinsèques à la nature d'agents économiques. Nous accompagnons donc les acteurs de la DeFi pour leur apporter cet accès à la recherche en finance traditionnelle, tout en faisant nous-même avancer la frontière de la recherche en finance digitale et décentralisée.

Par nature, les barrières à l'entrée dans le monde de la DeFi sont assez faibles, et le coût de changement de protocole (pour un utilisateur) est relativement faible à cause de l'interopérabilité.

4 PROTOCOLES DE PRÊTS DÉCENTRALISÉS (LENDING)

TVL (Total Value Locked) : **32,8 Md$** **Evolution : +119% 1 an**

Taux d'intérêt annuel prêteur (USDC - Aave) : **7,26%** (moyenne 6 mois)

Parts de marché du leader Aave **: 37,12%**

Sources : coinmarketcap.com, coingecko.com, defillama.com (données à fin juin 2024)

Ces protocoles constituent l'un des rouages essentiels de l'écosystème DeFi en permettant à leurs utilisateurs d'emprunter ou prêter des crypto-actifs à un taux d'intérêt généralement variable et sans aucun tiers de confiance.

Leur fonctionnement est ainsi totalement différent du schéma classique dans lequel la banque joue le rôle de tiers de confiance, et va évaluer le risque de crédit de l'emprunteur avant de le financer, et se refinancer elle-même auprès d'une banque centrale ou d'autres banques sur le marché monétaire.

Dans l'écosystème DeFi où la confiance repose uniquement sur le code et où les utilisateurs sont représentés de manière pseudonyme par une clé cryptographique publique, les emprunts doivent être systématiquement collatéralisés afin de pallier l'absence de système de notation de crédit.

De nombreux protocoles permettent d'effectuer ce type d'opérations, nous allons ici étudier les plus emblématiques :

4.1 COMPOUND

Compound est un protocole qui permet à ses utilisateurs de prêter ou emprunter instantanément des crypto-actifs, moyennant un taux d'intérêt variable déterminé de manière algorithmique.

Les prêts ne sont pas bilatéraux mais transitent par un smart contract appelé pool de liquidité. Aucune maturité n'est prédéfinie, les utilisateurs pouvant retirer leurs fonds ou rembourser leur emprunt à chaque nouveau bloc miné sur la blockchain Ethereum, soit environ toutes les 12 secondes.

4.1.1 MODÈLE DE TAUX D'INTÉRÊTS

Les taux de prêt et d'emprunt sont recalculés à chaque nouveau bloc, en fonction de l'offre (liquidité présente dans le pool – $\boldsymbol{Cash_a}$) et de la demande (montant des emprunts en cours - $\boldsymbol{Cash_b}$). Ce ratio d'utilisation $\boldsymbol{Ua}$ de la liquidité est déterminé par la formule suivante :

$$U_a = Borrows_a \,/\, (Cash_a + Borrows_a)$$

Le taux d'intérêt à payer par les emprunteurs est ensuite déterminé par la fonction suivante :

$$Borrowing\ Interest\ Rate_a \;=\; 2.5\% + U_a * 20\%$$

Le taux fixe de 2.5% est donné à titre indicatif, de même que le facteur ($\boldsymbol{Multiplier}$) de 20% ; ces deux constantes sont fixées par vote, par les détenteurs de COMP, le token de gouvernance du protocole.

Le taux d'intérêt reçu par les prêteurs est calculé en multipliant celui des emprunteurs par le ratio d'utilisation $\boldsymbol{Ua}$.

Ce mécanisme de taux variables indexés sur un ratio d'utilisation vise à orienter la liquidité vers les pools où la demande d'emprunt est forte et donc présentant un rendement élevé. Il permet également de dissuader les emprunteurs d'utiliser un pool à la liquidité insuffisante, équilibrant ainsi l'offre et la demande.

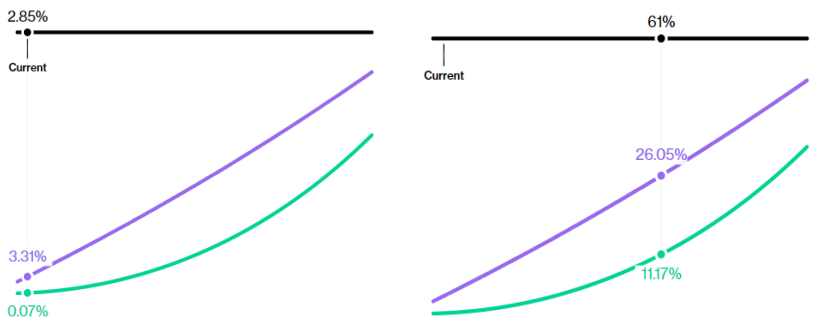


Figure 15 : Fonction des taux d'intérêts et du taux d'utilisation (Source : compound.finance)

Certains pools utilisent un modèle à saut sensiblement différent, dans lequel le taux d'intérêt va croître de manière accélérée ($\boldsymbol{Jump\ Multiplier}$) lorsqu'un certain seuil ($\boldsymbol{Kink}$) va être dépassé :

$$\boldsymbol{Borrow\ Interest\ Rate} = \boldsymbol{Multiplier} * \min(U_a, \boldsymbol{Kink}) + \boldsymbol{Jump\ Multiplier} * \max(0, U_a - \boldsymbol{Kink}) + \boldsymbol{base\ rate}$$

(voir Figure 16 page suivante)

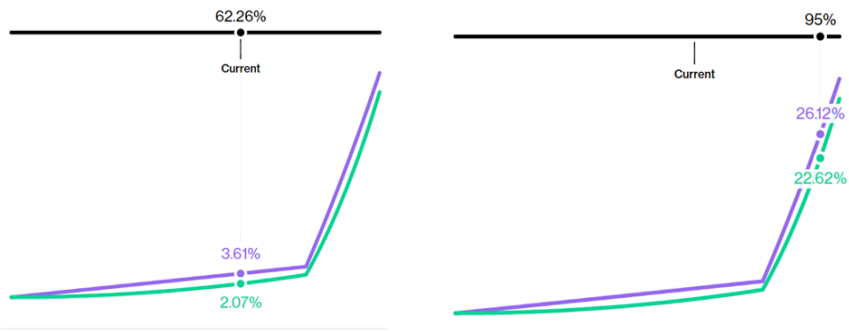


Figure 16 : Fonction des taux d'intérêts et du taux d'utilisation
(Source : compound.finance)

4.1.2. CTOKEN

Lorsqu'un utilisateur apporte de la liquidité sur un pool, il reçoit en échange des cTokens. Ces crypto-actifs ERC20 peuvent être échangés ensuite à tout moment (ou plutôt à chaque nouveau bloc miné) contre l'actif d'origine présent dans le pool. Leur valeur augmente à chaque bloc de 1/2102400 du taux d'intérêt variable annuel calculé via la formule vue précédemment. Rappelons ici que l'écosystème DeFi étant ouvert, les cTokens peuvent être échangés, prêtés ou bien placés dans des pools de liquidités sur des Dex, les autres protocoles pouvant interagir avec les smart contracts de Compound sans permission.

Il peut donc exister une multitude de marchés secondaires ou de produits dérivés basés indirectement sur le protocole compound. La finance décentralisée peut être envisagée comme un jeu de lego géant où les protocoles s'imbriquent les uns avec les autres, et où tout le monde peut construire par-dessus la structure existante.

4.1.3. MÉCANISME D'EMPRUNT

Avant de pouvoir emprunter via le protocole, il faut dans un premier temps déposer des crypto-actifs dans un ou des pools de liquidité. Les cTokens obtenus en échange vont alors constituer le collatéral qui va permettre d'emprunter d'autres crypto-actifs, pour un montant maximum défini par un facteur de collatéral, déterminé pour chaque pool par vote des détenteurs de Comp. A l'instar du fonctionnement du protocole Maker décrit précédemment, le collatéral de l'emprunteur sera liquidé en dessous d'un certain seuil. Et comme pour Maker, les positions sont valorisées à partir de prix de marchés alimentés par un Oracle, encore une fois sélectionné par vote.

Le protocole Compound constitue une brique importante de l'écosystème DeFi, en offrant ce qui s'apparente à un marché « monétaire » fixant des taux d'intérêts selon les lois de l'offre et de la demande, et ce, sans tiers de confiance. De plus les règles (crypto-actifs autorisés, modèles de taux, réserve …) sont entièrement définies par vote de la communauté des détenteurs de Comp.

4.2. AAVE

Aave, le principal concurrent de compound, qui l'a dépassé en termes de TVL (Total Value Locked, représentant le montant de liquidité présent sur le protocole), offre également un service de prêt/emprunt collatéralisé et sans tiers de confiance.

Le fonctionnement des deux protocoles est assez similaire (modèles de taux, token de gouvernance, émission de crypto-actif qui représente le montant prêté dans un pool de liquidité…). Aave offre cependant différentes fonctionnalités supplémentaires, notamment des prêts à taux fixe, basés sur la moyenne des taux variables d'un pool de liquidité. Il offre également une fonctionnalité innovante et endogène à la DeFi : les flash loans.

4.2.1. FLASH LOANS

Aave permet à ses utilisateurs d'emprunter des crypto-actifs sans collatéral, sous réserve qu'ils soient remboursés au sein de la même transaction. Le fait que l'emprunt et le remboursement soient réalisés de manière simultanée, car au sein d'une même transaction et donc d'un même bloc sur la chaîne, permet d'éliminer tout risque de contrepartie, d'où l'absence de collatéral requis.

Ce mécanisme peut permettre aux utilisateurs de réaliser des arbitrages sans avoir à mobiliser de fonds : par exemple si une opportunité d'arbitrage existe entre deux Dex, un utilisateur pourra emprunter un certain montant sur Aave qui va lui permettre d'acheter un crypto-actif sur un Dex A, de le revendre à un prix supérieur sur un Dex D, puis d'effectuer le remboursement du montant initial sur Aave, le tout au sein d'une transaction unique et sans mobiliser de fonds. Il empochera donc instantanément un gain.

Cet accès instantané, à d'importantes quantités de liquidités, a également rendu possible des attaques sophistiquées contre des protocoles d'échanges présentant des vulnérabilités au sein de leurs smart contracts : un attaquant peut se servir de ce formidable effet de levier pour déséquilibrer fortement un pool de liquidité sur un DEX, créant par là une opportunité d'arbitrage qu'il va exploiter. Des dizaines de millions d'euros ont ainsi été subtilisés depuis l'invention des flash loans.

Le fait que l'écosystème DeFi soit ouvert et modulaire l'expose à des attaques permanentes de la part d'acteurs malhonnêtes. Des centaines de millions d'euros sont dérobés chaque année. Cependant, l'écosystème s'adapte, se renforce et devient de plus en plus résistant au gré des attaques, la moindre faille devant être rapidement corrigée. Une certaine sélection naturelle s'opère, les protocoles les plus vulnérables disparaissant. La croissance véritablement organique de la DeFi rend ainsi le secteur d'autant plus fascinant.

4.3. NOUVEAUX ACTEURS

Pour la plupart des protocoles de prêts décentralisés, le mécanisme repose sur le modèle peer-to-pool : les fournisseurs de liquidité déposent leur liquidité dans un pool tandis que l'emprunteur fournit du collatéral au protocole en échange de la liquidité présente dans ce même pool. L'emprunteur verse ensuite des intérêts qui sont partagés par tous les fournisseurs de liquidité du pool (« socialized yields »). Ce mécanisme induit un spread important entre les intérêts payés par les emprunteurs et ceux versés aux prêteurs.

Asset	Total supplied	Supply APY	Total borrowed	Borrow APY, variable
Ethereum ETH	855.84K $2.93B	2.57%	770.91K $2.64B	3.37%
Tether USDT	1.80B $1.80B	4.90%	1.33B $1.33B	7.48%
USD Coin USDC	1.44B $1.44B	6.81%	1.25B $1.25B	8.83%
Wrapped eETH weETH	550.05K $1.96B	0.46%	112.33K $400.16M	4.17%
Wrapped BTC WBTC	32.99K $2.04B	0.14%	4.62K $286.31M	1.25%

Figure 17 : Spread entre les intérêts payés par les emprunteurs et ceux versés aux prêteurs sur le protocole Aave (Source : app.aave.com, fin juin 2024)

Cet écart significatif (plus de 2,5% pour l'USDT par exemple sur la figure 17) s'explique par le fait que dans la plupart des pools il y ait beaucoup plus de prêteurs que d'emprunteurs. Pour compenser la sous-utilisation de la liquidité dans les pools, les protocoles se voient contraints d'augmenter les intérêts payés par les emprunteurs et diminuer ceux versés aux prêteurs, entraînant ainsi le spread observé.

Certains acteurs comme le DApp **Morpho** se sont fixés comme objectif de résoudre ce problème afin de proposer le même taux d'intérêt aux prêteurs et aux emprunteurs. Pour ce faire, la plateforme fait directement correspondre les emprunteurs et les prêteurs sur la base d'une queue first-in-first-out (FIFO) : les premiers prêteurs déposant leur liquidité sont les premiers à être associés à un emprunteur. Une fois que la paire prêteur-emprunteur est formée, le protocole peer-to-peer va ensuite choisir le taux d'intérêt (appliqué aux deux membres de la paire) à l'intérieur du spread existant sur les protocoles Aave et Compound afin d'être avantageux pour les deux parties. Pour les prêteurs qui n'ont pas encore été associés à des emprunteurs, Morpho va déposer leurs liquidités sur les protocoles de lending peer-to-pool (Aave et Compound) afin de leur garantir de recevoir au minimum le rendement proposé sur ces protocoles.

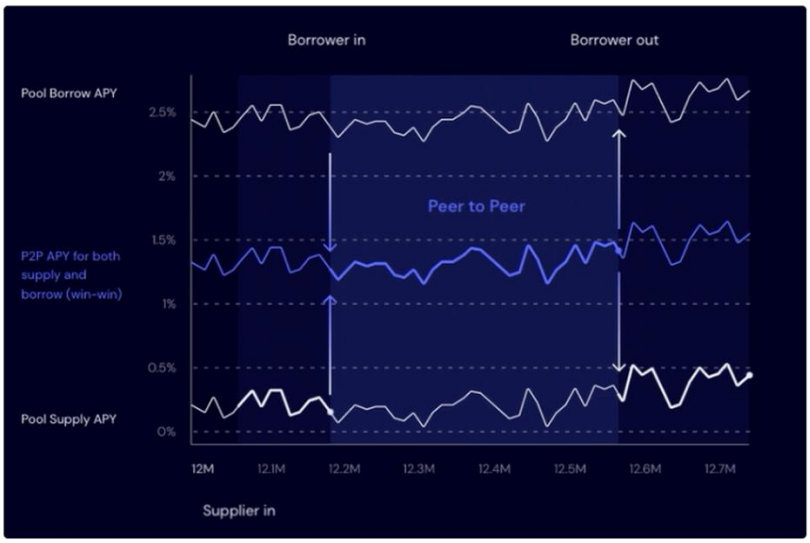


Figure 18 : Système de matching entre prêteurs et emprunteurs sur Morpho (Source : morpho.org)

Parmi les protocoles de lending les plus récents on compte également **Liquity**. Ce protocole se démarque des autres en offrant des prêts à taux zéro en échange d'une garantie minimale de 110% en ETH uniquement. Liquity est un système à deux tokens, à l'instar de MakerDAO, où son stablecoin LUSD (adossé au dollar) est prêté en échange d'ETH alors que son token LQTY est utilisé comme récompense pour encourager les utilisateurs à maintenir la solvabilité du protocole. Les seuls frais pour l'emprunteur sont des frais fixes payés lors de l'emprunt et du remboursement des LUSD. A noter que Liquity est un protocole sans gouvernance où les règles de fonctionnement fixées au moment de sa création sont immuables ce qui est également très différent des autres protocoles décrits précédemment.

Contrairement à la finance traditionnelle, l'ensemble des prêts accordés dans l'écosystème de la DeFi doivent être collatéralisés et même sur-collatéralisés pour la majorité d'entre eux. L'éclosion des prêts non-collatéralisés dans l'écosystème de la DeFi, au-delà des flash loans, pourrait permettre d'accélérer l'adoption de ces outils financiers.

A noter que certains protocoles comme BendDao permettent de réaliser des emprunts en apportant des NFT (Non Fungible Token) en tant que collatéral. Ce pont entre le monde de l'art digital et la finance décentralisée est un autre exemple de la composabilité permise par la blockchain et les smart contracts.

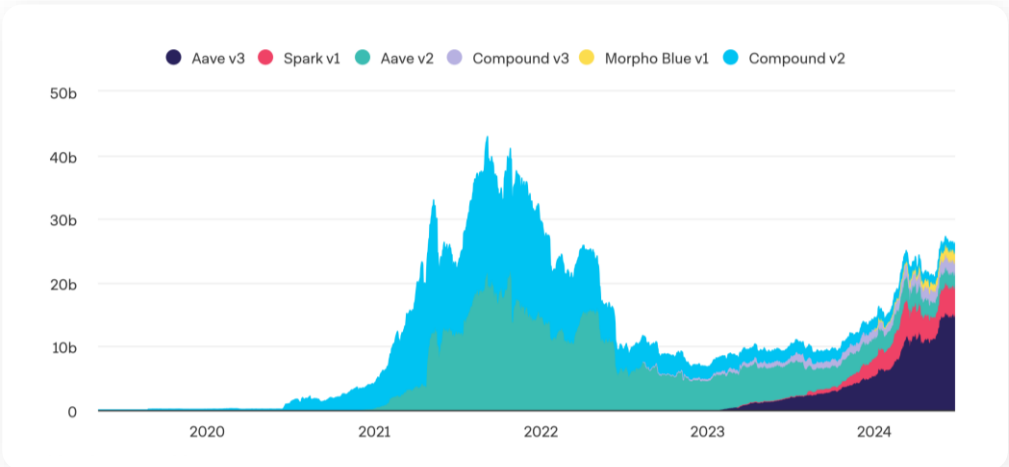


Figure 19 : Montant total déposé (USD) sur les protocoles de lending d'Ethereum (Source : theblock.co)

LES NFT

A l'image du marché des œuvres d'art « physiques », les non fungible tokens (NFT) se sont développés au sein de l'univers digital de la blockchain à partir de 2017 avec la publication de la norme ERC-721.

Les NFT désignent des fichiers numériques reliés à des certificats d'authenticité numérique. Le fichier numérique seul est fongible, mais le certificat garantit sa propriété exclusive, d'où la caractéristique non fongible. Les droits d'auteur et de reproduction peuvent toutefois être conservés par l'artiste ou transférés selon les termes du contrat. Les NFT peuvent être associés à une peinture, une vidéo, un meme, une photographie, des objets de collection, des éléments de jeux-vidéos, de la musique, etc...

A la suite de la publication de la norme ERC-721 plusieurs projets NFT ont vu le jour tels que les crypto-punks qui se vendent encore aujourd'hui pour un floor price égal à environ 26 ETH tout en enregistrant des centaines de transactions par mois.

L'année 2021 a connu un engouement particulier pour les NFT, notamment avec la collection "Bored Ape Yacht Club" qui a généré à elle seule un volume de vente supérieur à 1.08 millions d'ETH et affiche aujourd'hui un floor price à environ 9 ETH.

Aujourd'hui, les places de marché principales sur lesquelles s'échangent les NFT sont Blur et Opensea qui enregistrent chacune un volume de transaction d'environ 10 000 ETH hebdomadaire sur leur plateforme respective.

BLUR OpenSea

5 PRODUITS DÉRIVÉS ET STRUCTURÉS

Volume d'échange dérivés (juin 2024) : **202 Md$** (perpetual DEXs) **13,8 M$** (options premiums)

Liquid Staking Derivatives TVL : **52,3 Md$**

C'est naturellement que des protocoles DeFi proposant des produits dérivés ont émergé, afin de permettre aux utilisateurs de couvrir certains risques ou bien de spéculer avec effet de levier.

La nature ouverte, modulable et non régulée de la DeFi donne lieu à l'émergence constante de nouveaux produits plus ou moins sophistiqués, et plus ou moins sécurisés. Contrairement à la finance traditionnelle où les nouveaux produits mettent des années à évoluer, sous une contrainte réglementaire forte, dans la DeFi nous assistons à l'émergence fréquente de nouveaux produits. Nous allons ici explorer de manière synthétique les principaux instruments et protocoles apparus à ce jour :

5.1. PERPETUAL SWAP CONTRACTS

Introduits par Bitmex en 2016, les perpetual swap contracts (perpetuals) ont révolutionné le trading de crypto-actifs. Appartenant à la catégorie des dérivés futures, les perpetuals permettent de prendre une position sur le prix de l'actif sous-jacent sans le détenir physiquement. A la différence des futures traditionnels, les perpetuals n'ont pas de date d'expiration et le contrat reste donc ouvert jusqu'à ce que le détenteur décide de fermer sa position.

En échange d'un apport de collatéral, les traders peuvent utiliser un effet de levier pouvant aller jusqu'à x100. Une fois ouverte, la position sur le perpetual est similaire à du margin trading : si la valeur de la position descend en dessous d'une certaine marge, le trader doit augmenter son collatéral sinon il voit sa position être liquidée.

Si l'offre de ce produit s'est fortement développée dans l'écosystème de la DeFi, le marché des perpetuals reste cependant largement dominé par les CEX comme Binance.

La première plateforme décentralisée ayant réussi à capturer le plus de parts de marché est dYdX. Cependant, depuis 2023, la concurrence s'est fortement accrue et le protocole a vu son volume d'échanges stagner voire baisser. (voir Figure 20)

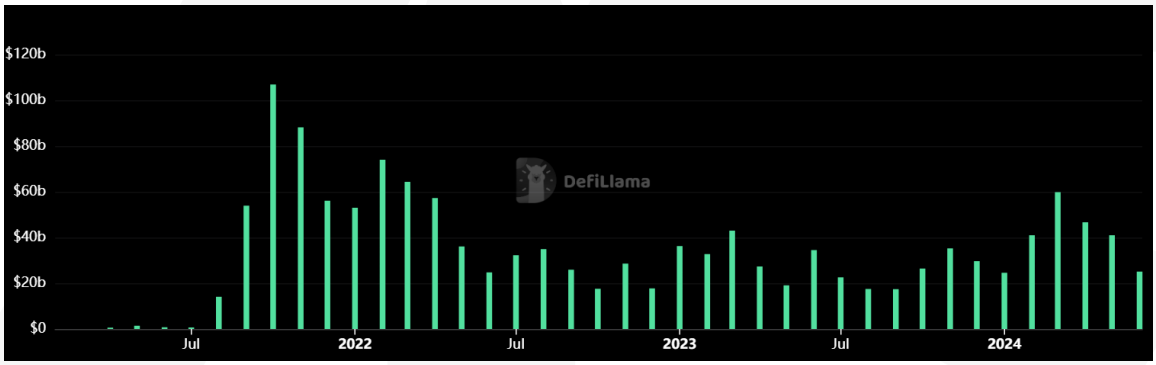


Figure 20 : Évolution du volume mensuel de dérivés échangés sur dYdX (Md$)
(Source : DefiLlama.com)

DYDX

Lancé en 2017, dYdX propose des contrats de perpetuals swaps avec un effet de levier allant jusqu'à x20.

Afin de maintenir le prix du perpetual le plus proche possible du prix de l'actif sous-jacent, les perpetuals échangés sur dYdX sont soumis à un funding rate. Il s'agit de frais payés par les investisseurs en position long aux investisseurs en position short, lorsque le prix du contrat se situe au-dessus du prix de l'actif sous-jacent, ou inversement lorsqu'il se situe en dessous. Le prix de référence servant à calculer le funding rate est fourni par un oracle (ici, Chainlink).

Toutes les heures, un utilisateur ayant une position sur le marché reçoit ou paye un montant égal à :

$$F = (-1) * S * P * R$$

Avec :

- **S :** "Size", le montant de sa position (positif si long, négatif si short)
- $\boldsymbol{P}$ **:** l'Index price renseigné par l'oracle
- $\boldsymbol{R}$ **:** le funding rate (calculé toutes les heures). Avec : R = Moyenne Premium / 8 + Taux intérêt fixe du marché

La composante principale du funding rate est le premium, calculé toutes les minutes :

$$\boldsymbol{Premium} = (\boldsymbol{Max}(\boldsymbol{0}, \boldsymbol{IBP} - \boldsymbol{P}) - \boldsymbol{Max}(\boldsymbol{0}, \boldsymbol{P} - \boldsymbol{IAP}))/\boldsymbol{P}$$

- $\boldsymbol{IBP}$ **:** "Impact Bid Price" représente le prix moyen de vente du perpetual.
- Réciproquement, $\boldsymbol{IAP}$ ("Impact Ask Price") représente le prix moyen d'achat du perpetual.

Le funding rate étant réactualisé toutes les heures, celui-ci s'appuie sur la moyenne des 60 derniers premiums calculés (comme indiqué dans la formule de R ci-dessus). De plus, s'ajoute à son calcul un taux d'intérêt fixe prenant en compte la différence de taux d'intérêts native entre les deux devises.

En 2021, la plateforme développe son propre layer 2, une surcouche s'ajoutant à la blockchain Ethereum et permettant de traiter une quantité de transactions beaucoup plus importante dans un temps minimal. Le layer 2 permet de disposer d'un carnet d'ordre branché directement sur la blockchain et updaté en permanence. La contrepartie de cette évolution étant l'augmentation de la complexité du système et le risque de dysfonctionnement de ce dispositif.

dYdX émet des tokens de gouvernance, servant à rémunérer les développeurs mais également les traders et les fournisseurs de liquidité. Ces tokens permettent de participer à la gouvernance du protocole via un système de vote.

En 2023, dYdX déploie une quatrième version, tout en migrant vers sa propre blockchain basée sur Cosmos et Tendermint, la "DYDX Chain". Le protocole devient à cette occasion 100% décentralisé et open-source dès octobre 2023. Le token $dYdX passe d'un token ERC-20 de la blockchain ETH à un token du layer 1 de la blockchain propre à dYdX.

5.2. OPTIONS ET OPTIONS VAULTS

Instruments phares de la finance traditionnelle, les options sont également disponibles dans l'écosystème de la DeFi. Pour rappel, une option offre à son acheteur le droit, et non l'obligation, d'acheter ou de vendre le sous-jacent (ici les devises cryptos telles que BTC et ETH) à un prix fixé à l'avance.

Une nouvelle catégorie de produit spécifique à la DeFi a été créé : les Option Vaults. Il s'agit de "coffres" digitaux dans lesquels les utilisateurs peuvent poster leurs crypto-actifs. Ces coffres sont ensuite gérés de manière automatisée par des smart contracts selon des stratégies d'achat et de vente d'options prédéfinies. De plus, certains de ces coffres intègrent des mécanismes de staking ou de gouvernance afin de maximiser le rendement.

Si des plateformes centralisées comme Deribit offrent déjà du trading d'options, l'offre en options vaults est encore assez limitée dans l'espace CeFi. En revanche, plusieurs protocoles DeFi proposent ce type de stratégies à leurs utilisateurs, c'est le cas notamment de Dopex.

HEGIC

Créée en 2020, la plateforme permet aux utilisateurs de souscrire différents types d'options sur BTC et ETH contre de l'USDC.

Elle propose différentes stratégies et une large plage de strikes et maturités permettant de profiter de différentes dynamiques de marchés :

- **Tendance haussière :** Call, Strap, Bull Call spread, Bull Put spread
- **Tendance baissière :** Put, Strip, Bear Call spread, Bear Put spread
- **Faible volatilité :** Long Butterfly, Long Corridor
- **Haute volatilité :** Straddle, Strangle

Pour proposer cette vente d'options et couvrir les pertes du protocole, Hegic met en place un pool de liquidité nommé « S&C (Stake & Cover) pool » dans lequel les LPs déposent leurs liquidités en échange des premiums des options vendues. De cette façon, 100% du P&L issu des ventes d'options est redistribué aux LPs.

DOPEX - SINGLE STAKING OPTIONS VAULT (SSOV)

Lancée en juin 2021, la plateforme Dopex propose aux utilisateurs d'investir dans des SSOVs. Ce produit permet aux investisseurs de poster leurs crypto-actifs comme collatéral couvrant des stratégies de vente d'option, en contrepartie d'un certain rendement, de manière similaire au S&C pool d'Hegic.

Ces rendements peuvent prendre la forme de premiums issus des options vendues, de DPX (token de gouvernance de Dopex) ou encore d'actifs (tels que des options) eux-mêmes générateurs de rendement. Dans ce dernier cas, les options gratuites fournies en compensation permettent de couvrir les éventuelles fluctuations de marché défavorables aux actifs déposés en tant que collatéral dans le SSOV.

La plateforme Dopex permet également aux utilisateurs de faire du staking directement dans des OLP (Option Liquidity Pool), de manière plus classique. La différence entre les SSOVs et les OLPs étant que les actifs verrouillés dans les SSOVs servent directement de collatéral pour l'émission des options (marché primaire) et pour être utilisés au sein de différentes stratégies spécifiques au vault dans lesquels ils sont investis. Les OLPs servent quant à eux de réserves de liquidité pour le trading des options (marché secondaire). Enfin, il est possible d'emprunter directement le collatéral contenu dans les options via l'achat d'un produit que la plateforme nomme "Atlantic Options".

Opérant en tant que DAO, la plateforme émet ses propres tokens :

- Le DPX est le token de gouvernance de la plateforme, il permet aux détenteurs de voter les décisions impactant la plateforme et de percevoir des rendements sur les frais appliqués aux utilisateurs pour l'utilisation de la plateforme.
- Le rDPX est un token distribué aux fournisseurs de liquidités qui ont subi des pertes afin de compenser ces dernières. Ce token permet de miner des actifs synthétiques : les $DSCs (Dopex Synthetic Coins).

On peut citer Opyn, qui offre des services similaires via un protocole DeFi, comme principal concurrent de Dopex.

5.3. VOLATILITÉ

La nature extrêmement volatile des crypto-actifs rend ce marché particulièrement intéressant pour la création de produits dérivés basés sur la volatilité. Bien que les projets DeFi proposant ce nouveau type d'instruments aient jusqu'à présent attirés peu de liquidité, ils témoignent de la forte innovation du secteur et de l'élargissement constant de son éventail de produits financiers.

VOLMEX

Cette plateforme, créée début 2023, développe des indices de volatilité implicites sur les cryptomonnaies et permet à ses utilisateurs de négocier des tokens de volatilité, en particulier sur BTC et ETH. Le niveau des indices est calculé via des smart contracts, sur la base de données de marché issues d'oracles et représentant la volatilité du crypto-actif sous-jacent.

Pour chaque actif sous-jacent sont générés deux types de tokens : VOL et iVOL (volatilité inversée). Lorsque la volatilité du sous-jacent augmente, la valeur du VOL augmente tandis que celle d'iVOL baisse symétriquement, et inversement, ce qui permet aux traders de prendre des positions sur la volatilité future des actifs sous-jacents sans les détenir directement. Pour le calcul des prix respectifs des tokens VOL et iVOL, le protocole utilise un AMM faisant appel à une formule de produit constant (à la manière du mécanisme décrit dans la partie de l'étude traitant du protocole Uniswap), à ceci près qu'il ajoute un coefficient dit « de levier » prenant en compte la réserve de tokens VOL et iVOL.

Comme pour les autres protocoles, les fournisseurs de liquidité jouent un rôle crucial et obtiennent en récompense un rendement en VOL et iVOL. Ils bénéficient également de frais générés par les transactions opérées sur la plateforme ainsi que des tokens de gouvernance Volmex. En contrepartie, ces fournisseurs de liquidités sont exposés au risque d'Impermanent Loss.

Volmex est un protocole relativement récent qui peut être sujet à un manque de liquidité en particulier pendant les périodes de faible activité de trading. Les utilisateurs peuvent également être confrontés à des frais de gaz élevés, que d'autres protocoles plus établis ont su couvrir avec le développement de layer 2.

5.4. DÉRIVÉS DE TAUX

Le swap de taux, un des instruments les plus couramment utilisés dans la finance traditionnelle pour la gestion des taux d'intérêt, est également disponible dans l'écosystème de la DeFi. Ce type de produit offre aux utilisateurs la possibilité d'échanger un taux d'intérêt fixe contre un taux variable, ou vice-versa. Cette nouvelle brique apporte une profondeur et une sophistication accrues au marché des crypto-actifs, en se fondant sur l'interopérabilité propre aux protocoles de la blockchain.

IPOR

Créé en 2022, IPOR est l'un des principaux protocoles permettant à ses utilisateurs la possibilité d'entrer dans des swaps de taux d'intérêts. L'infrastructure du protocole se compose des éléments suivants :

- Le calcul de l'IPOR Index permettant de définir les taux sous-jacents aux swaps.

- L'AMM d'IPOR et des réserves de liquidités issues des investisseurs.
- Des smart contracts « gestionnaires d'actifs » chargés de générer un rendement sur les stablecoins détenus par le protocole en les plaçant sur Aave et Compound.

L'IPOR Index représente le taux sans risque de l'actif correspondant, tel que l'IPOR ETH et est défini pour plusieurs maturités 1M, 3M, 6M. Le calcul de cet indice repose sur les données d'autres plateformes, en particulier des protocoles de lending tels qu'Aave et Compound pour lesquels le calcul de taux d'intérêt est décrit plus en amont dans notre étude.

Le protocole possède plusieurs réserves de liquidités (notamment USDC, USDT, DAI, stETH, et d'autres) utilisées par l'AMM conjointement avec l'IPOR Index afin de fournir des swaps (payeurs et receveurs) aux utilisateurs.

En échange de leurs actifs, les fournisseurs de liquidité du protocole obtiennent des tokens de liquidité permettant de profiter des frais de transaction issus de la vente de swaps ainsi que des rendements obtenus par les smart contracts de gestion d'actifs.

A la création du protocole, 100 000 000 IPOR tokens ont été émis et sont échangeables sur UniSwap. Ces tokens peuvent être placés en staking pour générer des tokens pwIPOR pouvant être utilisé par les fournisseurs de liquidité afin d'augmenter leur rendement. Les pwIPOR servent également de token de gouvernance pour IPOR DAO.

NOTIONAL FINANCE

Notional est un protocole permettant aux utilisateurs d'accéder à des rendements fixes peu risqués sur le marché de la DeFi. Le protocole se décompose en trois entités : les prêteurs et emprunteurs de taux fixe, et les fournisseurs de liquidité :

- **Prêteurs de taux fixe :** Ces utilisateurs déposent leurs tokens (DAI, ETH, USBC, ou wBTC) pour lesquels ils souhaitent percevoir un intérêt fixe pour une certaine maturité dans un pool, et reçoivent en échange des « ftokens » (fDAI, fETH, etc…) représentant l'actif prêté à taux fixe. Des frais de transaction s'appliquent lors du dépôt de l'actif, et ce dernier peut être retiré de manière anticipée à tout moment, à l'image d'un call américain. En revanche, si les actifs sont retirés avant la date de maturité, l'utilisateur doit alors payer une seconde fois les frais de transaction. Il rend alors les ftokens au pool et retire ses tokens natifs.
- **Emprunteurs de taux fixe :** Les utilisateurs souhaitant accéder à du capital sans vendre leurs crypto-actifs peuvent les poster en collatéral d'un emprunt. Le mécanisme est similaire à celui décrit dans la partie lending de cette note : les crypto-actifs sont déposés dans un pool et échangés contre des cTokens servant de collatéral. Afin de limiter les risques, les prêts sont surcollatéralisés et soumis à des frais de transaction. Notional se démarque cependant en proposant des taux fixes aux emprunteurs et prêteurs.

- **Mécanisme des taux fixes :** Le protocole Notional utilise un modèle de pools à échéance fixe. Les prêts et emprunts à taux fixe sont organisés autour de ces pools spécifiques, où les conditions de taux sont prédéterminées pour chaque maturité. Lorsqu'un prêteur dépose ses actifs dans un pool de taux fixe, il reçoit des ftokens représentant ces actifs, et les emprunteurs empruntent à partir de ces pools en déposant des collatéraux. Les taux sont fixés grâce à des algorithmes qui prennent en compte les conditions de marché et la demande pour ces prêts spécifiques. Ce mécanisme permet de sécuriser des rendements stables pour les prêteurs et des coûts de financement prévisible pour les emprunteurs.

- **Fournisseurs de liquidité (LPs) :** Les LPs assurent la fluidité entre emprunteurs et prêteurs en déposant leurs tokens dans les pools respectifs du protocole. Le mécanisme de dépôt de liquidité fonctionne de la façon suivante : l'utilisateur souhaitant déposer 100 DAI va automatiquement miner 100 fDAI qu'il va déposer dans le pool DAI de Notional, il dispose alors dans son portefeuille de -100 fDAI et de tokens de liquidité du protocole (appelés « nTokens ») attestant des actifs déposés et pouvant être rééchangés à tout moment pour retirer ses actifs. Les LPs bénéficient d'un rendement composé du taux variable de l'actif sous-jacent, des frais de transaction payés par les autres catégories d'utilisateurs, ainsi que de tokens « NOTE » qui sont les jetons de gouvernance du protocole. Les LPs perçoivent un rendement moyen plus élevé que les prêteurs à taux fixe, mais ce dernier est variable et est soumis à plus de risque, notamment au risque d'Impairmanent Loss lorsque le taux du pool varie selon les quantités respectives de cTokens et de fTokens qu'il contient. Les LPs peuvent aussi utiliser leur nTokens comme collatéral pour emprunter sur Notional, permettant de réaliser des stratégies de rendements complexes et diversifiées.

Le protocole dispose aussi de vaults à levier avec lesquels les utilisateurs peuvent miser sur des stratégies spécifiques avec un levier allant jusqu'à x10. Ces stratégies sont très diverses, plus risquées, et font intervenir d'autres protocoles pour obtenir des rendements plus élevés.

Enfin, Notional est un DAO dont les tokens NOTE servent de jetons de gouvernance. Ces tokens peuvent également être stakés via Balancer, un protocole AMM (Automated Market Maker).

5.5. LIQUID STAKING DERIVATIVES (LSD)

LIQUID STAKING (LIDO)

Il existe aujourd'hui une barrière à l'entrée importante pour participer au staking natif sur Ethereum. En effet, le capital nécessaire est de 32 ETH (soit environ 100 000€ à fin juin 2024). Afin de faciliter et rendre accessible à tous le staking, la plateforme décentralisée Lido a vu le jour en 2021. L'engouement des acteurs de la DeFi pour le staking a porté ce protocole pour en faire actuellement le leader au sein de la DeFi avec une TVL (Total Value locked) de plus de 33 milliards de dollars.

Lido simplifie le processus de staking natif décrit précédemment en agrégeant les tokens déposés par ses utilisateurs sur sa plateforme, puis en les "stakant" via plusieurs validateurs appartenant au réseau "Lido DAO", le DAO gouvernant la plateforme.

En stakant sur Lido, un utilisateur se voit attribuer des tokens stETH, représentant le montant total d'ETH stakés ainsi que les revenus de staking cumulés. Ces tokens, appelés staking derivatives en raison de leur nature indexée sur le sous-jacent ETH, sont liquides et peuvent être immédiatement utilisés dans d'autres plateformes DeFi pour prêter, emprunter, ou apporter de la liquidité.

Enfin, le protocole est gouverné de manière décentralisée par un DAO, via des tokens de gouvernance distribués aux utilisateurs actifs. A l'issue d'un vote, le DAO a notamment décidé que les rendements issus du staking des tokens des utilisateurs par la plateforme soient reversés à hauteur de 10% aux validateurs et aux fonds du DAO.

La plateforme Lido a récemment transitionné vers sa version 2, améliorant notamment sa méthode de sélection des validateurs. Dans sa première version, les validateurs étaient sélectionnés aléatoirement parmi une liste de stakers, ce qui impliquait un risque de slashing (voir encart staking) plus important et ainsi des rendements moyens plus faibles. Lido utilise à présent un système de sélection dynamique des validateurs, fonction de diverses métriques comme le montant staké ainsi que les conditions actuelles du réseau.

Bien que le staking sur le réseau Ethereum soit la priorité de la plateforme Lido, celle-ci permet également le staking sur d'autres réseaux, comme Polygon et Solana.

LE STAKING

Le réseau Ethereum a récemment transitionné, dans sa version 2.0, vers une méthode de validation des transactions opérées en son sein depuis un mécanisme "proof of work" à un mécanisme "proof of stake" (PoS) (ou preuve d'enjeu).

Le PoS implique que le réseau choisit des validateurs dont la tâche primordiale est de valider les transactions en créant les nouveaux blocs à ajouter à la chaîne, tout en verrouillant du collatéral, le "stake", afin de s'assurer d'un comportement honnête. Les validateurs sont récompensés pour chaque bloc créé, et les validateurs agissant de façon malhonnête ou en échouant à leur tâche se voient pénalisés par de la perte au niveau de leur stake (pénalisation appelée le "slashing").

Dans le cas d'Ethereum 2.0, le stake minimum à verrouiller pour devenir validateur est de 32 ETH. Devenir validateur n'est donc pas un processus évident, en plus du montant minimum à verrouiller il faut avoir les composants hardware nécessaires (carte graphique, SSD), une connexion internet stable, et être un validateur actif et juste pour ne pas subir de slashing. En raison de cette barrière à l'entrée, plusieurs plateformes et protocoles tels Lido ont été développés afin de rendre le staking accessible à tous.

Plus récemment, certains protocoles ont introduit la notion de **Restaking**, qui consiste à réutiliser les tokens de staking afin de percevoir un rendement supplémentaire, permettant d'engager des stratégies de rendements composés, au détriment d'un risque accru. EigenLayer est actuellement le leader dans ce domaine avec une TVL de plus de 17 milliards de dollars.

5.6. PRODUITS STRUCTURÉS

Segment encore émergent de la finance décentralisée, les protocoles permettant la création de produits structurés se multiplient, surfant notamment sur la vague des RWA (Real World Assets).

STRUCTURÉS DE CRÉDIT

Centrifuge, protocole créé en 2017, constitue un premier pont entre la DeFi et les structurés de crédit portant sur des actifs du monde réel. A fin juin 2024, le protocole a déjà financé la tokenisation de près de 1500 actifs pour plus de de 600 millions de dollars.

La plateforme permet à d'autres sociétés mais également à des utilisateurs particuliers d'investir dans des prêts collatéralisés par des pools d'actifs du monde réel. Ce fonctionnement réplique le fonctionnement d'une opération de titrisation avec tranching, les investisseurs pouvant verrouiller leurs actifs (principalement du DAI) au sein de différentes tranches catégorisées en fonction du risque de crédit encouru (Junior et Senior). (Voir schéma ci-dessous).

Parmi les pools disponibles, on peut retrouver des produits titrisés comme des ABS (tels que des RMBS, CMBS, ...) ou des CLO (Collaterized Loan Obligation).

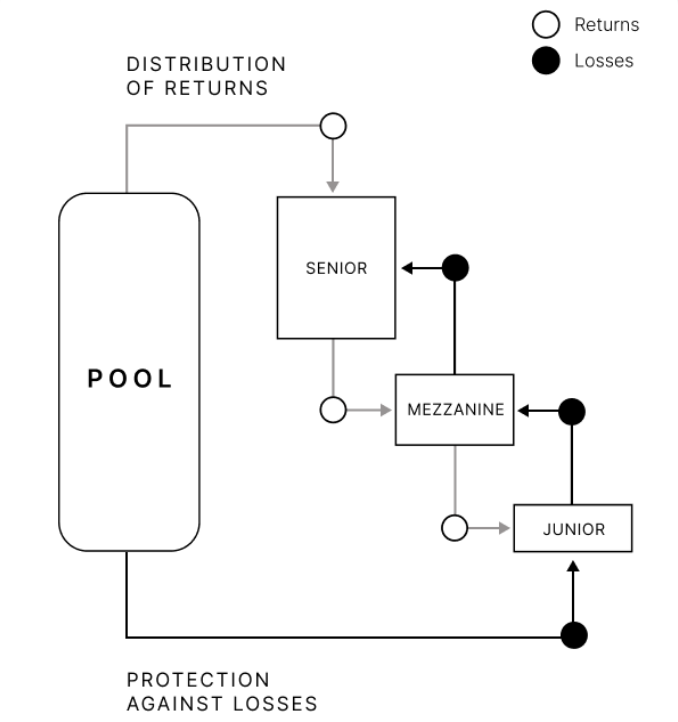


Figure 21 : Schéma descriptif des titrisations tranchées
(Source : centrifuge.io)

La plateforme assure l'ensemble des étapes requises pour financer les actifs réels sur la blockchain, de la tokenisation, à la titrisation, en passant par l'architecture permettant l'intégration des liquidités provenant des investisseurs. La plateforme possède également son propre système de gouvernance développé avec une partie off-chain sous la forme d'un forum afin de proposer des idées, et une partie on-chain dans laquelle les suggestions sont soumises à un vote des détenteurs du token de gouvernance CFG.

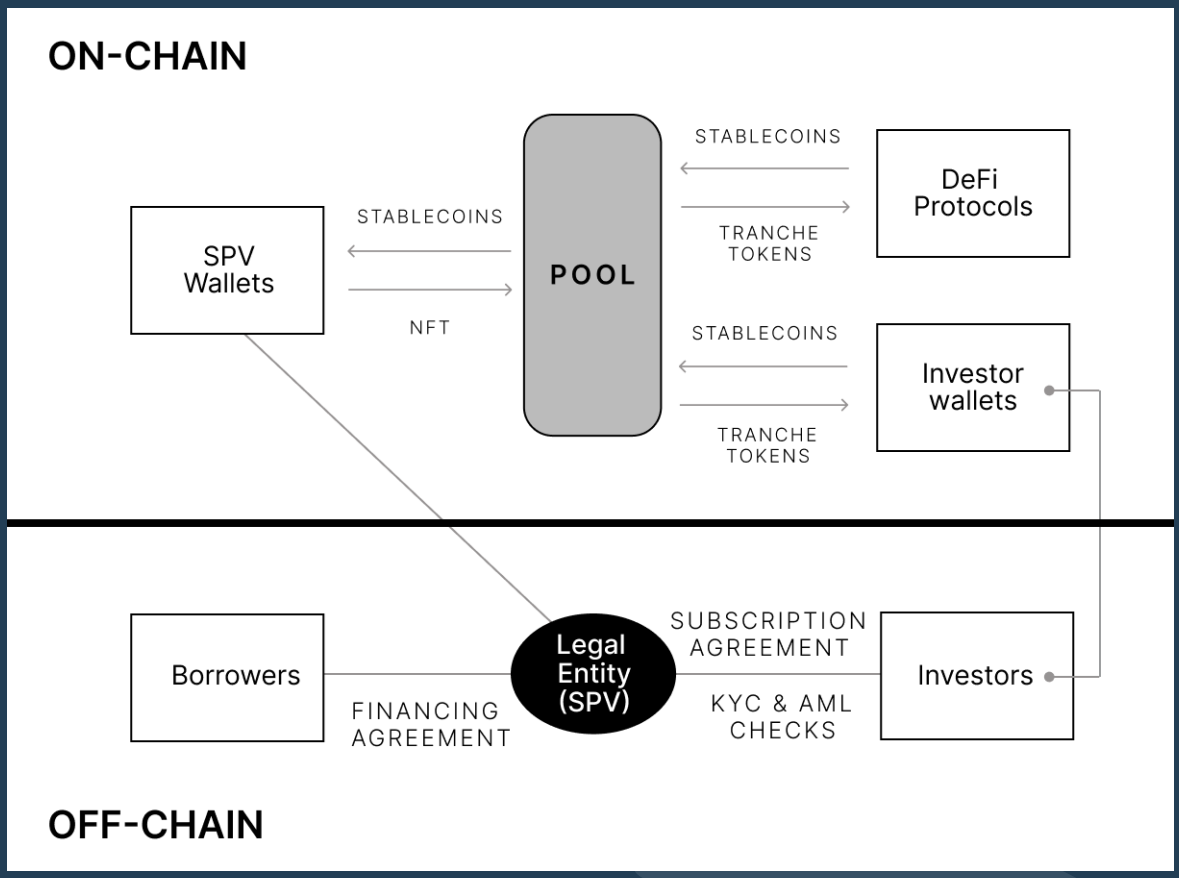


Figure 22 : Architecture on-chain et off-chain de Centrifuge (Source : centrifuge.io)

6 AGRÉGATEURS : BROKERS ET PORTFOLIO MANAGERS DE LA DeFi

Volume mensuel **DEX Aggregators** Ethereum (mai 2024) : **15,2 Md$**

Parts de marché du leader 1inch **: 55%**

TVL (Total Value Locked) **Yield Aggregators** : **2,3 Md$**

Parts de marché du leader ether.fi **: 41%**

Sources : coinmarketcap.com, coingecko.com, defillama.com (données à fin juin 2024)

La dernière couche du "DeFi stack" est composée d'agrégateurs. Ces protocoles permettent d'interagir simultanément avec plusieurs autres protocoles de la couche inférieure, comme des plateformes d'échanges ou de prêts.

On peut distinguer deux types d'agrégateurs : les « yield optimizers » et les « DEX aggregators» :

6.1. AGRÉGATEURS D'ÉCHANGES DÉCENTRALISÉS

Les « DEX aggregators » permettent de résoudre le problème d'insuffisance de liquidité inhérent à l'écosystème DeFi dû au nombre important de Dex entraînant un morcellement de cette liquidité.

Ils donnent accès à de multiples protocoles via une interface unique, en utilisant des algorithmes permettant de décomposer les transactions entre plusieurs Dex afin de trouver de la liquidité, diminuer l'effet de slippage, et déterminer le chemin le plus efficient en termes de prix et de coûts de transaction pour l'utilisateur. Ils permettent également l'échange de crypto-actifs sur des paires n'existant sur aucun Dex, en transitant par des paires intermédiaires.

6.1.1. 1INCH

C'est le premier et le plus important agrégateur en termes de volume échangé quotidiennement (plus de 200M$ quotidien, mai 2024). En plus de son algorithme de recherche de liquidité et de routing de transactions, il propose plusieurs autres fonctionnalités intéressantes :

- **Ordres limites :** permet de placer un ordre à un prix défini et avec une date d'expiration, ce qui n'est généralement pas possible sur les Dex classiques où l'ordre est instantané et va puiser directement dans le pool de liquidité. Le smart contract dédié de 1inch permet d'exécuter ce type d'ordre en le faisant matcher avec des ordres inverses sur le protocole. 1inch propose également des ordres de type RFQ (Request For Quotation), principalement utilisés par des market makers, et équivalent au système existant sur des OMS de la finance traditionnelle comme Bloomberg.

- **Fusion swaps :** depuis fin 2022, 1inch propose un système de passage d'ordre innovant, les "fusion swaps". L'ordre classique passé par l'utilisateur est en fait soumis à une enchère de type "dutch auction" auprès de market makers appelés "resolvers". L'ordre est d'abord proposé à un prix très avantageux pour l'utilisateur puis progressivement modifié jusqu'à ce qu'un resolver accepte le trade ou que le prix dépasse les limites d'exécution de l'utilisateur. Les frais de réseaux (gas) sont ici payés par les market makers, et une protection est offerte à l'utilisateur contre les stratégies de MEV (maximum extractable value) de type "sandwich". Le système des fusion swaps peut s'apparenter aux dark pools, qui permettent aux investisseurs institutionnels de passer des ordres sur des quantités importantes d'actifs, à l'abri du regard des marchés, afin d'éviter les risques de front-running ou de décalage de prix.

Le protocole propose ainsi des ordres adaptés non seulement aux particuliers mais également aux institutionnels en permettant à un marché OTC de se former grâce aux ordres RFQ et fusion swaps, tout en protégeant ses utilisateurs d'attaques de type front-running, ou de payer des frais de transaction exagérés (gas fees) sur la blockchain.

La gouvernance du protocole est assurée sous forme de DAO. Les détenteurs de 1INCH token participent aux décisions sur l'avenir du réseau et peuvent déléguer leurs droits de votes à des market makers qui vont profiter de conditions plus avantageuses, assurant ainsi la stabilité du protocole.

6.1.2. PARASWAP

Ce protocole français lancé en septembre 2019 propose également un système de routage des ordres vers les différents Dex pour aller chercher de la liquidité, le meilleur prix et les frais de réseau les plus faibles.

Il propose également des transactions OTC, ainsi que son propre DEX composé de pools alimentés par des market makers sélectionnés.

Le protocole ne prélève pas de frais sur les transactions, mis à part une partie du 'positive slippage' le cas échéant. Le positive slippage apparaît lorsqu'un trade est effectué à un meilleur prix que celui indiqué initialement.

A l'instar de 1Inch, Paraswap est gouverné par un DAO dont le token est le PSP.

MEV & ATTAQUE SANDWICH

MEV (Maximum Extractable Value) désigne la valeur maximale pouvant être extraite de chaque bloc produit sur la blockchain par les mineurs en incluant, excluant ou changeant l'ordre des transactions dans un bloc.

Outre des stratégies d'arbitrage classique, la MEV peut être composée de stratégies plus agressives, s'apparentant au front running pouvant avoir lieu sur les marchés traditionnels. L'attaque la plus connue est l'attaque dite "sandwich", dans laquelle l'attaquant repère une transaction dans le Mempool (pool des transactions en attentes), paie des frais de réseaux plus élevés pour placer une transaction qui passera en priorité avant la transaction d'origine et fera décaler le prix d'origine de la paire de crypto-actifs concernée dans le DEX. La transaction d'origine passe donc ensuite à un prix moins avantageux, et l'attaquant peut immédiatement passer une transaction inverse, profitant du décalage de prix et empochant une plus-value instantanée.

C'est la transparence inhérente aux blockchains qui rend ce type de transaction possible, bien que dans les marchés financiers traditionnels, souvent plus opaques, les arbitrages de type front-running, bien qu'interdits, restent monnaie courante.

6.2. YIELD OPTIMIZERS / PORTFOLIO MANAGERS

Les yield aggregators, ou optimizers, sont des protocoles qui proposent des stratégies automatisées de placements dans une série d'autres protocoles de la couche inférieure (ce qu'on appelle communément "yield farming" dans l'univers DeFi). Outre le fait de permettre aux utilisateurs de placer leurs crypto-actifs sur plusieurs protocoles, ils réduisent les frais de réseau en agrégeant les fonds des utilisateurs et peuvent réinvestir automatiquement les intérêts gagnés.

Ces protocoles équivalent à des asset managers, « on-chain », et sont totalement automatisés.

6.2.1. YEARN

Yearn est le plus ancien des yield optimizers. Ce protocole propose d'investir au sein de différents portefeuilles (yVaults) qui exécutent différentes stratégies d'investissement afin de maximiser leur rendement.

Un portefeuille peut exécuter simultanément plusieurs stratégies, en y allouant une portion prédéfinie du capital sous gestion. Ces stratégies peuvent aller du simple prêt sur un protocole de lending, à des transactions plus sophistiquées impliquant des flash loans, en passant par de l'apport de liquidité sur des DEX.

Tout le monde peut proposer une nouvelle stratégie, celle-ci devant suivre un processus de validation rigoureux (concept, code, sécurité, testing) à la suite duquel elle obtient un score de risque sur chaque catégorie et peut être activée. Les créateurs de stratégie sont ensuite rémunérés par une partie des performance fees.

Yearn est gouverné à travers son token YFI, qui lorsque bloqué et converti en veYFI, donne un droit de vote pour les décisions afférentes au protocole : niveau de frais prélevés, nouveaux vaults et toute autre évolution.

D'autres protocoles proposent des fonctionnalités plus poussées de gestion de portefeuille de crypto-actifs :

6.2.2. INSTADAPP

Instadapp propose une interface utilisateur unifiée nommée "smart account" pour interagir directement et suivre ses positions sur les protocoles de lending ou Dex. Il permet également de déployer des stratégies automatisées personnalisées, le tout directement à partir d'une surcouche de smart contracts.

6.2.3. ARRAKIS NETWORK

Arrakis Network est spécialisé dans la gestion de la liquidité sur la version 3 du principal protocole d'échange décentralisé (Dex) UniSwap V3.

Il propose des fonds (vaults) avec des stratégies prédéfinies et automatisées, des fonds managés par des market-makers professionnels ou encore des fonds pouvant être gérés directement par les utilisateurs du protocole. Les vaults et stratégies sont « on-chain » et donc totalement transparentes et auditables.

Arrakis propose également aux protocoles et DAOs une infrastructure de gestion automatisée de liquidité, leur permettant de créer un marché pour leur token natif sans délégation à un market-maker traditionnel.

6.2.4. SET PROTOCOL

Set permet la création de fonds décentralisés, qui prennent la forme d'un pool de crypto-actifs dont les parts sont tokenisées sous format ERC-20 et donc échangeables, à l'instar d'un OPCVM. La gestion de ces fonds peut être intégralement automatisée via des règles prédéfinies ou bien assurée par un gestionnaire.

Set permet ainsi la création de produits de type ETF, répliquant la performance d'indices, à l'instar du DeFiPulse Index, constitué d'un panier de tokens des principaux protocoles DeFi.

Les différents types d'agrégateurs décrits précédemment proposent des solutions d'investissement qui s'inspirent de la finance traditionnelle. En optimisant la recherche de liquidité, les DEX aggregators viennent ainsi jouer le rôle de brokers, alors que les yield aggregators permettent aux investisseurs d'être exposés à une grande variété de stratégies de la DeFi se rapprochent du rôle des portfolio managers. Les solutions proposées par les agrégateurs bénéficient par ailleurs de l'écosystème de la DeFi : la transparence leur permet d'améliorer plus facilement les solutions existantes alors que les transactions peuvent être exécutées avec moins de frictions que sur les marchés traditionnels.

AUDIT DE SMART CONTRACTS

Les protocoles de finance décentralisée doivent garantir la fiabilité de leurs smart contracts, car une faille peut causer des pertes monumentales, comme l'a montré le premier hack emblématique de la DeFi qu'est celui de The DAO en 2016 avec une perte de 50 millions de dollars ou encore le récent piratage de Curve, qui a subi un préjudice de 73 millions de dollars.

Ces incidents nuisent non seulement financièrement mais érodent également la confiance des utilisateurs. De plus, il est vital que ces contrats soient optimisés pour limiter les frais de gaz associés aux transactions blockchain et garantir l'efficacité des API qu'ils utilisent, notamment face aux attaques potentielles comme le DDoS.

En conséquence, plusieurs sociétés d'audit ont émergé afin d'assurer ces tâches, telles que Certik, Solidproof, ou encore ConsenSys diligence. Pour effectuer ces audits, les protocoles font appel à ces sociétés ou bien à leur communauté à travers un bug bounty, c'est-à-dire en donnant des récompenses aux individus parvenant à déceler des failles. La plateforme HackerOne en particulier, permet aux protocoles de mettre en place ce type de programme.

7 RISQUES ET RÉGLEMENTATIONS

7.1. RISQUES

Bien que la finance décentralisée permette de se passer de nombreux intermédiaires nécessaires au fonctionnement de la finance classique, et donc de réduire le risque de contrepartie mais également le risque systémique associé à la complexité et l'opacité du système, elle n'en demeure pas moins connue pour les risques souvent extrêmes auxquels ses participants sont exposés. En effet, l'innovation a apporté son lot de nouveaux risques, et l'exploitation des failles existantes fait parler de la DeFi à chaque nouvelle attaque d'envergure. **Nous ne parlerons pas ici des risques "classiques" auxquelles la DeFi est exposée (marché, liquidité, fraude, blanchiment des capitaux et financement du terrorisme, etc.) à l'instar des marchés traditionnels, mais plutôt des différents types de risques qui lui sont endémiques :**

7.1.1. RISQUE DE SMART CONTRACT

Comme nous l'avons vu précédemment, les smart contracts, ces programmes auto-exécutables basés sur la blockchain constituent l'une des bases du DeFi Stack sur lequel repose l'innovation financière de l'écosystème. Mais ce sont ces mêmes lignes de codes qui peuvent également constituer la vulnérabilité la plus importante de l'écosystème. Le code étant open-source, et une fois déployé, ces programmes fonctionnant de manière entièrement automatisée, la moindre faille dans le code peut permettre à un attaquant de détourner le système en sa faveur et siphonner les fonds d'un protocole de manière plus ou moins sophistiquée. Ce risque est démultiplié par la composabilité des protocoles DeFi qui réalisent entre eux des transactions automatisées. Ainsi, une faille dans un protocole peut "véroler" toute une chaîne de transactions entre plusieurs protocoles. Rappelons ici l'irréversibilité des transactions sur la blockchain, propriété qui rend extrêmement difficile la récupération de fonds détournés.

La nature open-source de l'écosystème et les attaques incessantes que les protocoles subissent rendent néanmoins le système de plus en plus robuste. Les acteurs les plus vulnérables étant immanquablement attaqués et voués à disparaître rapidement, bien souvent au prix de pertes importantes en capital de leurs utilisateurs. Cette jungle qu'est la DeFi opère ainsi une sélection naturelle entre les différents protocoles et évolue de manière étonnamment organique.

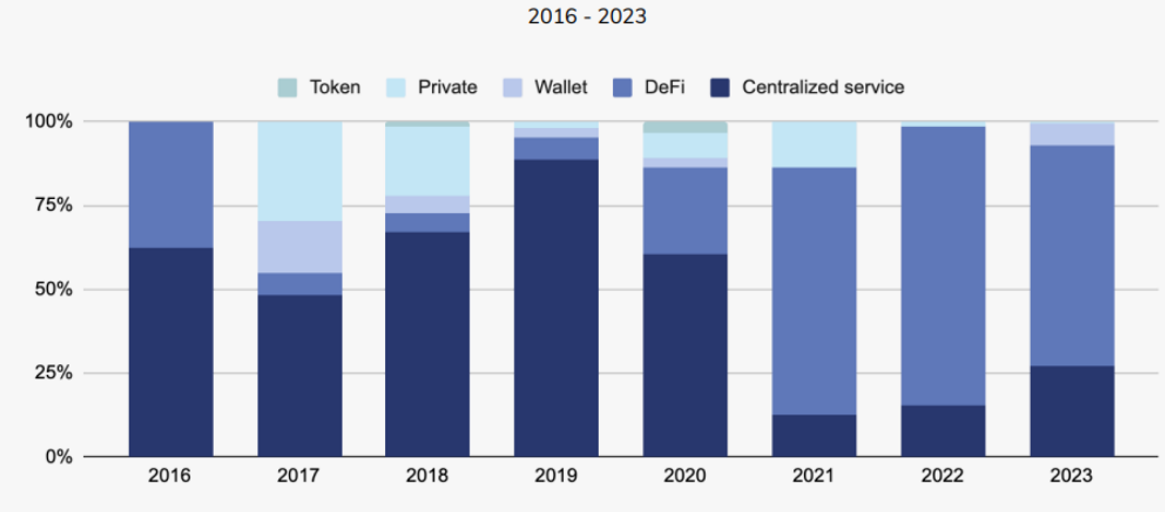


Figure 22 : Répartition du montant de devise crypto hacké par type de plateforme (Source : go.chainalysis.com/crypto-crime-2024.html)

7.1.2. RISQUE D'ORACLE

Les oracles constituent la brique permettant de relier les protocoles aux données provenant d'autres blockchains et du monde extérieur, telles que le prix des actifs. Ils sont indispensables au bon fonctionnement de la plupart des protocoles, notamment les applications de lending qui s'en servent afin de valoriser le collatéral et déterminer les événements de liquidation. Il existe de nombreux oracles mais le plus important d'entre eux, Chainlink, fournirait l'écrasante majorité des données de marché au sein de la DeFi.

Les oracles constituent un point d'attaque privilégié pour la manipulation de prix, ou le front-running. Les protocoles dépendants de ces données sont donc à la merci d'une attaque indirecte, et la situation de quasi-monopole de Chainlink va à l'encontre de la volonté de décentralisation du secteur et constitue ainsi un risque systémique

Un équilibre est à trouver entre décentralisation et efficacité. En effet, les oracles centralisés, plus rapides car pouvant être connectés à une seule source de données, peuvent être victimes d'attaque ciblées, à l'instar du protocole Value DeFi qui s'est fait dérober 6 millions de $ par un hacker ayant exploité une vulnérabilité dans son code.

Les oracles décentralisés comme Chainlink sont de conception plus complexe, devant être connectés à de multiples sources de données, ce qui peut affecter leur rapidité en comparaison à des solutions centralisées. Ils sont cependant moins sujets à des attaques ciblant leur code, et la multiplication de sources de données leur permet d'être plus résistant face aux manipulations de prix.

LES ORACLES

En DeFi, les services proposés par les dApps fonctionnent via des smart contracts s'exécutant automatiquement lorsque des conditions prédéfinies sont remplies.

Lorsque ces conditions existent en dehors de la blockchain native au smart contract, leur vérification s'effectue à travers l'utilisation d'un oracle alimentant le smart contract en données externes. Ces conditions peuvent être extrêmement variables : données météorologiques, résultat d'une élection ou d'un pari sportif, cours d'un actif, etc.

Il existe différents types d'oracles :

- **Oracles d'entrée :** Les plus courants, il s'agit des oracles alimentant les données off-chain aux smart contracts.
- **Oracles de sortie :** Permettent d'exécuter une action en dehors de la blockchain (informer un réseau bancaire d'un paiement).
- **Oracles cross-chain :** Permettent de récupérer des données issues d'autres blockchains, ce qui donne la possibilité au smart contract d'effectuer des opérations entre les blockchains (déplacement de données et d'actifs).
- **Oracles de calcul :** Permettent d'effectuer des calculs off-chain lorsqu'il s'agit de fournir un service décentralisé qui n'est pas pratique à effectuer au sein de la blockchain pour des raisons techniques ou juridiques.

Étant donné que les smart contracts sont exécutés automatiquement et qu'il est impossible de revenir en arrière, il est crucial que les données fournies soient parfaitement fiables. Bien qu'il existe des oracles centralisés, il est utile qu'un oracle soit une entité la plus décentralisée possible afin d'éviter tout risque de manipulation et de dépendance à un tiers de confiance. Dans ce cas, le dilemme est donc à nouveau d'allier fiabilité et décentralisation. Prenons par exemple le cas de Chainlink.

Chainlink est l'oracle le plus utilisé avec plus de 40 milliards de dollars de Total Value Secured (TVS), et plus de 12,000 milliards de dollars de Transaction Value Enabled (TVE). Cet oracle met à disposition des Data Feeds, s'appuyant sur l'agrégation de données issues de "Decentralized Data Networks" et de "Off-chain reportings".

Les Decentralized Data Networks sont des bases de données alimentées par des opérateurs indépendants de ChainLink. Ces opérateurs sont rémunérés pour leur publication de données et il n'est pas nécessaire que ces réseaux soient validés par ChainLink (bien qu'ils soient tout de même catégorisés par fiabilité). Ces opérateurs peuvent eux-mêmes être qualifiés d'oracles, ce qui implique que ChainLink est en réalité un réseau d'oracles, et c'est la multitude d'oracles imbriqués dans le réseau ChainLink qui augmente son caractère décentralisé.

Les Off-chain reportings améliorent l'agrégation des données : il s'agit de réseaux de nœuds récoltant individuellement des données, et communiquant entre eux via un réseau P2P afin de les agréger, puis de les transmettre à ChainLink comme support supplémentaire aux données issues des Decentralized Data Networks.

C'est cet ensemble de données issues de multiples sources qui permet leur fiabilisation et qui autorise ChainLink à faire appel à des réseaux qui ne sont pas nécessairement labélisés "de confiance" par l'oracle. En effet, il est invraisemblable que l'ensemble des différentes sources s'accordent toutes ensemble sur une donnée erronée.

En plus d'être décentralisé dans la sélection des données, le réseau ChainLink est un DAO à part entière disposant de son propre token de gouvernance (LINK).

Certains protocoles utilisent simultanément différents oracles afin de diversifier et ainsi augmenter la fiabilité de leurs données. C'est notamment le cas du protocole Synthetix qui utilise par exemple Pyth Network, en plus de ChainLink, pour alimenter ses smart contracts utilisant massivement des données issues du monde réel et en particulier des marchés financiers traditionnels.

7.1.3. RISQUE DE GOUVERNANCE

Nombre de protocoles fonctionnent selon un mode de gouvernance décentralisé reposant sur un système de vote accessible aux détenteurs de token natif. Ce mode de fonctionnement peut être sujet à des attaques, lorsqu'un acteur malveillant parvient à s'emparer d'un nombre suffisant de tokens de gouvernance et propose de voter des décisions en sa faveur. Beanstalk Farm, un protocole de stablecoin, s'est fait ainsi dérober 182 millions de dollars de collatéral en 2022, lorsqu'un attaquant, via un flash Loan de 1 milliards de dollars, est parvenu à prendre le contrôle de 67% des tokens de gouvernance afin de faire passer sa propre proposition frauduleuse.

Un autre risque induit par ce système réside dans la concentration de pouvoir entre les mains d'un groupe restreint d'acteurs pouvant prendre des décisions à leur avantage et allant à l'encontre des utilisateurs et de la communauté du protocole, mettant ainsi en risque la viabilité de ce dernier. Nous avons vu précédemment dans le paragraphe dédié au protocole Curve que les guerres de gouvernance font rage dans l'univers de la DeFi, et bien que le système soit dit « décentralisé », l'on y retrouve bien souvent des niveaux de concentration égaux voire supérieur au monde dit « centralisé ».

7.1.4. RISQUE D'INTEROPÉRABILITÉ

L'interopérabilité entre protocoles ou blockchains constitue à la fois une force et une faiblesse. En effet, la multiplication de "points de passage" rend l'écosystème plus complexe, fragile et accroît la surface d'attaque potentielle pour des acteurs malveillants. Ainsi, plusieurs bridges ont été hackés ces dernières années pour des montants souvent astronomiques... On peut citer le hack spectaculaire de 320 millions de $ du bridge « Wormhole », reliant les blockchains Ethereum et Solana. De plus, l'interopérabilité accroît également le risque de contagion, l'attaque d'un protocole pouvant déclencher une réaction en chaîne au sein de l'écosystème, notamment en faisant chuter le niveau de collatéralisation des prêts sur les protocoles de lending et entrainant des défauts en cascade. Ces défauts entraînent alors des liquidations et in fine la chute de valeur d'autres crypto-actifs.

7.1.5. RISQUE DE CONSERVATION (CUSTODIAL)

Afin de déplacer des fonds ou interagir avec les protocoles DeFi, les utilisateurs doivent être en possession de clés privées permettant de signer les transactions correspondantes. Bien que ce mécanisme permette de se passer totalement d'intermédiaires, les utilisateurs sont exposés à un risque opérationnel très important : s'ils perdent l'accès à leur clé privé, ils perdront de manière définitive leurs fonds associés. De plus, étant donné la propriété d'irréversibilité des transactions sur une blockchain, s'ils transfèrent leurs fonds à la mauvaise adresse, ils en perdront totalement le contrôle. Des solutions existent pour limiter ces risques opérationnels, tels que des portefeuilles « physiques », à la main de l'utilisateur, ou bien des systèmes de conservation plus élaborés mais qui impliquent souvent de déléguer le contrôle des fonds à une entité tierce. Certaines solutions hybrides, utilisant des technologies de type MPC (multi-party computation) permettent de ne pas déléguer totalement le contrôle des fonds tout en offrant un niveau de sécurité élevé.

Le risque de conservation est l'un des principaux freins à l'entrée des acteurs institutionnels dans le monde de la DeFi, c'est pourquoi plusieurs solutions destinées à ces derniers ont été lancées. Parmi les plus grands acteurs on peut citer Fireblocks ou Bitgo, qui proposent des plateformes de conservation de niveau (grade) institutionnel, ainsi que des infrastructures de trading qui permettent d'interagir avec les protocoles DeFi tout en limitant grandement les risques opérationnels.

7.1.6. RISQUE D'INFRASTRUCTURE BLOCKCHAIN

La DeFi reposant sur la technologie blockchain, elle hérite donc des risques inhérents à cette infrastructure. Une blockchain peut être sujette notamment à des attaques utilisant son mécanisme de consensus, via la fameuse "attaque 51%", qui peut voir un ou des acteurs malveillants prendre le contrôle de la création de nouveaux blocs de transactions via l'obtention de la majorité de la puissance de calcul sécurisant le réseau (dans le cadre des blockchains POW de type Bitcoin), ou bien la majorité des crypto-actifs natifs stakés (dans le cadre des blockchains de type POS comme la nouvelle version d'Ethereum). Outre ce type d'attaque systémique qui viendrait remettre en cause l'intégralité de l'écosystème et sa blockchain sous-jacente, les protocoles DeFi sont à la merci d'engorgement au niveau des transactions, pouvant engendrer des ralentissements et des frais de transaction très élevés.

7.1.7. RISQUE RÉGLEMENTAIRE

La DeFi est suivie de près par les régulateurs du monde entier. En atteste le récent rapport de l'ACPR, agrémenté d'un appel à la réflexion publique.

En effet, les protocoles DeFi fournissent souvent des services financiers réglementés de manière non conforme. Leur mode de fonctionnement est par nature incompatible avec les cadres réglementaires existants, conçus pour un système incluant des intermédiaires financiers, des procédures KYC/AML rigoureuses et des autorisations d'exercice liées à des juridictions définies. Or, les protocoles n'ont souvent pas d'existence légale donc pas d'emplacement géographique défini, pas de responsable identifié s'ils fonctionnent sous un mode de gouvernance décentralisé (DAO) et leurs utilisateurs sont anonymes, ou du moins pseudonymes, les portefeuilles de crypto-actifs n'intégrant pas de contrôle KYC/AML. De plus, la protection des utilisateurs est faible voire inexistante.

En l'absence de cadre réglementaire clair, ces protocoles pourraient tomber sous le coup des juridictions existantes et être interdits. Les régulateurs peuvent néanmoins envisager d'ajuster les cadres réglementaires ou adopter de nouvelles exigences couvrant les innovations apportées par les protocoles DeFi et ses nouveaux risques associés.

7.1.8. L'ÉMERGENCE D'ASSUREURS « ON-CHAIN »

Devant les risques encourus par les investisseurs sur la DeFi, des protocoles offrant des couvertures assurantielles ont vu le jour ces dernières années. Ces protocoles DeFi tentent de répliquer les systèmes de couverture des assurances traditionnelles tout en tirant profit des innovations technologiques offertes par l'écosystème des blockchains.

L'acteur principal de l'assurance décentralisée est actuellement Nexus Mutual (TVL : ~230 M $, juin 2024) qui couvre près de 5 Mds $ de fonds sur divers protocoles de la DeFi. Les contrats proposés par ce DAO permettent de s'assurer contre une grande variété de failles pouvant engendrer la perte de fonds sur plus une centaine de protocoles reposant sur Ethereum. Ces failles incluent notamment les hacks, les « exploits », les manipulations d'oracles ou encore les attaques de gouvernance. Comme le décrit la figure 23, le protocole repose sur un pool de capital dans lequel les assurés versent leur frais de couverture sous forme d'ETH, de DAI ou d'USDC. Les fournisseurs d'assurances alimentent quant à eux ce pool en ETH en échange de tokens NXM. Le pool de liquidité permet de répondre aux engagements des passifs et également d'investir sur des actifs permettant de générer des revenus pour le DAO et les fournisseurs d'assurance. Il est à noter que les décisions d'investissement sont votées par les membres du DAO dont le pouvoir de décision est déterminé par le nombre de tokens NXM détenus. Ces tokens peuvent par ailleurs être stakés afin de générer un profit supplémentaire pour les membres.

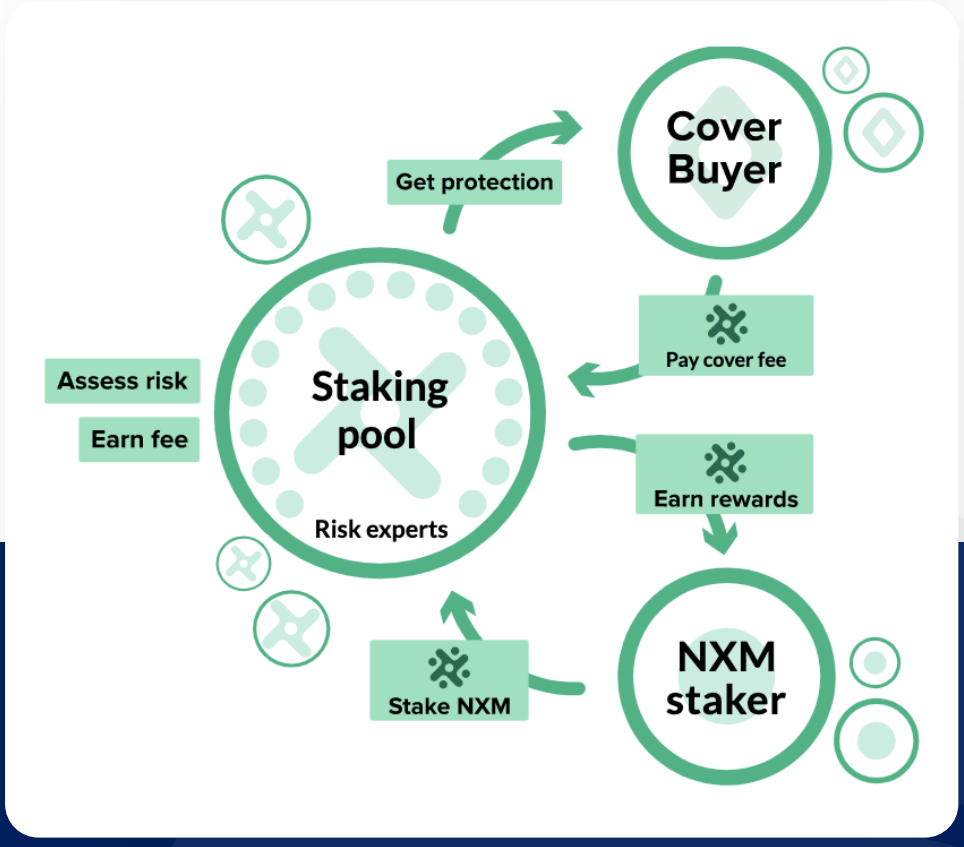


Figure 23 : Fonctionnement du système de couverture de Nexus Mutual (Source : docs.nexusmutual.io/protocol)

7.2. UNE RÉPONSE RÉGLEMENTAIRE EN ORDRE DISPERSÉ

7.2.1. CADRE RÉGLEMENTAIRE EUROPÉEN – MICA

L'Union Européenne marque le pas dans la régulation du marché des crypto-actifs avec l'entrée en vigueur du règlement MiCA (Markets in Crypto-Assets) le 29 juin 2023. Cette règlementation sera applicable à compter du 30 décembre 2024 et remplacera les cadres nationaux européens pour régir :

- La mise à disposition et l'intégration aux échanges de jetons numériques.
- La prestation de services liés aux crypto-actifs par des fournisseurs spécialisés.
- La lutte contre les pratiques de marché abusives concernant les crypto-actifs.

S'ensuivra une période transitoire de 18 mois au bout de laquelle, le 30 juin 2026, les Prestataires de Services sur Actifs Numériques (PSAN) devront être agréés par la réglementation MiCA pour continuer à offrir leurs services en Europe.

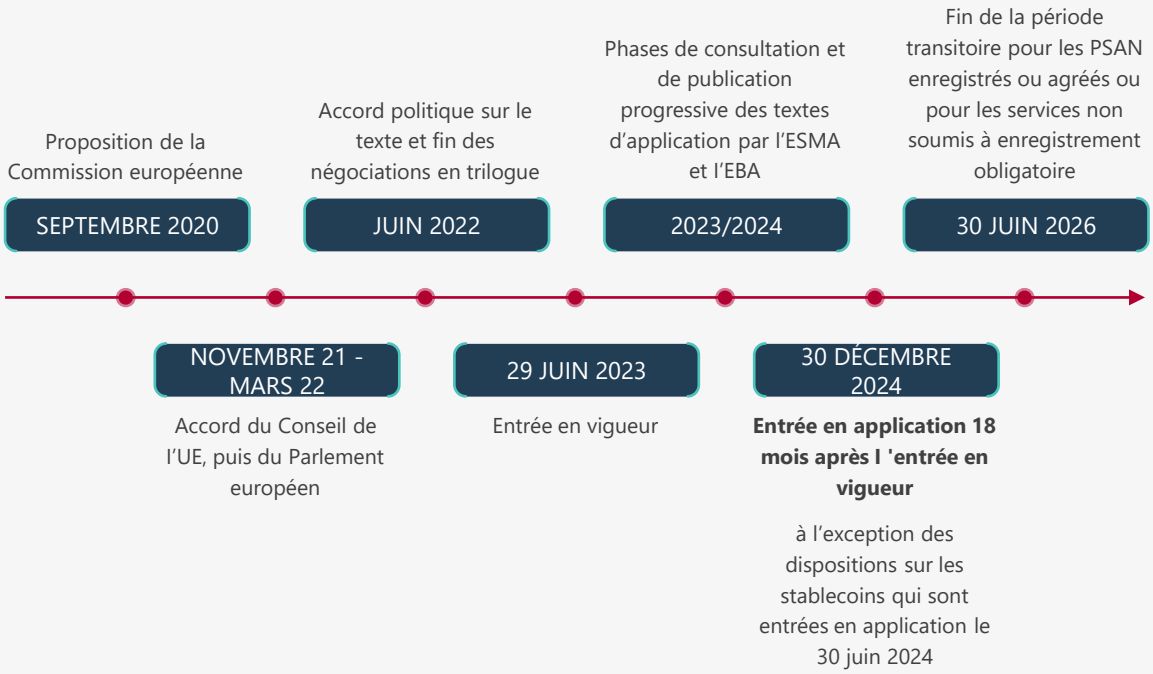


Figure 24 : Chronologie de la réglementation MiCA
(Source : www.amf-france.org/fr/actualites-publications/actualites/marches-de-crypto-actifs-publication-du-reglement-europeen-mica)

En revanche, la réglementation ne concerne que les prestataires centralisés (CeFi). Il est néanmoins prévu d'intégrer les protocoles décentralisés ainsi que les échanges de NFT dans de prochains volets.

L'AMF, dont le PSAN a fait figure de précurseur et a inspiré MICA, salue avec enthousiasme l'approbation de ce texte et les progrès réalisés dans le processus législatif européen. Ce règlement aidera à stimuler la compétitivité des intervenants français et européens, en établissant un cadre réglementaire harmonisé à travers l'Europe, et en garantissant une protection renforcée pour les investisseurs. L'Europe se distingue ainsi par sa position de leader en termes de réglementation, surpassant les États-Unis dans ce domaine.

Toutefois, certaines critiques ont pu être émises contre la réglementation MiCA, notamment concernant la mention d'un cap sur le volume maximal échangé quotidiennement à 200 millions d'euros pour les stablecoins adossés à d'autres monnaies que l'euro comme l'USDT et l'USDC. A titre de comparaison, le volume échangé quotidiennement sur l'USDT avoisine les 30 milliards d'euros en juin 2024.

7.2.2. L'ACPR – APPEL À LA RÉFLEXION SUR LA DEFI, POUR PALLIER SON ABSENCE DANS MICA

En avril 2023, l'ACPR (Autorité de contrôle prudentiel et de résolution), chargée de la régulation et de la supervision du système financier, publie un document de réflexion concernant la mise en place d'une réglementation de la finance décentralisée. Cette réflexion se positionne dans le prolongement de la réglementation MiCA afin de proposer un cadre juste et cohérent avec les réglementations appliquées à la CeFi, et dans le but d'étendre son champ d'application à la DeFi, ou plutôt à la finance "désintermédiée" comme ses auteurs préfèrent la qualifier.

En effet, l'ACPR définie la DeFi comme étant "un ensemble de services sur crypto-actifs, comparables à des services financiers et effectués sans l'intervention d'un intermédiaire", mais cette définition est imprécise, les protocoles DeFi possédant une gouvernance dont le niveau de centralisation est très varié, et parfois opaque, ce qui amène également son lot de risques identifiés par l'ACPR (cf. Risque de gouvernance).

Dans un premier temps, l'ACPR identifie comme piste le renforcement de la sécurité des infrastructures. Une première solution pourrait consister à imposer une homologation autorisant seulement les blockchains publiques qui reposent sur des standards minimaux de sécurité (certification du code informatique, nombre de validateurs minimal, maximum de concentration des capacités de validation).

Une seconde solution pourrait être de basculer sur des blockchains privées intermédiées par des acteurs publics ou privés de confiance, mais cela irait partiellement à l'encontre de la décentralisation et limiterait l'attrait, le développement et l'innovation du secteur au prix d'une sécurité plus robuste.

Une troisième solution consisterait à renforcer la sécurité des smart contracts via la mise en place d'une certification sur le code informatique les constituant, sur le service proposé, ainsi que sur la gouvernance de l'entité proposant ce service. La certification devrait respecter les trois règles suivantes :

- Pouvoir être retirée à tout moment
- Être à durée limitée afin de tenir compte de l'évolution rapide de l'écosystème, sa technologie, ses pratiques et de l'évolution des réglementations le régissant.
- Être réitérée à chaque changement significatif du code.

Dans un second temps, le document propose de mieux encadrer la fourniture de services financiers par les intermédiaires qui les proposent. Une première idée serait d'opérer une "recentralisation" de ces entités, notamment lorsque plusieurs acteurs exercent un contrôle significatif sur un service sensible, en leur imposant la création d'une entité juridique, en particulier dans le cas des DAOs. Cela permettrait de mieux pouvoir assujettir l'entité à un contrôle afin de pouvoir ou non l'homologuer publiquement.

L'ACPR envisage également un cadre de contrôle renforcé pour les intermédiaires facilitant l'accès à la finance désintermédiée, notamment en les encourageant à la sensibilisation de leurs utilisateurs aux risques inhérents à la DeFi. En ce sens, il est envisagé également de soumettre aux utilisateurs des tests objectifs afin de mesurer leur compétence et leur appétence au risque.

Ainsi, agissant conjointement et en cohérence avec MiCA, l'appel à la réflexion de l'ACPR présage d'un cadre réglementaire de la finance décentralisée européen en avance sur le reste du monde.

7.2.3. CADRE RÉGLEMENTAIRE AMÉRICAIN

Aux Etats-Unis, le cadre réglementaire concernant la CeFi, et parallèlement la DeFi, manque de clarté et prend du retard sur la régulation européenne. En l'occurrence, la régulation hésite encore quant à la définition des actifs intrinsèques à la CeFi et à la DeFi. Par exemple, les tokens émis par les acteurs sont-ils des commodities ? Sont-ils des securities ? Dans le premier cas ils devraient être régulés par la CFTC (Commodity Futures Trading Commission) selon le CEA (Commodity Exchange Act). Dans le second cas, ils devraient être régulés par la SEC (Securities and Exchange Commission). Peut-être n'appartiennent t'ils à aucune de ces catégories; dans ce cas quelle régulation s'impose ? Cette ambiguïté est un frein au développement de la DeFi aux USA, en témoigne le procès de la SEC envers Ripple, important acteur de la CeFi, pour lequel la nature du procès a le potentiel de s'appliquer à la DeFi dans un futur proche.

En effet, les ventes par Ripple de leur token XRP au grand public ont déclenché les foudres de la SEC. En 2020, un procès est ouvert contre Ripple, les accusant d'avoir vendu aux investisseurs des tokens pouvant être assimilés à des titres (ou "securities"), sans avoir pour autant validé une demande de listing officielle leur permettant cette vente ; ce qui est illégal selon leur règlement.

En juillet 2023, la juge Analisa Torres a statué que les ventes de XRP aux investisseurs institutionnels constituaient des titres, tandis que les ventes aux investisseurs individuels via des échanges ne l'étaient pas. Cette décision partielle laisse encore des zones d'ombre quant à la régulation des actifs numériques.

Ainsi, tout l'enjeu de ce procès repose sur la question suivante : est-ce que les XRP peuvent être assimilés à des securities ? Le Howey test définit 4 critères requis pour qu'un actif soit catégorisé comme étant une security :

- L'actif représente un investissement d'argent.
- La raison principale de l'investissement dans ce titre est l'espérance de faire des bénéfices.
- La valeur de l'actif ne dépend pas des efforts des investisseurs.
- L'investissement doit être dans une entreprise commune où les bénéfices des investisseurs sont interdépendants..

S'il semble que XRP remplit les 3 premiers critères, sa position quant au 4e est ambigüe : la SEC estime que Ripple Labs est bien la société mère de XRP, mais XRP possède d'un côté un registre décentralisé (donc ne pouvant pas être désigné comme géré par une entreprise commune), et de l'autre des fonctionnalités détachées des investissements liés à Ripple. La décision finale, attendue avant la fin de l'été 2024, sera décisive pour l'écosystème entier car elle inspirera directement les sanctions appliquées aux autres entités CeFi comme DeFi présentant des caractéristiques similaires. En particulier, les protocoles DeFi Opyn, ZeroEx et Deridex ont déjà été sanctionnés par la CFTC pour avoir proposé des activités de trading jugées illégales avec des amendes allant de 100 000$ à 250 000$.

C'est la raison pour laquelle le manque d'une régulation claire de la DeFi aux Etats-Unis place ce pays, habituellement en avance dans le secteur de la tech, en retard par rapport au reste du monde et notamment par rapport à l'Europe en ce qui concerne les sujets réglementaires.

7.2.4. CADRES RÉGLEMENTAIRES EN ASIE

Japon :

Le Japon a initialement adopté une régulation stricte pour protéger les consommateurs après plusieurs incidents, comme le piratage de CoinCheck en 2018. Cependant, ces régulations se sont assouplies récemment, facilitant la cotation de nouveaux tokens. Les législateurs japonais cherchent désormais à attirer davantage d'entreprises du secteur des cryptomonnaies dans le pays, avec des changements fiscaux significatifs proposés en 2023 pour encourager les émissions de tokens sans de trop lourdes taxes. Concernant les DAO, la législation poursuit les discussions pour leur légalisation au sein d'un cadre réglementaire clair et adapté, en particulier concernant les offres de titres et les règles de gouvernance interne.

Hong Kong :

Autrefois un bastion pour de grandes entreprises crypto telles que Bitmex, mais aussi FTX, Hong Kong a connu un déclin dû à une pression réglementaire accrue et de l'incertitude liée à la politique de la Chine sur la crypto-monnaie. Cependant, malgré le scepticisme, Hong Kong a maintenu sa porte ouverte aux entreprises crypto. Le 31 mai 2023, la SFC (Securities and Futures Commission) d'Hong Kong publie un circulaire définissant les conditions d'une période transitoire pour l'obtention d'une nouvelle licence que les plateformes centralisées proposant des services de trading de crypto assets doivent obtenir pour poursuivre leur activité. La période transitoire s'élève à un an pour les VATPs (Virtual Asset Trading Platforms) ayant déjà une activité substantielle localisée à Hong Kong pour obtenir cette licence. La licence à obtenir est définie par l'AMLO (Anti-Money Laundering and Counter-Terrorist Financing Ordinance) et est applicable depuis le 1er juin 2023 pour les VATPs non éligibles à la période transitoire. Même si cette licence concerne seulement les acteurs de la finance centralisée, celle-ci est un pas en avant pour l'établissement d'un futur cadre réglementaire englobant à la fois CeFi et DeFi.

Singapour :

A la recherche d'un équilibre entre protection des consommateurs et innovation financière, Singapour est devenue un lieu de prédilection pour les entreprises crypto. Toutefois, après la chute de grandes entreprises crypto basées à Singapour, les régulateurs ont cherché à prioriser la protection des consommateurs. Des propositions comprennent des restrictions sur le prêt de tokens d'investisseurs particuliers et des exigences techniques comparables à celles des banques pour les fintechs. La régulation des stablecoins pointe également à l'horizon, avec des questions en suspens sur les exigences en matière de capital pour les émetteurs autres que les acteurs bancaires.

Globalement, bien que chaque pays ait une approche unique, tous recherchent l'équilibre entre croissance de l'industrie crypto et protection des consommateurs. Les pays asiatiques cités pourraient, en 2024, se placer juste derrière l'Union Européenne en termes de cadre réglementaire robuste et adapté pour la DeFi.

Figure 25 : Réglementations sur les crypto-actifs dans le monde
(Source : lucidityinsights.com/infobytes/crypto-regulations-around-the-world)

INTERVIEW

BENJAMIN MESSIKA

Group Head of Legal & Compliance

RAYN

Benjamin Messika est l'actuel directeur juridique et compliance de Rayn (ex-akt.io). Ancien avocat fiscaliste spécialisé dans le secteur des services financiers chez PwC France, Benjamin a été le responsable fiscal de la société McDonald's France avant d'avoir été le directeur juridique, puis secrétaire général d'une plateforme d'échange d'actifs numériques régulée en France. En parallèle de son activité, Benjamin a été enseignant en droit des affaires et fiscalité à l'Université Paris Panthéon-Sorbonne de 2016 à 2021.

Lancée en 2022, Rayn fusionne la fiabilité de la finance traditionnelle avec l'innovation de l'IA et de la blockchain pour offrir une plateforme d'épargne et d'investissement 3.0. Actuellement active dans plusieurs pays européens, Rayn continue de croître, repoussant les limites de la finance moderne.

> *La réglementation en la matière doit pouvoir soutenir l'innovation tout en protégeant les consommateurs contre les risques potentiels.*

Le défi de la DeFi, entre centralisation et décentralisation

La blockchain ouvre la voie à une nouvelle génération dans le domaine des services financiers caractérisés par leur décentralisation, leur innovation, leur interopérabilité et leur transparence. Ces services, alimentés par la technologie blockchain, offrent des perspectives uniques pour créer une infrastructure financière plus ouverte, robuste et transparente. D'une part, les régulateurs sont désormais confrontés à cette tache non aisée de comprendre, d'analyser l'état de l'écosystème actuel et, le cas échéant, de proposer une réglementation de la Finance Décentralisée (« DeFi »). D'autre part, une analyse structurelle de certains projets qualifiés de "décentralisés" révèle qu'ils sont en réalité moins décentralisés lorsqu'on examine leur infrastructure, principalement en raison d'un manque de clarté concernant la notion de décentralisation.

Actuellement, la DeFi progresse en dehors des limites établies par les réglementations nationales françaises et européennes, notamment au regard du nouveau règlement de l'Union européenne sur les marchés de crypto-actifs (MiCA)[1]. Sans pour autant être mis à l'écart puisqu'elle exclut de son champ d'application les services du crypto-actifs fournis de manière « entièrement décentralisée sans aucun intermédiaire », il a été toutefois demandé à la Commission européenne d'évaluer le développement de la DeFi et d'examiner la nécessité et la faisabilité de sa réglementation avant le 30 décembre 2024.

INTERVIEW

BENJAMIN MESSIKA

En effet, la réglementation en la matière doit pouvoir soutenir l'innovation tout en protégeant les consommateurs contre les risques potentiels. Dès lors, il a été demandé aux régulateurs d'adopter une approche innovante des enjeux de la DeFi pour garantir un niveau de protection équivalent à celui de la réglementation traditionnelle sans pour autant lui appliquer cette dernière qui, en l'état des textes, ne réponde aux défis complexes que pose les défis de la finance décentralisée.

Les rapports rédigés par l'Autorité des marchés financiers (AMF)[2] et l'Autorité de contrôle prudentiel et de résolution (ACPR)[3] vont dans le bon sens tant en termes de méthodologie (appel à consultation) qu'en matière de compréhension, dans les grandes lignes, des enjeux que posent une réglementation innovante et protectrice de notre écosystème. Nombreux sont les acteurs qui tentent de définir cette notion de décentralisation qui leur permettrait de ne pas entrer dans le champ de la réglementation MiCA. Toutefois, un faisceau d'indices se dégage à la lecture des rapports de l'AMF et l'ACPR et comprenant les critères suivants :

- L'utilisation d'une blockchain publique
- Une gouvernance décentralisée
- Un protocole fondé sur des smart contracts
- Un code open source

A ce jour, aucun des critères présentés ci-dessus n'est suffisant, à lui seul, pour qualifier un projet comme entièrement décentralisé et rien ne permet de constater qu'il faille remplir tous les critères, de manière cumulative, pour entrer dans cette définition d'« entièrement décentralisée sans aucun intermédiaire ». Il est fort probable que le régulateur d'un État membre de l'Union européenne choisisse de ne pas s'engager dans une bataille juridique sur le niveau de décentralisation attendu des acteurs de l'écosystème DeFi dans l'attente du projet de réglementation à l'initiative de la Commission Européenne d'ici le 30 décembre 2024.

Par précaution, il est toutefois conseillé aux acteurs de passer en revue les différents rapports français et internationaux afin de préciser davantage les critères identifiés et de se préparer à atteindre le niveau de décentralisation nécessaire pour éviter cette première vague de réglementation de l'écosystème blockchain. En d'autres termes, ces initiatives sont louables puisqu'elles témoignent d'une approche prudente et mesurée en adéquation avec un écosystème encore peu mature en termes de volume et d'usage par rapport à la finance traditionnelle.

[1] Règlement n° 2023/1114, du 31 mai 2023, sur les marchés de crypto-actifs
[2] Finance décentralisée (DeFi), protocoles d'échange et gouvernance : vue d'ensemble, tendances observées et points de discussion réglementaires, Juin 2023
[3] Finance « décentralisée » ou « désintermédiée » (DeFi) : quelle réponse réglementaire ?, 12 octobre 2023

8 OPPORTUNITÉS POUR LES INSTITUTIONNELS ?

Bien que la finance décentralisée soit une tentative de disruption majeure du modèle financier traditionnel, vise à désintermédier le secteur et puisse donc représenter une menace à long terme pour ces derniers, de nombreux institutionnels surveillent de près l'évolution de l'écosystème et commencent à interagir directement avec lui.

8.1. DE NOMBREUSES INITIATIVES

Les principaux acteurs bancaires ont créé des divisions dédiées, et déjà réalisé nombre d'expérimentations, principalement sur des sujets de tokenisation, bien souvent en circuit clos sur des blockchains privés, mais parfois directement sur des blockchains publiques via les protocoles DeFi existant. On peut lister entre autres initiatives :

- **JP Morgan :**
  création de Onyx (business division pour les projets blockchain de la banque) et lancement du projet Guardian, avec l'autorité monétaire de Singapour (MAS) : version modifiée du protocole Aave et du Dex UniSwap sur la blockchain Polygon : réalisations de transactions sur devises et obligations gouvernementales.

- **Société Générale :**
  création de la filiale SG Forge : premier agrément PSAN en France, création du stablecoin « CoinVertible », interactions avec le protocole MakerDAO (voir partie stablecoins), émission et vente d'un green bond à des investisseurs institutionnels (AXA IM et Generali Investments).

- **Crédit Agricole :**
  lancement d'une blockchain publique pour l'émission de bonds. Cette blockchain fonctionne selon un consensus PoCR (Proof of Climate awaReness), qui vise à quantifier l'impact climatique de chaque nœud et récompenser les mineurs en conséquence.

- **Goldman Sachs / banque de France / EIB :**
  lancement d'une plateforme de tokenisation (GS DAP) avec émission d'un digital bond de 100M de l'European Investment Bank (EIB) sur la blockchain privée GS Blockchain. Le paiement a été réalisé via CBDC expérimentale émise par la Banque de France.

- **HSBC :**
  émission d'un bond de 50MGBP via la plateforme de tokenization HSBC Orion (par l'EIB).

- **Santander :**
  bond de 20M€ émis sur Ethereum.

BlackRock :

création du fonds tokenisé BUIDL (BlackRock USD Institutional Digital Liquidity Fund) sur Ethereum, avec déjà plus de 480M$ investis principalement en bons du trésor américain à fin juin 2024.

UBS :

375M$ digitable bond, sur la blockchain de SIX (Six Digital exchange), avec dual listing sur SIX exchange et SDX. La banque, ainsi que plusieurs autres banques suisses, est membre de SDX.

BNP, GS, Deutsche Börse, Microsoft, Moody's, Deloitte & autres :

The canton network : un "réseau de réseaux » (basé sur DAML – digital asset smart contract langage), première blockchain permettant l'interopérabilité entre différentes blockchains utilisées par le système financier, facilitant par exemple les « Atomic transaction » et éliminant tout besoin de réconciliation par une synchronisation des actifs, données et cash entre les systèmes.

Swift & Chainlink :

Chainlink, le réseau décentralisé d'oracles, a développé le protocole CCIP en collaboration avec Swift, BNP Paribas, BNY Mellon, Citi, Clearstream, Euroclear, Lloyds Banking Group et Six Digital Exchange (SDX). Ce protocole vise à permettre aux institutions de connecter leurs infrastructures existantes à différentes blockchains. Il est par exemple possible pour deux banques de réaliser une transaction « on-chain » avec règlement/livraison instantanée (Atomic settlement), entre deux blockchains différentes, qu'elles soient publiques ou privées, et en initiant l'opération via l'infrastructure Swift existante.

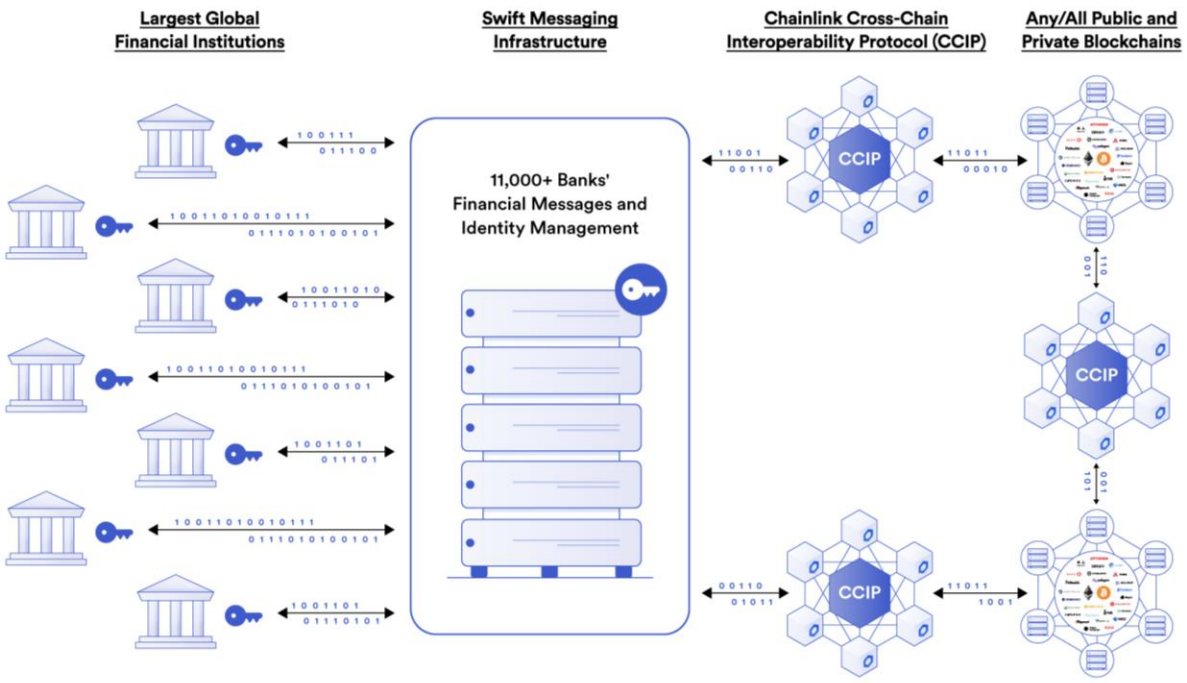


Figure 26 : Architecture simplifiée de l'utilisation de CCIP par les banques et le FMI via le réseau Swift (Source : blog.chain.link/ccip-mainnet-early-access/)

La grande majorité des initiatives précitées portent sur la tokenisation de RWA (real world assets) tels que des bonds. Ce « pont » entre circuit financier traditionnel et finance décentralisée est en effet le principal cas d'usage à présent identifié par les acteurs de l'industrie traditionnelle, qui y voient un immense potentiel de modernisation et de développement. Citi prévoit ainsi qu'en 2030 jusqu'à 4 trillions de dollars d'actifs pourraient être tokénisés.

La tokenisation des actifs présente en effet de nombreux avantages :

- **Atomic settlement** : règlement livraison quasi-instantané : élimination totale du risque de règlement/livraison.
- **Automatisation** de la quasi-intégralité du cycle d'émission d'actifs grâce aux smart contracts : par exemple KYC, confirmations, listing, opérations sur titres : forte baisse des coûts et réduction des risques.
- **Fractionalisation :** création d'un marché pour les actifs traditionnellement illiquides (Private Equity, art, etc…), permettant démocratisation et liquidité accrue.
- **Intéropérabilité et composabilité :** permet d'agréger la liquidité entre marchés et créer un marché des capitaux global et intégré.

8.2. DE LA DEFI À LA HYFI ?

Les banques pourraient donc se diriger vers une modernisation de leurs infrastructures et de leurs réseaux via l'utilisation de la technologie blockchain. Mais tenteront-elles d'y transposer leur pré carré en isolant les protocoles de finance décentralisée qui seraient voués à exister en marge ? Ou bien les deux systèmes pourraient-il collaborer et à terme fusionner ?

La plupart des projets portés par les acteurs institutionnels se basent sur des blockchains privées, le risque est donc de voir émerger un archipel complexe de systèmes clos présentant peu d'avantages comparativement aux anciennes infrastructures de marché et de paiement. Pour que le nouveau système révolutionne vraiment le secteur, il faudra qu'une blockchain publique telle qu'Ethereum prenne le dessus et fasse consensus (par ex. Ethereum associé à un Layer 2), ou bien que les acteurs s'entendent sur un standard unique de communication inter-blockchain, rendant l'archipel existant facilement interopérable, à l'instar du projet porté par Chainlink et Swift (CCCIP). Le terme DeFi pourrait alors devenir HyFi pour « Hybrid Finance ».

L'un des principaux obstacles entravant cette « fusion » entre la DeFi et les institutionnels, reste l'absence de KYC et de système de whitelisting. Sans connaissance des contreparties, ces derniers se heurtent à un mur réglementaire et une impossibilité de réaliser des transactions sur les blockchains publiques. La sécurisation des actifs via la gestion des clés privés est également un défi de taille. Sur les blockchains publiques, les transactions sont irréversibles, qu'elles soient légitimes ou bien liées à un vol ou une erreur humaine. Enfin, la confidentialité des données est également un enjeu important : bien que pseudonymes, les transactions sur blockchains offrent un certain niveau de transparence qui n'est pas systématiquement souhaitable pour les acteurs de la finance traditionnelle. Des protections supplémentaires pour préserver l'anonymat des transactions doivent être mises en place.

Les pure players de l'industrie de la blockchain n'ont en tout cas pas attendu que les acteurs institutionnels viennent les chercher, mais ont approché depuis longtemps ces derniers en tentant de leur proposer des solutions satisfaisantes en termes de sécurité, de discrétion et de compliance.

Des acteurs de la CeFi comme Coinbase ou encore Kraken proposent des offres dédiées aux institutionnels, et des protocoles se sont également lancés sur le segment, comme Alkemy, ou encore le wallet Metamask.

Aave, en collaboration avec Fireblocks, a par exemple déployé un pool de liquidité destiné aux institutionnels, avec un système d'accès sur Whitelist via un processus KYC (Know Your Customer) et un monitoring AML (Anti Money Laundering). Les institutionnels peuvent déposer et accéder à leurs fonds via Fireblocks sur un environnement hautement sécurisé utilisant une combinaison de technologie MPC (multi–party computation) et d'infrastructure Intel SGX. L'ambition du protocole et de la société de « custody » de crypto-actifs est de créer le plus grand marché de « permissioned » DeFi, alliant les avantages de l'innovation technologique tout en préservant un niveau de sécurité et de conformité standard aux institutions financières.

UniSwap semble vouloir s'attaquer également à ce marché, en projetant pour 2024 de proposer la création de pools accessibles uniquement via KYC sur sa version V4.

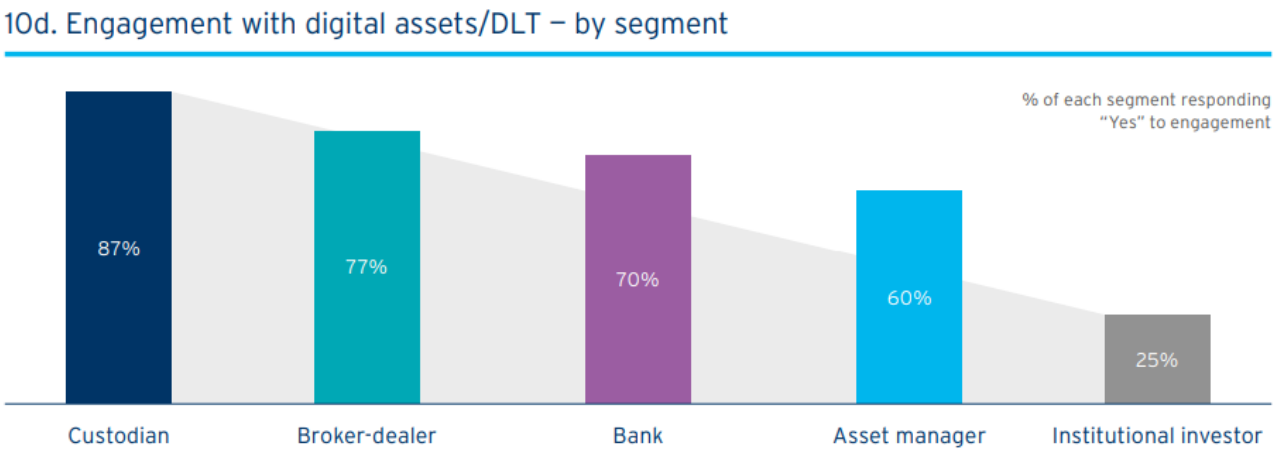


Figure 27 : Résultats d'un sondage réalisé par Citi auprès de 483 professionnels de la finance (2023) (Source : www.citibank.com/mss/docs/Citi_Securities_Services_Evolution_2023.pdf)

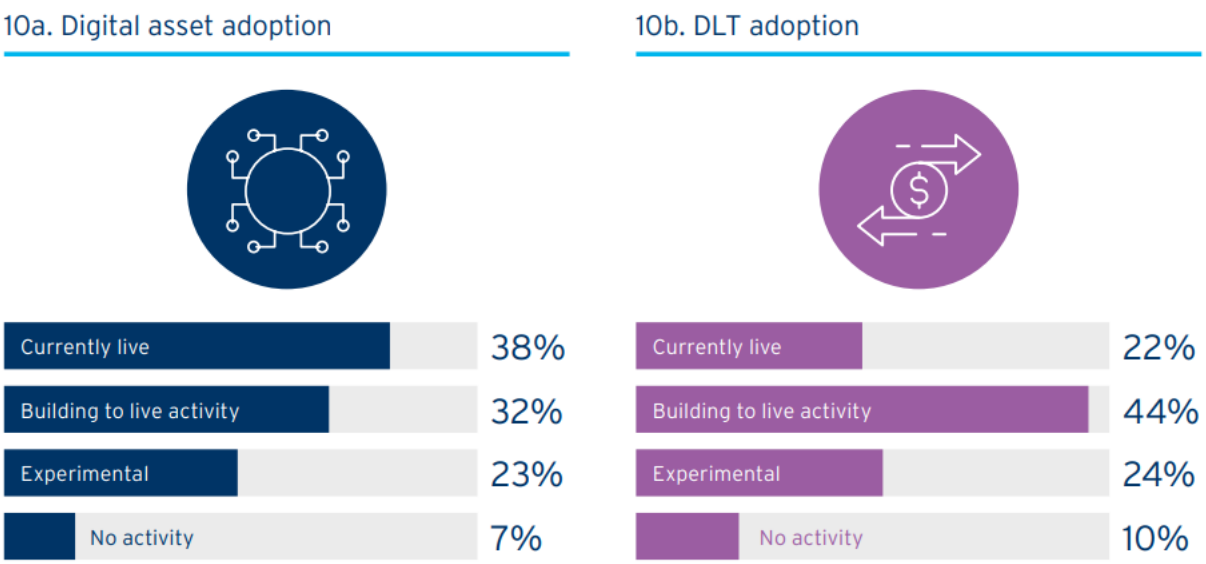


Figure 28 : Résultats d'un sondage réalisé par Citi auprès de 483 professionnels de la finance (2023) (Source : www.citibank.com/mss/docs/Citi_Securities_Services_Evolution_2023.pdf)

Tokenisation des RWA

L'écosystème de la DeFi, grâce à des protocoles innovants, a permis de créer une infrastructure permettant le développement d'un nouveau système financier plus performant. Jusqu'à présent, néanmoins, les crypto-actifs échangés dans cet écosystème ont été principalement des actifs intangibles entachés d'une réputation d'actifs volatils à valeur essentiellement spéculative. Cependant, l'écosystème de la DeFi vit actuellement une vraie révolution avec la tokenisation des real world assets (RWA).

Cette tokenisation consiste à transférer les droits de propriété des actifs du monde réel comme des actions, des obligations ou encore des actifs immobiliers vers des blockchains. Dans le cas d'un actif immobilier, par exemple, le titre de propriété peut être digitalisé et intégré à une blockchain. Une fois « on-chain », ce titre va pouvoir bénéficier des avantages offerts par les smart contracts. La sécurité des transactions pourra être améliorée grâce à une traçabilité accrue et l'absence d'intermédiaires (agents immobiliers, notaires, banques etc.) va permettre de rendre les transactions plus rapides et moins couteuses notamment. Par ailleurs, pour des biens immobiliers illiquides ou trop onéreux, certains protocoles vont permettre la fractionalisation du titre digitalisé : un certain nombre de tokens vont être émis pour représenter le titre et à l'image des SCPI dans la finance traditionnelle, ce mécanisme va permettre à des

investisseurs d'acquérir une part du bien et profiter ainsi des rendements locatifs et de sa potentielle plus-value avec un apport en capital réduit. Ce type de fractionalisation peut être, de la même manière, appliqué à d'autres marchés illiquides ou onéreux comme le marché des œuvres d'art ou des voitures de collection.

En juin 2024, les protocoles RWA comptaient plus de 3,8 mds $ de TVL selon DeFiLlama. Cela semble encore peu comparé aux marchés de la finance traditionnelle comme celui des actions (plus de 100 T $) mais le marché RWA est relativement jeune (2021) et a connu une progression spectaculaire en 2023. Cette progression est notamment due au lancement du protocole stUSDT (« staked USDT ») par RWA DAO en juillet 2023. Initialement lancé sur la plateforme décentralisée JustLend (blockchain Tron), le protocole est désormais accessible sur Ethereum. Le DAO est doté d'une direction des investissements (RWA arranger) qui établit une allocation stratégique et tactique sur des RWA (principalement des obligations gouvernementales de qualité et à échéances courtes) sous la supervision d'un conseil consultatif qui soumet ensuite les propositions d'allocations au vote des membres du DAO. A l'image d'un fonds d'investissement, les investisseurs vont apporter du capital (sous la forme de staking d'USDT ou TUSD) et vont pouvoir ainsi profiter des rendements des investissements du fonds. Le rendement actuel est de 4.6%.

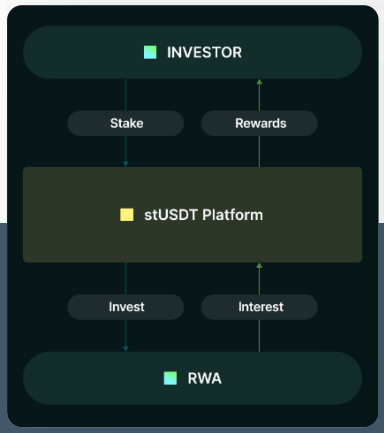


Figure 29 : Flux de capitaux et revenus entre investisseurs et RWA DAO (Source : stusdt.io)

Figure 30 : Fonctionnement du RWA DAO (Source : stusdt.io)

Une multitude d'autres acteurs permettent également déjà l'accès aux RWA. Parmi les plus importants on peut citer Ondo Finance (TVL : ~550m $) focalisé sur les bons du trésor américain, ou encore RealT (TVL : ~100m $) spécialisé dans la tokenisation et fractionalisation d'actifs immobiliers. Par ailleurs, si MakerDAO n'est pas un protocole de tokenisation de RWA à proprement parler, celui-ci dispose actuellement de près de 2 mds $ de RWA jouant le rôle de collatéral pour son stablecoin.

LENDING	COMMODITIES	ESG	RWA-BACKED STABLECOINS	DEBT SECURITIES & EQUITY	OTHER
Centrifuge (CFG)	**PAX Gold** (PAXG)	**Toucan Protocol** (TCO2)	**MakerDAO** (DAI)	**Ondo Finance** (ONDO)	**RealT**
Maple Finance (MPL)	**Tether Gold** (XAUT)	**KlimaDAO** (KLIMA)	**Frax Finance** (FRAX)	**Matrixdock** (STBT)	**RWA.xyz**
Goldfinch (GFI)	**CACHE Gold** (CGT)	**Senken**	**Angle Protocol** (agEUR)	**Backed Finance** (bTokens)	**SteakFi**
Credix			**Flux Finance** (fUSD)	**Aktionariat** (DAKS)	**Avalanche Sqruce** (AVAX)
TProtocol			**Tangible** (USDR)	**Hashnote** (SDYC)	**Canto** (CANTO)
TrueFi (TRU)				**OpenEden** (TBILL)	**Kinto**
					Pendle (PENDLE)
					FortunaFi

Figure 31 : Acteurs de la tokenisation de RWA

INTERVIEW

RAMZI AMAIRI

Tech Hub Director
Digital Assets Lead

NATIXIS CIB

Ramzi Amairi, Directeur à la Banque de Grande Clientèle de Natixis CIB, couvre les entreprises innovantes dans le domaine de la New Tech. Pilier du Tech Hub, Ramzi a plus de 15 ans d'expérience dans le secteur bancaire à des postes stratégiques, aussi bien en France qu'à l'international. Sa passion pour l'innovation et les nouvelles technologies l'a amené à explorer les opportunités offertes par la blockchain et à développer une franchise client dans l'écosystème Web3.

« Le développement rapide de la DeFi souligne aux banques l'urgence de l'adaptation. »

Comment les banques perçoivent-elles l'émergence de la DeFi et plus largement du Web3, entre opportunités et menaces ?

Les banques reconnaissent le potentiel de la technologie blockchain pour innover dans les services financiers et atteindre de nouveaux marchés. Elles sont conscientes que cela remet en question leur modèle traditionnel et pourrait potentiellement les rendre obsolètes dans certains domaines.

Les banques cherchent donc à comprendre et à s'adapter à ces changements, en explorant des collaborations, des investissements dans des startups ou même en développant leurs propres solutions dans le domaine de la blockchain et de la finance décentralisée (CBDC, stablecoins, RWA tokens).

La finance décentralisée reste cependant un système récent dont il faut comprendre les limites. Lorsque les banques sont l'intermédiaire principal, elles offrent une protection aux investisseurs, une stabilité et un environnement régulé.

Le cadre réglementaire est-il aujourd'hui adapté pour accompagner et stimuler le développement du secteur Web3 en France ?

Le cadre règlementaire pour le Web3 en France est en constante évolution pour accompagner son développement. Bien que des progrès aient été réalisés, il reste encore des défis à relever pour assurer une régulation efficace tout en favorisant l'innovation. Les autorités règlementaires, telles que l'AMF et la Banque de France, travaillent à encadrer ces activités, tout en veillant à protéger les investisseurs et à prévenir les risques du secteur comme dans la finance traditionnelle.

INTERVIEW

RAMZI AMAIRI

Un dialogue entre les acteurs du secteur, les régulateurs et les législateurs est essentiel pour créer un environnement propice à l'émergence du Web3 en France. L'entrée en vigueur du règlement européen Markets in Crypto-Assets (MiCA) doit permettre à l'UE de s'adapter, avec un cadre harmonisé, aux innovations technologiques développées par le secteur de la fintech en général, et à la blockchain en particulier.

Comment la DeFi pourrait-elle redéfinir le paysage financier traditionnel au cours des prochaines années ?

La finance décentralisée fait bien évidement partie des grands moteurs de la transformation du paysage financier. Grace à la blockchain et aux smart contracts, la finance traditionnelle dispose désormais d'outils pour offrir des services plus rapides, moins couteux, plus transparents et plus accessibles à tous.

Le développement rapide de la DeFi souligne aux banques l'urgence de l'adaptation. A mesure que le paysage continue d'évoluer, la collaboration entre les acteurs historiques et les innovateurs devient cruciale pour un progrès durable. Il est fort probable que les acteurs de la DeFi s'associent à des groupes bancaires pour leur permettre d'adopter leurs nouvelles innovations afin de rester pertinents dans un paysage financier en constante évolution.

La DeFi ne pourra redéfinir durablement le paysage financier qu'en donnant la priorité à la gestion des risques et en conformant ses acteurs à une règlementation de plus en plus mature.

Quelle est la politique de Natixis CIB à l'égard du Web3 et quelles initiatives sont mises en place dans ce domaine ?

La blockchain suscite un intérêt particulier pour Natixis CIB depuis plus de dix ans. Dans ce cadre, nos experts ont exploré ce que la technologie pouvait apporter à nos métiers puis nous avons commencé à l'appliquer à des cas d'usages concrets pour notamment améliorer l'efficacité de nos processus internes.

Depuis 2021, Natixis CIB dispose d'un « Tech Hub » pour réunir le savoir-faire de ses équipes sur les sujets tech et accompagner ses clients dans leur transition technologique, qu'ils soient spécialisés ou non dans la tech. Avec le Tech Hub, Natixis CIB est en mesure de leur proposer des solutions de financements et de levées de capitaux ciblées sur leurs ambitions de développement dans le domaine du digital et des nouvelles technologies, incluant celles du Web3.

Il est fort probable que les acteurs de la DeFi s'associent à des groupes bancaires pour leur permettre d'adopter leurs nouvelles innovations afin de rester pertinents dans un paysage financier en constante évolution.

CONCLUSION

La finance décentralisée n'est pas seulement une innovation technologique ou un terrain de jeux pour geeks jouant aux apprentis sorciers de la finance ; c'est une révolution qui bouscule les conventions et pourrait redéfinir les règles du jeu en matière de services financiers.

Ce système se développe de manière organique, par essais et erreurs, via l'ajout de différentes briques interconnectées et le tout dans un environnement majoritairement open-source. Le bruit provoqué par l'éclatement des bulles et les nombreuses escroqueries et piratages ne doit pas faire oublier l'objectif originel encore partagé par une majorité d'acteurs de ce mouvement : rendre l'industrie financière plus transparente, rapide, efficace et accessible à tous, sans distinction de patrimoine ou de localisation géographique.

L'écosystème en est encore à ses balbutiements, et de nombreux obstacles se dressent sur son chemin. La sécurité, la régulation, et la scalabilité sont des défis cruciaux qui nécessitent des solutions innovantes et une collaboration étroite entre les acteurs de l'écosystème, les régulateurs, et les utilisateurs eux-mêmes.

Le futur de la DeFi est riche de possibilités, et son impact potentiel sur notre société est colossal. Il se dit de Bitcoin qu'il n'est pas la monnaie de l'Internet mais l'Internet de la monnaie. Si tel est le cas, la finance décentralisée constitue la couche applicative de ce nouveau réseau mondial.

Les institutions financières ont bien perçu ce potentiel et pour certaines tentent d'établir des ponts avec ce nouveau système. Outre leur intérêt pour les avantages technologiques, prometteurs en termes de réduction de coûts, elles doivent suivre le basculement générationnel qui s'opère chez leurs clients. L'écart s'accélère en effet entre le comportement des investisseurs « traditionnels » et les nouveaux « jeunes actifs » ayant grandi dans l'ère numérique : d'après une récente étude de l'OCDE réalisée pour l'AMF, les nouveaux investisseurs ont une forte préférence pour les crypto-actifs, et la majorité d'entre eux (54%) en sont déjà détenteurs. Cette proportion atteint même 63% pour la tranche 25-34 ans.

GLOSSAIRE

CRYPTO-ACTIFS

Bitcoin :

Première crypto-monnaie décentralisée basée sur la blockchain, lancée en 2009 par une personne ou un groupe de personnes sous le pseudonyme de Satoshi Nakamoto. Bitcoin permet des transactions peer-to-peer sans intermédiaire.

Crypto-actif :

Actif numérique basé sur la cryptographie et les technologies blockchain. Les crypto-actifs incluent les crypto-monnaies, les tokens et les actifs numériques uniques tels que les NFT.

cToken :

Token représentant les intérêts gagnés sur les actifs déposés sur Compound.

Curve (CRV) :

Token natif du protocole Curve utilisé pour la gouvernance et les récompenses.

DAI :

Exemple de stablecoin adossé à des crypto-monnaies. Créé par le protocole MakerDAO, le DAI est conçu pour maintenir une parité de 1 :1 avec le dollar américain en utilisant un mécanisme de collatéralisation et un système de gouvernance décentralisé.

ERC-20 :

Standard technique pour les tokens fongibles sur Ethereum. Les tokens ERC-20 sont largement utilisés pour les ICO (Initial Coin Offerings) et les projets basés sur Ethereum.

ERC-721 :

Standard technique pour les tokens non-fongibles (NFT) sur Ethereum. Les NFT représentent des objets uniques et peuvent être utilisés pour des biens numériques tels que des œuvres d'art.

Ethereum :

Plateforme blockchain open-source, lancée en 2015, permettant la création de contrats intelligents et d'applications décentralisées. Ethereum est connue pour son crypto-actif natif, Ether (ETH), utilisé pour payer les frais de transaction et de calcul sur le réseau.

Crypto-actif natif :

Crypto-actif natif d'une plateforme blockchain, comme l'Ether (ETH) pour Ethereum. Ces crypto-actifs sont souvent utilisés pour payer les frais de transaction et participer aux mécanismes de gouvernance de la plateforme.

Stablecoin :

Crypto-actif dont la valeur est liée à un actif de référence, souvent une monnaie fiduciaire, pour en réduire la volatilité. Les stablecoins permettent d'effectuer des transactions plus stables et sont souvent utilisés comme moyen d'échange ou de stockage de valeur dans l'écosystème crypto.

veCRV (vote escrowed curve) :

Version verrouillée du token CRV utilisée pour le vote dans la gouvernance de Curve.

PROTOCOLES

1inch :

Agrégateur de DEX populaire, offrant des échanges optimisés entre différentes plateformes.

Aave :

Protocole DeFi open-source qui permet aux utilisateurs de gagner des intérêts en déposant des actifs et d'emprunter des actifs contre des garanties. Aave offre également des fonctionnalités avancées telles que les flash loans et les swaps de taux d'intérêt.

Automated Market Maker (AMM) :

Protocole facilitant les échanges de tokens sur les DEX via des pools de liquidités.

CEX (Centralized Exchanges) :

Plateformes d'échange de crypto-monnaies centralisées, gérées par une entité unique.

Chainlink :

Réseau oracle décentralisé qui fournit des données externes aux smart contracts sur la blockchain. Chainlink permet aux contrats intelligents d'accéder à des données fiables et sécurisées provenant de sources hors chaîne.

Compound :

Protocole DeFi permettant aux utilisateurs de prêter et d'emprunter des crypto-actifs. Les utilisateurs gagnent des intérêts sur les actifs déposés et paient des intérêts sur les actifs empruntés, avec des taux déterminés par l'offre et la demande.

Convex (CVX) :

Plateforme optimisant les rendements pour les utilisateurs de Curve, avec son propre token natif.

Curve Finance :

Protocole d'échange décentralisé et marché monétaire pour stablecoins et actifs à faible volatilité. Curve Finance optimise les échanges en minimisant le slippage et en maximisant les rendements pour les fournisseurs de liquidité.

Dex aggregators :

Outils permettant d'obtenir le meilleur prix et la meilleure liquidité pour les échanges en interagissant avec plusieurs DEX simultanément.

Dopex :

Plateforme décentralisée d'options avec des mécanismes de tarification et de liquidités innovants.

dYdX :

Plateforme décentralisée offrant des produits dérivés tels que les perpetual swaps et les marges de trading.

Hegic :

Plateforme décentralisée d'options sur Ethereum.

MakerDAO :

Protocole DeFi qui permet de générer des DAI, un stablecoin adossé à des actifs, principalement des crypto-monnaies. Les utilisateurs déposent des actifs dans des "Coffres" (Vaults) pour générer des DAI, qui sont ensuite utilisés pour diverses activités DeFi.

Opyn :

Plateforme décentralisée d'options et de couverture de risques sur Ethereum.

Oracle :

Service fournissant des données externes aux smart contracts sur la blockchain.

Plateformes d'échanges décentralisées (DEX) :

Plateformes d'échange de crypto-monnaies sans autorité centralisée, utilisant des smart contracts.

Protocoles de prêts décentralisés (Lending) :

Protocoles permettant d'emprunter et de prêter des actifs de manière décentralisée.

Synthetix :

Protocole DeFi permettant la création et l'échange d'actifs synthétiques, représentant des actifs réels tels que des devises, des matières premières ou des indices boursiers. Synthetix utilise des smart contracts et un système de garanties pour émettre des actifs synthétiques.

Uniswap :

DEX populaire basé sur Ethereum, utilisant le modèle AMM.

Yield optimizers :

Protocoles automatisant la recherche et l'exploitation des meilleures opportunités de rendement en DeFi.

Yearn Finance :

Plateforme DeFi conçue pour simplifier l'investissement dans les protocoles DeFi et maximiser les rendements. Yearn Finance offre des services tels que l'agrégation de rendement, les pools de liquidité et l'optimisation du capital.

TERMES TECHNIQUES

APY (Annual Percentage Yield) :

Taux représentant le rendement potentiel d'un investissement sur un an, en tenant compte de la capitalisation des intérêts. L'APY est souvent utilisé pour comparer les rendements des différents protocoles DeFi et pour évaluer la rentabilité d'un investissement.

Blockchain :

Technologie de registre distribué permettant d'enregistrer les transactions de manière sécurisée et transparente. Les blockchains sont décentralisées, ce qui signifie qu'elles sont gérées par un réseau d'ordinateurs plutôt que par une seule entité.

Bonding Curve :

Modèle mathématique décrivant la relation entre la liquidité et le prix d'un token.

Bribing Economy :

Pratique consistant à inciter les détenteurs de tokens de gouvernance à voter en leur faveur en échange de récompenses.

Clé privée :

Clé cryptographique pour accéder et gérer les fonds d'un utilisateur. La clé privée doit être gardée secrète et sécurisée pour éviter le vol de fonds.

Crypto-actifs synthétiques :

Tokens représentant d'autres actifs tels que des actions, devises ou matières premières.

DAO :

Organisation décentralisée dont les règles sont définies par des smart contracts. Les DAO visent à créer des organisations plus équitables et transparentes en supprimant les intermédiaires et en impliquant les utilisateurs dans la gouvernance.

Dapp :

Application construite sur une plateforme blockchain utilisant des contrats intelligents. Les Dapps sont transparentes, résistantes à la censure et n'ont pas d'entité centrale de contrôle.

DeFi:

Écosystème de services financiers construits sur la technologie blockchain. La finance décentralisée (DeFi) vise à démocratiser l'accès aux services financiers en éliminant les intermédiaires traditionnels.

DeFi Stack :

Ensemble des couches technologiques pour la finance décentralisée. Le DeFi Stack comprend les protocoles, les smart contracts, les crypto-actifs, les wallets et les interfaces utilisateurs pour permettre l'accès aux services financiers décentralisés.

Farming de liquidité :

Pratique consistant à déposer des actifs dans un pool de liquidité pour gagner des récompenses, généralement sous forme de tokens de gouvernance ou d'intérêts. Le farming de liquidité incite les utilisateurs à fournir de la liquidité aux protocoles DeFi, améliorant ainsi la stabilité et l'efficacité des échanges.

Flash loan :

Prêt instantané et sans garantie offert par certaines plateformes DeFi. Les flash loans permettent aux utilisateurs d'emprunter des fonds le temps d'une seule transaction, à condition que les fonds soient remboursés à la fin de la transaction. Les flash loans sont souvent utilisés pour l'arbitrage, la migration de dettes et d'autres stratégies avancées.

Front-running :

Pratique consistant à exploiter les transactions en attente pour en tirer profit.

Gouvernance décentralisée :

Système de décision collective où les détenteurs de tokens de gouvernance participent au processus décisionnel d'un projet ou d'une organisation. La gouvernance décentralisée vise à rendre les projets plus démocratiques et à responsabiliser les utilisateurs.

Impermanent Loss :

Perte temporaire de valeur pour les fournisseurs de liquidité, causée par la fluctuation des prix des actifs déposés dans un pool de liquidité. L'impermanent loss peut être compensé par les récompenses de farming de liquidité, mais il est important pour les fournisseurs de liquidité de comprendre et de gérer ce risque.

Layer 2 :

Solutions de mise à l'échelle pour les plateformes blockchain. Les solutions Layer 2 fonctionnent au-dessus de la blockchain principale pour décharger une partie du trafic et optimiser les performances.

Liquidity Provider (LP) :

Utilisateur fournissant des actifs dans les pools de liquidités sur les DEX en échange de frais de transaction.

Liquid staking (Lido) :

Solution de staking décentralisée pour Ethereum 2.0, offrant des tokens stETH représentant les ETH déposés.

Perpetual swaps :

Contrats dérivés similaires aux contrats à terme, mais sans date d'expiration, permettant un échange continu.

Pool de liquidité :

Ensemble de fonds déposés pour faciliter les échanges de tokens, notamment sur les DEX. Les fournisseurs de liquidité (LP) déposent des actifs dans un smart contract. En échange, ils reçoivent des tokens de liquidité représentant leur part du pool, et perçoivent des récompenses sous forme de frais de transaction générés par les échanges effectués sur le pool.

Options vaults :

Pools de liquidités utilisés pour la gestion collective d'options.

Restaking :

Réutilisation de crypto-actifs stakés afin de sécuriser d'autres protocoles, sans avoir à les retirer du protocole initial.

RWA (Real World Assets) :

Actifs du monde réel tokenisés pour être utilisés comme collatéral ou échangés dans les protocoles DeFi.

Slippage :

Différence entre le prix attendu et le prix exécuté d'une transaction. Le slippage peut être causé par la volatilité du marché et le manque de liquidité.

Smart contract :

Programme auto-exécutable basé sur la blockchain qui déclenche des transactions conditionnelles. Les contrats intelligents permettent d'automatiser et de sécuriser des processus sans intermédiaires, favorisant la création d'applications décentralisées.

Staking derivatives :

Tokens représentant des actifs déposés pour le staking, qui peuvent être réutilisés sur d'autres protocoles, voire restakés.

Tokenisation :

Processus de conversion d'actifs physiques ou numériques en tokens sur une blockchain. Ce qui permet de faciliter l'échange, la gestion et la fractionnalisation de ces actifs.

Total Value Secured (TVS) :

Montant de TVL dépendante d'un oracle spécifique (cas de Chainlink).

Transaction Value Enabled (TVE) :

Somme totale des valeurs de transactions ayant fait appel aux Price Feeds d'un Oracle (cas de Chainlink).

TVL (Total Value Locked) :

Valeur totale des actifs déposés dans un protocole DeFi.

CONTRIBUTEURS

Auteurs :

- **Pierre Gineste** – Directeur – *Nexialog Consulting*
- **Reda Nekmouche** – Manager – *Nexialog Consulting*
- **Antoine Jacquet** – Consultant – *Nexialog Consulting*

Edition et design :

- **Mathilde Noel** – Responsable Marketing & Communication – *Nexialog Consulting*

Partenaire :

- **Cyril Armange** – Directeur Général Adjoint – *Finance Innovation*

Intervenants :

- **Leopold Wenger** – CFO – *Cometh*
- **Yann le Floch** – Digital Asset Banker – *Trakx*
- **Pablo Veyrat** – CoFounder – *Angle*
- **Louis Bertucci** – Head of Center for Digital and Decentralized Finance (C2DF) – *Institut Louis Bachelier*
- **Benjamin Messika** – Head of legal & Compliance – *Rayn*
- **Ramzi Amairi** – Tech Hub Director & Digital Assets Lead – *Natixis CIB*
- **Cyril Armange** – Directeur Général Adjoint – *Finance Innovation*

REMERCIEMENTS

Relecteurs :

- **Areski Cousin** – Directeur Scientifique – *Nexialog Consulting*
- **Adrien Misko** – Senior Manager – *Nexialog Consulting*
- **Bastien Lefiot** – Account Manager – *Nexialog Consulting*

SOURCES

Base technologique de la defi

Economic Research | Federal Bank of St. Louis - Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets (2021)
research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets

L2 beat
https://l2beat.com/scaling/summary

Stablecoins

Ayten Kahya, Bhaskar Krishnamachari, Seokgu Yun | Viterbi School of Engineering, University of Southern California - Reducing the Volatility of Cryptocurrencies - A Survey of Stablecoins
https://arxiv.org/ftp/arxiv/papers/2103/2103.01340.pdf

The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System
https://makerdao.com/en/whitepaper/

Sirio Aramonte, Wenqian Huang, Andreas Schrimpf - DeFi risks and the decentralisation illusion (2021)
https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf

Kevin Jayaraj - Algorithmic Stablecoins- Everything you NEED to Know! (2023)
https://www.coinbureau.com/education/algorithmic-stablecoins/

Ampl
www.ampleforth.org

Jupiter Zheng CFA, Research Director, HashKey Capital - Algorithm Stablecoin — The Holy Grail of Next-Generation DeFi (2021)
https://medium.com/hashkey-group/algorithm-stablecoin-the-holy-grail-of-next-generation-defi-c33ed6da606

Thomas A., La perspective des CBDC se rapproche ? Cointribune (2023)
https://www.cointribune.com/la-perspective-des-cbdc-se-rapproche

CBDC Tracker | Today's Central Bank Digital Currencies Status
https://cbdctracker.org/

Frax Finance | Frax Finance Stablecoin Protocol
https://docs.frax.finance/

SOURCES

Protocoles d'échange décentralisés (DEX)

Dmitriy Berenzon - Constant Function Market Makers: DeFi's "Zero to One" Innovation (2020)
https://medium.com/bollinger-investment-group/constant-function-market-makers-defis-zero-to-one-innovation-968f77022159

Nat Eliason - Field Guide to the Curve Wars: DeFi's Fight for Liquidity (2022)
https://every.to/almanack/curve-wars

Vijay Mohan - Automated market makers and decentralized exchanges: a DeFi primer (2022)
https://jfin-swufe.springeropen.com/articles/10.1186/s40854-021-00314-5

Hayden Adams, Noah Zinsmeister, Noah Zinsmeister, River Keefer, Dan Robinson - Uniswap v3 Core (2021)
https://uniswap.org/whitepaper-v3.pdf

Convex Finance Documentation. (2024)
https://docs.convexfinance.com/convexfinance

Curve Finance - Curve Whitepaper (2021)
https://classic.curve.fi/whitepaper

Protocoles de prêts décentralisés (lending) – NFT

Robert Leshner, Geoffrey Hayes - Compound: The Money Market Protocol (2019)
https://compound.finance/documents/Compound.Whitepaper.pdf

dYdX Documentation
https://docs.dydx.community/dydx-token-migration

Hegic
https://www.hegic.co/

Ian - Understanding Compound Protocol's Interest Rates (2020)
https://ianm.com/posts/2020-12-20-understanding-compound-protocols-interest-rates

Aave Team - Aave Protocol GitHub Repository
https://github.com/aave

Liquity Team - Liquity Protocol Documentation (2024)
https://docs.liquity.org/

Morpho Team - Morpho Protocol Whitepapers (2024)
https://docs.morpho.org/whitepapers/

SOURCES

Produits dérivés et structurés

Dopex Documentation
https://docs.dopex.io/

Volmex Team - Volmex IV: A DeFi Index for Market Volatility (2024)
https://volmex.finance/Volmex-IV-paper.pdf

IPOR Team - IPOR: The Interest Rate Protocol on Ethereum (2024)
https://docs.ipor.io/research-whitepapers/white-paper

Notional Finance Team - Notional Finance Documentation (2024)
https://docs.notional.finance/notional-v3

Lido Finance Team - Lido Protocol Documentation (2024)
https://docs.lido.fi/

Agrégateurs : Brokers et portfolio managers de la DeFi

1inch Team - 1inch Protocol Documentation (2024)
https://portal.1inch.dev/documentation/overview

ParaSwap Team - ParaSwap Blog
https://paraswap.medium.com/

Yearn Finance Team - Yearn Finance Documentation (2024)
https://docs.yearn.fi/

Instadapp Team - Instadapp Protocol Documentation (2024)
https://docs.instadapp.io/

Arrakis Team - Arrakis Protocol Documentation (2024)
https://docs.arrakis.fi/

TokenSets Team - TokenSets Documentation (2024)
https://docs.tokensets.com/

Risques et réglementations

Autorité des marchés financiers (AMF) - Marchés de crypto-actifs : le règlement MiCA adopté par le Parlement européen (2023)
https://www.amf-france.org/fr/actualites-publications/actualites/marches-de-crypto-actifs-le-reglement-mica-adopte-par-le-parlement-europeen

Journal du Coin - MiCA : Opportunité pour l'Europe ou frein à l'adoption ? (2023)
https://journalducoin.com/economie/mica-opportunite-europe-frein-adoption/

SOURCES

Autorité de contrôle prudentiel et de résolution (ACPR) - Finance décentralisée désintermédiée (2023)
https://acpr.banque-france.fr/sites/default/files/medias/documents/20230403_finance_decentralisee_desintermediee_fr.pdf

Coin Bureau - What is DeFi? (2023)
https://www.youtube.com/watch?v=8SeIQ93xwyU

BeInCrypto - Test de Howey : De quoi s'agit-il ?
https://fr.beincrypto.com/apprendre/test-howey-quoi-sagit-il/

Bank for International Settlements (BIS) - Defi Risks and Opportunities (2023)
https://www.bis.org/fsi/publ/insights49.pdf

Chainalysis Team - Chainalysis Official Website
https://www.chainalysis.com/

Lucidity Insights - Crypto Regulations Around the World (2023)
https://lucidityinsights.com/infobytes/crypto-regulations-around-the-world

Nexus Mutual Team - Nexus Mutual Documentation (2024)
https://docs.nexusmutual.io/

Blockdata - Chainalysis Refutes Prevailing Cryptocurrency Myths Amongst Financial Institutions (2023)
https://www.cbinsights.com/research/bitcoin-blockchain/

Chainlink Team - Chainlink Documentation (2024)
https://docs.chain.link/

Chainalysis Team - Crypto Crime Report 2024 (2024)
https://go.chainalysis.com/crypto-crime-2024.html

Opportunités pour les institutionnels ?

RWA Team - RWA.xyz Official Website
https://app.rwa.xyz/

European Central Bank - Is DeFi Real Finance? (2023)
https://www.bankingsupervision.europa.eu/press/blog/2023/html/ssm.blog230405~03fd3d664f.en.html

J.P. Morgan Onyx - Institutional DeFi: The Next Generation of Finance (2023)
https://www.jpmorgan.com/onyx/documents/Institutional-DeFi-The-Next-Generation-of-Finance.pdf

Citibank - Citi Securities Services Evolution 2023 (2023)
https://www.citibank.com/mss/docs/Citi_Securities_Services_Evolution_2023.pdf

SOURCES

Chainlink Team - Chainlink Blog
https://blog.chain.link/

Staked USDT Team - Staked USDT Official Website
https://stusdt.io/#/home

OECD - Why Decentralised Finance (DeFi) Matters and the Policy Implications (2022)
https://www.oecd.org/en/topic/policy-issue/financial-markets.html

Oliver Wyman Forum - Institutional DeFi: The Next Generation of Finance (2022)
https://www.oliverwymanforum.com/future-of-money/2022/Nov/institutional-defi.html

J.P. Morgan Onyx - Onyx Digital Assets
https://www.jpmorgan.com/onyx/onyx-digital-assets

Conclusion

OECD - Les nouveaux investisseurs particuliers en France (2022)
https://www.amf-france.org/en/news-publications/news-releases/amf-news-releases/oecd-study-amf-profiles-new-french-retail-investors

Données de marché

CoinGecko Team - CoinGecko Official Website
https://www.coingecko.com/

CoinMarketCap Team - CoinMarketCap Official Website
https://coinmarketcap.com/

The Block Team - The Block Official Website
https://www.theblock.co/

DeFi Llama Team - DeFi Llama Official Website
https://defillama.com/

Nexialog Consulting

FINANCE | ACTUARIAT | GESTION DES RISQUES | DATA | ESG

Nexialog Consulting, cabinet de conseil spécialisé en actuariat, gestion des risques, transformation durable et services financiers, est votre partenaire de confiance dans les secteurs de la **banque** et de l'**assurance**.

Forts de nos 150 collaborateurs et d'un chiffre d'affaires de 18,5 millions d'euros, nous sommes fiers de notre parcours de croissance depuis notre création en 2006. Grâce à nos six pôles d'expertise : **Actuariat Conseil**, **Risk Management & Bank**, **Global Markets**, **Contrôle Finance Risques**, **Data Consulting** et **Finance Durable** et notre approche pragmatique du conseil qui combine des compétences métiers, réglementaires, de gestion de projet et de transformation, nous sommes en mesure d'offrir des solutions innovantes et durables à nos clients.

Notre capacité à intégrer ces différentes expertises de manière complémentaire, offre ainsi une vue à 360 degrés sur les enjeux opérationnels, réglementaires et de durabilité et nous permet d'anticiper les défis futurs de nos clients.

19
M€ de chiffre d'affaires

150
Collaborateurs intervenant auprès des grands acteurs de la banque et de l'assurance

35
Comptes clients actifs

6
Pôles d'expertise : Actuariat Conseil, Risk Management & Bank, Global Markets, Direction Financière, Data Consulting, Finance Durable

2006
Création de Nexialog Consulting. Le cabinet connaît une forte croissance et s'est imposé comme un acteur de référence.

NOTRE CELLULE R&D

Notre cellule R&D, construite autour de consultants seniors disposant d'expertises pointues, met en œuvre des projets afin d'anticiper les besoins de nos clients. Via le travail de cette équipe pluridisciplinaire, nous suivons avec attention les dernières évolutions règlementaires et méthodologiques des secteurs de la banque, de la gestion d'actifs et de l'assurance :

Exemples de travaux R&D et partages de connaissances :

- *Mesure de l'aversion au risque par les robo-advisors*
- *Benchmark des solutions de data anonymisation*
- *Working Paper Markov-Switching Mixture GARCH*
- *Benchmark des rapports ART.29 Loi Energie Climat en Assurance Vie*

CONTACTS

Ali Behbahani

Associé Fondateur

+33 (0)1 44 73 86 78
+33 (0)6 64 23 58 19
abehbahani@nexialog.com

Christelle Bondoux

Associée Direction commerciale et recrutement

+33 (0)6 99 30 42 49
cbondoux@nexialog.com

Pierre Gineste

Directeur – Global Markets

+33 (0)6 12 68 29 71
pgineste@nexialog.com

Areski Cousin

Directeur Scientifique - R&D

+33 (0)7 88 03 51 87
acousin@nexialog.com

2024

Droits d'auteurs – Nexialog Consulting