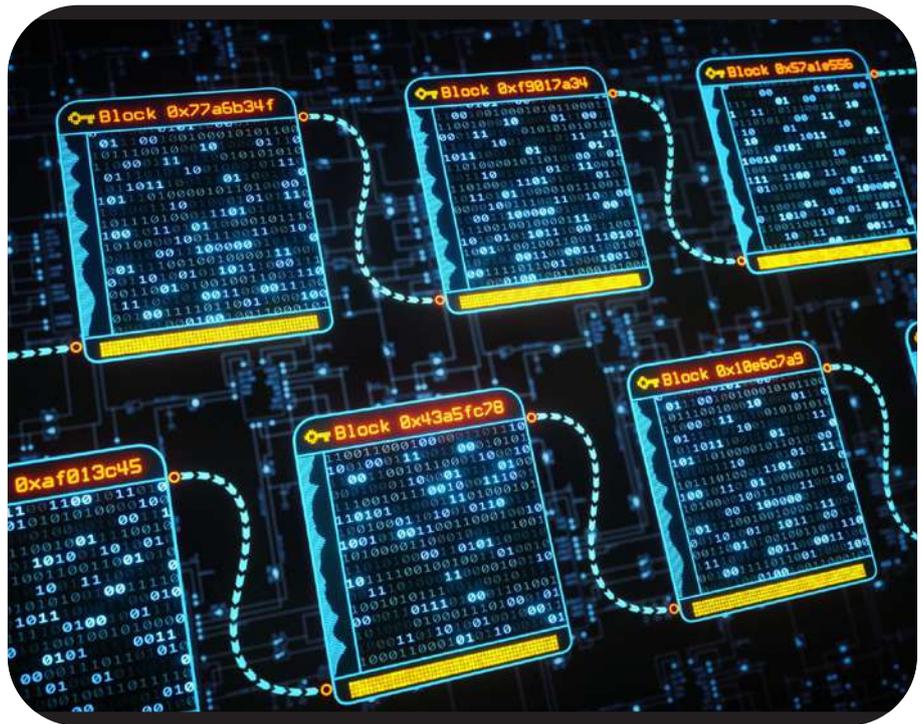


École Polytechnique, Palaiseau
Amphithéâtre BECQUEREL

DéFI, la finance réinventée

Jeudi 09 juin 2022



Coordination scientifique :

- David MENGA (EdF)
- Vidal CHRIQUI (Get Verso)



Renseignements, programme...

<https://www.association-aristote.fr/evenements/defi-la-finance-reinventee/>

ARISTOTE

À la croisée des révolutions numériques

Table des matières

INTRODUCTION PAR DAVID MENGA.....	2
1- LA REVOLUTION DE LA DEFI.....	3
2. AUTOMATED MARKET MAKERS, ÉTAT DES CONNAISSANCES.....	4
3. LE HARDWARE WALLET : UN COFFRE-FORT PERSONNEL POUR LA FINANCE DÉCENTRALISÉE.....	5
4. LA RÉGLEMENTATION DE LA FINANCE DÉCENTRALISÉE.....	6
5. DESIGNS ET ENJEUX DES STABLECOINS CENTRALISÉS ET DÉCENTRALISÉS.....	7
6. LA DÉFI EN PRATIQUE – LIVE DÉMO SUR LE PLACEMENT DE SES 1000 PREMIERS JEUR DANS LA DEFI.....	8
7. OPTIONS DÉCENTRALISÉES : ÉTAT DES LIEUX, LIMITES ET POTENTIEL.....	9
8. DÉMOCRATISATION DE LA DÉFI DANS LA GESTION DE PATRIMOINE.....	10
9. LA DÉFI EN JOUANT ET VICE-VERSA, LES APPLICATIONS DE LA BLOCKCHAIN DANS L'INDUSTRIE VIDÉOLUDIQUE.....	11
10. LES NFTS, SOLUTIONS DE PROTECTION DES ACTIFS DÉFI ?.....	12
11. GAMIFICATION DE LA DÉFI / FINANCIARISATION DES NFTS.....	12

Séminaire Aristote : DéFi, la finance réinventée

Ce séminaire a eu lieu le 9 juin 2022, à l'école Polytechnique. La coordination scientifique a été réalisée par David Menga, ingénieur chercheur pour EDF R&D, et Vidal Chriqui, auteur sur le site Bitconseil.



David Menga et Vidal Chriqui.

Introduction par David Menga.

[Video ici](#)

Ce séminaire est le premier en présentiel post-pandémie. David Menga rappelle qu'Aristote a une mission de vulgarisation des connaissances autour des usages du numérique. Il rappelle qu'il y a trois ans, avait eu lieu un séminaire sur les métiers de la blockchain, et que ce séminaire en est la suite logique, orientée sur les conséquences de cette technologie sur les métiers de la finance : la finance décentralisée. Pour rappel, David Menga a donné un interview spécifique sur le pourquoi de ce séminaire accessible [ici](#).

Pour rappel, la définition de la finance décentralisée est : *"l'ensemble des outils de la finance traditionnelle mais appliquée sur la blockchain. La majorité sont des projets open source, qui utilisent les avantages d'opérer sur une blockchain publique, résistante à la censure pour améliorer les services financiers."* (Source, le Cryptopolitain.)

Même si l'écosystème s'est complexifié sur ces dernières années, notamment autour de la blockchain Ethereum.

David Menga en profite alors pour donner une définition plus précise, donnée par Pierre Person, ancien député qui a rédigé un rapport sur le sujet. *"L'ère crypto sera un changement de paradigme. La crypto en tant qu'outil technologique est un outil de libération de l'individu, face aux rentes des méga-corporations du numérique et des grandes banques. Au même titre qu'internet a réussi à démocratiser l'information, les cryptos génèrent un nouveau rapport à la valeur."*

Il rappelle tout de même que comme dans tout changement de paradigme, certains sont contre, comme Christine Lagarde, totalement opposée. Il cite aussi Jamie Dixon, DG de JP Morgan, qui estime que même si ce n'est pas terrible, comme les clients le veulent, il faut bien y aller un peu.

Il rappelle alors que c'est un univers turbulent, et qu'il y a eu de nombreuses "corrections" sur le marché, notamment dans les semaines qui ont précédé le séminaire, puis revient sur les différentes étapes d'évolution du web : Web1, Web2 et Web3.

1. La révolution de la DéFi

Philippe Herlin, Économiste et Essayiste, spécialiste de la monnaie.

[Video ici.](#)

Philippe Herlin a écrit *Repenser l'économie*

Le spécialiste commence par une présentation générale de la finance décentralisée et notamment un rapide historique. En citant Andreas Antonopoulos, entrepreneur technologique, qui estime que dans l'évolution de la finance, Bitcoin va gagner, car son aspect ouvert et transparent lui donne les meilleures armes, en redonnant de la liberté aux utilisateurs. Selon le spécialiste qui prend souvent la parole sur internet, le système bancaire actuel est corrompu, il ne peut qu'asservir les populations. Il n'est plus adapté. Même s'il est encore imparfait et moins perfectionné à l'heure actuelle. Dans la finance décentralisée, c'est la transparence de la blockchain qui au coeur de ses avantages. N'importe quel informaticien peut auditer le code. Il est ouvert à tous. Il est automatisable, par les smart contract. Il supprime aussi le principe de contrepartie : personne n'a à faire confiance, car le code fait office de certificateur. Enfin c'est son accessibilité, car elle n'a pas de barrière à l'entrée. Même les personnes non bancarisées peuvent facilement ouvrir un compte avec une seule connexion internet.

Mais sans tomber dans l'idéalisme, Philippe Herlin revient sur les risques notamment la faille de programmation et notamment le hack de plateforme ou de comptes. Même si un système d'assurance ou de sécurité s'est mis en place, et ce risque diminue.

Il fait ensuite le parallèle entre l'arrivée du web et la finance décentralisée, dans le sens de la démocratisation. Internet a facilité l'accès au contenu, comme la finance décentralisée facilite l'accès aux produits financiers.

Il revient ensuite sur différents principes applicatifs, comme les prêts, les échanges de portefeuille à portefeuille, sans passer par les plateformes, qui ne centralisent rien. Il détaille aussi les pool de liquidités, le yield farming, et les différentes méthodes de dépôts de liquidités qui peuvent générer de la valeur, ou encore les dérivées synthétiques (sur des cours comme l'or, les actions d'entreprises...) Il évoque alors les stablecoins, dont le principe est d'être adossées à une monnaie fiduciaire.

En faisant l'inventaire des fonds de cyptomonnaies déposées au sein des plateformes on peut suivre l'évolution du marché. On comptait l'équivalent de 600 millions de dollars d'actifs au début de 2020, de 15 milliards fin 2020, et de 50 milliards au premier trimestre 2022.

Il détaille ensuite le mécanisme du Wrapped Bitcoin, WBTC, qui permet de créer un bitcoin synthétique en bloquant le bitcoin original sur la plateforme.

Philippe Herlin revient ensuite sur les risques liées à la finance décentralisée : la sécurité, l'expérience utilisateur, encore restreinte à l'heure actuelle, notamment pour rendre plus accessible les produits financiers. Il y a aussi la structure des blockchains, comme les frais élevés sur Ethereum, Même si des blockchains de second niveau ont été mises en place permettant de limiter ses points faibles.

2. Automated Market Makers, état des connaissances

Julien Prat, chercheur CNRS, ainsi qu'à l'IP Paris

[Vidéo ici](#)

Julien Prat revient sur le mécanisme lié au Automated Market Makers (AMM), la forme la plus dominante de fonctionnement des marchés d'échanges décentralisés. De récentes études mathématiques ont permis de mieux comprendre leur comportement. Les échanges décentralisés ont lieu par smart contract, et l'échange n'a lieu que lorsque la transaction est effectuée. A aucun moment la plateforme ne voit transiter les actifs. Donc l'utilisateur ne cède pas la propriété de son actif tout le temps de l'échange. Il n'y a donc aucun risque de vol, et cette propriété est fondamentale pour le mécanisme. Chaque échange a lieu de manière atomique. Ainsi on ne peut pas instaurer de "carnet d'ordres" ce qui est une conséquence également du fonctionnement de la blockchain, du fait des coûts de transaction, et de sa structure technique. Ceci fait que la structure principale d'échanges est donc celle des AMM.

Seul souci, il reste difficile aujourd'hui de les concevoir de manière optimale. On ne connaît pas leurs propriétés fondamentales. Ainsi, on ne sait pas lequel choisir en fonction de l'objectif que l'on veut atteindre.

Pour mieux les cerner, une road map de recherche a été établie. Ils font d'abord s'accorder sur un langage pour décrire un AMM (design space), puis établir les modèles économiques qui les régissent, enfin, in fine, concevoir des AMM optimaux, en fonction des différents usages que l'on en attend.

A ce jour, la recherche a notamment avancé sur le Design Space, soit la première étape.

Le langage, pour les décrire se base sur la théorie microéconomique standard, celle qui sert notamment à décrire le comportement des consommateurs. A partir de là, il devient possible d'en dégager quelques propriétés. Julien Prat décrit alors les bases de fonctionnement des AMM, pour l'équilibre des prix par exemples, dans un pool de liquidités. Le but est d'en déduire ainsi des paramètres optimaux, de manière formelle.

Il s'avère que c'est en passant dans l'espace dual que tout devient beaucoup plus simple et plus intuitif, pour cerner leurs comportements. On passe par exemple de l'espace des réserves du pool de liquidités, à l'espace des prix, pour appliquer les fonctions. Par ce principe, on peut alors dégager

des descriptions élémentaires de fonctionnements des AMM et tenter de répondre à plusieurs questions de bases : modélisation d'évolution des prix, des pertes du providers, calculs d'optimum... Julien Prat réalise alors plusieurs démonstrations et explique certains comportements des AMM, ainsi que différents principes. Les chercheurs arrivent ainsi à dégager des propriétés fondamentales de ces objets mathématiques. L'important dans son propos est de retenir que c'est en passant dans l'espace dual que l'on arrive à ces modélisations, et que cette découverte ouvre tout un champ d'analyse des AMM pour la suite. On doit ces principaux travaux mathématiques à Guillermo Angeris, un mathématicien de Stanford, qui a depuis rejoint Bain Capital Crypto.

3. Le hardware wallet : un coffre-fort personnel pour la finance décentralisée

Jean-Baptiste Bédrune, VP Security Product chez Ledger

[Video ici](#)



Ledger est une licorne française spécialisée dans la réalisation de hardware pour la conservation des clés de sécurité des cryptoactifs. Jean-Baptiste Bédrune présente d'abord la société, ainsi que ses différents produits, et reprecise la différence entre les wallets "software" (logiciel) et les wallets "hardware". Il insiste sur le fait que les hardware wallets ne contiennent pas les cryptoactifs, mais bien seulement les clés qui permettent d'y accéder. Les cryptoactifs, eux, restent bien conservés dans la blockchain.

Le spécialiste présente alors en quoi consiste la sécurisation des software wallets, en détaillant les différents modes d'attaques. Cela peut être réalisé par des malwares. Mais il est possible d'en atténuer la vulnérabilité en isolant les différentes applications, en créant des enclaves de sécurité.

A l'heure actuelle, on ne dénombre pas encore d'attaques de grande ampleur, notamment auprès des particuliers, mais celles-ci pourraient augmenter, notamment avec la démocratisation des cryptoactifs, et le manque de sécurité de leurs outils (ordinateur,

smartphones...) La sécurité est donc une question fondamentale.

Il revient ensuite sur la sécurisation des hardware wallets. Celle-ci est importante, car la veille de la conférence, lors du salon Out the Chain, deux hardware wallets ont été hackés, pour la première fois dans le monde. Les hardware wallets n'ont que très peu d'interactions avec l'extérieur, lorsqu'ils se connectent. Il développe alors plusieurs points de vulnérabilité, sur la sécurisation des

processeurs, et détaille où et quand le code peut être open-sourcé ou non (ce qui reste dans l'esprit Blockchain, mais pour des raisons légales dans certaines parties sécurisés ne peut être open-sourcé). Il précise donc que Ledger minimise au maximum la partie de code non open-source.

Parmi les attaques, il présente notamment une attaque sophistiquée opérée directement sur le hardware en passant par de l'écoute électronique. Cela permet de récupérer les secrets détenus sur le wallet lorsqu'ils ont été perdus par exemple. Et détaille, comment lui-même, en laboratoire, tente d'attaquer des hardware. Le principe consiste à écouter la signature électronique lors de son fonctionnement. Cela revient à écouter un coffre-fort avec un stéthoscope.

Une autre attaque s'appelle l'attaque par faute, où le but est de pousser le système à la faute, en modifiant la fréquence de l'horloge du processeur.

Il décrit ainsi en image le hacking réalisé sur un hardware wallet de marque Coldcard Mk2, équipé d'un microchip ATECC508A. Il est possible de modifier le fonctionnement du processeur avec un laser infra rouge, après l'avoir photographié aux infrarouges. Il l'écoute aussi pour savoir quand tirer avec le laser, lors de la vérification du code Pin, puis en tapant sur des zones aléatoires du composants, il arrive à le pousser à la faute.

Au total, l'équipe a réussi à récupérer les secrets en moins de deux minutes.

Les fabricants s'attaquent entre eux, et se préviennent, afin qu'ils modifient le composant ensuite.

Même s'ils sont concurrents, le marché n'est pas assez mûr, et la sécurité a besoin d'un maximum de moyens à l'heure actuelle, donc les fabricants se serrent les coudes pour augmenter le niveau de défense.

4. La réglementation de la finance décentralisée.

Thomas Verbiest, avocat pour le cabinet Metalaw

[Vidéos ici](#)



Thomas Verbiest commence en précisant que le milieu de la finance décentralisée évolue encore en eaux troubles, et que le régulateur se penche de plus en plus sur ce sujet, ce qui - évidemment - fait des malheureux.

La première question est celle de la responsabilité. Les autorités cherchent à savoir qui pointer du doigt en cas de problème. Le régulateur ne peut entendre qu'il n'y ait pas de responsable, que des systèmes soient automatisés etc.

Thomas Verbiest revient sur l'exemple du début d'internet, en 1997, où lors de l'explosion du secteur, des utilisateurs diffusaient par exemple, de la pédophilie sur le réseau (affaires Compulsor et Prodigy), les régulateurs, faute de pouvoir s'attaquer aux auteurs directement se sont rabattus sur les fournisseurs d'hébergements, et les fournisseurs d'accès. Et il a fallu plusieurs années avant qu'un Safe Harbour se mettent en place, afin de protéger les fournisseurs de technologie ou prestataires techniques, et éviter qu'ils n'aillent en prison chaque fois qu'un délit était commis sur internet. Et Thomas Verbiest, dit qu'on en est exactement au même stade en finance décentralisée, et que les autorités s'attaquent directement aux mineurs de cryptomonnaies.

Il précise que tout est pseudonyme, et qu'il est toujours possible de retourner aux personnes physiques. Il détaille ensuite la question de la DAO, qui en droit, peut être considérée comme une association de fait, et détermine donc une responsabilité solidaire de tous les participants. Et dans le Wyoming, une nouvelle réglementation tente de pallier ce problème en créant une entité juridique supérieure, qui une fois qu'ils se sont identifiés, limite la responsabilité des membres. Il invite sur ce sujet à parcourir les travaux de l'association Coala (Coalition of Automated Legal Applications).

Il revient ensuite de manière critique sur les recommandations du Gafi, l'organisme mondial qui lutte contre le blanchiment d'argent, qui recommande aux autorités de déterminer un responsable afin qu'il s'enregistre auprès d'elles et qu'il se plie aux règles de lutte contre le blanchiment. Mais s'il n'y en a pas, il recommande aux autorités d'en imposer un, allant jusqu'à vouloir le déterminer comme "toute personne qui tire avantage de la plateforme". Ce qui, pour l'avocat, pose problème. Ce flou traduit, selon Thomas Verbiest, une peur des autorités de perdre le contrôle.

Il revient ensuite sur les nouvelles directives des l'AMF concernant le statut Psan, attribué par défauts aux plateformes qui exerce des activités de lending ou de stacking.

Il revient ensuite sur les deux conceptions différentes du droit de la crypto aux Etats-Unis et en Europe (notamment la France), où dans le premier cas, le but est de faire rentrer cette activité dans le cadre du droit financier, tandis que le droit européen tentera davantage de créer une législation adaptée.

5. Designs et enjeux des stablecoins centralisés et décentralisés

Veyrat, Angle Protocol

[Vidéo ici](#)

Précisons qu'Angle Protocol est la seule entreprise française à être financé par le fonds Andreessen Horowitz, qui a misé 4,5 milliards de dollars sur le Web3. L'objectif concret d'Angle est de créer un stablecoin en euros. Ils ont réussi à obtenir jusqu'à 250 millions de dollars suggestion, et 180 millions de stablecoin euros en circulation, ce qui fait d'Angle le plus gros stablecoin euros à l'heure actuelle. Pablo Veyrat revient à la définition et au fonctionnement d'un stablecoin, une cryptomonnaie adossée à actif et construite de manière à gagner en stabilité. On peut imaginer des stablecoins sur tout et n'importe quoi (comme la température.) L'avantage est que c'est in-censurable. Vous pouvez l'échanger sans passer par le standard Swift, et permet de reconstruire des standards financiers ouverts sur les standards financiers classiques.

Il différencie ensuite les stablecoins centralisés (un actif basé sur une monnaie fiduciaire) mais qui ne sont pas transparents, des stablecoins décentralisés : dont le fonctionnement est basé sur des smartcontracts. C'est à dire de prendre des cryptomonnaies et de tenter d'en faire quelque chose de stables ensuite en output. Prendre un bitcoin, et en faire quelque chose qui vaille un dollar, ou un euro en sortie. Le protocole doit être construit pour absorber la volatilité. Et c'est ici que réside le problème. Pour réussir à cela, il faut abandonner une des propriétés fondamentales : l'efficacité en capital. Or le but d'Angle justement, a été de reconstruire cette efficacité en capital.

Il revient alors sur le mécanisme d'échange à la base du marché des stablecoins et le rôle joué par l'actif collatéral (au coeur de l'échange) ainsi que les arbitrages indirects qui vont assurer la stabilité de la valeur du stablecoin. En clair : la volatilité va être fractionnée sur chaque utilisateur, car chaque utilisateur va absorber une part de la variabilité.

Il revient ainsi sur la chute du stablecoin Terra, prévisible selon lui, par la relation induite par le jeton collatéral émis (le Luna) qui créait une instabilité en cas de manque de confiance dans l'UST.

Angle a ainsi construit un jeton appelé Perpetual Futures, des produits à effet de levier, dont le but est de neutraliser la variation du prix Euros/Dollars dans le protocole. En prenant des positions long termes sur des actifs, cela donne une réserve pour combler les liquidités des positions court termes. Angle se définit ainsi comme une place de marché entre ceux qui désirent de la stabilité et ceux qui désirent de la volatilité.

La question qui reste : qui prend des produits à effet de levier ? Angle a ainsi défini une troisième couche de sécurité, des standards liquidity providers. Ces derniers vont prêter du collatéral en échange d'intérêts et de frais de transaction. Ils assurent les liquidités en collatéral. Angle se définit ainsi comme un marché à trois entrées pour répondre à différents besoins : ceux qui désirent des stablecoins, ceux qui désirent des produits à fort effet de levier en jouant sur la variabilité, ceux qui désirent du revenu.

6. La DéFi en pratique – Live démo sur le placement de ses 1000 premiers jEUR dans la DEFI

Vidal Chriqui, PDG de Verso

[Video ici](#)

Vidal Chriqui a pour but de présenter la dimension pratique de la conférence : comment investir ses premiers 1000 premiers jetons. Il est le créateur du Wallet Verso, qui permet de convertir ses actifs en carte cadeaux à dépenser dans des magasins, lié à un service de cashback.

Il indique qu'il faut absolument aller sur Twitter, principale source d'informations sur la finance décentralisée. Il rappelle qu'on est dans une phase, pour encore 18 mois, de sentiments négatifs. Mais la Defi n'est pas réservé qu'aux personnes qui veulent faire de l'argent, mais que c'est bien un univers qui cherche à réinventer les outils de la finance.

Vidal Chriqui va principalement présenter des outils, et effectuer en live la démonstration de ces outils et leurs différents fonctionnements. Ils commencent par un dashboard général pour comprendre le monde des cryptomonnaies : DefiLlama.com

Ce dernier permet par exemple de découvrir de nouveaux protocoles, et d'observer leurs évolutions. Il en profite pour redéfinir certaines notion (air drop, oracle, centralized exchange, bridge...)

Il revient ensuite sur Uniswap Protocol, plateforme d'échanges de cryptoactifs. L'interface permet d'échanger un actif contre d'autres, et matérialise la variation du prix en fonction du nombre de liquidités demandées. Il détaille les différents rôles au sein du pool de liquidités,

Troisième outil à être passé en revue : DefiBasket, développé au Brésil, qui permet de créer un portefeuille d'actifs, sans passer par une application tierce, avec beaucoup de paramètres associés pour le gérer. Vidal Chriqui rappelle qu'il n'a pas de compétences en gestion d'actifs, mais ne présente que les outils pour pouvoir gérer les siens. NFT, Metavers... le site permet de gérer différents types d'actifs.

Il prévient qu'il faut se méfier des fausses publicités sur Google avant de connecter son wallet à un service, et toujours bien vérifier le nom de domaine.

Il présente ainsi Beefy, Curve (pour les pools de liquidités) ou encore Coindix, qui permet de mieux visualiser cryptomonnaie par cryptomonnaie pour bien gérer ses actifs.

Vidal Chriqui rappelle d'avoir une vision long terme, que c'est un travail de longue haleine, que le secteur est encore en plein émoi, et qu'il faut explorer soi-même, pour bien saisir toutes les finesses des opportunités.

7. Options décentralisées : état des lieux, limites et potentiel

Omar Mehdi Roustoumi, MGH Protocol

[Vidéo ici](#)

Omar Mehdi Roustoumi, diplômé de l'X, estime qu'il n'y aura pas d'adoption massive de la finance décentralisée sans outils appropriés de gestion des risques, pour que le grand public puisse s'y confronter. Car il existe toujours beaucoup de limites aux différents outils existants à ce jour. La solution de MGH Protocol, qu'il a co-fondée, concerne essentiellement les options sur le marché. Il rappelle donc d'abord ce qu'est une option : la possibilité d'acheter dans le futur un actif à un prix garanti d'avance.

Il rappelle qu'en matière de finance, dans le monde, le marché des produits dérivés est 7 à 10 fois plus gros que le marché des actions et obligations. Et rien qu'aux US, les options sur actions représentent 35 fois le marché des actions. Donc, s'il y a des actifs dans le monde de la crypto, il n'y a aucune raison pour que le marché des produits dérivés ne se développe pas. Et le potentiel est énorme. Même si à l'heure actuelle, le rapport entre les deux n'est que de 2%. Nous ne sommes pour l'instant, qu'au tout début du marché des produits dérivés dans la finance décentralisée. Et tout reste à faire.

Le but de sa solution est de créer un système qui permet de s'assurer contre la chute des cours de cryptoactifs, en jouant sur différents paramètres.

Omar Mehdi Roustoumi présente ensuite les trois différentes catégories d'options qui existent à l'heure actuelle sur le marché. La première est surtout informatisée et fonctionne en se basant sur les variations de prix des actifs, tentant d'acheter selon leur évolution. En clair, il profite des imperfections des systèmes pour créer des options. La deuxième tente de répliquer le fonctionnement de la finance centralisée, avec un carnet d'ordres et tente de connecter un vendeur avec un acheteur. La troisième tente de créer des produits à part entière adaptés à la Défi. Ce sont les trois principaux systèmes d'options à ce jour.

Le spécialiste revient ensuite sur le fonctionnement des options dans un pool de liquidités : établir des options dès que le liquidity provider émet sa cryptomonnaie. Il pointe alors du doigt un

dysfonctionnement d'un pool de liquidités précis qui avait eu un grand succès via son mécanisme d'options, avec pourtant un total de liquidités qui ne faisaient que baisser au cours du temps. Comment est-ce possible que le projet ait tenu dans la durée ? Les providers étaient compensés par les tokens du protocole, mais qui malheureusement sont en quantité limitée. Ceci pose donc un problème de fonds quand ils arriveront à épuisement.

Le principe de base de la solution de MGH Protocol consiste à voir la volatilité comme une énergie, un flux et un mouvement. Puis de construire un système qui permet de transférer le risque du liquidity provider à d'autres entités, comme la DAO.

Le but consiste à récupérer les pertes dans le temps, en profitant de la volatilité des prix. Omar Mehdi Roustoumi présente alors les résultats d'un backtest effectué sur plusieurs mois en réalisant 10 calls par jour et 10 Puts par jour, et le protocole MGH apparaît alors comme plus performant que les autres solutions du marché. Mais il rappelle que le succès pour les liquidity providers ne proviennent pas des tokens collatéraux distribués lors du protocole, forcément en quantité limitée. Mais de la fructification des actifs entre le temps où l'option a été émise et où elle a été payée.

Mais le système a des failles en cas de baisse de volatilité, si le prix plancher n'est pas atteint de nouveau. Aussi, MGH a mis en place un système de Flight to Volatility, qui permet de transférer le risque (d'absence de liquidités) auprès des Stackers au bout de six mois, puis ensuite auprès de la DAO six mois plus tard.

Le but global, et ce qu'il faut retenir, c'est que le système joue surtout sur la volatilité. Mais beaucoup de questions restent à l'heure actuelle en suspens. Notamment s'il y a un trend (une évolution stable quasi linéaire) le modèle atteint quelques limites.

8. Démocratisation de la Défi dans la gestion de patrimoine

Gael Itier, AKT.io

[Vidéo ici](#)

AKT.io a été fondée en 2017 par le groupe Automata, une start-up française qui s'attaque au monde des banques par l'investissement et l'épargne. Gael Itier, son fondateur estime que les néobanques se sont focalisées sur les moyens de paiements. Lui et ses cofondateurs se sont dits qu'il fallait faire autrement, et se focaliser sur la génération de revenu et sur l'épargne. Ainsi AKT rentre sur le marché par la gestion de patrimoine plutôt que par le paiement, à l'inverse des entreprises comme N26 ou autres. La société s'est alors approchée de la finance décentralisée. Elle se base sur une approche et des outils de finance centralisée classique et de finance décentralisée. Le but étant d'aller chercher le meilleur des deux, tout en tentant d'en gommer le moins bon. Mais le juridique prend son importance. Et l'équipe estime que c'est à travers un travail avec les régulateurs, les auditeurs et les institutions financières qu'il sera possible de démocratiser la finance décentralisée en l'apportant avec quelque chose de vérifié et audité par des pros.

Ainsi, plutôt que de s'armer contre la régulation, AKT.io compose avec, et détient trois types de licences : celui des monnaies électroniques pour toutes les néo-banques, celui d'échange de cryptomonnaies, et celui d'asset management. Elle propose alors trois types de services pour le grand public : compte courant, compte d'épargne et compte d'investissements, tous accessibles depuis une application lancée en mars 2022. Le but étant de faire fructifier l'argent des clients, dans un portefeuille diversifié, avec des algorithmes précis, par assets, comme un acteur de l'asset management classique mais en se permettant d'aller chercher de la diversification sur d'autres actifs (modèle coeur-satellite). Au total, une centaine de cryptos sont prises en compte. Le tout fonctionne

sur une application qui a encore maints projets devant elle, pour que chacun puisse épargner sur la finance décentralisée en gérant son propre niveau de risque, comme un livret classique. Le produit sera composé de différentes offres, adaptées notamment aux formats familiaux, qui permettent de n'investir que les gains, par exemple.

Après avoir développé la partie régulation en Angleterre, la société a posé ses valises sur le campus de Sophia Antipolis pour la partie produit. Elle mise sur les synergies avec les autres acteurs.

9. La DéFi en jouant et vice-versa, les applications de la blockchain dans l'industrie vidéoludique

Vincent le Gallic, CTO Cometh

[Vidéo ici](#)

Cometh, fondée il y a un an, est composée de 20 personnes et réalise des jeux vidéos dans la blockchain. Le but est de démocratiser la Defi par les jeux vidéos. Car dans cet écosystème, il est courant qu'une économie accompagne le scénario, et permettent d'avoir accès à des services. Avec une monnaie, des biens digitaux etc. Si le jeu est impliquant, le geste de créer un wallet apparaît de manière plus naturelle pour le joueur, et se fait sans effort.

De nombreux business modèle existants dans les jeux vidéo, comme obtenir des ressources pour obtenir un items, ou le dessiner, le créer, peuvent être appliqués à des modèles de finance décentralisée, avec des tokens associés. On pourrait même imaginer des modèles de souscription, où les liquidités apportées feraient office de droit pour jouer, comme un abonnement, et l'utilisateur ne récupérerait qu'une partie de sa somme s'il partait avant une période de temps définie à l'avance. Ce qui permettrait de générer du yield.

Mais Cometh essaye vraiment d'intégrer de la finance décentralisée dans les jeux vidéos. Lors d'une partie, un joueur gagne des tokens, et il peut alors choisir de les revendre sur le marché, ou de leur donner de la valeur en continuant la partie. Idem pour certains items, qui correspondent à un apport de liquidités au départ. Il peut jouer avec ou la détruire au bout d'un certain temps, et récupérer ses liquidités. Entre temps, elles auront permis de générer des fees.

Le but consiste donc à dire que lorsque le joueur joue, il participe également à une économie en apportant de la liquidité au départ. Même si se pose aujourd'hui la question de la régulation totalement inexistante.

Il présente ensuite un exemple basé sur un jeu de carte à valeur et rareté différentes. L'avantage consiste dans la faculté à pouvoir vérifier la table de répartition de la valeur des cartes, quand, pour la Française des Jeux, par exemple, vous devez faire confiance. Un autre avantage consiste à créer les cartes en fonctions du succès du jeu, et de s'adapter à la quantité de joueurs, et non de devoir créer un stock de cartes existant en établissant leur valeur au départ, quitte à la modifier en inondant le marché.

Le principe de jeux organisés sur la Defi permet également de donner le contrôle, aux joueurs, des assets des items. Et ainsi pourquoi pas de créer une interopérabilité en différents jeux ? Une carte d'un item particuliers pourrait ainsi servir pour un autre jeu. Et ainsi une économie entre différentes plateformes de jeux peut se créer, par la seule initiative des joueurs.

Enfin, Vincent le Gallic donne quelques informations supplémentaires : le code est open source et audité.

10. Les NFTs, solutions de protection des actifs DéFi ?

Clément Tequi, fondateur de Terno

[Video ici](#)

Terno est une blockchain française layer 1 dédiée à la sécurisation des NFT. Son but est de donner une nouvelle valeur aux NFT. Elle fonctionne avec Capsule Corps Labs, principale développeur de Terno, fournisseur de technologie pour les grands comptes et les start-up qui voudraient participer à l'écosystème Terno. Elle crée le lien entre la blockchain et l'univers applicatif construit dessus.

Il présente ensuite les principales fonctions d'un NFT : une utilité (son rôle dans un jeu, pour un concert), un aspect social (exhibition), un sentiment d'appartenance (obtenir des privilèges), le côté financier, et l'authenticité garantie par la transparence de son historique.

Ils opèrent dans différents domaines : Entertainment, video games, sport, santé, immobilier. Le NFT devient le coeur des prochaines interactions digitales.

Le NFT constitue un actif car il contient de la data, donc étant propriétaire du NFT, le détenant est par voie de conséquence aussi propriétaire de la data contenu. D'où la nécessité de la sécuriser. Il existe pour cela diverses solutions : les wallet digitaux, les wallet hardware, les coffre-forts numériques, mais il manque à ce jour les coffre-forts basé dans la blockchain. C'est ce que fait Terno, dans un projet développé avec les notaires, dans un espace ultra-sécurisé.

Depuis l'avènement du digital, on croule sous les actifs numériques. Le but est de se dire qu'avec la blockchain, on pourra garder sur le long-terme des données digitales à transmettre.

Ce sont les notaires qui distribuent la solution lors de cas de transmission d'actifs numériques, comme des mots de passe, ou de clés de crypto wallet. Le but est donc de favoriser et sécuriser la transmission du patrimoine digital à ses enfants ou ses proches. L'interface est assez simple, selon un clic&drop, puis le tout est conservé de manière décentralisée. Les notaires font office d'oracle pour valider l'événement lors de la transmission. Plusieurs use case sont évoquées : le monde de l'édition, de l'industrie musicale, des jeux vidéos...

11. Gamification de la DéFi / Financiarisation des NFTs

TokenBrice, influenceur et producteur de contenu sur les NFT

[Video ici](#)

Brice revient sur les bases des NFT et l'historique de ses principales propriétés.

- la fongibilité : sur les 80 dernières années, tout devenait fongible (échangeable, standards...) nous sommes en plein coeur du mouvement de balancier inverse.
- la notion d'historicité : tout le passé d'un NFT est transparent et accessible à tous.
- sa composabilité: qui lui permet d'être intégré de manière générale dans un grand nombre de plateforme via un seul standard unique.

De la même manière que l'apparition de la 3D a permis de créer de nouveaux types de jeux qui n'était pas faisable en 2D, les NFT vont ouvrir des portes qu'on ne peut pas encore imaginer à l'heure actuelle, sans se limiter à des évolutions de choses existantes, donc.

Brice revient ensuite sur les enjeux des NFT avec la Defi, comment les deux notions s'imbriquent.

Un des principaux problèmes à l'heure actuelle concernant les NFT concernent la liquidité : il faut un acheteur en face, au risque de la vendre à un prix non optimal, contrairement à d'autres actifs décentralisés dont le fonctionnement de marché est régi par les AMM.

On peut donc, grâce à une approche issue de la Defi, obtenir une meilleure liquidité des NFT. Par exemple, il est possible de créer de nouveaux smart contract basés sur les NFT de départ, et donc de créer de nouveaux token issus des premiers. Cela permet par exemple d'acheter une portion de NFT correspondant au NFT de départ, et donc de s'exposer à la variation du cours du NFT de départ, sans avoir à investir la totalité de la somme pour entrer dans le jeu.

On peut aller jusqu'à créer de l'emprunt autour de son NFT. De nombreux produits dérivés peuvent ainsi être construit sur la base du NFT correspondant. De la même manière, il est possible de collectiviser le NFT en fractionnant le token de départ en multiples token, gérés collectivement, qui peuvent à tout moment, être reprivatisés dans le token de départ quand toute la communauté est d'accord.

Idem, cette logique peut être appliquée à plusieurs éléments d'une collection, pour recréer une sous collection sur le marché. 100 NFT sont mis ensemble pour recréer de nouveaux token, fractions des 100 NFT de départ.

Brice présente alors un autres système, Alpha, qui permet de louer son NFT. Un outil particulièrement utile lorsque l'on veut tester un jeu accessible via un NFT sans réaliser totalement l'acte d'achat.

A l'inverse, Brice donne aussi des exemples d'initiatives de la finance décentralisée qui utilise des NFT pour représenter des positions sur le marché. Uniswap, dans sa version 3, a ainsi mis en place un NFT pour représenter différentes positions sur la courbe de prix en un seul endroit. Comme un indice mais qui a une valeur intrinsèque car il représente une réelle position d'actifs sur le marché. Le NFT contient donc des actifs.

Idem, ENS.domaine permet de créer NFT associé à un nom de domaine sur la blockchain. Très utile pour simplifier la transmission de token.

On trouve aussi FloorDAo qui permet une gestion collective du NFT pour en améliorer la valeur qui ajoute de la liquidité dans l'écosystème.

Enfin, il revient sur le Play2earn, qui permet de créer un jeu, où les éléments sont des NFT, et chaque joueur peut gagner des Tokens.

D'autres systèmes tentent de faire le lien entre le réel et la finance décentralisée : par exemple Stepn, permettait de donner de la valeur à ses actifs en bougeant dans la vraie vie. Plus vous faisiez de l'effort, plus votre token prenait de la valeur. Il présente ensuite un projet plus personnel : luchadores.io, un jeu tour-par-tour, dont les stratégies se définissent avant les matchs automatisés, qui permettra également de gagner en valeur en fonction des résultats. Entièrement hébergée sur Ethereum et Polygon, ce qui en limite les graphismes.