La finance décentralisée (DeFi) : Quelle est cette approche alternative aux services financiers?

Mémoire de Master 1 Economie Appliquée

Gabriel Edde
gabriel.edde2@etu.univ-lorraine.fr
Université de Lorraine, UFR DEA

Professeur référant :
Patrick Kouontchou
Patrick.kouontchou@univ-lorraine.fr
Université de Lorraine, UFR DEA

Introduction :

La finance décentralisée est l'ensemble des services financiers qui sont pourvus en passant par une blockchain au lieu d'une institution financière traditionnelle. Le problème fondamental qu'essaie de résoudre la DeFi est : comment assurer des services financiers (transfert de liquidité dans le temps, dans l'espace, et entre les personnes en besoin ou en capacité de financement) entre des acteurs économiques qui ne se font pas confiance (ménages, entreprises, intermédiaires financiers), et sans faire confiance en une institution centrale (banque centrale, gouvernement) ? Pour cela, la DeFi utilise une infrastructure et une fondation technologique différente, basée sur les innovations que sont la blockchain et les smarts contracts. Ces différences peuvent lui donner des avantages vis-à-vis de la finance traditionnelle mais il reste de nombreux obstacles à l'adoption de masse. La question est alors de savoir comment fonctionne la DeFi, à quoi ressemble le secteur et ce que l'avenir lui réserve.

Partie 1 : Les fondations technologiques de la DeFi

I/ Point de départ : la blockchain et la cryptomonnaie

On considère le manque de confiance comme le point de départ de la logique, et on veut y remédier mathématiquement, informatiquement, économiquement. Il semblerait que c'était la motivation principale derrière la conception de la blockchain par le pseudonyme Satoshi Nakamoto qui, à la suite de la crise de 2008, a laissé des indices qu'il ne faisait plus confiance aux intermédiaires financiers ou au gouvernement pour la gestion de la monnaie. Il a publié le 28 octobre 2008 son white paper "Bitcoin : a peer-to-peer electronic cash system"[1] qui explique le fonctionnement de Bitcoin et de la blockchain pour la première fois, marquant donc la genèse de cette potentielle « grappe d'innovation » (pour reprendre la formule de Schumpeter).

1. Public Ledger

Admettons un registre ou un compte, publiquement accessible, et modifiable par ses utilisateurs pour qu'ils y notent des transactions dans une monnaie arbitraire propre au registre. On imagine pour le moment que les acteurs du registre commencent avec une quantité donnée de monnaie sur le registre et qu'un individu ne peut effectuer une transaction que s'il a la quantité requise, ce qui est vérifié en regardant l'historique des transactions. Ainsi, la monnaie arbitraire existe uniquement au sein de ce registre et n'a de valeur que pour effectuer des transactions entre les acteurs.
Le problème qui émerge alors est l'absence de vérification : un acteur économique malintentionné peut arbitrairement dire qu'un autre lui doit de la monnaie.

2. Signatures digitales

En réponse à cela, on peut utiliser une signature digitale, une innovation qui nous provient du domaine de la cryptographie.
Chaque acteur sur le registre a une clé publique et une clé privée (ou secrète). La combinaison de la clé privée et du message à ajouter au registre (l'enregistrement de la transaction) produit une signature digitale unique à cette transaction sous la forme d'une suite binaire (de 1 et 0). La clé publique est utilisée avec le message de transaction pour que tout le monde puisse vérifier la validité de la signature.

[1] https://bitcoin.org/bitcoin.pdf

Désormais, un acteur ne peut arbitrairement déclarer une transaction dont il est le bénéficiaire sans la clé secrète du débiteur. Néanmoins, un problème persiste : la signature ne change pas si la transaction est la même, un acteur malintentionné peut donc copier une transaction avec la signature associée. La solution ici est assez simple, on peut simplement rajouter un identifiant unique à chaque transaction au moment de la signer.

3. Registre distribué

Jusqu'ici on imaginait un registre central, donc unique, que tout le monde peut modifier mais cela nécessite de faire confiance en un lieu ou une entité centrale pour l'héberger.
Admettons désormais un registre distribué, ou registre partagé (« distributed ledger » dans son anglais d'origine). Les acteurs possèdent chacun une copie du registre et se communiquent entre eux leurs transactions pour qu'ils mettent à jour leur copie.
Néanmoins un individu malintentionné peut transmettre aux autres un registre dont l'historique des transactions est modifié afin de le favoriser pour qu'il puisse dépenser la même monnaie plusieurs fois d'où le nom « double spend » ou double dépense. Le problème est alors de savoir à quelle version/copie du registre on peut se fier.

4. Proof Of Work (POW)

La réponse est le proof-of-work ou la preuve de travail computationnel.
Pour comprendre comment cela fonctionne, il faut parler des fonctions hash cryptographiques. Une telle fonction prend pour input n'importe quel texte et produit une suite binaire, appelée ''Hash'', qui semble aléatoire mais ne change pas lorsque l'input reste le même, bien que le moindre changement à l'input modifie le Hash de façon imprévisible. Si on veut trouver l'input qui produit un hash spécifique il n'y a donc pas de meilleure stratégie que de tester des inputs au hasard.
Ainsi, si on a un message, on peut y rajouter une suite de chiffres tels que son hash commence par un nombre 'n' de 0 à la suite. Ensuite il est facile de vérifier si cette suite de chiffres produit bel et bien un hash avec n 0 lorsqu'elle est ajoutée au message. Cette suite de chiffre est la preuve qu'un certain travail computationnel a été effectué, d'où le nom Proof of Work.

La blockchain de Bitcoin utilise SHA256, cette fonction hash cryptographique produit un Hash de 256 bits, elle est utilisée pour le chiffrement d'informations par de nombreux services de par le monde dont les plus grandes plateformes d'internet.

5. La Blockchain

Pour créer une blockchain, on part d'un registre distribué sur lequel on échange une monnaie spécifique au registre. On requiert une signature digitale pour chaque transaction afin d'assurer qu'un agent ne peut prendre la monnaie d'un autre sans sa vérification. On divise le registre distribué en plusieurs parties, ou blocks, qui chacune contiennent un certain nombre de transactions et finissent par une Proof-of-work. Chaque block a pour en-tête le hash du block précédent, de cette manière si l'on veut changer un block passé ou échanger la position de deux blocks il faut refaire la proof-of-work pour tous les blocks qui suivent. Ceci permet donc d'assurer l'ordre des blocks. Ce qui en résulte est donc une chaine de blocks ou Blockchain.

Avec ce système on peut permettre à tout le monde de rejoindre le registre, désormais appelé Blockchain, d'écouter des transactions, les arranger en block, produire une preuve de travail et transmettre le block nouvellement validé aux autres. Pour récompenser ces créateurs de block, on les autorise à rajouter, au block qu'ils ont validé, une transaction spéciale qui leur procure une quantité donnée de la monnaie du registre, augmentant la masse monétaire de la blockchain pour chaque block qui est validé. On appelle cela le minage. Dans le cas de bitcoin, cette récompense est divisée par deux pour tous les 210 000 blocks qui sont minés (soit tous les 4 ans environ) et parce que cette baisse est géométrique, il n'y aura jamais plus de 21 000 000 de Bitcoins au monde.

En tant que personne qui ne veut pas miner de block et qui veut simplement effectuer des transactions, il suffit d'écouter les blocks transmis par les mineurs (ou validateurs de block) et mettre à jour sa propre copie de la blockchain. Si on reçoit deux versions de la blockchain avec des historiques conflictuels, on se réfère à celle la plus longue et qui a donc le plus de travail computationnel. Si les deux font la même taille alors on attend que de nouveaux blocks arrivent.

De cette manière, un acteur malintentionné ne peut faire passer sa copie de la blockchain pour la vraie version que s'il arrive à produire plus de travail computationnel que le reste du réseau (majorité absolue ~50% du travail). En faisant confiance à la chaine la plus longue, on arrive à un consensus sans faire confiance à une entité centrale.

C'est cela, en réalité, la véritable innovation de Satoshi Nakamoto qu'il présente dans le white paper de bitcoin: un protocole de consensus en passant par la proof-of-work.

6. Remarques

Quelqu'un qui veut effectuer une transaction peut y rajouter un frais de transaction pour inciter les mineurs à inclure la transaction dans le prochain block.

Dans le cas de Bitcoin, chaque block ne contient que 2400 transactions, et le travail requis pour la preuve de travail (le nombre de 0 à la suite à trouver dans le hash) varie de tel qu'un nouveau block ne soit miné que toutes les 10 minutes (s'il y a plus de mineurs sur le réseau, le minage devient donc plus difficile).

Parce que la majorité contrôle la blockchain, elle a une structure presque démocratique et des modifications à sont fonctionnement peuvent être fait du moment que la majorité applique le changement, comme cela a été le cas par le passé avec Bitcoin pour résoudre des bugs. Certains groupes ont aussi appliqués des changements plus importants au protocole de bitcoin mais, parce qu'ils étaient minoritaires, cette blockchain n'est pas considérée comme la ''vraie'' et devient le début d'une nouvelle cryptomonnaie. On appelle cela une « hard-fork » et c'est le processus qui a donné naissance à Bitcoin Cash, Bitcoin Gold et Ethereum Classic entre autres.

II/ L'utilité : des smart contracts à web3

1. Les smarts contracts

Une application web normale fonctionne en deux parties : le client et le serveur. Le client est l'appareil de l'utilisateur individuel de l'application et le serveur est l'appareil ou sont stockées les informations nécessaires pour faire tourner l'application. Lorsqu'on ouvre une webapp, dans google chrome par exemple, google va passer par la connexion internet pour demander au serveur les informations pour faire tourner l'application dans le moteur de recherche de l'utilisateur. Lorsque ces applications permettent aux utilisateurs d'interagir entre eux, le serveur doit récupérer des données sur les utilisateurs (que ça soit un réseau social ou un jeu web multijoueur). Même si le serveur n'est pas centralisé géographiquement, son contrôle est centralisé autour d'une entité qui est propriétaire du code, peut le modifier, récupérer les données qu'elle veut et changer les états internes du code.

Dans le cadre de la blockchain de bitcoin, seules des transactions sont écrites dans la blockchain alors qu'on pourrait théoriquement y écrire ce qu'on veut. On pourrait, par exemple, créer une blockchain dans laquelle on peut écrire du code dans la blockchain qui pourra être exécuté par le

réseau selon certaines conditions, et dont l'exécution est surveillée par les validateurs du réseau. On peut ainsi créer une application stockée dans la blockchain, donc décentralisée, qui agit de manière transparente et sécurisée. Dans ce cadre, la blockchain remplace le serveur web et décentralise le fonctionnement de l'application. C'est cette idée que Vitalik Buterin a mis en pratique lorsqu'il a créé Ethereum, menant au développement des dApps ou « decentralized applications ».

2. Ethereum & Cardano

Ethereum[2] est sortie en 2016, créée par Vitalik Buterin et Charles Hoskinson en autres. Cette plateforme est une blockchain qui permet d'exécuter des smarts contrats et donc de faire fonctionner des applications sur internet où le serveur web est remplacé par la blockchain. Pour que le réseau compute l'application il faut payer des frais (appelés « gas fees ») en Ether, qui est la cryptomonnaie de la blockchain Ethereum. Les développeurs d'application créent le même code client qu'avant et adaptent le code serveur pour qu'il fonctionne sur la blockchain. Cette nouvelle infrastructure web, et l'apparition d'autres blockchains comme Ethereum, telles que Cardano et Eos, ont mené au développement de ce qu'on appelle aujourd'hui web3.

Ethereum est actuellement en train de passer d'un protocole Proof-of-work à Proof-of-stake (ce processus franchira l'importante étape du ''merge'' en août 2022). Ce protocole de consensus alternatif consomme beaucoup moins d'énergie que le proof-of-work, la barrière à l'entrée pour valider des locks est plus basse et les possibles soucis de sécurité supplémentaires sont compensés par la taille importante du réseau Ethereum.

Cardano[3], un concurrent à Ethereum, a été créé en 2017 par Charles Hoskinson après qu'il ait quitté l'équipe d'Ethereum. Il utilise déjà un protocole proof-of-stake et a des frais de transactions beaucoup plus faibles mais a toujours du mal à dépasser son prédécesseur.

3. Web3

Afin de comprendre ce qu'est web3 il faut d'abord comprendre ce qu'on veut dire par web1 et web2. Web1 était la première forme d'internet dans les années 80 et début 90. Internet était alors nouveau et n'avait pas beaucoup de fonctionnalités, les pages internet étaient statiques et la seule interaction possible était de cliquer sur un hyperlien, ainsi cela servait surtout à des individus et

[2] https://ethereum.org/
[3] https://cardano.org/

des communautés de s'exprimer. Ce sont ces communautés qui géraient web1, qui était donc marqué par une forte indépendance et décentralisation.

Web2 est arrivé lorsque les moteurs de recherche sont devenus compatibles avec Adobe Flash et avec le langage de programmation JavaScript qui ont permis aux développeurs de rajouter des fonctionnalités dans leurs sites, créant les premières WebApps. C'est alors que sont apparus les géants actuels du web comme Amazon (1995), Google (1998) et Facebook (2004). En permettant aux utilisateurs d'internet d'interagir plus profondément avec les sites, ceux-ci ont pu récolter des informations sur eux pour s'en servir. Les effets de réseaux sont devenus beaucoup plus forts, c'est-à-dire que plus une application a d'utilisateurs, le mieux elle devient et donc le plus d'utilisateurs elle attire, créant un cercle vertueux et menant à des situations de « winner-takes-all ». C'est pourquoi web2 est marquée par une forte centralisation autour de grandes multinationales qui jouissent d'un quasi-monopole dans leurs « jardins fermés ». Web2 a donc sacrifié la décentralisation et l'esprit de communauté de web1 pour davantage de fonctionnalité et d'utilité.

Le but de web3 est de regrouper la décentralisation de web1, afin qu'internet appartienne aux utilisateurs, avec la fonctionnalité de web2. Pour cela, web3 est construit sur des blockchains - comme Ethereum et Cardano – qui font tourner les applications dans des smarts contracts. Pour fonctionner, une WebApp a besoin d'un frontend (client side) qui tourne sur l'appareil de l'utilisateur, et d'un backend (ou server side) qui tourne sur des serveurs et distribue des informations aux différents ''clients''. Les blockchains remplacent ici les serveurs (au moins pour certains aspects) et, de fait, la partie contrôlée par les multinationales. Aujourd'hui dans web2, la plupart des pages et services internet sont hébergés par un oligopole : AWS 33% du marché cloud, Microsoft Azure 21%, google cloud 10%, etc, tandis que les organisations qui le peuvent hébergent leurs services sur leurs propres serveurs.

Partie 2 : L'état actuel de la DeFi : Services et écosystème

1. Tokens

Grâce à des plateformes comme Ethereum, on peut créer un actif digital sans devoir créer sa propre blockchain. En effet, on peut utiliser la blockchain d'Ethereum pour y faire fonctionner ses propres actifs décentralisés basés sur un smart contract de type ERC20. Ces actifs appelés Tokens peuvent avoir plusieurs utilisations.

Il y a d'abord les **Security tokens** qui représentent une propriété sur un autre actif. On peut rattacher la valeur d'un token sur l'or pour pouvoir détenir de l'or mais avec la sécurité d'une blockchain au lieu de le garder chez soi ou dans un coffre-fort. Pour que cela fonctionne il faut généralement que les tokens soient garantis par l'actif qu'ils émulent. Les **Equity Tokens** rentrent dans cette catégorie, ils représentent un droit de propriété sur une part d'un projet ou d'une entreprise mais l'information contractuelle est écrite dans la blockchain au lieu d'un certificat de part.

Les **Utility Tokens**, eux, permettent d'accéder à des services sur les plateformes digitales qui les offrent, ce qui leur procure une réelle valeur. Par exemple, le token FIL permet d'utiliser le service Filecoin[4], un réseau de stockage décentralisé qui utilise la blockchain pour enregistrer de l'information de manière sécurisée.
Une startup, ou un projet, peut passer par la blockchain pour émettre des tokens qu'elle vend pour lever des fonds, cette opération s'appelle « Initial Coin Offering » ou **ICO** et représente une source de financement alternative qui n'est pas soumise aux même régulations qu'une IPO. C'est une bonne façon de lancer un projet et de mettre sur le marché un Utility Token, mais le manque de régulation a mené à des abus tels que des « pump and dump » et des « rugs pulls ». En 2017 en particulier, beaucoup de tokens étaient lancé à partir d'une simple idée et de grandes promesses, sans projet réel à l'appui, mais beaucoup de personnes ont investi néanmoins. Cela a poussé à la hausse le prix des tokens, permettant aux émetteurs des actifs de revendre leurs importantes réserves et de faire fortune sans jamais apporter de produit ou service concret.

Les **Governance Tokens** représentent un droit de vote pour une utilisation spécifique ou, plus généralement, dans un corps décisionnel comme une DAO (ou « Decentralized Autonomous Organization »). Une DAO est une organisation dont le fonctionnement, la gestion et la maintenance sont opérés par des smarts contracts sur une blockchain. Le code dans les smarts

[4] https://filecoin.io

contracts est open source et peut être modifié à la suite d'un vote par les détenteurs de token, où 1 token vaut 1 vote. Beaucoup de projets en crypto sont gérés ainsi ou ont vocation à l'être.

Les Transactional Tokens sont utilisés pour effectuer des transactions rapidement, facilement et avec frais de transaction très faible, comme xDai qui est une également une stablecoin (cf. prochaine page) avec une valeur bloquée sur le dollar et des frais de transaction de 0,000021 USD.

Les Non-Fungible Tokens ou NFT représentent un droit de propriété unique qui est inscrit dans la blockchain. Ils servent à authentifier qu'une adresse (un individu) est le propriétaire d'un bien, physique ou digitale, présent ou non sur la blockchain. NFT signifie « token non-fongible », faisant référence au concept économique de la 'fongibilité' où, selon Larousse, un bien fongible peut être remplacé par à un autre de même nature, même quantité et même qualité.[5]
Les NFTs ont récemment été très utilisé, et ont eu beaucoup de succès, dans la vente d'art digitale : des artistes comme Beeple et Pak ont vendu des œuvres pour 69,3m$ et 91,8m$ respectivement (en équivalent ether, les enchères ayant lieu sur la blockchain ethereum). A cause de cela, les NFTs ont acquis une réputation d'actifs dans une bulle spéculative, néanmoins leur utilité potentiel est réelle et ils pourraient un jour remplacer les notaires et avoir la même valeur légale qu'un certificat d'authenticité.

2. Les stablecoins

Il existe une catégorie de tokens et cryptomonnaies appelées « stablecoins » qui se caractérisent par la stabilité de leur valeur. Ces actifs se différencient entre eux par la façon dont ils maintiennent leur prix stable (souvent autour de 1 Dollar US). D'abord il y a des stablecoins garanties qui sont adossées à une monnaie fiduciaire, une autre cryptomonnaie ou un autre actif boursier (des commodités généralement). Les principales cryptomonnaies stables se basent sur ce système, comme USDC, Tether et BinanceUSD qui sont appuyées sur un stock de Dollar US.

Il y a aussi des stablecoins non-adossées, dites « de seigneuriage » ou encore « stablecoins algorithmiques » dont la valeur est contrôlée en modulant la masse monétaire algorithmiquement, à la manière d'une banque centrale. Cette forme de stablecoin est très critiquée car leur valeur n'est pas réellement garantie par un collatéral. En mai 2022, une importante stablecoin algorithmique appelée UST et créée par Do Kwon a perdu sa stabilité autour de 1 USD et son prix est tombé à 10 centimes USD, remettant encore en question la viabilité de ce système.

[5] https://www.larousse.fr/dictionnaires/francais/fongible

3. Les Exchanges & DEX

Afin d'échanger des actifs décentralisés entre eux et pour effectuer des transactions, on passe par des plateformes d'échange. Beaucoup des plus utilisées dans le monde de la crypto sont des plateformes centralisées, telles que Binance[6], Coinbase, BitStamp et Kraken. Ces plateformes sont tout de même très intégrées à l'écosystème de la cryptomonnaie et de la DeFi.

Les Decentralized Exchanges ou DEXs sont des plateformes servant de marché qui permettent l'échange non-custodial d'actifs digitaux sur la blockchain et où les échanges sont donc publiquement vérifiables. Ils n'étaient à l'origine compatibles qu'avec les actifs natifs de la blockchain, mais des solutions d'interopérabilité entre les chaines ont été développées. Il existe plusieurs types de DEXs, comme les order book DEX, mais la plupart d'entre eux aujourd'hui sont des « automated market makers » (AMM) qui remplissent des commandes algorithmiquement. Au lieu d'employer des order book pour déterminer les prix, ce qui est inefficient sur une chaîne, les AMM créent des « liquidity pool » auxquels tout le monde peut contribuer, être un market maker et être récompensé en fonction de sa contribution au pool. Pour échanger une paire d'actifs, des réserves pour les deux actifs sont bloqués dans un smart contract, de la liquidité est ajoutée à la réserve d'un actif et retirée à celle de l'autre actif. Un frais de trading est conservé par une des pools de liquidité et réparti entre les procureurs de liquidité selon le nombre de token de liquidité qu'ils ont (proportionnel à leur contribution à la liquidité). Participer à une pool de liquidité s'appelle faire du « staking ».
Les plus grands DEXs aujourd'hui sont Uniswap[7], PancakeSwap, Curve et dYdX, ils ont chacun leur propre token qui est utilisé pour effectuer des transactions et des échanges sur de nombreuses paires d'actifs.

La liquidité est très importante car elle permet de réduire la volatilité du prix des actifs et empêche des acteurs importants (appelés « Whales » ou Baleines) de manipuler le marché avec des sommes conséquentes. Il y a donc souvent des incitations supplémentaires pour encourager les détenteurs d'actifs à contribuer de la liquidité, on appelle ces incitations « farming » ou « liquidity mining », et elles consistent en l'attribution de tokens supplémentaires créés pour les récompenser. 'Minter' de nouveaux tokens a cependant un effet inflationnaire. Pour y remédier, certains nouveaux protocoles comme OlympusDAO[8] sont propriétaires de leur propre liquidité ou la rachète à ceux qui 'stake' leurs tokens grâce à une importante trésorerie qui sert de collatéral. Ainsi, ils n'ont pas besoin de générer de la masse monétaire pour encourager d'autres acteurs à contribuer à la liquidité.

[6] https://www.binance.com
[7] https://uniswap.org/
[8] https://www.olympusdao.finance/

4. Les dettes et créances

Des plateformes de prêt en cryptomonnaie se sont développés pour amener les services financiers traditionnels au monde de la crypto comme Aave[9] et Compound[10]. Or ces plateformes sont souvent créées de manière décentralisée dans l'esprit de ce secteur et fonctionne généralement en pair à pair. Elles fonctionnent à partir d'un protocole qui met en lien des débiteurs et des créanciers directement, ou met en commun des dépôts dans un smart contract servant de fonds qui peuvent être empruntés au taux d'intérêt du marché dont la méthode de calcul est définie par le protocole. Il y a généralement deux types de prêts : les over-collateralized debt et les flashs loans. Les overcollateralized debt sont des emprunts où le débiteur doit présenter un collatéral d'une valeur supérieure à l'emprunt, qui pourra être racheté à un prix réduit par un autre membre de la chaine (appelé keeper) en cas de non-remboursement de la dette. Les flash loans, eux, ne nécessitent pas de collatéral mais doivent être remboursé dans le même block qu'ils ont été empruntés, sinon le prêt lui-même est annulé. Cela est réalisé par un smart contract qui vérifie d'abord si l'opération financière permettra de rembourser les emprunteurs à temps. Les flash loans sont plutôt utilisés pour de l'arbitrage dans des DEXs mais ont aussi été abusés pour attaquer des plateformes ou manipuler des marchés.

5. L'assurance et les Oracles

Le fonctionnement des smart contracts fait qu'ils sont particulièrement aptes à codifier des contrats d'assurance. Ainsi, les termes du contrat d'assurance sont inscrits dans la blockchain, donc transparents, et si un événement se produit, une somme en cryptomonnaie sera envoyée à une adresse spécifiée.

Certaines applications basées sur des smarts contracts, et donc sur la blockchain, peuvent nécessiter l'utilisation de données en dehors de la blockchain comme pour la vérification d'un contrat d'assurance. Pour faire cela de manière sécurisée, sans qu'un acteur de la blockchain puisse manipuler les données entre leur source et leur utilisation, on peut utiliser un Oracle. Les Oracles, comme Chainlink[11], permettent à des applications sur d'autres blockchains d'obtenir des données provenant de sources spécifiées qui sont récupérées par la blockchain oracle et transmises de manière sécurisée.

[9] https://aave.com/
[10] https://compound.finance/
[11] https://chain.link/

6. Les dérivés

Naturellement, des produits dérivés se sont aussi développés dans la cryptomonnaie même si c'est actuellement surtout en utilisation sur des plateformes centralisée, les plateformes de finance décentralisée étant encore limitée technologiquement et par la nouveauté du secteur.

Certaines plateformes DeFi proposent des Options Call et Put mais elles nécessitent d'être garanties par un collatéral et la plupart des plateformes utilisant un AMM ont du mal à leur donner un prix car elles ne prennent pas en compte une dimension temporelle de l'actif, pourtant nécessaire avec des options.

Les contrats futures existent mais sont peu utilisés à cause de la volatilité des actifs sous-jacents. Les Futures Perpétuels (ou Swaps Perpétuels) sont similaires mais n'ont pas de date d'expiration et ont été développés pour les marchés crypto. Ils sont couverts par un collatéral et la position doit être refinancée sous risque de liquidation pour protéger le contracteur. A cause du manque de dimension temporelle, le prix de ces dérivés est proche ou le même que celui du sous-jacent donc ils sont surtout utilisés pour échanger son collatéral avec un autre actif.

On peut aussi utiliser des tokens pour créer des actifs synthétiques, comme les Security Tokens, qui émulent sur la blockchain des actifs extérieur à la blockchain.

Partie 3 : L'avenir de la DeFi : Potentiel et Obstacles

I/ Un potentiel transformateur

La finance décentralisée est construite sur une infrastructure et des principes fondamentaux différents de la finance traditionnelle (i.e. centralisée), et les innovations qui y ont mené lui procurent des caractéristiques pouvant l'avantager.

1. Transparence

Parce qu'elle est basée sur des smarts contracts inscrits dans la blockchain, la finance décentralisée se démarque par sa transparence. Les transactions sont enregistrées et visibles publiquement pour ceux qui inspectent l'historique du registre et toutes les données financières on-chain peuvent être facilement récupérées.

De plus, le code dans les smarts contracts est également visible dans la blockchain, permettant à chacun de savoir comment fonctionne un protocole (si l'on comprend son code source), d'y identifier des bugs ou de potentiels problèmes et de pouvoir s'engager dans différents protocoles en pleine connaissance (ils s'exécutent de manière déterministe). Cela rend les plateformes décentralisées *de facto* open-source (en logiciel libre), ce qui permet à leurs communautés d'utilisateurs de participer à leur amélioration et de trouver des vulnérabilités plus facilement (ce qui a des effets pervers en permettant aussi aux attaqueurs de trouver plus facilement des vulnérabilités). Cela permet également au secteur d'être très agile car on peut modifier, combiner et connecter entre eux différents protocoles pour faire quelque chose de nouveau à partir de ce qui existait déjà.

2. Gouvernance

Les plateformes dans web3, dont les protocoles DeFi, peuvent être modifiées si la Blockchain 'vote' en appliquant majoritairement un changement, même si c'est rare. Certaines plateformes sont organisées en DAO ce qui codifie la façon dont leur fonctionnement peut être modifié. Cette façon de gérer l'évolution d'une plateforme s'oppose aux géants d'internet qui contrôlent unilatéralement leurs services, avec une motivation de générer des profits. Dans web3 on peut considérer que l'avenir des services appartient, dans une certaine mesure à ceux qui s'en servent.

3. Accessibilité

Les services DeFi ne sont pas limités par les mêmes régulations que la finance traditionnelle, comme les règles KYC (« know your customer ») en place qui nécessitent de vérifier des informations sur l'identité de ses clients avec pièce d'identité, justificatif de domicile, voire déclaration de revenu à l'appui alors qu'en DeFi il n'y a pas de discrimination par défaut. Plus encore, des personnes dans de nombreux pays aujourd'hui ne peuvent pas faire confiance en leurs institutions ou leurs intermédiaires financiers. Pour accéder à la DeFi, il suffit d'avoir un appareil connecté à internet et une adresse Ethereum, ce qui abaisse la barrière à l'entrée des services financiers pour beaucoup de personnes en nécessitant relativement peu d'infrastructure dans le monde réel.

4. Efficience sans confiance

L'utilisation de la Blockchain pour décentraliser les services financiers permet à ceux-ci de fonctionner systémiquement en alignant les intérêts des agents économiques, même s'ils ne se font pas confiance. Grâce aux protocoles qui ont été mis au point, on peut donc réduire certains types de risques et se passer de tiers-partis qui sont nécessaires en finance traditionnelle. Par exemple, l'échange d'actifs entre deux partis ne nécessite pas de garantie d'une CCP (contrepartie centrale) car les deux transactions peuvent être exécutées atomiquement. Autrement dit, soit les deux transactions sont exécutées, soit aucune ne l'est, ce qui réduit grandement le risque de contrepartie.

5. Une infrastructure parallèle

La DeFi s'inscrit dans une mouvement plus large de décentralisation : on assiste au développement d'un écosystème de services parallèle, une alternative potentielle aux gouvernements et aux grandes entreprises. Le fait que cette décentralisation a vu ses débuts dans une monnaie digitale a fait que le secteur de la finance s'est rapidement développé, d'autant plus qu'un système financier efficace est nécessaire pour le bon fonctionnement d'un marché et d'une économie, même si elle est digitale. En février 2022, la valeur des actifs utilisés en finance décentralisée s'élevait à 200 milliards $[12], ce qui témoigne de son importance alors que c'est un secteur encore jeune. D'autres applications décentralisées se développent également, comme des jeux décentralisés ou des versions décentralisées de certaines plateformes très importantes sur internet. Cela a beaucoup de potentiel, notamment avec l'avènement du 'Metaverse' car la blockchain permet d'introduire de la rareté dans le monde digitale.

[12] https://en.wikipedia.org/wiki/Decentralized_finance

II/ Des obstacles persistent

1. les limitations technologiques

Le risque de smart contract, est le risque associé au fait que tout smart contract doit être codé par des humains, pour qui il est difficile de créer une application 'parfaite' sans bugs ou dysfonctionnements. Il y a donc toujours le risque qu'une vulnérabilité soit laissée par les développeurs, mettant à mal la sécurité du protocole même si la blockchain effectue bien son travail. Il existe des solutions potentielles comme des audits, des assurances ou des vérifications formelles du code, mais un risque humain persistera toujours.

Pour modifier un smart contract (par exemple pour l'améliorer ou effectuer une fermeture d'urgence) l'équipe de base possède des clés d'administrateur. Il y a un risque qu'une clé soit mal dissimulée et se retrouve entre les mains d'un acteur malintentionné.
Même si la modification des contrats est soumise à un vote basé sur des Governance Token, en réalité ces tokens sont souvent mal distribués et reste très centralisés, ce qui mène aux même risques.

Le fait que les différents aspects de la DeFi soient autant liés ensemble, comme des protocoles construit sur d'autres protocoles, apporte son propre lot de risque. L'interconnexion des services entre eux fait qu'un problème sur une seule plateforme peut se répercuter sur beaucoup d'autres et provoquer des chocs importants sur tout le secteur. Par exemple, des frais de transactions Ether volatiles pourrait rendre des protocoles DeFi inutilisables.

Il y a un arbitrage, à la manière d'un triangle d'impossibilité, dans le design de blockchain entre la décentralisation, la sécurité et la scalabilité du réseau. Bitcoin et Ethereum ont fait le choix de sacrifier la scalabilité pour plus de décentralisation et de sécurité, or cela pèse sur eux maintenant qu'ils sont adoptés par de plus en plus d'utilisateurs. C'est pour cela que les frais de transaction d'Ethereum sont élevés, comparé à ceux de plateformes alternatives comme Cardano et Solana.

Le protocole de consensus en proof-of-work est potentiellement en danger si les ordinateurs quantiques se développent suffisamment. Ils pourraient casser la fonction hash cryptographique utilisée par ces réseaux et permettraient de trouver un hash spécifique exponentiellement plus rapidement qu'un ordinateur classique.

2. Les obstacles régulatoires

La defi est un secteur encore tout nouveau et donc la régulation des états ne s'y est pas encore rattrapée. A cause de cela, il y a eu au cours des dernières années de nombreuses fraudes financières tels que des « pump and dump » et des « rug pulls », notamment en 2017 lors de « l'explosion des ICO ». Au fur et à mesure que le secteur se développe et capture plus d'argent des ménages et des investisseurs, les Etats vont vouloir le réguler de plus en plus. A cause de cela il persiste des inconnus importants quant à l'avenir de la DeFi, introduisant de la volatilité dans les marchés. Les plateformes arrivent actuellement à éviter la régulation, par exemple en s'assurant que leurs actifs ne soient pas considérés comme des Sécurités.

Mais les régulateurs aux Etats-Unis et dans l'Union Européenne ont récemment montré une volonté de réguler davantage ces services, ce qui est très controversé. En effet, même si plus de régulation pourrait aider à l'adoption de masse en rassurant les utilisateurs, beaucoup pense que cela pourrait ralentir l'innovation du secteur, qui est très importante étant donné qu'il est encore en développement et en train de se chercher.

La parlementaire européenne Aurore Lalucq s'est récemment attiré les critiques des fans de la crypto, allant jusqu'au harcèlement, pour avoir proposé que les cryptoactifs et services financiers liés à la crypto soient réglementés comme la finance traditionnelle.

Une autre inquiétude des régulateurs par rapport à la cryptomonnaie est son utilisation pour des activités illicites. Certains protocoles sont complètement anonymes, comme Monero et Kucoin, mais généralement la plupart sont pseudonyme comme Bitcoin et Ethereum. Cette intimité peut être une bonne chose pour beaucoup de personne, mais elle suffit également à certains individus malintentionnés pour effectuer des opérations illégales. Réguler le passage entre la monnaie fiat (réelle) et les cryptoactifs semble être la meilleure façon de lutter contre ces abus

Bibliographie

- 3blue1brown : But how does bitcoin actually work?

https://www.youtube.com/watch?v=bBC-nXj3Ng4&vl=en

- Bitcoin white paper:

https://bitcoin.org/bitcoin.pdf

- Defi and the future of finance :

Campbell R. Harvey Duke University, Durham, NC USA 27708
National Bureau of Economic Research, Cambridge MA USA 02138
Ashwin Ramachandran, Dragonfly Capital
Joey Santoro, Fei Protocol

- CeFi vs. DeFi — Comparing Centralized to Decentralized Finance :

Kaihua Qin, Imperial College London
Liyi Zhou, Imperial College London
Yaroslav Afonin, Imperial College London
Ludovico Lazzaretti, Independent
Arthur Gervais, Imperial College London

- Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets

Fabian Schär, University of Basel

- SoK: Decentralized Finance (DeFi)

Sam M. Werner, Imperial College London
Daniel Perez, Imperial College London
Lewis Gudgeon, Imperial College London
Ariah Klages-Mundt, Cornell University
Dominik Harz, Imperial College London
William J. Knottenbelt, Imperial College London

- Lex Fridman Podcasts

Vitalik buterin:
https://youtu.be/3x1b_S6Qp2Q
https://youtu.be/XW0QZmtbjvs
Chainlink: https://youtu.be/TPXTmVdlyoc
Algorand: https://youtu.be/zNdhgOk4-fE
Cardano: https://youtu.be/FKh8hjJNhWc
Jack Dorsey & Block: https://youtu.be/60KJz1BVTyU

- Whiteboard Crypto

DeFi :
https://youtu.be/o9ObYRjpIhs
https://www.youtube.com/watch?v=17QRFlml4pA
Smart contracts : https://youtu.be/pyaIppMhuic
Proof of Stake: https://youtu.be/x83EVUZ_EWo
Tokens: https://www.youtube.com/watch?v=422HORNUfkU&t=327s
Defi 2.0 : https://www.youtube.com/watch?v=I34lOvUWsNc&t=389s

- Perpetual swaps

Coindesk perpetual swapshttps://www.coindesk.com/learn/what-is-a-perpetual-swap-contract/
Binance perpetual swaps: https://youtu.be/H7Irc5jSk0A

- Sites de plateformes

https://ethereum.org/
https://cardano.org/
https://filecoin.io
https://www.binance.com
https://uniswap.org/
https://www.olympusdao.finance/
https://aave.com/
https://compound.finance/
https://chain.link/