



by **KPMG**

Cryptoactifs: vers une révolution financière

Juin 2021



Cryptoactifs : vers une révolution financière.

Sommaire

Edito.....	4
Avant-propos : les cryptoactifs sont un sujet stratégique.....	6
Bitcoin : un nouvel actif protéiforme à l'ère Internet	8
Bitcoin : un actif associé à l'espace Internet.....	10
Bitcoin : une meilleure réserve de valeur que l'or ?	12
Des usages divers et une adoption croissante par les institutionnels et les entreprises	16
Bitcoin est une fondation permettant l'émergence de nouveaux applicatifs avec Lightning Network et/ou RGB.....	18
Stablecoins et MNBC : l'émergence des monnaies fiduciaires sur la Blockchain.....	22
Les Stablecoins : des rampes d'accès vers le monde Blockchain	24
Les bénéfices des stablecoins pour l'industrie financière	27
Les Stablecoins : l'enjeu politique	28
La réponse des banques centrales	30
DeFi et Tokenisation des actifs, l'avènement d'une nouvelle industrie financière	34
La DeFi : l'Internet de la valeur & "Wall Street API"	36
La DeFi, un écosystème en cours de structuration	40
L'hybridation entre la finance traditionnelle et la DeFi	44
Web 3, une nouvelle itération d'Internet	46
Les limites du Web 2.....	48
Le Web 3 comme révolution d'Internet	49
Les différents services du Web 3	50
Conclusion	53
Conclusion.....	54
Présentation des auteurs	55
Lexique.....	56



Édito

La révolution des cryptoactifs concrétise l'émergence d'un nouvel Internet : un Internet de la valeur.

Ces technologies bouleversent le paradigme - aujourd'hui centralisé - de la gestion de valeur en ligne : elles proposent un fonctionnement nativement numérique, décentralisé et accessible à tous, remettant ainsi pour la première fois la souveraineté des individus au cœur de l'innovation technologique.

Les crypto-actifs répondent à plusieurs grands enjeux économiques et sociétaux actuels. Leur croissance soutenue entraîne une vague d'innovations de grande ampleur, comme l'émergence de la finance décentralisée, qui bouleverse les systèmes financiers et économiques traditionnels et joue un rôle fondamental dans la transformation numérique des entreprises ; en révélant dans tous les secteurs des développements et des opportunités à saisir.

Dans ce contexte, conscients de la dimension stratégique de ces transformations pour tous nos clients, les équipes de Blockchain Partner ont rejoint KPMG en Mars 2021 pour devenir ensemble la référence du conseil blockchain et cryptoactifs en France.

Avec ce rapport, notre objectif est d'aider les décideurs à comprendre certains enjeux économiques et techniques des cryptoactifs et des applications associés et aussi de partager quelques convictions sur leur évolution. Il n'a pas pour objet de présenter une analyse exhaustive de l'ensemble des enjeux juridiques, risques et réglementaires de ces actifs.

Catherine Philippe

Associée KPMG
Blockchains & Cryptos
KPMG France



Avant-propos

Les cryptoactifs sont un sujet stratégique

L'année 2020 marque un tournant pour le secteur "Blockchain & Cryptoactifs".

La pandémie a accéléré l'émergence des cryptoactifs voire agit comme un catalyseur de la tendance à l'institutionnalisation du secteur.

Microstrategy, Tesla, Mass Mutual, BNY Mellon sont autant d'acteurs traditionnels qui ont renforcé la visibilité du secteur en 2020 par l'acquisition de bitcoins ou l'ouverture de nouveaux services liés aux cryptoactifs.

Cela fait suite au retentissement qu'a eu Diem (ex "Libra" mené par Facebook) sur les pouvoirs publics et dans les milieux financiers en 2019. L'infrastructure technique évoquée sans ambages était la Blockchain et les cryptoactifs, présentée comme les technologies adéquates pour une plus grande inclusion financière.

Les institutions privées et publiques ne peuvent plus faire l'économie du sujet, **ni l'appréhender sous l'angle purement technique** en essayant de créer un cas d'usage pour améliorer un service existant.

Après l'avènement d'internet qui affecte fortement depuis près de 30 ans quasiment tous les domaines d'activités (autant dans l'industrie que dans les services), une seconde révolution numérique s'amorce avec l'émergence de l'internet de la valeur. De la même façon que toute entreprise communique via Internet, et est donc concernée par la révolution numérique, toute entreprise ou institution est aussi concernée par l'utilisation et le transfert de valeur. **Les cryptoactifs sont un sujet qu'il faut considérer sous l'angle stratégique.**

Une feuille de route est à déterminer dans chaque entreprise, chaque institution publique, pour anticiper le sujet à court, moyen et long terme. Les avantages économiques ne sont plus à démontrer au regard des résultats financiers publiés par Paypal, Coinbase, ou Square, stimulés par la demande des particuliers, mais aussi et surtout des entreprises. Avec l'entrée en bourse de Coinbase, qui marque la sortie symbolique de l'état de "marché de niche", et la multiplication des acquisitions des jeunes pousses du secteur par des acteurs traditionnels, c'est toute une industrie qui est en train d'apparaître sous nos yeux.

Les mouvements actuels sur le prix d'actifs ne doivent pas faire perdre de vue les sous-jacents et les problématiques posées par l'émergence du secteur à savoir :

- La transformation des acteurs financiers et l'émergence de nouveaux (Coinbase, Blockfi, et autres....)
- La dollarisation et l'extraterritorialité du droit américain
- L'inclusion financière
- La protection de la vie privée
- Une nouvelle économie numérique moins concentrée autour des GAFAM : le Web 3

Ce document permet de répondre en détail à quelques-unes de ces questions et d'esquisser les transformations que l'on voit poindre en traitant les 4 sujets suivants :

- Bitcoin et la rareté numérique
- Les stablecoins
- La Finance Décentralisée : nouvelle infrastructure financière
- Le Web 3, nouvelle itération d'Internet



Une feuille de route est à déterminer dans chaque entreprise, chaque institution publique, pour anticiper le sujet à court, moyen et long terme.

Claire Balva

Directrice Blockchains & Cryptos



Croire que les cryptoactifs ne concernent que l'industrie financière revient à croire qu'Internet n'affecte que les industries de la communication.

Alexandre Stachtchenko

Directeur Blockchains & Cryptos

1.



Bitcoin : un nouvel actif protéiforme à l'ère Internet

Bitcoin : un actif associé à l'espace Internet

Première des cryptomonnaies, Bitcoin s'inspire directement de la philosophie à l'origine d'Internet. Axée sur le respect de la vie privée à l'ère numérique et la volonté d'une plus grande indépendance de l'individu par rapport aux institutions, Bitcoin a été créé en 2009 par le pseudonyme Satoshi Nakamoto. Il est le résultat d'une profonde réflexion sur la nécessité d'un outil pour s'affranchir du pouvoir du système financier traditionnel et de la censure.

L'objectif est double : transférer de la valeur sans intermédiaire de confiance, et créer un système électronique de paiement en pair à pair¹. Ainsi, Bitcoin repose sur un registre décentralisé, incorruptible et transparent (la "*Blockchain*") : les règles du protocole ne peuvent être modifiées que par [consensus*](#), et les transactions sont publiques et réputées infalsifiables. Afin de préserver sa rareté, et donc sa valeur, il n'existera à terme qu'une quantité finie de bitcoins : 21 millions. En Mars 2021, environ 18,5 millions de bitcoins ont déjà été créés, et la limite de 21 millions devrait être atteinte en 2140.

À la différence des monnaies traditionnelles, Bitcoin est un actif **nativement numérique**. À l'inverse, une monnaie traditionnelle est d'abord un outil physique, dont la représentation numérique est gérée sur des registres bancaires, dont il est important de s'assurer qu'ils sont cohérents (que chaque banque soit d'accord sur les montants possédés par chacun). Ainsi, l'exécution d'un

paiement numérique pour une monnaie classique relève de la tenue de compte, tandis qu'un paiement bitcoin relève d'un "[véritable](#)" [transfert de possession](#) numérique, sans intervention d'un tiers de confiance. Là où les risques de délai d'exécution et de blocage d'un paiement persistent dans le système bancaire traditionnel, un transfert de valeur en Bitcoin est **transnational, presque instantané, et ne peut être bloqué par aucune institution**.

Bitcoin se caractérise également par son **accessibilité**, dans la mesure où une connexion à Internet suffit pour l'utiliser. Cela représente un avantage certain pour les particuliers, confrontés aux nombreux critères qui conditionnent l'accès à un compte bancaire. Certes, de plus en plus de plateformes d'échanges - Coinbase, Kraken, Binance - sont contraintes d'appliquer la procédure de vérification d'identité imposée par les régulateurs "*KYC (Know Your Customer)*". Pour autant, et contrairement aux actifs financiers traditionnels, il est toujours possible de créer et gérer un portefeuille de cryptoactifs indépendamment de tout tiers de confiance. En ce sens, du fait de son caractère **incensurable** et de son **accessibilité**, Bitcoin est comparable à du **cash numérique**.

Du point de vue des particuliers et des citoyens - pour lesquels Bitcoin a été initialement conçu -, il revêt donc **deux intérêts principaux** :

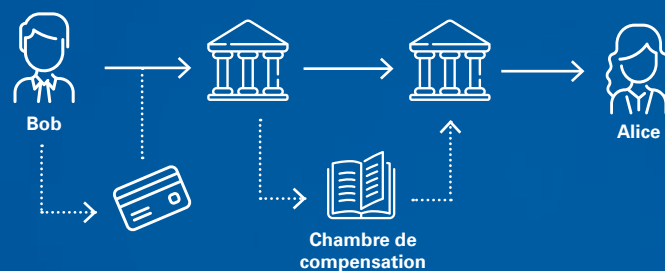
* Les mots soulignés en bleu se réfèrent aux définitions du lexique, page 56.

- Tout d'abord, il s'agit d'un **outil anti inflationniste**. Par exemple, des pays comme la Turquie, l'Argentine, le Venezuela, l'Iran, le Liban, le Brésil, le Nigeria, ou encore le Zimbabwe (totalisant près de 700 millions d'habitants) ont tous vu leurs monnaies se déprécier d'au moins 20% face au dollar depuis le 1er Janvier 2020². Bitcoin s'est largement apprécié par rapport aux monnaies nationales tant celles-ci ont été dévaluées par les crises économiques³ et les politiques monétaires qui s'en sont suivies. Nous reviendrons sur cet aspect plus en détail par la suite. Il constitue donc de plus en plus pour les populations exposées un outil de préservation du capital sur le temps long, malgré sa volatilité.

- Ensuite, Bitcoin est une **barrière contre la censure**. Avec l'inquiétude liée à l'émergence de dérives dans l'utilisation de la donnée à l'ère d'Internet (atteinte aux libertés individuelles et confidentialité) et de la possibilité, pour les Etats et les institutions publiques et privées, d'exercer un plus grand contrôle sur la population, Bitcoin apparaît comme un bouclier à la censure et à l'interdiction des transactions : son registre décentralisé empêche toute entité d'en prendre le contrôle. De telles caractéristiques présentent par exemple un intérêt certain pour la protection des lanceurs d'alertes, comme Edward Snowden⁴, ou pour certaines populations, comme à Hong Kong⁵ ou au Venezuela⁶. Bien que Bitcoin soit plus traçable que le cash, il demeure incensurable.

Ces différentes caractéristiques amènent naturellement le bitcoin à souvent être comparé à des métaux précieux et en particulier l'or, dans sa fonction de réserve de valeur.

Paieement classique



Paieement Bitcoin



1. [Bitcoin: A Peer-to-Peer Electronic Cash System](#)
 2. [Skybridge Bitcoin Fund L.P., 2020](#)
 3. [As Bitcoin's Price Hits a New All Time High, What Happens Next?](#)
 4. [Edward Snowden used Bitcoin to buy servers for 2013 mass surveillance leak](#)
 5. [Hong Kong protests are accelerating bitcoin adoption](#)
 6. [Venezuela's Bitcoin Use Soars Amid Hyperinflation: 3rd on Global Crypto Adoption Index](#)

Bitcoin : une meilleure réserve de valeur que l'or?

Grâce à ses propriétés intéressantes, Bitcoin épouse les caractéristiques d'une réserve de valeur de plus en plus reconnue. Il permet aujourd'hui d'accumuler du capital et de constituer une épargne sur le long terme. En effet, et ce malgré sa volatilité, Bitcoin s'inscrit dans une tendance haussière depuis sa création en 2009, et sa volatilité a globalement fortement diminué depuis cinq ans⁷.

Caractéristiques	Or	Bitcoin
Rareté	Limite finie inconnue	Limite finie connue
Taux d'inflation	En fonction de l'extraction	Prévisible et connu de tous
Portabilité	Couteux à transporter	Simplicité de la numérisation
Fongibilité	Possibilité de le fondre	Traçabilité à double tranchant
Fragmentabilité	Processus industriel complexe	Divisible jusqu'à 10^{-8}
Résistance à la fraude	Nécessite un tiers pour vérifier	Vérification simple
Stockage	Sécurité coûteuse	Combinaison software & hardware
Capacité à rendre productif l'actif	Difficulté	Caractère numérique rendant aisé sa productivité avec la Finance Décentralisée
Historicité	2 500 ans d'Histoire	Lindy Effect: 11 ans mais se renforce chaque jour passant

Comparatif des caractéristiques de l'or et de Bitcoin - Blockchain Partner by KPMG

⁷ Bitcoin: Implications for the Developing World, p.18

Cette association entre Bitcoin et l'or, que les institutionnels s'approprient de plus en plus, est justifiée pour plusieurs raisons.

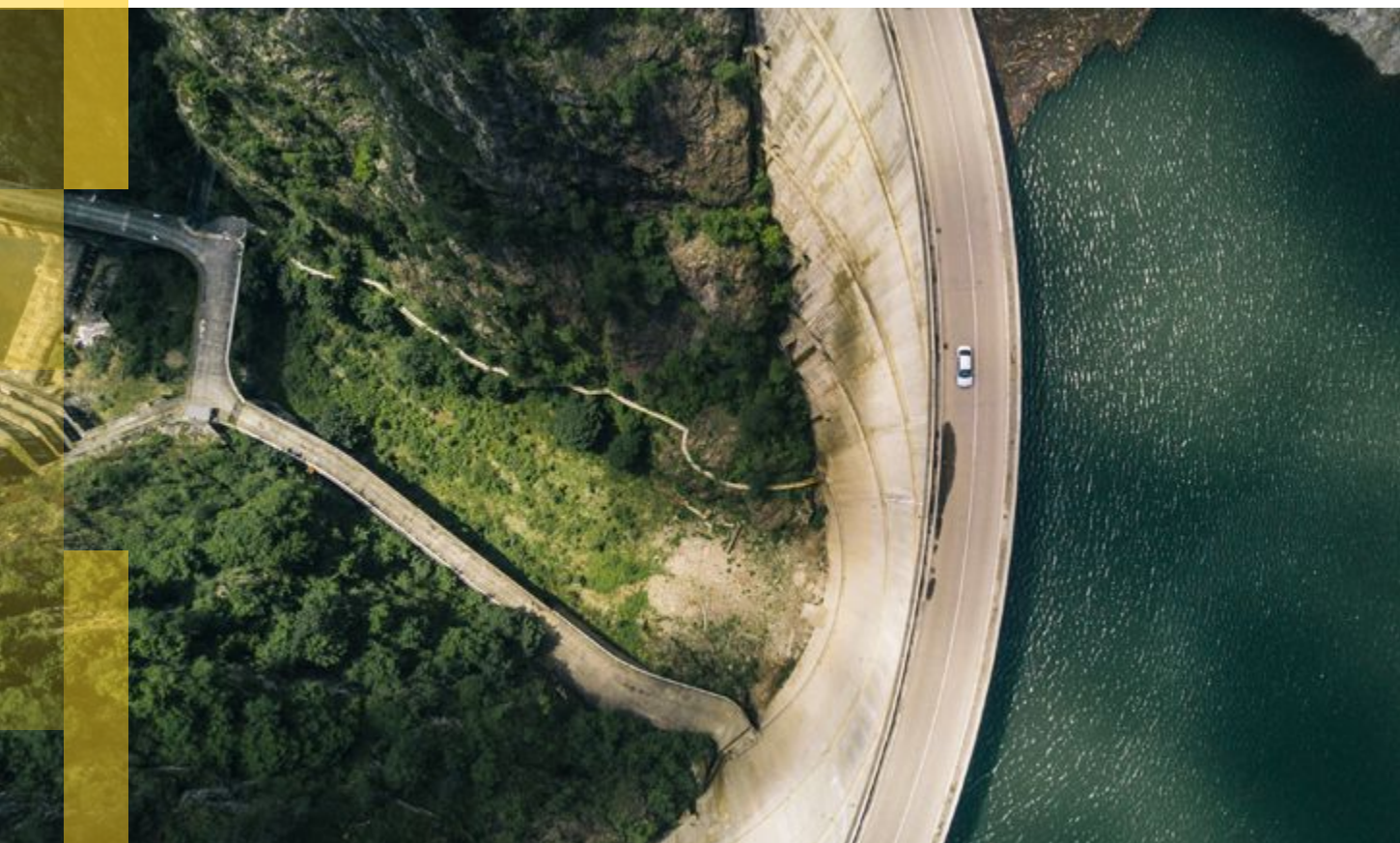
Tout d'abord, et principalement, comme l'or, **Bitcoin se caractérise par sa rareté**. S'il existe une quantité finie d'or sur Terre, Bitcoin existe en quantité limitée également - comme nous l'avons vu précédemment.

Ensuite, ces deux actifs sont **fongibles, durables et aisément identifiables**, ce qui représente d'autres critères constitutifs d'une réserve de valeur. Le matériau qu'est l'or est fongible (un gramme d'or vaut un autre gramme d'or), résiste particulièrement bien à la corrosion, et est aisément identifiable par sa couleur. De la même façon, un bitcoin est fongible, et sa sécurité ainsi que sa non-duplicabilité sont assurées notamment par la technologie Blockchain. Cette technologie a prouvé sa robustesse depuis 2009, et plus elle prouve sa résistance aux attaques, plus elle génère de confiance quant à la capacité de Bitcoin à constituer une réserve de valeur fiable.

Une autre caractéristique essentielle réside dans la **faible corrélation entre les actifs comme les cryptomonnaies ou l'or, et les autres classes d'actifs comme les obligations d'État et les actions**. En effet, tout comme l'or, Bitcoin a montré qu'il était peu corrélé aux actifs financiers traditionnels depuis sa création. Comme toute cryptomonnaie, Bitcoin n'est adossé à aucune institution telle une banque centrale : sa valeur intrinsèque ne dépend aucunement des performances d'une personne ou d'une entreprise. Cette non-corrélation est pour l'instant une tendance observable empiriquement, et sur des périodes longues. En effet, il arrive que sur des périodes courtes (quelques mois), le bitcoin soit corrélé par exemple aux marchés des actions.

	Bitcoin (BTC)	Indice S&P500	Or
Bitcoin (BTC)	1	0,01	0
Indice S&P500	0,01	1	0,02
Or	0	0,02	1

Tableau de présentation des corrélations entre Bitcoin, l'Or & l'indice S&P500 (de 2012 à 2020)
Source: Morningstar



Au-delà de leurs similarités, Bitcoin présente plusieurs avantages par rapport à l'or :

LA DIVISIBILITÉ

Bitcoin est plus facilement divisible, accessible et stockable que l'or du fait de sa nature numérique. Diviser un bitcoin revient à faire une transaction, ce qui est possible en quelques secondes avec n'importe quel portefeuille numérique, et ne coûte que quelques euros.

L'ACCESSIBILITÉ

Bitcoin est accessible avec un simple accès Internet. En d'autres termes, il est accessible aisément à près de 60 % de la population mondiale⁸.

LA CONSERVATION

Conserver du bitcoin revient à conserver un mot de passe, et à établir des procédures et bonnes pratiques de sécurité. À l'inverse, l'or mobilise des ressources pour son stockage (et en particulier pour assurer sa sécurité).

L'IMPACT ÉCOLOGIQUE ET SOCIAL

Bitcoin repose sur l'algorithme de Proof of Work permettant d'assurer un très haut niveau de sécurité au réseau nécessitant une importante quantité d'énergie pour fonctionner, ce qui lui est souvent reproché. **Néanmoins, Bitcoin pourrait être un moteur de la transition écologique⁹. Il permet notamment de rentabiliser les énergies renouvelables en leur fournissant un talon de consommation qui compense leur intermittence.**

A ce titre, l'entreprise norvégienne Aker, dont les intérêts portent principalement sur le pétrole et le gaz, a créé une filiale pour investir dans Bitcoin et utiliser des énergies renouvelables sous-exploitées pour "miner" des cryptomonnaies¹⁰. Les mineurs ont donc tendance à s'installer à proximité de centrales électriques sous-exploitées pour obtenir un prix du kWh moins cher, et rentabiliser leur activité.

À titre d'illustration, une étude de l'université de Cambridge de 2020 révèle que **76 % des mineurs**

utilisent des énergies renouvelables dans leur mix énergétique, et 39% de la consommation énergétique totale du minage provient d'énergies renouvelables¹¹, ce qui fait du minage l'une des industries mondiales les plus tournées vers les énergies propres. En l'occurrence, l'énergie hydraulique est la première source d'électricité renouvelable utilisée par les mineurs.

D'un point de vue de l'impact social, la Human Rights Foundation évoque même Bitcoin comme étant *"une force puissante en faveur des droits de l'Homme dans le monde"* (protection de la vie privée, des lanceurs d'alerte, de la liberté sous des régimes autoritaires etc.)¹².

A l'inverse, l'impact environnemental de l'or, principal "concurrent" de Bitcoin, est fréquemment pointé du doigt : l'orpaillage illégal au Pérou, en Guyane ou encore en Afrique de l'ouest est une des principales sources de déforestation (voire la plus importante par exemple à Madre de Dios au Pérou), et de pollution des cours d'eau par le rejet de tonnes de mercure¹³.

LA PRODUCTIVITÉ

S'il n'est pas un actif intrinsèquement productif, Bitcoin peut générer des intérêts en le plaçant sur des infrastructures de la finance décentralisée. Contrairement aux actifs traditionnels, il est possible de le rendre productif en l'utilisant comme représentation du Bitcoin sur Ethereum, que ce soit pour financer des projets, prêter ou emprunter des liquidités à d'autres personnes, par exemple. Nous analyserons les cas d'usages plus en détail dans la troisième partie consacrée à la finance décentralisée (DeFi).

De plus, Bitcoin peut également être [collatéralisé](#) pour garantir des emprunts en monnaie fiduciaire, sur le modèle du [crédit lombard](#). Cette collatéralisation génère des intérêts pendant la durée du prêt - ce que permet la plateforme [BlockFi](#) par exemple. Bitcoin permet donc, par rapport à l'or, de réaliser des transactions plus rapidement du fait de l'absence d'intermédiaire, d'obtenir plus de liquidités et d'améliorer l'efficacité de son propre capital. Beaucoup d'autres possibilités existent dans l'écosystème DeFi.

Tous ces avantages font l'objet d'une reconnaissance croissante chez les investisseurs institutionnels, ce qui contribue à leur adoption ces dernières années, en particulier depuis la pandémie de Covid 19, qui a entraîné des réponses d'assouplissement quantitatif de la part des principales banques centrales.

8. Chiffres clés 2020 sur les utilisateurs Internet, mobile et réseaux sociaux dans le monde

9. Selon la Deutsche Bank, "capital currently engaged in the cryptocurrency market could be used to develop green technological advancements" *The Future of Payments: Series 2 - Deutsche Bank Research*, p.6

10. Ce géant de l'investissement norvégien se lance dans le Bitcoin (BTC)

11. 3rd Global Cryptoasset Benchmarking Study

12. <https://twitter.com/gladstein/status/1357757736394444800>

13. La NASA révèle les ravages de l'orpaillage au Pérou



Des usages divers et une adoption croissante par les institutionnels et les entreprises

Bitcoin est donc certes une réserve de valeur, mais il ne se limite pas à cela : actif potentiel de règlement international, outil de trésorerie et de diversification de portefeuille... Les possibilités sont nombreuses, et Bitcoin fait l'objet d'une adoption croissante par les entreprises, particulièrement en 2020-2021¹⁴.

Suite à la pandémie de Covid-19, la crise économique a accentué la dévaluation des monnaies traditionnelles, et la perte de confiance des entreprises et des investisseurs à leur égard. En effet, les politiques monétaires expansionnistes ont pu susciter une crainte croissante de la part des investisseurs, comme Michael Saylor, directeur de MicroStrategy¹⁵. Leur fiabilité comme réserve de valeur pour sécuriser son patrimoine a été remise en cause, notamment le dollar dont le cours a baissé de 12% par rapport à l'euro depuis mars 2020¹⁶.

Parallèlement, nombreux sont ceux qui ont pris conscience des enjeux autour des cryptomonnaies, et se sont tournés vers ces nouveaux actifs. C'est le cas des banques institutionnelles comme Morgan Stanley¹⁷, BNY Mellon¹⁸, Goldman Sachs¹⁹, BBVA²⁰ ou encore JP Morgan, qui proposent des nouveaux services liés aux

cryptomonnaies face à la demande croissante de leurs clients²¹, et intègrent les plateformes d'échanges de Coinbase et Gemini comme clients. Ces acteurs étaient souvent, il y a quelques années, les plus grands contempteurs de cet actif, avant de prendre conscience des opportunités et des enjeux, contribuant donc à sa légitimité.

De la même manière, des autorités de régulation comme l'OCC (*Office of the Comptroller of the Currency*) déclarent vouloir donner des licences aux banques décentralisées et être convaincues du potentiel révolutionnaire de la finance décentralisée²². L'OCC s'adonne d'ailleurs à la rédaction d'articles pointus sur la *DeFi*²³, et autorise désormais les banques américaines à ouvrir des comptes aux détenteurs de [stablecoins](#), et à les utiliser comme moyen de paiement²⁴.

D'autres entreprises, non financières, utilisent Bitcoin pour diversifier leurs trésoreries : l'équivalent de plus de deux milliards de dollars pour MicroStrategy²⁵, 170 millions de dollars pour Square²⁶, ou encore 1,5 milliard de dollars pour Tesla²⁷, qui a fait beaucoup de bruit lors de son annonce.

D'autres encore, spécialisées dans les services de paiement comme Paypal, proposent à leurs consommateurs de payer leurs achats en cryptomonnaies²⁸. Actif résilient et protéiforme, Bitcoin permet donc de répondre à de nombreux besoins dans le secteur économique. Ces différentes raisons laissent penser qu'il sera largement adopté par les entreprises dans les prochaines années.

14. Voir la liste des entreprises dans l'étude Deutsche Bank, page 10 [The Future of Payments: Series 2 - Deutsche Bank Research](#)

15. [MicroStrategy Adopts Bitcoin as Primary Treasury Reserve Asset](#)

16. [Le dollar, révélateur d'une Amérique affaiblie](#)

17. [Morgan Stanley becomes the first big U.S. bank to offer its wealthy clients access to bitcoin funds](#)

18. [BNY Mellon, la plus vieille banque américaine fait \(aussi\) le pari du bitcoin](#)

19. [Goldman Sachs restarts cryptocurrency desk amid bitcoin boom](#)

20. [BBVA launches its first commercial solution for the trading and custody of bitcoin in Switzerland](#)

21. [Big Ideas Report 2021. ARK Invest](#)

22. [Get ready for self-driving banks](#)

23. [Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets](#)

24. [OCC authorizes banks to use blockchains and stablecoins for payments](#)

25. [MicroStrategy buys more than \\$1 billion worth of bitcoin, adding to massive holdings](#)

26. [Square buys \\$170 million worth of bitcoin](#)

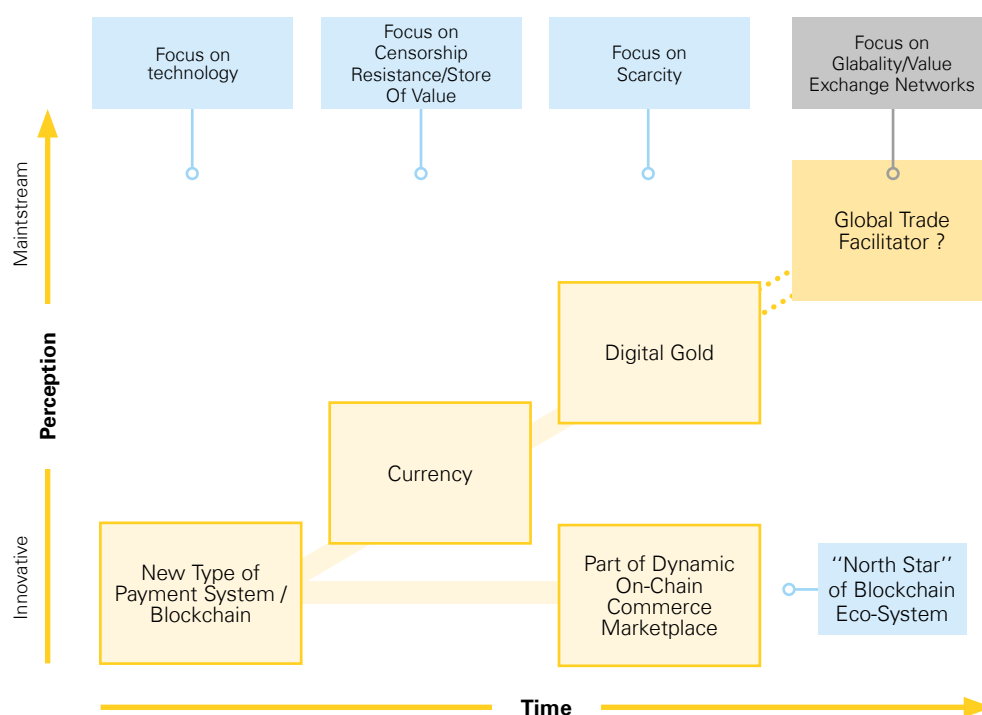
27. [Pourquoi Elon Musk embarque Tesla dans la folie bitcoin](#)

28. [PayPal lance son service de paiement en bitcoin](#)

Bitcoin est une fondation permettant l'émergence de nouveaux applicatifs avec Lightning Network et/ou RGB

La perception de Bitcoin évolue avec le temps et devient multidimensionnelle.

Le rapport de Citibank²⁹ publié en Mars 2021 propose un diagramme illustrant cette perspective à mesure que Bitcoin mûrit.



Source : Citi Business Advisory Services

29. Bitcoin At the Tipping Point

Citibank pose la question du devenir de Bitcoin en ajoutant la dimension potentielle de solution de paiement transnational facilitant le commerce international. Bitcoin est donc protéiforme et ne peut être réduit à des définitions restrictives de la monnaie.

Ainsi, Tesla diversifie sa trésorerie et accepte le Bitcoin, alors que les argentins ou vénézuéliens fuient l'hyperinflation de leur monnaie nationale.

Bitcoin est une machine de confiance que l'on peut assimiler à une fondation ouvrant la voie à de nombreux usages dont il est quasiment impossible d'anticiper la nature dans les prochaines années et décennies.

D'une manière comparable à l'Internet, de nouvelles couches successives ajoutent de la valeur, avec des initiatives comme Liquid, le Lightning Network, RGB ou le système d'identité numérique de Microsoft intitulé [ION](#) :

- Liquid est une chaîne parallèle fonctionnant avec une fédération d'acteurs afin de permettre les transferts entre plateformes d'échange avec plus de rapidité et de confidentialité au prix d'un compromis de sécurité. Cette sidechain ouvre la voie à d'autres usages et donc à la représentation d'actifs financiers par-dessus Bitcoin.

- Lightning Network est une solution dite de [scalabilité](#) permettant le transfert de bitcoin sur de petits montants de manière quasi instantanée et à peu de frais avec un compromis assumé entre scalabilité et décentralisation.

- RGB est un projet visant à créer des [smart-contracts](#), de manière privée et plus [scalable](#) et pouvant être connecté au Lightning Network.

- ION est une solution de [Layer 2](#) liée à Bitcoin et proposée par Microsoft qui fonctionne comme un protocole de gestion de l'identité numérique ouvert à tous.

La mise en perspective des usages de Bitcoin en fait la première pierre d'un système financier natif de l'espace Internet. Il faut donc considérer stratégiquement le sujet et se forger une conviction avant d'anticiper les cas d'usage métiers qui sont, aujourd'hui, difficiles à envisager. Peu de personnes dans les années 90 anticipaient les usages offerts par le web aujourd'hui. Il est important pour les acteurs économiques et politiques de ne pas reproduire les mêmes erreurs sous peine de déclassement (fuite d'une industrie émergente entraînant une dépendance à des géants étrangers type Coinbase, sous-exposition à cette nouvelle classe d'actifs, ...).

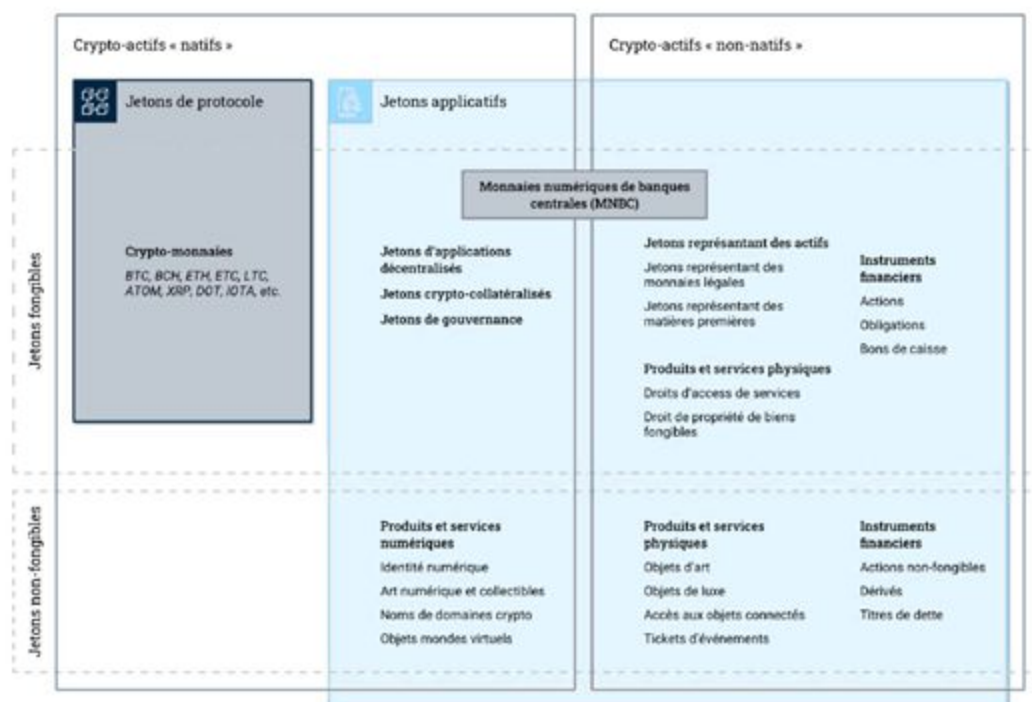
Points clés à retenir

- 1 Bitcoin permet de transférer de la valeur sans intermédiaire de confiance ; c'est un outil pour se protéger de l'inflation et un bouclier contre la censure.
- 2 Bitcoin épouse les caractéristiques d'une réserve de valeur, mais, du fait de sa nature numérique, il est aussi divisible, accessible, transférable et donc plus liquide qu'un actif tel que l'or.
- 3 Bitcoin fait l'objet d'une adoption croissante de la part des entreprises et des institutionnels qui s'approprient ses différents usages.
- 4 Des autorités de régulation déclarent vouloir donner des licences aux banques décentralisées, en particulier aux États-Unis.
- 5 Le cas d'usage socle de Bitcoin est une fondation sécurisant les transferts on-chain, mais sa perception évolue avec le temps et de nouvelles couches successives vont pouvoir y ajouter de la valeur, avec de nouveaux applicatifs.

Avant-d'aller plus loin...

Focus sur la tokenisation

Classification fonctionnelle des cryptoactifs



Classification fonctionnelle des cryptoactifs - Association pour le Développement des Actifs Numériques (ADAN)

Pour mieux comprendre les propos qui vont suivre, il importe de revenir sur la notion et tokenisation et la classification des cryptoactifs.

La tokenisation des actifs est un procédé qui vise à représenter un actif, numérique ou physique, par un token sur une Blockchain, lui faisant ainsi bénéficier de ses caractéristiques (liquidité, cessibilité, divisibilité, etc.).

Comme présenté sur l'image ci-contre, il existe deux manières de catégoriser les différents types de cryptoactifs :

- **Cryptoactifs “natifs”** : il s'agit à la fois des cryptomonnaies (propres à différentes infrastructures Blockchain et permettant l'utilisation de ces différents protocoles Blockchain) mais également de jetons applicatifs représentant des services et des droits sur des actifs nativement numériques (gouvernance des Dapps, noms de domaine, art numérique, ...).
- **Cryptoactifs “non-natifs”** : ce sont des représentations d'actifs physiques ou immatériels mais qui ne sont pas propres aux technologies Blockchain. La représentation de ces actifs sur les infrastructures Blockchain vise à bénéficier des caractéristiques de la Blockchain pour améliorer le fonctionnement existant.

Au-delà de ces deux catégories d'actifs, il convient de distinguer 2 types de token émis sur les Blockchain. D'une part les **jetons fongibles** qui sont des jetons qui peuvent être échangés entre eux sans distinction aucune d'un jeton à l'autre (exemple : les stablecoins USDC sont tous les mêmes et interchangeables comme pour des monnaies fiduciaires où 1\$ est échangeable sans distinction contre un autre dollar).

D'autre part, les **jetons non-fongibles** (connus sous l'acronyme NFT) sont caractérisés par leur unicité et rareté. Ainsi chaque jeton non-fongible possède des spécificités qui le distingue des autres jetons (exemple : 1 titre de propriété est unique et représente donc l'unicité d'un titre de propriété).

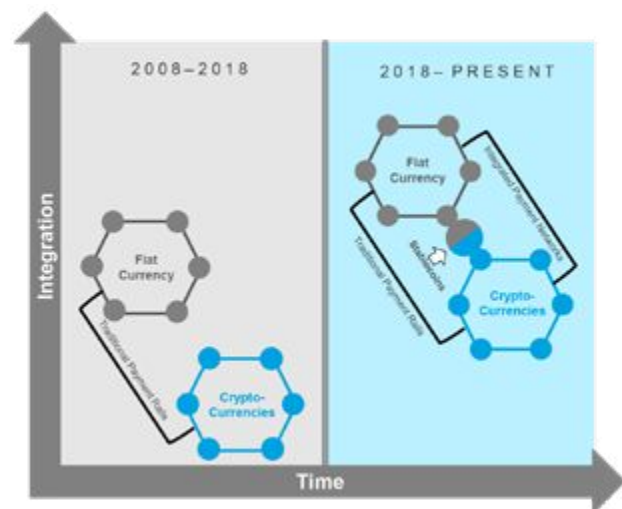
2.



Stablecoins & MNBC : l'émergence des monnaies fiduciaires sur la Blockchain

Les Stablecoins : rampes d'accès vers le monde Blockchain

Les *stablecoins* sont des *tokens* (jetons numériques) conçus pour conserver une valeur stable sur le marché par rapport à une valeur de référence - souvent une monnaie traditionnelle. Bien que les mécanismes varient, ils sont censés résister aux fluctuations de prix. Par exemple, à l'inverse d'un bitcoin, dont le prix de marché peut varier (environ 29 000 USD au 1er Janvier 2021 contre environ 46 000 USD au 1er Mars 2021), un "stablecoin dollar" vaut en permanence 1 dollar.



Source : Citi Business Advisory Services

En pratique, les stablecoins sont les rampes d'accès vers le monde des cryptomonnaies, et ce pour deux raisons : ils présentent à la fois les avantages des cryptomonnaies par leur **programmabilité**, et ceux des monnaies fiduciaires par la relative **stabilité** de leur cours.

Premièrement, et contrairement à une monnaie dite "classique", **un stablecoin est programmable** : il permet d'instaurer des logiques d'automatisation par le biais de **smart-contracts**. Cette possibilité, spécifique aux Blockchains, contraste avec le délai des procédures de l'industrie financière traditionnelle, de la banque à l'assurance, en passant par la gestion d'actifs. A titre d'exemple, un dollar n'est pas programmable, tandis qu'un stablecoin dollar l'est. Un stablecoin dollar rend donc indirectement le dollar programmable.

Deuxièmement, les stablecoins, comme leur nom l'indique, sont stables par rapport à leur valeur de référence. La grande majorité des stablecoins **sont d'ailleurs collatéralisés à d'autres actifs pour stabiliser leur cours (généralement au ratio 1 pour 1)**. La plupart de ces actifs sont des monnaies fiduciaires comme le dollar (Tether USDT, USD Coin). **D'autres sont collatéralisés par des cryptomonnaies** comme l'Ether, le Bitcoin (DAI, sUSD...), **voire non-collatéralisés** et que l'on appelle "stablecoins algorithmiques" (AMPL, ESD), bien que beaucoup plus rares sur le marché.

Le choix du stablecoin dépend avant tout de la philosophie de l'utilisateur : aspire-t-il à un système monétaire entièrement décentralisé ? Préfère-t-il, au contraire, un certain contrôle par une institution

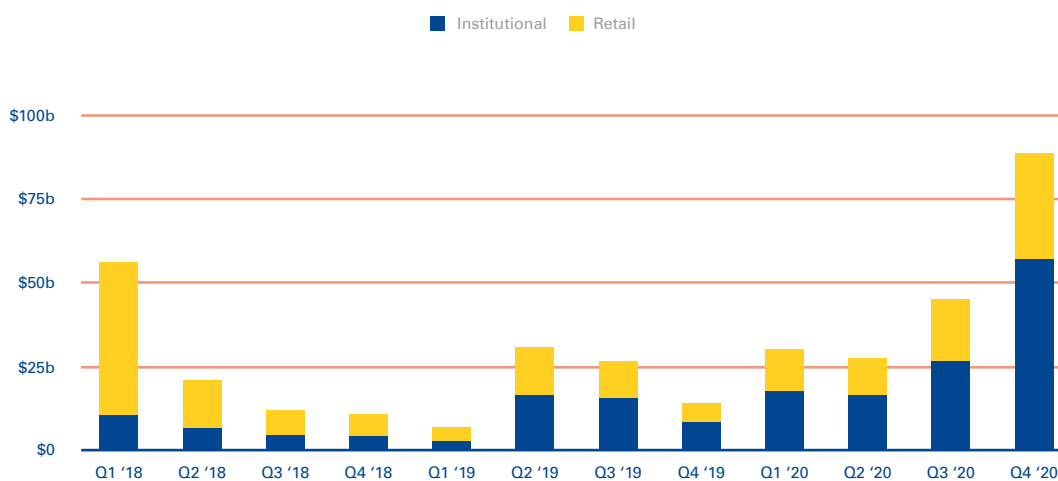
centralisée, ou un groupement d'acteurs financiers par exemple ? Les stablecoins sont donc à mi-chemin entre une monnaie fiduciaire classique (dite "fiat") et une cryptomonnaie.

En mai 2021, la capitalisation de marché totale des stablecoins a atteint 85 milliards de dollars, soit une augmentation de près de 1500% sur une année (de 5 à 85 Milliards de dollars)³⁰. Une telle hausse témoigne de l'engouement non seulement autour de Bitcoin comme réserve de valeur passive, mais aussi et surtout de services financiers plus élaborés nécessitant une protection contre la volatilité encore problématique des cryptomonnaies. Les services d'emprunts et de prêts dans la DeFi, par exemple, s'appuient fortement sur des stablecoins comme le DAI, l'USDT ou encore l'USDC.

De manière générale, l'entrée des entreprises dans le monde des cryptomonnaies est conditionnée à l'existence de tels outils. En parallèle de la forte progression de l'usage des stablecoins, la part des entreprises est en croissance soutenue dans les achats de cryptomonnaie par rapport aux particuliers - comme le montrent les chiffres de la plateforme d'échange américaine Coinbase. Alors qu'elles ne représentaient qu'un cinquième de la valeur des échanges au premier trimestre 2018, elles représentent près des deux tiers au premier trimestre 2021. Quant à la valeur totale échangée, elle progresse de près de 60% sur la même période - passant de 56 à 89 milliards de dollars. On peut formuler l'hypothèse que l'émergence des stablecoins incite à l'adoption des cryptomonnaies en général.

30. 2020 CoinGecko Yearly Crypto Report

Coinbase's Volume by Customer Segment



Trading Volume - Coinbase

Les stablecoins jouent un rôle de protection contre la volatilité des cryptomonnaies d'une part et contre l'inflation d'autre part. Contre la volatilité d'abord, car elles permettent aux investisseurs détenant des cryptomonnaies de sécuriser une position plus facilement, sans retourner dans le monde bancaire. Contre l'inflation d'autre part car, agissant comme du cash numérique accessible sans compte en banque, ils permettent à des populations exposées à des monnaies fragiles, et qui souhaiteraient se protéger sans pour autant s'exposer à la volatilité

des cryptomonnaies classiques, d'avoir accès facilement à des monnaies considérées comme plus stables, notamment le dollar américain. À ce titre, par exemple, une collaboration a eu lieu entre la plateforme de paiement Circle et le gouvernement américain pour permettre la circulation de l'USD Coin au Venezuela - un stablecoin collatéralisé par du dollar -, et contourner les interdictions bancaires face à l'inflation de 2 358.5%³¹ du bolivar pour la seule année 2020.

31. US Government Enlists USDC for 'Global Foreign Policy Objective' in Venezuela: Circle CEO

Les bénéfices des stablecoins pour l'industrie financière

Les stablecoins, ces actifs hybrides à la fois cryptomonnaie et monnaie traditionnelle, présentent un certain nombre d'avantages par rapport aux formats traditionnels de la monnaie. Par rapport à la finance traditionnelle, les **stablecoins** offrent plus de transparence et de sécurité pour la réalisation d'audits, plus d'interopérabilité entre différents actifs, et plus de liquidité.

Ainsi, un stablecoin peut être un moyen d'auditer des flux de manière indépendante et décentralisée. En effet, les Blockchains publiques, en particulier Ethereum, sur laquelle circulent la plupart des stablecoins, permettent à quiconque de vérifier les transactions d'un utilisateur sans intervention d'un tiers de confiance. Des entreprises se sont d'ailleurs spécialisées dans l'analyse des Blockchains comme Chainalysis, et fournissent des outils permettant d'identifier les transactions suspectes ou encore les comptes associés à des entités criminelles, car il est en effet possible de tracer les transactions et de déduire le montant des cryptomonnaies et des jetons propres à une adresse. Ici encore, la transparence et l'accès à l'information facilitent les contrôles sur les flux de paiement et remplacent notamment les procédures de circularisation actuelles.

De plus, un stablecoin permet d'améliorer l'interopérabilité entre différents actifs.

Il est désormais possible d'utiliser des représentations de la monnaie fiduciaire, mais également d'autres actifs comme des titres de propriété, des titres financiers, des dettes, des actions, ou encore des cartes de foot (cf : partie 4.c sur les NFT avec la start-up Sorare) sur une même infrastructure. Ces actifs peuvent ensuite être échangés de manière très simple, sans aucune friction (paiement, services, investissement, etc.) et avec des frais de transactions indépendants du montant de la transaction, ce qui les rend compétitifs sur les transferts de sommes importantes. L'utilisation de stablecoins, couplée à des jetons numériques représentant toute une série d'actifs, permet d'effectuer des échanges et transactions complexes en toute sécurité et sans s'exposer à une forte volatilité.

Un stablecoin s'apparente donc à un moyen d'échange dans un nouveau système financier à la croisée des chemins entre la relative stabilité des monnaies traditionnelles et la programmabilité des cryptomonnaies. Mais dans cette recherche d'hybridation, ils ne sont pas les seuls outils monétaires novateurs inspirés de ces nouvelles technologies. Certaines entreprises, au premier rang desquelles Facebook, cherchent à surfer sur la vague d'innovation pour prendre leur place dans un jeu monétaire chamboulé.



L'enjeu politique et géopolitique

Pour répondre aux besoins d'accessibilité et de simplification des systèmes financiers, Facebook a lancé une association, initialement appelée "Libra" renommée depuis "Diem".

Diem ambitionne de se positionner à la fois comme une nouvelle monnaie numérique et un nouveau système de paiement alternatif. Il vise une capacité de traitement de plusieurs milliers de transactions par seconde, tout en intégrant des portefeuilles numériques directement dans des applications grand public comme Messenger, WhatsApp ou encore Instagram. L'objectif presque explicite est de proposer aux utilisateurs, en particuliers hors OCDE, un système monétaire alternatif dans lequel ils pourraient avoir plus confiance que dans leurs systèmes locaux.

Ce projet a suscité la crainte de régulateurs soucieux de préserver la souveraineté des banques centrales en matière de politique monétaire : l'implication d'acteurs privés dans la réforme du système financier traditionnel — et en particulier de GAFA comme Facebook — représente un enjeu politique de taille. C'est la raison majeure pour laquelle, alors que la cryptomonnaie Diem devait initialement s'adosser à un panier de monnaies fiat (dollar, yen, euro, livres sterling), il repose aujourd'hui exclusivement sur le dollar américain. Cela permet à Diem d'avoir l'assentiment des régulateurs américains consacrant la puissance monétaire et la souveraineté des Etats-Unis.

Qualifiée de “cryptomonnaie de Facebook”, Diem ressemble davantage à une **monnaie privée qu’à une cryptomonnaie**. En effet, **Diem ne repose pas sur une Blockchain publique** : l’infrastructure fermée de Diem, accessible uniquement aux membres de l’association, limite la transparence et l’interopérabilité de cette monnaie. Sa gestion est dévolue à l’association Diem, bien que l’idée consiste à ouvrir progressivement l’infrastructure pour la rendre plus accessible. Diem a une proposition de valeur sensiblement différente de celle d’autres cryptomonnaies comme Bitcoin notamment sur les sujets relatifs à l’indépendance et l’incensurabilité.

Du point de vue juridique, là où Bitcoin avait pour objectif de faire changer les règles du jeu en proposant un système alternatif, Diem, à l’inverse, devra s’inscrire dans le cadre existant. C’est une conséquence directe de sa plus forte centralisation : Bitcoin n’a pas de responsable légal, c’est un protocole [open source](#), tandis que Diem a des responsables légaux désignés.

Diem sera un système financier qui devra donc respecter les législations et réglementations des pays et zones dans lesquels il opérera. A ce titre, Diem n’est pas aussi résistant et robuste que les cryptomonnaies face aux risques de censure ou de corruption du réseau qui peuvent exister dans certains pays.

Si Diem présente quelques points communs avec les cryptomonnaies dans son idée originelle de réforme du système financier traditionnel, il s’en éloigne par son fonctionnement, similaire à une monnaie privée numérique. Mais Diem aura eu le mérite de forcer une réaction de la part des États et des acteurs traditionnels envers les cryptomonnaies en général, qui n’ont pris conscience de la mesure du choc technologique et financier à venir qu’à l’aune des annonces de Facebook, en 2019. Cette réaction se traduit notamment par l’émergence du concept de MNBC, les Monnaies Numériques de Banque Centrale.

La réponse des banques centrales

Les Monnaies Numériques de Banque Centrale (MNBC, parfois appelées MDBC pour “Monnaies Digitales de Banque Centrale”) désignent des projets de monnaies émises par les banques centrales dans le monde numérique. Face à l’émergence des cryptomonnaies, les banques centrales ne veulent pas perdre la bataille de la compétitivité et de l’usage : elles ont besoin de rendre leurs monnaies programmables — chose impossible dans la finance traditionnelle — et d’améliorer leur interopérabilité — et donc permettre l’utilisation de la monnaie sur plusieurs plateformes et services.

Mais surtout : quel sera l’intérêt par rapport à l’existant ?

En théorie, une MNBC interbancaire (“de gros”) permet non seulement d’optimiser le système traditionnel d’une monnaie fiat - en réduisant, par exemple, les frais de transfert entre les banques commerciales et la banque centrale -, et de rendre programmables les transferts entre les acteurs de la finance traditionnelle. **Cependant, il n’existe encore aucun élément tangible pour assurer ces avantages.**

Concernant une MNBC “de détail”, son principal atout, du point de vue des banques centrales, serait un meilleur contrôle des politiques monétaires. En effet, la possibilité pour les citoyens d’avoir un compte directement à la banque centrale permettrait à ces dernières de court-circuiter les banques commerciales, qui agissent aujourd’hui comme des intermédiaires dans les politiques monétaires expansionnistes, et sont parfois critiquées pour cela. Une MNBC de détail permettrait donc par exemple de faire de la création monétaire directement dans le portefeuille de citoyens, ce qui pourrait permettre de stimuler la consommation. Elle pourrait même, puisque la monnaie serait programmable, flécher plus directement certaines dépenses, ou investissements, des citoyens pour renforcer l’impact des politiques monétaires. Une MNBC “de détail” aurait donc, sur le papier en tout cas, des conséquences qui dépasseraient la simple optimisation opérationnelle, et permettrait de nouveaux leviers d’action pour les politiques monétaires.

Cependant les mêmes critiques que celles formulées contre Diem s’élèvent pour relever les dangers que cela représenterait sur la vie privée. Le citoyen devrait, en plus de donner le contrôle sur nos données sociales et personnelles à des plateformes numériques, généralement américaines, donner le contrôle total sur sa liberté financière à une banque centrale. Et ce avec les dangers que cela comporte, comme on a pu le voir avec les affaires des lanceurs d’alerte : Edward Snowden aurait-il pu continuer de survivre dans un monde de MNBC ?

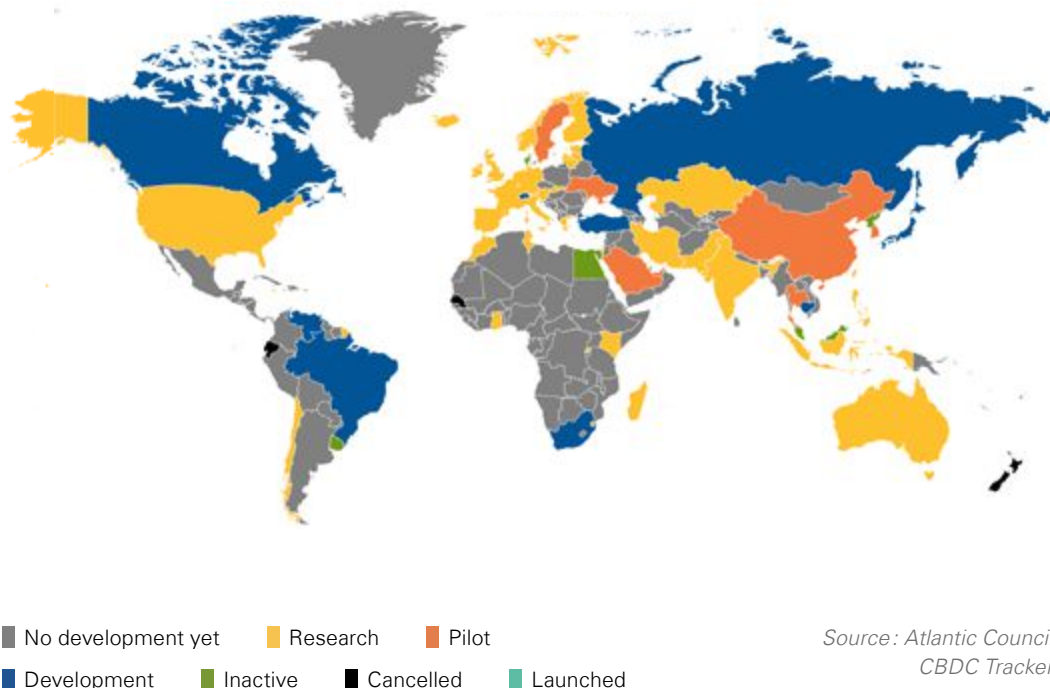
De plus, on peut penser qu’une MNBC sera moins compétitive qu’un stablecoin : son infrastructure centralisée ne lui permet pas de bénéficier des standards technologiques déjà établis sur les [Blockchains publiques](#), ni de leur écosystème - à savoir l’interopérabilité, la transparence et l’incensurabilité propres aux Blockchains. A l’heure actuelle, les projets d’expérimentation reposent principalement sur des infrastructures centralisées³², et sont donc censurables et programmables exclusivement par les acteurs gérant l’infrastructure.

De fait, une MNBC, telle qu’elle est envisagée aujourd’hui en France et Europe, rendra probablement plus optimal le système financier traditionnel utilisant de l’euro. Mais les banques centrales ratent probablement le vrai sujet : plutôt que de chercher à adapter leur infrastructure et leur monnaie à l’Internet de la Valeur (les cryptomonnaies), elles cherchent à s’approprier la technologie pour la recentraliser. D’une certaine façon, cela fait penser à la stratégie adoptée par la France avec le Minitel : se rassurer avec une infrastructure centralisée, et refuser de s’adapter à Internet avec les résultats que l’on connaît.

Résultats de l’analyse de la consultation publique de la Banque centrale, sur un Euro numérique. Par ordre de préoccupation :

La protection de la vie privée est la principale préoccupation du public et des professionnels (43 %), suivie de la sécurité (18 %), de la possibilité de payer dans toute la zone euro (11 %), sans frais supplémentaires (9 %) et hors ligne (8 %).

32. Voir les rapports de la Banque de France : “Monnaie digitale de banque centrale : une, deux ou aucune ?” ; “La monnaie digitale de banque centrale” et ses expérimentations menées depuis 2020



Au-delà des banques centrales, les Etats-Unis ont pris le parti de soutenir l'innovation, prenant de l'avance sur le terrain économique. Plusieurs groupes d'entreprises, financières ou non, ont déjà créé des stablecoins USD (Circle & Visa, Tether, ...). Cette prévalence des stablecoins USD semble transposer la suprématie du dollar dans le monde des cryptomonnaies. Actuellement, le dollar est en train de devenir, au détriment de l'euro, la monnaie "non-volatile" de référence pour les transactions dans le monde des cryptomonnaies : **sur un total de 85 milliards de dollars (en valeur) de stablecoins circulant sur la Blockchain Ethereum, 99% circule en tant que représentation du dollar américain** (USDT, USDC, BUSD, DAI, PAX...).³³

En conclusion, s'il est intéressant pour les banques centrales d'expérimenter sur les sujets MNBC, de

détail comme de gros, pour améliorer l'efficacité opérationnelle, les coûts, les délais, voire développer de nouveaux leviers de politique monétaire, cela ne doit pas se faire au détriment de la confidentialité et de la vie privée des citoyens. En parallèle, il est primordial d'adapter la monnaie à la finance de demain. Pour l'Europe et la BCE, il semble pertinent de concurrencer directement les cryptomonnaies sur leur propre terrain : il serait par exemple intéressant de pallier l'absence d'un stablecoin euro sur la Blockchain Ethereum. En créer un via une Banque Centrale, ou favoriser son émergence en stimulant l'innovation sur le terrain, permettrait de rendre l'euro programmable, et donc d'utiliser les services de la finance décentralisée.

33. <https://www.theblockcrypto.com/data/decentralized-finance/stablecoins>

Points clés à retenir

- 1 Les stablecoins présentent les avantages des cryptomonnaies par leur programmabilité, et ceux des monnaies fiduciaires par la stabilité de leur cours.
- 2 Pont entre la finance traditionnelle et le monde Blockchain, les stablecoins offrent plus de transparence, d'interopérabilité et de liquidité que les actifs traditionnels.
- 3 Diem repose sur un système centralisé, ce qui limite son caractère transparent, incensurable et interopérable propre aux cryptomonnaies comme Bitcoin.
- 4 Pour rester compétitive face aux cryptomonnaies, les banques centrales veulent rendre leur monnaie programmable et plus interopérable.
- 5 Une MNBC pourra optimiser le système traditionnel. Cependant elle repose sur une gestion centralisée et ne peut donc pas bénéficier de certaines caractéristiques propres aux cryptomonnaies.
- 6 Les États-Unis prennent de l'avance par rapport aux Européens en autorisant la création et l'utilisation de stablecoin USD.

De nouvelles infrastructures décentralisées existent et représentent des solutions innovantes pour proposer de nouveaux actifs tels que les stablecoins: la finance décentralisée (DeFi) d'une part, et le Web 3 d'autre part. Si ces deux mondes sont connexes par leur usage des cryptomonnaies, ils diffèrent par leurs fondements techniques: l'un vise plutôt à réformer les infrastructures actuelles, l'autre plutôt à créer les bases de nouvelles infrastructures financières ouvrant la voie d'un Internet plus ouvert, plus libre et décentralisé.

3.



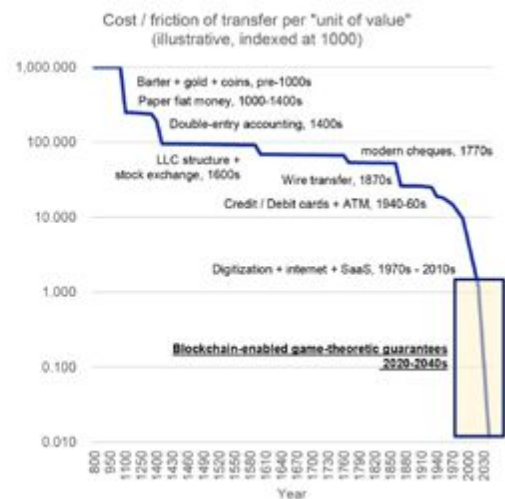
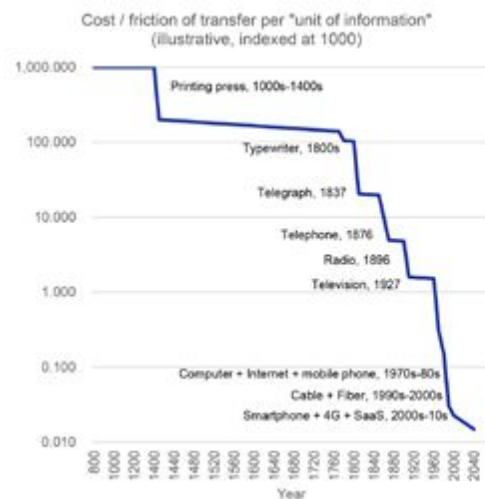
DeFi et Tokenisation des actifs, l'avènement d'une nouvelle industrie financière

La DeFi : l'Internet de la valeur & "Wall Street API"

La Finance Décentralisée (abrégiée **DeFi** pour Decentralized Finance en anglais) est un **système financier alternatif** fondé principalement sur les **Blockchains publiques** et les **cryptomonnaies** (et plus généralement les **cryptoactifs**).

En remettant en perspective l'apparition de cette technologie, **la DeFi s'inscrit pleinement dans la continuité des innovations financières** qui pourraient se résumer à la quête d'une réduction des coûts associés à un transfert financier.

Comme l'explique le schéma ci-dessous, les coûts de transferts associés à l'information ont été réduits par les innovations successives et accélérées avec l'apparition d'Internet, puis du smartphone avec la 4G puis la 5G à ce jour. Le raisonnement est sensiblement équivalent avec la valeur. La vague actuelle détaillée dans ce document représente la nouvelle grande innovation financière.



Source : Maple Leaf Capital

Cette réduction drastique des coûts de transfert de valeur est également liée à une réduction des délais nécessaires pour proposer de nouveaux services financiers. En effet, la DeFi repose sur une infrastructure transparente et ouverte.

La transparence des données facilite les processus et renforce la confiance des parties prenantes en évitant la multiplication des acteurs nécessaires pour effectuer une opération financière. L'ouverture et l'accessibilité à ces nouveaux services proposent un nouveau paradigme comparé au système financier actuel orienté avant tout vers la protection des investisseurs particuliers.

Institutions financières	Fintech	Finance décentralisée
Ouvrir un compte ~ jours	Ouvrir un compte ~ heures	Ouvrir un compte ~ secondes
Investir dans un fond ~ jours	Investir dans un fond ~ heures	Investir dans un fond ~ secondes
Constituer un produit bancaire ~ années	Constituer un produit bancaire ~ mois	Constituer un produit bancaire ~ jours

Source : Blockchain Partner by KPMG

La DeFi est développée en parallèle du système financier existant, qu'elle complète et concurrence à la fois. Elle se distingue du système financier traditionnel par trois caractéristiques principales :

- Elle est **nativement numérique** ;
- Elle fonctionne sur des **infrastructures décentralisées** ;
- Elle est **ouverte à tous**, aussi bien en termes d'usage et de consultation que de participation à sa construction.

La DeFi se caractérise aujourd'hui par sa **modularité** : ce système se compose de **multiples services** centrés sur des **besoins spécifiques** ([échange de cryptoactifs](#), usage de [cryptoactifs stables](#) (stablecoins), [prêts](#), produits dérivés, fonds d'investissement, [marchés prédictifs](#)...) qui se **combinent** souvent les uns avec les autres.

Les primitives financières exposées existent déjà dans le monde financier traditionnel. Cependant, l'infrastructure fait que l'automatisation des logiques financières devient un élément clé, tels des Legos qui s'imbriquent entre eux de manière automatisée et sans tiers. C'est le principe de [composabilité](#).

Ce secteur entend répondre à un certain nombre de limites du système financier actuel (inégalités

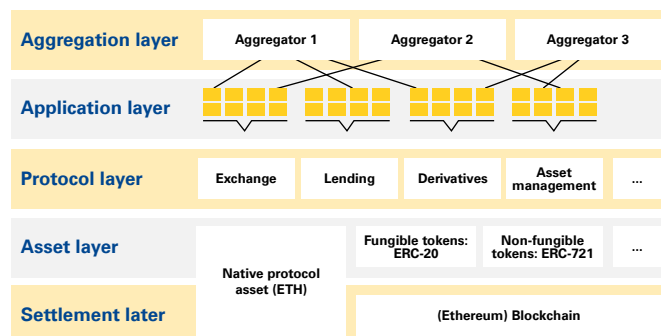
d'accès, risques de contrepartie, transparence perfectible, frais importants...) en **créant les fondations d'un nouveau système plutôt qu'en apportant des améliorations incrémentales à l'existant**.

Le même raisonnement en couche que pour l'Internet peut s'opérer :

- En effet, un protocole Blockchain de type Ethereum constitue la première couche de ce schéma autrement dit [Layer 1](#), fondation de tout le système comme le protocole TCP/IP l'est pour Internet
 - L'infrastructure est donc découplée des applicatifs. La sécurité de cette infrastructure étant dévolue à des entreprises spécialisées et les applicatifs le fruit d'entreprises ou projets dont l'incarnation pour le web serait Facebook, Netflix ou Amazon. La sécurité de cette couche réside dans les mécanismes économiques et de théorie des jeux induits par l'algorithme de [consensus](#) et de la rémunération en cryptoactifs. Par exemple, sur la Blockchain Bitcoin vue précédemment, les acteurs spécialisés s'appellent des "mineurs" et sont rémunérés en bitcoins pour fournir de la puissance de calcul et sécuriser le réseau.

- La couche “Asset Layer” sont les standards utilisés pour tokeniser les actifs tangibles ou intangibles c’est à dire la faculté à créer des stablecoins ou tout actif tokenisé sur Ethereum par exemple
- La couche protocolaire représente les primitives financières exposées dans la partie suivante (prêt, emprunt, échange, etc...)
- Les applicatifs et la couche d’agrégation incarnent les interfaces propres à un protocole ou intégrant différents applicatifs. Ce sont les interfaces visuelles avec lesquelles l’utilisateur interagit

Une entreprise peut donc proposer son propre applicatif financier ou s’interfacer avec celui d’un tiers. Cependant, il est peu probable qu’à terme chaque entreprise dispose de son propre protocole ; des applicatifs s’ancreront sur une poignée de protocoles déjà existants et fonctionnels.

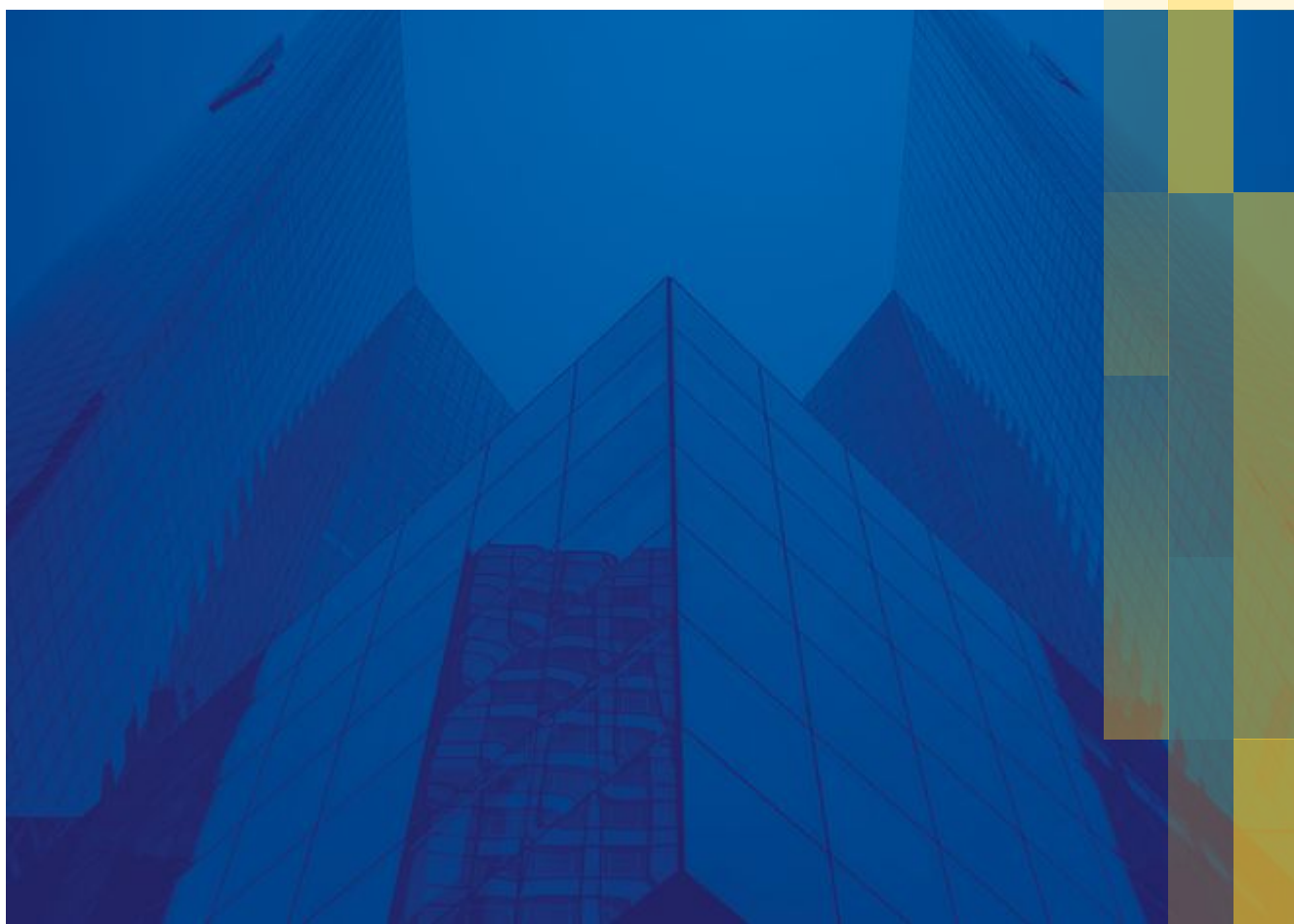


Source : Fabien Schär pour la FED Saint Louis

Pour reprendre la formule de MapleLeaf, l’écosystème tel qu’il se crée prend la forme d’un “Wall Street API” abattant les barrières à l’entrée d’un univers financier **dans son entièreté**.

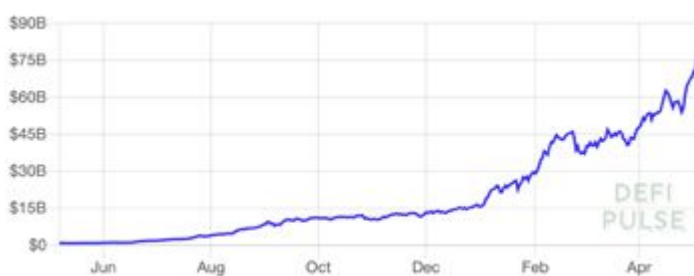
Quelques unes des particularités suivantes se dégagent avec son émergence :

- La transformation et parfois même la disparition d'intermédiaires pour des raisons techniques paraît inéluctable (transformation des dépositaires par exemple).
- La **composabilité** et l'émergence de nouvelles caractéristiques liées au caractère numérique et programmable comme la réhypothécaction du capital ou les *flash-loans*.
- L'accessibilité pour les institutions et les particuliers à une infrastructure commune. Seule changera l'interface graphique adaptée aux besoins de chacun.
- Un particulier autant qu'un professionnel peut tantôt être utilisateur et fournisseur de service avec son capital pour maximiser le rendement.
- Le secteur nécessitant une connaissance approfondie de la partie technique, tout acteur financier devra posséder les compétences d'audit et d'évaluation de cryptoactifs en interne.
- Certains risques inhérents à l'innovation demeurent (risque systémique, méconnaissance des produits proposés...) mais la structuration de cette nouvelle industrie devrait permettre de rapidement dépasser ces limites.



La DeFi, un écosystème en cours de structuration

À début Mai 2021, 78 milliards de dollars sont gérés par les [smart-contracts](#) et applicatifs de la DeFi. La progression est de x75 par rapport à l'été 2020. Ce montant représente une goutte d'eau relativement à la finance traditionnelle, mais sa croissance n'est pas négligeable.



Total Value Locked in Defi ecosystem (Source: Defi Pulse)

Il est probable que deux écosystèmes parallèles se constituent avec l'institutionnalisation progressive du secteur :

- Un écosystème d'innovation ouvert dit « pirate » utilisé seulement par les connaisseurs et professionnels, où l'innovation sera poussée à son maximum.

- En parallèle, un autre écosystème reprendra les mêmes codes (sur la même infrastructure ou non) mais sera conforme au prix de compromis sur l'incensurabilité, notamment en matière de KYC.

Ce monde sera irrigué des innovations techniques et économiques du premier, imposant aux régulateurs et pouvoirs publics une adaptation nécessaire d'un droit séculaire inadapté.

Il pourra être l'infrastructure de la tokenisation des actifs traditionnels que l'on connaît déjà : actions, obligations, dettes.

Cette partie balaye l'état de l'écosystème ouvert, dit pirate, avant d'attaquer ce que pourrait être le second dans le prochain paragraphe.

L'écosystème d'applicatifs de la DeFi se décompose comme suit :

Des solutions de sécurisation et de gestion des cryptoactifs pour les particuliers et les entreprises.

Des plateformes d'échanges de jetons décentralisées proposant un modèle de [market making automatisé](#).

Des protocoles d'assurance donnant accès à une couverture contre la défaillance technique et économique de projets.

Des interfaces agrégeant des services de la Finance Décentralisée adaptées à la structure et aux besoins de chacun des acteurs. Cela se rapproche de l'application bancaire qui fait état de nos comptes courants particuliers et propose des solutions d'investissements.

Des applicatifs agrégeant le capital et appliquant des stratégies automatisées pour identifier le meilleur rendement sous forme de hedge-Fund automatisés.

Des projets dit "oracles" créant des réseaux distribués afin d'injecter une donnée vérifiée de prix d'un actif externe au monde Blockchain ou toute information requise par une application financière.

Des stablecoins, représentations de monnaies fiduciaires dans le monde Blockchain (voir partie 2).

Des dérivés sous forme jetonisée que ce soit pour l'or, des actions, ou tout titre financier existant dans la finance traditionnelle faisant déborder du seul cadre des cryptomonnaies et autres tokens la DeFi.

Des organisations décentralisées votant sur la gouvernance et l'évolution des projets.

Des marchés monétaires permettant de prêter et emprunter des cryptomonnaies sans tiers fonctionnant avec un mécanisme de [sur-collatéralisation](#).

Des représentations de Bitcoin sous différentes formes circulant dans les différents applicatifs pour un total à début Mai 2021 de 12,3\$ Mds de bitcoins soit 215134 bitcoins.

Des jetons de gouvernance conférant une faculté de voter sur le devenir d'un projet, et pouvant donner accès à la capture d'une partie des frais générés par un protocole, permettant de modéliser la valeur des protocoles générateur de cash flow. Cela rompt avec les levées sous forme d'ICO dont la résultante était un jeton donnant exclusivement un droit d'usage.

L'explosion cambrienne de projets et de synergies entre eux a un effet d'augmentation de la liquidité de la plupart des actifs, de complexification et d'interdépendance des projets.

En effet, la DeFi sort peu à peu de la boîte de pétri pour proposer des primitives nouvelles augmentant celle de la finance traditionnelle :

- Création de protocoles créant des tranches de risque (Tranching).
- Protocoles créant des taux d'intérêts fixes (Fixed Interest Rate).

- Création d'indices intelligents avec des stratégies de trading automatisées entre les actifs.

- Une avance jetonnée sur rendement créant un titre de dette qui se rembourserait avec le rendement généré automatiquement par un service.

Néanmoins, l'ambition de certains projets dépasse le seul cadre DeFi. Pour illustrer l'intérêt de suivre l'émergence de cette nouvelle infrastructure financière, nous allons analyser deux des plus gros projets de la DeFi : [Aave](#) et [Uniswap](#).

Aave

Aave est un marché monétaire permettant aux utilisateurs de prêter et/ou d'emprunter des crypto-monnaies en pair à pair, de manière sécurisée et décentralisée.

Ce protocole est construit sur la technologie Ethereum.

Les entreprises et particuliers peuvent générer un rendement passif sans risque de contrepartie et sans intermédiaire, sans besoin d'emprunter.

D'autre part, des acteurs tiers peuvent proposer un marché monétaire construit sur celui d'AAVE. C'est déjà le cas pour CrescoFin et APYWine qui vont lancer leur service à partir du protocole AAVE. (cf Schéma en couches)

A terme, une banque commerciale pourrait octroyer une ligne de crédit non-collatéralisée en stablecoins ou dans un autre actif au prix d'une mesure du risque sur la capacité à rembourser et d'un contrat dans le "monde réel". AAVE deviendrait donc l'infrastructure bancaire de crédit pour cet acteur en parallèle du *legacy system*.

L'appétit de l'équipe AAVE ne se borne pas à la sphère crypto :

- Ils ont obtenu une licence EMI permettant d'opérer avec des monnaies traditionnelles directement devenant d'eux mêmes une rampe d'accès vers les services financiers de la DeFi et court-circuitant les acteurs traditionnels.
- Ils ont un projet de carte de crédit pour dépenser directement ses cryptomonnaies en monnaie fiduciaire.
- La solution de conservation hardware et software Taurus destinée aux banques permet d'accéder aux services proposés par AAVE.

Indicateurs clés :

Date de création : EthLend (2017)

Total Value Locked : \$10,57 Mds (06/05/21)

Valorisation : \$5,8 Mds (06/05/21)

Investisseurs externes : Three Arrows Capital, ParaFi Capital, DTC Capital, Defiance Capital, Carnaby Capital

Uniswap

Uniswap est un service d'échange décentralisé entre tokens. L'innovation réside dans le concept de [market making automatisé](#), et l'absence de tiers centralisateur permettant l'échange (d'où les appellations suivantes : [DEX](#) pour Decentralized Exchange et AMM pour Automated Market Maker).

Les échanges sont rendus possibles par des dépôts de liquidités par des utilisateurs qui souhaitent rentabiliser leur capital (frais perçus à chaque échange).

Uniswap concurrence d'ores et déjà, en termes de volume, des plateformes d'échanges centralisées comme Coinbase ou Kraken. Le protocole permet d'échanger des tokens [synthétiques](#) d'options ou d'actions. C'est un projet essentiel de la finance décentralisée, et de la finance de demain...?

Indicateurs clés:

Date de création : 2018

Total Value Locked: \$ 7,29 Mds (06/05/21)

Volume d'échanges cumulés depuis

le lancement: \$120 Mds

Valorisation : \$22 Mds

Investisseurs externes: Andreessen Horowitz,

Parafi Capital, A_capital ventures



L'hybridation entre la finance traditionnelle (TradFi) et la DeFi

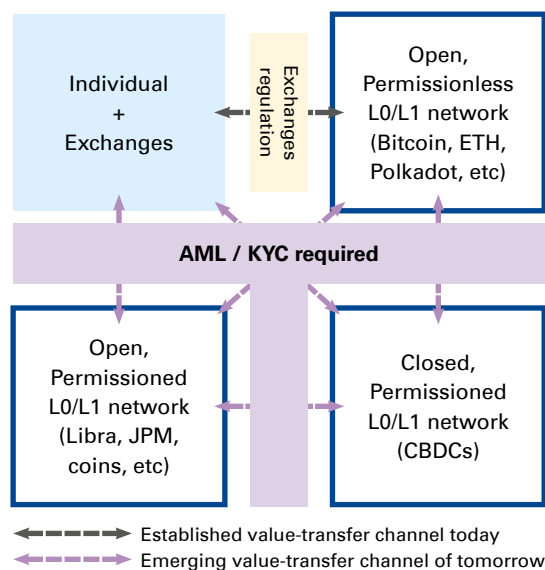
Les différentes études et projections font état d'un potentiel de marché de plusieurs milliers de milliards de dollars sur la tokenisation des actifs.

L'édiction au niveau national et supranational d'une régulation (loi Pacte en France, et réglementation MiCa au niveau européen), et des acteurs centralisateurs par essence de type GAFA vont probablement pousser à la création de :

- Réseaux privés similaires à Diem
- Standards sur les réseaux ouverts où le KYC

et la création de listes blanches seront la norme entre autres, et où toute décision de justice sera techniquement applicable avec le gel de fonds par exemple (chose impossible en l'état)

Les réseaux pourront communiquer entre eux et le KYC deviendra une condition sine qua non à l'entrée et à la sortie pour faire circuler les actifs comme l'illustre le schéma ci-dessous :



(Source: Maple Leaf)

Des projets vont dans ce sens avec la Société Générale qui a réalisé une expérimentation sur une obligation à 100 millions d'euros sur la Blockchain Ethereum ou travaille à un [framework](#) CAST (Compliant Architecture for Security Token) de tokenisation des actifs avec la société SG Forge.

Dans cette même logique, Euronext a participé à une levée de fonds en capital de la plateforme Tokeny ayant le même objectif avec un standard proposé sur Ethereum.

Les avantages de la tokenisation des actifs traditionnels sont multiples :

- Rendre les actifs plus liquides
- Créer un marché secondaire aisément accessible, réel besoin pour des actifs non-cotés
- Bénéficier d'applications tierces sur lesquelles le jeton peut circuler (marché monétaire, assurances)

En guise d'exemple pour le secteur de l'immobilier, il devient en pratique possible de représenter sous forme de jetons la propriété de fonds ou de biens directement. Il en résulte une fragmentation simplifiée des parts du fonds, la possibilité de les céder sur un marché secondaire, ou de les placer en [collatéral](#) pour emprunter d'autres parts etc.

Points clés à retenir

- 1 La DeFi propose une nouvelle infrastructure financière.
- 2 La DeFi est caractérisée par sa décentralisation, sa composabilité, son accessibilité et sa flexibilité.
- 3 L'écosystème DeFi gère et automatise la gestion de la valeur de 78\$ Mds (au 04/05/21) et propose des services sur toutes les verticales financières existantes (avec des projets comme Aave sur le prêt et l'emprunt ou encore Uniswap pour du change).
- 4 La DeFi commence déjà à s'interfacer avec la finance traditionnelle en proposant une hybridation de services avec l'infrastructure DeFi.

4.



Web 3, une nouvelle itération d'Internet

Les limites du Web 2

«**Content is King**» : le contenu est roi. Lorsque Bill Gates assène cette phrase en 1996, il désigne, selon lui, la véritable valeur produite sur Internet à l'ère du Web 2. Et à raison : première forme du web social et interactif, le Web 2 se caractérise par la création d'une multitude de contenus et applications animées par les internautes eux-mêmes : blogs, streaming, réseaux sociaux, mail ou encore messagerie instantanée... Il s'agit aujourd'hui de la forme majoritairement connue d'Internet.

Si les propos de Bill Gates se sont avérés visionnaires, la décentralisation des services et l'autonomie des créateurs de contenu ne sont pas des aspects dont le Web 2 permet de bénéficier à l'heure actuelle. **Au contraire, la dynamique de l'économie numérique tend vers toujours plus de centralisation.** À titre d'illustration, la décennie 2010 n'a vu émerger aucun nouveau géant du numérique capable de rivaliser avec les leaders du secteur. En effet, l'architecture actuelle du Web ne favorise pas l'arrivée de concurrents : le marché des applications se réduit, en l'occurrence, à Google et Apple. L'approbation de ces acteurs est donc nécessaire pour répertorier une application mobile dans leurs magasins respectifs, ce qui constitue un frein certain à la concurrence et l'innovation.



Le Web 3 comme révolution d'Internet

À cela, une nouvelle vision du web s'oppose : le Web 3. Ce dernier représente un **changement radical dans la manière de percevoir et de valoriser Internet**, conçu pour être profitable aux utilisateurs en priorité, et non plus aux entités centralisées. Son *ethos* se retrouve dans les architectures décentralisées élaborées dès les années 1990 comme la Blockchain, les primitives des cryptomonnaies telles que les protocoles open-source et solutions libres (noms de domaine décentralisés comme BitDNS, etc.), mais également la finance décentralisée, comme vu précédemment.

Plus concrètement, le Web 3 repose sur trois idées sous-jacentes : une infrastructure fiable et sécurisée, s'affranchir des intermédiaires, et rendre aux utilisateurs la souveraineté de leurs données personnelles. L'objectif consiste donc à créer un modèle davantage collaboratif entre les internautes au moyen de la cryptographie, la connectivité P2P, des interopérabilités de confiance, ainsi qu'un stockage de données décentralisé grâce aux *dApps* (*decentralized applications*).

Finalement, le Web 3 s'apparente à l'étape finale dans l'évolution de l'Internet du contenu. Comme Messari l'analyse dans son rapport *"Crypto Theses for 2021"*³⁴, on distingue trois ères successives :

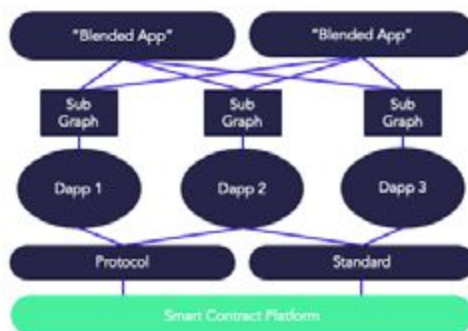
- **L'ère de la distribution** : dans un premier temps, les consommateurs recherchent un moyen qui centralise gratuitement un contenu donné sur Internet, et confère une large audience aux créateurs avec des plateformes comme Medium.
- **L'ère de l'abonnement** : dans un second temps, les créateurs individuels se transforment en marque avec des plateformes dédiées comme Spotify - ce qui leur permet d'obtenir une rémunération par de l'abonnement et de la publicité - bien que toujours très centralisées.
- **L'ère de la possession** : les créateurs deviennent pleinement propriétaires du contenu qu'ils produisent. Les plateformes travaillent davantage en synergie avec les créateurs de contenu par des mécanismes incitatifs et rémunérateurs (faible commission, rémunération proportionnelle au succès d'une oeuvre, distribution de NFT, etc.)

The Web3 Revolution is Built on Open Standards and Protocols

The Closed Platforms of Web 2.0



The Web 3.0 Open Standard



The Web3 Revolution is Built on Open Standards and Protocols - Messari

[Comme illustré sur l'image ci-dessus, le Web 2 se caractérise par des réseaux fermés, alors que le Web 3 contient plateformes ouvertes prenant la forme de briques composables].

Cette présentation du Web 3, de ses prémices et de ses objectifs, permet d'introduire à présent les différents services proposés par ce nouveau modèle, ainsi que leur plus-value par rapport au Web 2.

³⁴. *Crypto Theses for 2021 - Messari*



Les questions du stockage décentralisé de données, du transfert de valeur sans intermédiaire, ou encore la préservation des informations personnelles sont des problématiques clés que le Web 3 vise à résoudre. Les technologies prétendant y répondre seront donc présentées: IPFS, Filecoin, les NFT, ZKP...

Les différents services du Web 3

IPFS et Filecoin

Avant toute chose, il faut comprendre que le **Web 3 n'a de sens que sur une infrastructure fiable sur laquelle faire reposer ces services. En l'occurrence, cette infrastructure pourrait être IPFS** (*InterPlanetary File System*). Protocole décentralisé, IPFS se caractérise par son objectif ambitieux: se substituer au protocole mondial HTTP (*Hypertext Transfer Protocol*).

Concrètement, IPFS permet d'accéder à du contenu grâce à un identifiant unique attribué à chaque donnée, et non plus grâce à la localisation de celle-ci. Cela signifie que **l'échange de fichiers se fait en pair-à-pair: l'utilisateur ne prend plus le risque de perdre l'accès aux données en cas de dysfonctionnement ou de censure d'un serveur centralisé**. De fait, IPFS a pour avantage de

fragmenter l'information, et donc de la rendre plus résiliente et résistante à la censure.

Or, IPFS doit instaurer des logiques économiques pour inciter les utilisateurs à utiliser l'infrastructure, et récompenser les personnes qui maintiennent le réseau. En ce sens, **de nouveaux systèmes de paiement décentralisés se sont développés sur IPFS. Le plus notable d'entre eux, Filecoin, est évalué à 60 milliards de dollars³⁵**, contre 8 milliards de dollars pour des entreprises de l'écosystème traditionnel comme Dropbox.

L'objectif de Filecoin est de créer un marché de stockage distribué. Concrètement, cela signifie que certaines personnes ayant de grandes capacités de stockage pourront louer leurs espaces drive

sous-utilisés. Un tel service serait complémentaire de la Blockchain, dès lors que les transactions se réaliseraient sur un registre fiable et sécurisé comme Ethereum.

Protocol Labs, l'entité créatrice de Filecoin, estime que les coûts de stockage seraient 15 fois moins chers qu'un stockage standard sur Amazon, par exemple - ce qui représente un atout indéniable pour les consommateurs. Cela pose également un avantage d'un point de vue stratégique : les serveurs ne sont plus centralisés dans un

pays donné comme les Etats-Unis ou l'Union Européenne, ce qui permet donc de s'affranchir de certaines problématiques juridiques.

IPFS et Filecoin sont donc deux protocoles complémentaires conçus pour stocker de la donnée de manière décentralisée et sécurisée, et devenir tantôt utilisateur, tantôt fournisseur de service. Tous deux ouvrent la voie vers un Web incensurable.

Les NFT (Non Fongible Tokens)

Au-delà du stockage de données, **le Web 3 rend possible la représentation et la programmabilité d'un actif tangible ou intangible comme un titre, un fragment de propriété d'un immeuble, une obligation, une action d'une entreprise, ou encore un joueur de football.** C'est ce que l'on appelle la tokenisation. Il existe de nombreux types de tokens, comme nous l'avons vu précédemment.

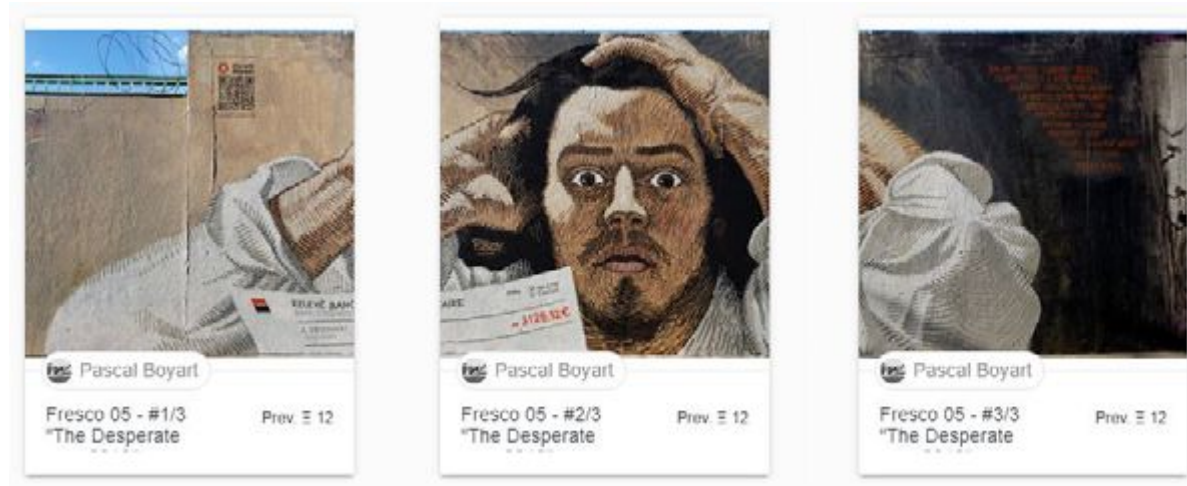
Parmi les plus singuliers d'entre eux, les NFT (*Non Fongible Tokens*) présentent la particularité, comme leur nom l'indique, d'être non fongibles et donc rares. Ils répondent à plusieurs promesses : l'unicité en raison de leur caractère unique

et vérifiable sur Blockchain ; la permanence – un NFT encapsule un lien ou une donnée textuelles comme un message, une image, une signature, une musique etc. ; la programmabilité – la valeur numérique peut être transférée sans tiers de confiance par le biais de smart-contracts, et utilisée en guise de collatéral ; et la propriété - la Blockchain sert de preuve de contrôle.

La représentation numérique d'un actif rare trouve de nombreuses applications : l'art avec l'artiste Pascal Boyart qui vend, sur la plateforme OpenSea, des titres de propriété numérique sur ses oeuvres ; **le gaming** avec Sorare qui crée un jeu de Fantasy Football

dont les cartes sont représentées par des NFT ; **le luxe** avec Arianee qui représente des montres sous forme de NFT... Les NFT s'inscrivent potentiellement dans d'autres secteurs que l'on ne soupçonne pas encore, sachant qu'un lien avec le monde physique n'est pas toujours nécessaire.

Dans le cas d'un NFT lié à une oeuvre d'art - comme celles de Pascal Boyart par exemple -, celui-ci devra être accompagné d'une image représentant la partie de l'oeuvre à laquelle il correspond, d'un titre, d'une description, d'un prix, d'un historique de propriété, ainsi que du nom du propriétaire actuel.



ZKP (Zero-Knowledge Proof)

Mais le Web 3 ne se limite pas au stockage de données ou au transfert de valeur. La **préservation des données personnelles** représente un enjeu crucial à l'ère des plateformes centralisées. En effet, le système actuel implique la transmission d'un certain nombre d'informations pour accéder à un service (patronyme, date de naissance, adresse mail etc.). Cela pose des problèmes de confidentialité, voire de risque d'usurpation d'identité en cas de perte de données liées aux failles de sécurité du système informatique, comme nous l'ont montré les scandales récents liés à des pertes de données sensibles : une agence gouvernementale américaine a été victime d'une attaque de ses serveurs, dont il a résulté un vol massif de données personnelles³⁶.

Le Web 3 propose donc un modèle alternatif à l'authentification centralisée : la *Self Sovereign Identity (SSI)*. L'objectif de la SSI est de conférer aux individus une plus grande maîtrise de leur identité numérique par des technologies comme ZKP (*Zero Knowledge Proof*). En principe, il ne sera plus nécessaire de révéler des informations confidentielles pour accéder à une plateforme, mais seulement de prouver la concordance d'une information. Par exemple, au lieu de donner sa carte d'identité, avec toutes ses informations sensibles, pour acheter de l'alcool, il s'agira simplement de prouver, sans le révéler, que son âge répond positivement à la question "*Est-il supérieur à 18 ?*".

Concrètement, la technologie ZKP consiste à résoudre conjointement des problématiques de confiance et de confidentialité, en remplaçant le partage de données par la preuve de leur possession. L'intérêt se présente notamment pour les entreprises soucieuses de préserver des données confidentielles, tout en garantissant un meilleur accès à leurs services. A titre d'exemple, JPMorgan utilise ZKP pour préserver la confidentialité du montant d'une transaction sur Blockchain³⁷, et RCI Bank and Services expérimente ces technologies pour anonymiser les données de géolocalisation des véhicules pour être conforme aux dispositions du RGPD³⁸.

³⁶ [Cybersecurity Resource Center](#)

³⁷ [JPMorgan Adds Privacy Features to Ethereum-Based Quorum Blockchain](#)

³⁸ [Les ZKP pour anonymiser et exploiter les données de véhicules](#)

³⁹ [Web3 FL15: What is Web3?](#)

Conclusion : la re-décentralisation d'Internet

En définitive, le modèle économique du Web 3 perpétue le "règne du contenu" sur Internet, mais transfère le contrôle aux créateurs par des outils décentralisés et sécurisés. En ce sens, le Web 3 révolutionne le stockage et le partage de données en combinant un plus grand accès à l'information, et une plus grande protection de la vie privée. Démocratisation des noms de domaine (*Unstoppable Domains*), monétisation de ses données personnelles (*Ocean Protocol*, *Streamr*, *Numerai*), partage de contenu audio en pair-à-pair (*Audius*)⁹⁹... Si l'écosystème des cryptomonnaies n'est qu'un sous-ensemble au sein de ce nouveau modèle, il contribue largement à en accélérer la marche.

Points clés à retenir

- 1 Le Web 3 apporte un changement radical dans la manière de percevoir et de valoriser Internet, conçu pour être profitable aux utilisateurs en priorité, et non plus aux entités centralisées. Il révolutionne le stockage et le partage de données en combinant un plus grand accès à l'information et une plus grande protection de la vie privée.
- 2 Il repose sur trois idées sous-jacentes : une infrastructure fiable et sécurisée, la désintermédiation de la gestion des données, et la souveraineté des utilisateurs sur leurs données et leur identité numérique. Cela nécessite de nouveaux fournisseurs de services capables d'atteindre ces objectifs.
- 3 IPFS est un protocole décentralisé qui permet d'accéder à du contenu grâce à un identifiant unique attribué à chaque donnée. L'échange de contenu se fait en pair-à-pair : l'utilisateur ne prend plus le risque de perdre l'accès aux données en cas de dysfonctionnement ou de censure d'un serveur centralisé.
- 4 Le Web 3 ne se limite pas au stockage de données ou au transfert de valeur. La préservation des données personnelles représente aussi un enjeu crucial.
- 5 Il propose un modèle alternatif à l'authentification centralisée : la Self Sovereign Identity (SSI). L'objectif de la SSI est de conférer une plus grande maîtrise de son identité numérique par des technologies comme ZKP (Zero Knowledge Proof).
- 6 La technologie ZKP consiste à résoudre conjointement des problématiques de confiance et de confidentialité, en remplaçant le partage de données par la preuve de leur possession.

Conclusion

Internet a transformé l'information comme la Blockchain et les cryptoactifs transforment la valeur.

Tout d'abord, Bitcoin s'institutionnalise et s'apparente à un actif protéiforme à part entière pour des entreprises souhaitant diversifier leur trésorerie autant que pour des lanceurs d'alertes en quête d'un système de paiement non censurable.

Les stablecoins, de leur côté, pesant pour \$80 Mds (Mai 2021), deviennent la rampe d'accès pour les particuliers et les professionnels vers l'écosystème Blockchain pour opérer avec une représentation des monnaies fiduciaires sous forme tokenisée.

Ensuite, la finance décentralisée propose une nouvelle infrastructure financière automatisée, transparente et dont les fondements auront des conséquences majeures sur la finance et les intermédiaires.

Tout cela s'inscrit dans une perspective plus globale, celle du Web 3, une tentative de déconcentrer l'Internet du quasi-monopole des GAFAM avec des réseaux distribués et une monétisation associée que permettent les cryptoactifs. Entreprises et particuliers peuvent autant être utilisateurs que fournisseurs de services ouvrant ainsi la voie à de nouvelles sources de revenus.

En prenant un peu de recul, on s'aperçoit que les dynamiques à l'œuvre sur la gestion de la valeur sont similaires à celles qui ont accompagné l'émergence d'Internet. Pour les entreprises donc, la question ne semble plus être "pour ou contre les cryptoactifs", tout comme la question "pour ou contre Internet" aurait pu sembler désuète dans les années 2000.

La question qu'il faudrait se poser semble être "comment s'adapter" ou encore "comment tirer le meilleur des cryptoactifs".

Comme souvent, les Etats-Unis font office de laboratoire prometteur: déjà **14% des américains possèdent des cryptomonnaies**, avec **un investissement moyen compris entre 8,5k et 11k USD⁴⁰** (pour les cryptos principales). Par ailleurs, les deux tiers des américains indiquent vouloir en apprendre plus, ou même envisagent d'acheter bientôt des cryptomonnaies, ce qui laisse présager de bonnes perspectives d'évolution pour ce marché. **Coinbase, début mai 2021, était l'application la plus téléchargée aux Etats-Unis**, devant les géants Tik-Tok, Youtube, Facebook, Instagram etc. **Pour les institutions financières, il devient clair que le risque de ne rien faire et de voir le train passer est plus fort que celui de construire une stratégie claire pour agir dans cet écosystème naissant.**

Blockchain Partner by KPMG avec son équipe dédiée sur ces sujets propose une vision généraliste incluant les dimensions stratégiques, techniques, juridiques, et d'autres pour aider au mieux nos clients à s'acculturer, s'adapter et à se transformer.

40. <https://www.gemini.com/state-of-us-crypto>

Auteurs



Catherine Philippe
Associée Blockchains
& Cryptos

Catherine est Associée KPMG spécialisée sur les technologies du Secteur Financier. Elle a une expérience de plus de 20 années du conseil et de l'audit dans ce secteur. En charge de l'Offre Blockchain et Crypto de KPMG France depuis 2017, elle développe l'offre de services liée à ces technologies pour les clients de KPMG France.



Alexandre Stachtchenko
Directeur Blockchains
& Cryptos

Alexandre est un entrepreneur franco-canadien, fort de 6 ans d'expérience dans le secteur crypto. Cofondateur de Blockchain France en 2015, devenu Blockchain Partner en 2017, leader français du conseil & développement technique sur les technologies blockchain & crypto, il est aussi cofondateur & membre du board de l'ADAN, l'association des professionnels français du secteur crypto en France.



Claire Balva
Directrice Blockchains
& Cryptos

Claire est la cofondatrice de la startup Blockchain Partner, leader français de l'accompagnement sur les blockchains et cryptoactifs. Co-auteur du livre «La Blockchain décryptée» paru en 2016, elle s'emploie à démocratiser la blockchain à l'occasion d'événements grand public, de conférences et d'interviews dans différents médias.



Stanislas Barthélémi
Analyste Blockchains
& Cryptos spécialiste
des sujets DeFi



Charles Aubert-Couturier
Project Lead Blockchains
& Cryptos



Salomé Tibloux-Galas
Cheffe de projet
Blockchains & Cryptos



Elodie Messéant
Analyste Blockchains
& Cryptos

5



Lexique

Aave

Aave est un protocole & une application permettant aux utilisateurs de prêter et/ou d'emprunter des cryptomonnaies sans intermédiaire. Ce protocole est construit sur la technologie Ethereum.

Blockchain

Une Blockchain est une technologie qui permet de stocker et de transmettre de la valeur numériquement. Il s'agit d'une base de données infalsifiable, transparente et décentralisée qui stocke un ensemble de transactions dont chacun peut vérifier la validité.

Blockchain publique

Une Blockchain publique est une Blockchain qui ne nécessite pas d'autorisation pour y accéder (« *permissionless Blockchain* »). N'importe quel utilisateur peut lire le registre, et participer au bon fonctionnement du réseau sous réserve de respecter les règles de consensus. Une Blockchain publique se caractérise par sa résilience et sa forte décentralisation.

Blockchain privée

Une Blockchain privée est une Blockchain qui repose sur un réseau privé, et qui nécessite une autorisation pour y accéder (« *permissioned Blockchain* »). Elle permet aux entreprises de garantir un certain niveau de sécurité, de confidentialité, de conformité et de performance. Seuls des utilisateurs prédéfinis ont le droit de lire le registre, et de participer au fonctionnement du réseau et d'en modifier les règles d'utilisation. Le protocole Proof-of-Authority est souvent utilisé, une Blockchain privée n'implique pas nécessairement l'utilisation d'actifs numériques.

Blockfi

BlockFi est une plateforme de dépôt en cryptomonnaies et de prêt en fiat. A la manière d'un fond d'investissement, elle permet aux utilisateurs de générer des intérêts en déposant leurs cryptomonnaies sur la plateforme mais également d'emprunter en monnaie fiat collatéralisés avec des cryptomonnaies. Contrairement à des protocoles comme Compound, BlockFi est centralisé.

CEX

Un CEX (ou “*Centralized Exchange*”) est une plateforme d’échange centralisée qui consiste à mettre en relation l’offre et la demande sur un marché donné, en passant par un tiers de confiance qui héberge les ordres d’achat et de vente. Les plateformes comme *Coinbase*, *Kraken* ou encore *Binance* sont des CEX.

Collatéraliser

Collatéraliser des actifs, titres ou liquidités renvoie au fait de les déposer à un créancier en garantie. En cas de défaillance du débiteur, le créancier a le droit de conserver le collatéral afin de se dédommager de la perte financière subie. Actuellement, de nombreux projets DeFi nécessitent de sur-collatéraliser des actifs pour emprunter. Il est donc nécessaire pour les utilisateurs de ces services de déposer un collatéral donc la valeur est supérieure à celle de l’emprunt réalisé.

Composabilité

La composabilité renvoie à la possibilité, pour des outils et plateformes de la finance décentralisée, de pouvoir interagir les uns avec les autres.

Consensus

Le consensus est un procédé par lequel les utilisateurs d’un réseau pair-à-pair se mettent d’accord sur un ensemble de règles. Il s’agit du mode de gouvernance inhérent au système décentralisé de la Blockchain. Chaque modification du code source du protocole implique l’approbation de la majorité.

Le plus connu d’entre eux, qui est à la base de Bitcoin, est l’algorithme de consensus par preuve de travail (Proof-of-Work). Celui-ci se base sur un principe simple : chaque bloc est ajouté à la Blockchain grâce à une dépense énergétique (preuve de travail), et la chaîne de blocs la plus longue (celle comportant le plus de preuve de travail) est la chaîne qui est considérée comme valide par le réseau.

Crédit lombard

Le crédit lombard est un prêt adossé à des actifs principalement mobiliers (actions, obligations, fonds communs de placement, etc.) mis en gage dans le but d'obtenir une avance en trésorerie. Le détenteur des actions conserve la propriété des actifs nantis, et reçoit les intérêts et dividendes produits par ces actifs.

Cryptomonnaie

Une cryptomonnaie est une monnaie basée sur les principes de la cryptographie, et échangée sur un réseau décentralisé en pair-à-pair grâce aux technologies Blockchain. À la différence des monnaies traditionnelles, les cryptomonnaies n'ont pas de cours légal. Les cryptomonnaies sont l'une des catégories composant les cryptoactifs. Une autre définition des cryptomonnaies, sous un angle technique, désigne les actifs numériques qui sécurisent directement le consensus d'une Blockchain. Par exemple, la cryptomonnaie bitcoin sécurise la Blockchain Bitcoin, la cryptomonnaie Ether sécurise la Blockchain Ethereum. À l'inverse, un jeton comme AAVE circule sur la Blockchain Ethereum, mais ne sécurise directement aucune Blockchain propre.

Cryptoactifs

Les cryptoactifs sont des biens immatériels incluant un droit de propriété, et qui reposent sur une Blockchain. Ils incluent notamment les cryptomonnaies, utility tokens, security tokens, non-fungible tokens, etc.

DEX

Un Dex (ou “Decentralized Exchange”) est une plateforme d’échange décentralisée qui consiste à mettre en relation l’offre et la demande sur un marché donné, sans tiers de confiance pour héberger les ordres d’achat et de vente.

Voir notre article : [Les DEX : Echanger ses cryptomonnaies avec l'exemple d'Uniswap](#)

Framework

En informatique, un framework est un cadre ou une structure conçue pour le développement et le déploiement d’applications et de services web.

Layer-one

Layer-one (couche 1) est le terme utilisé pour décrire la principale architecture d’une Blockchain.

Layer-two

Layer-two (couche 2) est un réseau superposé à une Blockchain sous-jacente. L’objectif principal de ce protocole est souvent de résoudre les problèmes de vitesse et d’échelle auxquels sont confrontés les principaux réseaux Blockchains, et d’améliorer leur scalabilité. À titre d’exemple, le réseau Bitcoin est le protocole de la couche 1, tandis que le réseau Lightning est le protocole de la couche 2

Marché prédictif

Un marché prédictif est une plateforme de paris en ligne conçue pour générer des prévisions fiables. Chaque prévision est cotée sous forme d’actions, telle une société cotée en Bourse. Les parieurs décident de la valeur d’une action en l’échangeant sur le marché jusqu’à ce que la prévision soit avérée ou non.

Market making automatisé

Dans l'écosystème des cryptoactifs, un market maker automatisé ou AMM (*Automated Market Maker*) est un programme informatique qui assure l'existence de réserve de liquidités sur une plateforme d'échange.

Microsoft ION

ION est un réseau décentralisé de gestion de l'identité reposant sur Bitcoin, et conçu par Microsoft.

Minage

Le minage est un processus qui consiste à valider les transactions en cryptomonnaies et à sécuriser le réseau. Le mécanisme du Proof-of-Work est majoritaire à l'heure actuelle, et consiste en la résolution, par des ordinateurs, de problèmes mathématiques complexes. Chaque transaction minée donne droit à une récompense sous la forme d'une distribution de nouvelles cryptomonnaies.

Monnaie fiduciaire

Monnaie dont la valeur repose uniquement sur la confiance qu'a le public dans celle-ci et non sur la valeur du support (billet, pièce, carte bancaire, chéquier, etc.). Fiduciaire vient du latin fiducia qui signifie confiance.

Open Source

Un logiciel Open Source est un code informatique conçu pour être accessible à tous : n'importe qui peut voir, modifier et distribuer le code à sa convenance. Développé de manière collaborative et décentralisée, il repose sur l'examen en pair-à-pair et est souvent moins cher, plus flexible et durable par rapport à ses équivalents propriétaires parce qu'il est développé par des communautés, et non par une entité ou un auteur.

Satoshi Nakamoto

Satoshi Nakamoto est le pseudonyme de la personne ou du groupe de personnes qui, de 2009 à 2010, ont créé Bitcoin.

Scalabilité

La scalabilité désigne la capacité d'une Blockchain à s'adapter à un nombre croissant d'utilisateurs et de transactions, sans compromettre la décentralisation et la sécurité. Il s'agit du plus grand défi actuel des Blockchains pour pouvoir prétendre à une adoption massive.

Sidechain

Une sidechain est une Blockchain secondaire ([layer-two](#)) qui se développe parallèlement à une Blockchain principale ([layer-one](#)), mais qui y est rattachée afin de pouvoir accroître le volume d'informations normalement limité. L'objectif est d'améliorer la scalabilité du réseau.

Smart-contract

Un smart-contract est un programme informatique qui exécute automatiquement des transactions en cryptomonnaies. Les conditions sont préalablement définies avec des instructions conditionnelles de type « if – then » (si telle condition est remplie, alors telle conséquence s'exécute). Ces programmes s'appuient sur la Blockchain du réseau Ethereum, et visent à rendre infalsifiables les termes et les conditions de leur exécution.

Stablecoin (USD, etc.)

Un stablecoin est un type de cryptomonnaie conçu pour conserver une valeur stable sur le marché. Bien que les mécanismes varient selon chaque stablecoin, ces cryptomonnaies sont censées résister à la volatilité du marché, et ne devraient donc pas connaître des fluctuations de prix importantes. Elles peuvent être adossées à de la monnaie fiduciaire: c'est le cas du Tether (USDT) ou encore du DAI de MakerDAO.

Voir notre article: [Les stablecoins](#)

Synthétique

Un cryptoactif synthétique est un actif sur la Blockchain dont la valeur fluctue en fonction de celle d'un autre actif, appelé sous-jacent. Un synthétique sert donc à s'exposer à un autre actif, le sous-jacent, sans nécessairement le posséder.

Voir notre article: [Les cryptoactifs synthétiques](#)

Uniswap

Uniswap est un protocole & une application fournissant d'une part un Dex pour permettre aux utilisateurs d'échanger sans tiers de confiance et d'autre part un protocole de market making automatisé (AMM).

"Véritable" transfert de valeur numérique

Un "Véritable" transfert de possession se définit par la possession directement par l'utilisateur (et non via un tiers de confiance) d'un actif numérique. Cela donne de nouvelles propriétés à ces actifs, comme leur caractère incensurable ou encore la possibilité pour l'utilisateur d'utiliser cet actif en dehors de son écosystème natif. Par exemple, la start-up Sorare propose aux utilisateurs d'acheter des vignettes de footballeur "panini" numériques (sous forme de NFT). L'utilisateur peut ensuite en faire l'usage qu'il souhaite : jouer avec Sorare, jouer sur un jeu tiers, revendre, collectionner ou encore la prêter.

Wall Street API

Expression évoquée par Maple Leaf en référence à la composabilité et aux interactions existantes entre la multitude de services et d'infrastructures qui composent la DeFi. Elle englobe à la fois l'émergence de ce nouvel écosystème financier mais également la manière dont, à terme, celui-ci pourrait faciliter tout transfert de valeur.



KPMG France, avec l'acquisition des équipes de Blockchain Partner, souhaite afficher son ambition, et propose à tous ses clients une expertise stratégique, technique ainsi que sur les enjeux touchant au droit, à la comptabilité ou à la fiscalité des cryptoactifs.

KPMG France, Leader de l'Audit et du Conseil, réunit 10 000 professionnels dédiés à la performance économique et financière des institutions et des entreprises de toute taille, dans tous les secteurs. KPMG apporte à ses clients la puissance d'un réseau mondial pluridisciplinaire à travers 150 pays et se singularise par son maillage territorial grâce à ses 220 bureaux en France.

AUDIT – CONSEIL – EXPERTISE COMPTABLE – DROIT ET FISCALITE.

KPMG est une structure internationale qui fédère des cabinets indépendants, spécialisés en Audit, Conseil et Droit et Fiscalité. Aujourd'hui présents dans 146 pays, nous comptons 227 000 professionnels à travers le monde. Les cabinets KPMG sont des entités juridiquement distinctes et séparées, et se décrivent comme tel. KPMG International Limited est une société privée de droit anglais, à responsabilité limitée par garantie. KPMG International Limited et les entités qui y sont liées ne fournissent pas de services aux clients.

Les informations contenues dans ce document sont d'ordre général et ne sont pas destinées à traiter les particularités d'une personne ou d'une entité. Bien que nous fassions tout notre possible pour fournir des informations exactes et appropriées, nous ne pouvons garantir que ces informations seront toujours exactes à une date ultérieure. Elles ne peuvent ni ne doivent servir de support à des décisions sans validation par les professionnels ad hoc. KPMG S.A. est le membre français de l'organisation mondiale KPMG constituée de cabinets indépendants affiliés à KPMG International Limited, une société de droit anglais (« private company limited by guarantee »). KPMG International et ses entités liées ne proposent pas de services aux clients. Aucun cabinet membre n'a le droit d'engager KPMG International ou les autres cabinets membres vis-à-vis des tiers. KPMG International n'a le droit d'engager aucun cabinet membre.

© 2021 KPMG S.A., société anonyme d'expertise comptable et de commissariat aux comptes, membre français de l'organisation mondiale KPMG constituée de cabinets indépendants affiliés à KPMG International Limited, une société de droit anglais (« private company limited by guarantee »). Tous droits réservés. Le nom et le logo KPMG sont des marques utilisées sous licence par les cabinets indépendants membres de l'organisation mondiale KPMG. Imprimé en France.

Création, réalisation: Blockchain Partner by KPMG — Juin 2021. Photos : iStock, Getty, Unsplash



by **KPMG**

KPMG

Tour EQHO
2 avenue Gambetta
92066 Paris La Défense Cedex
France
Tél.: +33 (0)1 55 68 86 66

kpmg.fr/socialmedia



kpmg.fr