



HAL
open science

Enjeux et promesses des stablecoins décentralisés

Louis Bertucci, Sébastien Choukroun, Julien Prat

► **To cite this version:**

Louis Bertucci, Sébastien Choukroun, Julien Prat. Enjeux et promesses des stablecoins décentralisés. Revue d'économie financière, A paraître. hal-03912747

HAL Id: hal-03912747

<https://hal.science/hal-03912747>

Submitted on 25 Dec 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Enjeux et promesses des stablecoins décentralisés

Louis BERTUCCI¹

Sébastien CHOUKROUN

Julien PRAT²

Abstract – Français :

Cet article propose une analyse économique des stablecoins mettant en évidence les liens avec la finance traditionnelle. Même s'il existe des stablecoins dont l'arrimage est garanti par un tiers de confiance, cet article se concentre principalement sur les stablecoins gérés directement par un système d'incitations sur une blockchain décentralisée. Nous mettons en évidence les enjeux de gouvernance et de liquidation des stablecoins décentralisés, qui sont au cœur du système de maintien de leur valeur. Enfin, nous discutons des risques associés à ces stablecoins, notamment les mécanismes entraînant une perte de stabilité.

Classification JEL : E49, G23, G29

Abstract – English :

This article presents an economic analysis of stablecoins, highlighting their links with traditional finance. While there are stablecoins whose value is maintained by a trusted third party, this article focuses largely on stablecoins managed directly by a system of incentives on a decentralized blockchain. We highlight the governance and liquidation challenges of decentralized stablecoins, which are at the heart of their value-maintaining system. Finally, we discuss the risks associated with these stablecoins, most notably the mechanisms inducing a loss of stability.

JEL classification : E49, G23, G29

INTRODUCTION

Tout système financier a besoin d'une unité de compte. La finance décentralisée n'échappe pas à cette règle. La communauté crypto a eu beau appeler de ses vœux l'adoption de Bitcoin comme point de référence, il est très rapidement apparu que son insularité et sa volatilité faisaient de Bitcoin un substitut plus qu'imparfait aux monnaies fiduciaires et, tout particulièrement, au dollar. En l'absence de monnaies numériques de banque centrale, des acteurs privés se sont substitués aux banques centrales en émettant des *stablecoins*, c'est-à-dire des jetons numériques en principe arrimés à une monnaie légale.

¹ Institut Louis Bachelier

² CNRS, Ecole Polytechnique, IP Paris, CREST. Email: julien.prat@ensae.fr

Apparus en 2014, les stablecoins se sont rapidement imposés en tant qu'unités de compte pour l'industrie de la finance décentralisée. De nombreuses applications financières voient le jour sur des blockchains permettant d'échanger sans intermédiaire, de créer des produits dérivés, d'emprunter contre garantie. Alors que les cryptoactifs sont par nature volatils, les stablecoins permettent à leurs détenteurs de sécuriser leurs gains et de couvrir leurs positions (cf. Pfister et Melachrinou, 2021).

Suite à leur succès foudroyant, les stablecoins se sont vite retrouvés au centre de polémiques quant à leur réelle stabilité. Bien que jeunes et relativement petits par rapport à la finance mondiale, ces titans de la blockchain cumulent plusieurs dizaines de milliards d'euros de valeur. Leur croissance météorique n'est pas sans soulever des inquiétudes quant à la gestion des risques de marchés et même des risques potentiellement systémiques. Face à ces problématiques, la réglementation européenne MiCA, en attente de ratification au moment de la rédaction de cet article, vise à imposer un cadre réglementaire aux émetteurs de stablecoins. Un préalable à la conception d'une réglementation adaptée est la compréhension des enjeux économiques et financiers décrits dans cet article.

Dans la première partie de cet article nous posons les bases d'une taxonomie des stablecoins et analysons leur positionnement vis-à-vis de la finance traditionnelle. La deuxième section se concentre sur l'analyse des stablecoins dit décentralisés car leur gestion n'est pas déléguée à un tiers de confiance. La dernière section porte sur l'analyse de la solvabilité et des risques de panique bancaire liés aux stablecoins.

STABLECOINS

Définition et classification

Les stablecoins sont des actifs numériques, ou jetons, qui sont censés avoir une valeur stable par rapport à un autre actif, généralement une monnaie légale.³ Comme tout autre actif numérique, ils sont virtualisés sur une ou plusieurs blockchains et peuvent généralement être utilisés par des applications de finance décentralisée (DeFi) populaires sur leur blockchain hôte, comme les protocoles de prêt ou les protocoles d'échange décentralisés. Il existe plusieurs mécanismes pour atteindre cette stabilité, qui génèrent chacun des types différents de stablecoins. Nous distinguons deux classes principales de stablecoins : les stablecoins centralisés et les stablecoins décentralisés. Parmi les stablecoins décentralisés, il est utile de distinguer trois types d'implémentation : les stablecoins sur-garantis, les stablecoins algorithmiques et les stablecoins fractionnaires. Notre taxonomie diffère de celles déjà proposées⁴ en ce qu'elle s'organise autour de deux niveaux bien distincts. Le premier niveau est lié à la présence ou non d'un tiers de confiance, qui

³ Certains stablecoins suivent le dollar ajusté de l'inflation comme le Frax par exemple, mais l'idée principale reste la même.

⁴ Pour une classification reposant sur le type d'actif utilisé en garantie, voir D. Hays. (2019), pour une classification basée sur la présence ou non de blockchain, voir Berensten et Schär (2019), pour une classification basée sur le montant de collatéralisation voir Lipton (2019). Lipton *et al.* (2020) considèrent une classification en 3 catégories, à savoir les stablecoins avec garantie bien définie, ceux basés sur la confiance et ceux qui reposent exclusivement sur des mécanismes de stabilisation automatique. Pour une classification avec une perspective basée sur l'émetteur, voir Bullmann *et al.* (2019).

est une notion fondamentale de l'écosystème blockchain, tandis que le second niveau adopte un point de vue comptable et financier, à savoir la méthode de stabilisation retenue. Cette section présente chaque catégorie en suivant une approche incrémentale afin de guider le lecteur de l'architecture la plus simple à la plus sophistiquée.⁵

La façon la plus simple de créer un stablecoin est par l'intermédiaire d'un tiers de confiance. Dans ce cas, une société tierce devient le dépositaire de la garantie qui est investie dans des actifs censés être liquides et peu risqués et émet en contrepartie un jeton numérique utilisable sur une ou plusieurs blockchains. Tant que l'entité émettrice reste solvable et que le marché a confiance en la qualité des actifs, donc en la solvabilité du tiers de confiance, la valeur des jetons numériques est stable par rapport à la devise de référence. L'arsenal classique d'audit et de gestion des risques peut alors se mettre en place pour de tels acteurs, même lorsqu'ils ne sont pas concernés par les réglementations financières. Bien que ces stablecoins soient librement échangeables sur une blockchain, ils sont créés par un tiers de confiance et sont donc qualifiés de centralisés. Les autres types de stablecoins sont, quant à eux, émis et gérés directement sur une blockchain.

Pour profiter pleinement des avantages des blockchains, qui seront détaillés dans la section suivante, les *stablecoins sur-garantis* se proposent de gérer le collatéral directement sur-chaîne. Le principal défi pour les émetteurs de ces stablecoins consiste à contrôler le risque de réserve afin d'assurer leur solvabilité. C'est pourquoi ils requièrent une sur-garantie de la part de leurs utilisateurs. Plus précisément, ces derniers peuvent librement ouvrir un coffre-fort digital sur une blockchain, sous la forme de smart contract, en y déposant des cryptoactifs. Ce smart contract émet en retour des stablecoins en prélevant des frais de transaction et, le cas échéant, en versant des intérêts proportionnels à la durée de détention des stablecoins.

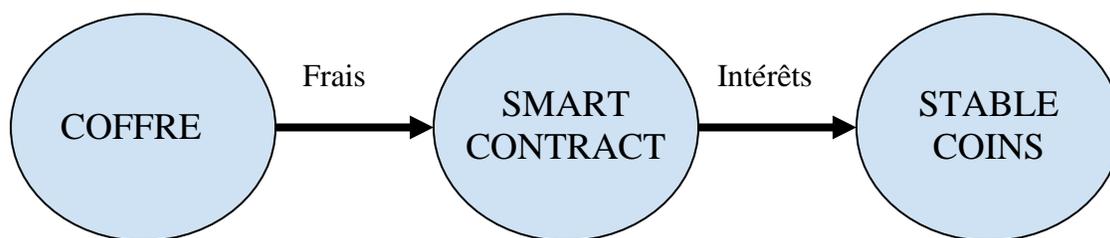


Figure 1: Emission de stablecoins décentralisés

Le bilan d'un stablecoin sur-garanti peut être schématiquement représenté de la façon suivante : l'actif est constitué de la garantie déposée par les utilisateurs et de la trésorerie accumulée par le smart contract; le passif est constitué de la masse de stablecoins en circulation, des marges de sur-garantie requises par le smart contrat et des jetons de gouvernance du protocole. Selon cette perspective comptable, les jetons de gouvernance correspondent à des parts sur les fonds propres du protocole. La gouvernance des stablecoins sur-garantis est détaillée dans la partie suivante.

⁵ Pour une approche générale sur ce qui fait qu'un stablecoin est effectivement stable voir Lyons and Viswanath-Natraj (2020).

Dans ce type de dispositifs, la quantité de stablecoins émise au moment de l'ouverture d'une position est toujours inférieure à la valeur de marché de leurs garanties. Cette sur-garantie permet au protocole d'assurer la convertibilité des stablecoins en dépit des fluctuations potentiellement significatives des cryptoactifs déposés en réserve. En cas de chute de leur valeur, le smart contract déclenche une mise aux enchères des actifs mis en garantis par les utilisateurs incapables de compléter leur couverture. Si la finalisation de la mise aux enchères est suffisamment rapide par rapport à la baisse du prix des cryptoactifs et si le marché est assez liquide pour absorber leur vente, le protocole est en mesure de clore les positions avant qu'elles ne deviennent sous-garanties. Les revenus générés par les liquidations peuvent alors être utilisés pour « stériliser » les positions liquidées, en rachetant et en détruisant la quantité de stablecoins mise en circulation.

Afin de s'assurer que les garanties ci-dessus soient satisfaites, les protocoles décentralisés requièrent des niveaux de sur-garantie élevés (cf. section suivante). La couverture contre la volatilité des cryptoactifs réduit donc significativement l'efficacité du capital investi dans ces protocoles.

ACTIF	PASSIF
Garantie	Stablecoins
Trésorerie	Marges Jetons de Gouvernance

Figure 2: Bilan d'un stablecoin sur-garanti

Les *stablecoins algorithmiques* cherchent à remédier à cette inefficience en s'appuyant sur un mécanisme de stabilisation basé sur des règles algorithmiques, mais en faisant disparaître l'adossement au moins un pour un à des garanties. En pratique, le modèle le plus courant consiste à émettre un second jeton dit de réserve. Quand le cours du stablecoin excède celui de la devise de référence, le jeton de réserve peut être échangé contre le stablecoin évalué à parité avec la devise. Cet arbitrage conduit à une augmentation du nombre de stablecoins en circulation, donc à une baisse de leur cours jusqu'à ce que la parité soit restaurée. Un mécanisme inverse est censé jouer quand le cours du stablecoin est inférieur à la parité, aboutissant à

une contraction du nombre de stablecoins, donc à une augmentation de leur cours. Le talon d’Achille de ce mécanisme de rappel est qu’il entraîne la multiplication et donc la dévaluation des jetons de réserve.⁶ Une “spirale de la mort” peut alors se mettre en place, entraînant une chute si rapide de la valeur du jeton de réserve qu’elle emporte avec elle la crédibilité du stablecoin. C’est précisément un tel scénario qui a conduit à l’effondrement du UST sur lequel nous reviendrons en détail plus loin dans l’article.

A première vue, il semble que les stablecoins algorithmiques cherchent à accomplir une opération alchimique au cours de laquelle des jetons symboliques seraient miraculeusement convertis en réserve de valeur. Leur échec peut donc sembler inéluctable. Mais alors, comment expliquer que le UST ait pu atteindre une capitalisation excédant 30 milliards de dollars ? Sans vouloir entrer dans des considérations portant sur la soutenabilité des bulles spéculatives qui nous éloigneraient trop du propos de cet article, nous nous contenterons de remarquer que les jetons de réserve matérialisent le pouvoir de seignuriage du protocole et qu’ils peuvent donc avoir une valeur significative quand la crédibilité du stablecoin est forte. Ce mécanisme auto-réalisateur est par nature fragile puisqu’il est soumis aux variations d’humeur du marché et donc difficilement conciliable avec la promesse de stabilité.

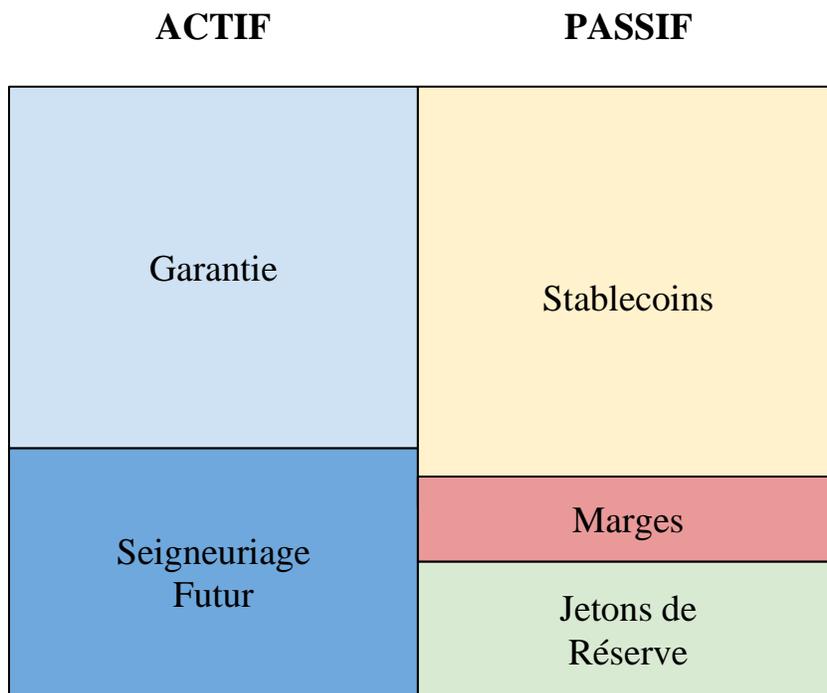


Figure 3: Bilan stablecoin fractionnel

La plus récente génération de stablecoins prend acte de ces limitations sans toutefois abandonner l’idée de valoriser le pouvoir de seignuriage afin de maximiser l’efficacité de leur protocole. Les *stablecoins fractionnaires* combinent les modèles des stablecoins sur-garantis et algorithmiques. Ils requièrent un certain niveau de garantie de la part de leurs utilisateurs mais cherchent à le réduire autant que faire se peut

⁶ Les banques centrales qui souhaitent maintenir un adossement de leur devise à une autre sont soumises à la même problématique.

à travers l'émission algorithmique de jetons de réserves. Ils ne sont donc pas généralement sur-garantis. La viabilité des stablecoins fractionnaires, tel que FRAX, reste sujette à caution et sera sûrement une des évolutions majeures à surveiller dans les années à venir.

Relation avec les fonds monétaires

En dépit de la nouveauté de leur infrastructure technologique, les stablecoins obéissent à des logiques économiques similaires à celles gouvernant le fonctionnement des fonds monétaires (*Money Market Funds* - MMFs).⁷ Ce type de fonds commun a pour objectif d'imiter les dépôts bancaires : au lieu de déposer leur argent dans une banque, les investisseurs peuvent acheter des parts d'un MMF. Du point de vue réglementaire, cela fait une énorme différence (cf. Gorton et al., 2022). Adoptée en 1933 en tant que disposition du Glass-Steagall Act, la réglementation Q est un règlement du Federal Reserve Board qui interdisait aux banques commerciales de payer des taux d'intérêt sur les dépôts à vue de leurs clients, et limitait l'intérêt des dépôts à terme. Pour satisfaire la demande des investisseurs, les banques ont eu l'idée de créer un nouveau type de fonds qui peut à la fois avoir une très faible volatilité, être remboursable à tout moment et rapporter un intérêt. Ceci est réalisé en structurant un fonds commun de placement qui investit uniquement dans des actifs à court terme et à faible risque tels que des bons du Trésor ou des billets de trésorerie. Tant que la qualité de la garantie est maintenue, tout fonctionne bien et la valeur de chaque part conserve une valeur fixe, 1 USD pour les MMFs dits « unitaires ». Cependant, comme toute forme d'actifs garantis, les parts de MMF sont sujettes à des paniques, c'est-à-dire à la crainte que le cours ne soit pas maintenu à 1 USD et que les investisseurs se précipitent pour vendre leurs parts dans l'espoir de récupérer au moins une partie de leur investissement. Pour un MMF, ces mouvements de panique peuvent se déclencher quand le fond rompt la parité ("break the buck"). En 2008, la faillite de Lehman Brothers a entraîné un tel événement pour plusieurs MMFs, ce qui a déclenché un cercle vicieux qui a été interrompu par une assurance à l'échelle de l'État fédéral similaire à l'assurance des dépôts.

Le mécanisme d'arrimage des MMFs est très similaire à celui des stablecoins garantis. Ces derniers sont rattachés à une unité de monnaie fiduciaire grâce à des actifs placés en garantie soit sur chaîne (stablecoins décentralisés) soit hors-chaîne (stablecoins centralisés). Alors que les stablecoins décentralisés maintiennent l'arrimage principalement en exigeant une sur-garantie qui peut être perçue comme inefficace, les stablecoins centralisés ont essentiellement la même structure qu'un MMF. Des sociétés comme Tether ou Circle émettent toutes deux un stablecoin en dollar qui est adossé à des actifs réels tels que des bons du Trésor à court terme et d'autres actifs à faible risque.

Une différence fondamentale entre les MMFs et les stablecoins est que ces derniers ne sont pas dans l'obligation de rémunérer leurs investisseurs en payant un taux d'intérêt⁸ car ils fournissent un service de liquidité unique à travers l'accès qu'ils permettent à l'ensemble des cryptoactifs. Cette connexion est rendue possible parce que les stablecoins sont tokenisés. Ils sont ainsi nativement intégrés dans un écosystème qui propose aussi bien des solutions de paiement que de conservation et d'investissement. Alors que les MMFs

⁷ Cette comparaison avec les fonds monétaire n'est pertinente que pour des stablecoins entièrement garantis, que la garantie soit gérée par un tiers de confiance ou par un protocole.

⁸ Cela dit, comme indiqué dans la section suivante, Aave prépare le lancement d'un nouveau stablecoin, GHO, qui générera un taux d'intérêt.

traditionnels sont de purs produits de gestion de liquidité, les stablecoins peuvent tirer parti de leur nature numérique pour être pleinement intégrés dans d'autres applications, au sein de la DeFi, dans des services de transferts internationaux et de commerce en ligne, ou même potentiellement directement dans l'activité économique au sein de la chaîne de valeur.⁹ Bien que les stablecoins en soient encore à leurs balbutiements, cette intégration crée une demande importante qui risque d'augmenter fortement dans les années à venir. Pour que l'histoire ne se répète pas, Gorton et al. (2022) proposent d'imposer aux stablecoins centralisés de fortes exigences de garantie ainsi qu'un niveau de transparence calqué sur celui imposé aux MMFs, afin que les investisseurs sachent quel type de produit ils achètent réellement.

Lorsqu'une entité tierce est chargée de la gestion des garanties, un certain nombre de mesures doivent être mises en place pour contrôler l'existence des garanties et s'assurer qu'elles présentent effectivement un risque faible, notamment concernant le risque de contrepartie. Un des avantages de la collatéralisation sur-chaîne mise en place par les stablecoins décentralisés est précisément la transparence totale, rendant possible des audits en temps réel permettant à tout un chacun de s'assurer de la quantité et de la qualité des garanties.

Avantages et inconvénients de la décentralisation

Comme les stablecoins centralisés s'appuient sur un modèle fortement inspiré des fonds monétaires traditionnels, ils sont naturellement exposés aux mêmes sources de fragilité. Leur stabilité repose entièrement sur la croyance partagée en leur convertibilité. Le moindre doute peut entraîner un mouvement de panique parmi les utilisateurs cherchant à convertir leurs stablecoins avant que le protocole ne devienne insolvable. En période de crise aiguë entraînant la vente au rabais des cryptoactifs, il existe un risque de liquidité sur un stablecoin pourtant solvable, ce qui pourrait entraîner sa disparition. Par exemple Tether détient des actifs qui sont plus ou moins liquide et pourrait donc être victime d'une panique bancaire.

Au vu de cette fragilité, il est peu surprenant que les MMFs soient soumis à une réglementation particulièrement stricte, exigeant entre autres qu'une part significative de leurs actifs soit constituée de titres hautement liquides et peu risqués. Les stablecoins ayant été introduits en dehors de tout cadre réglementaire, ils ne bénéficient pas d'un tel garde-fou. La crédibilité de l'organisation en charge de la gestion du stablecoin revêt donc une importance encore plus cruciale que dans la finance traditionnelle, ce qui n'est pas dénué d'ironie puisque la promesse originelle des blockchains était de proposer un système de paiement libéré du besoin de confiance.

Les doutes planant sur la probité des gestionnaires de stablecoins sont illustrés par les polémiques entourant Tether. En analysant les données de la blockchain Bitcoin, Griffin et Shams (2020) démontrent que les flux de Tethers sont cohérents avec une création monétaire non garantie, ayant pour objectif de manipuler à la hausse le prix de Bitcoin. Carol Alexander (2021) propose un diagnostic similaire dans des postes de blog où elle souligne l'intrication, suspecte à ses yeux, entre Tether et Binance. Afin de répondre aux critiques,

⁹ Cochrane (2014) propose dans un contexte différent d'utiliser des parts de fonds (monétaires ou pas) comme instruments de paiement.

Tether a demandé des attestations de réserves à des tiers puis annoncé en Octobre 2022 être entièrement investi en bons du Trésor américain à court terme, sans toutefois dissiper tous les doutes (cf. Coindesk, 2022).

Au moment de la rédaction de cet article, le débat autour de la solvabilité de Tether continue de faire rage, les divergences de vue s'expliquant principalement par des différences de perception quant à la crédibilité des audits fournis par Tether. C'est précisément à ce déficit de fiabilité des audits que les stablecoins décentralisés tentent d'apporter une solution. Quand les crypto-actifs sont gérés sur-chaîne par un smart contract, la composition du portefeuille est parfaitement observable en temps réel. Cette transparence rend improbable tout désaccord autour de la liquidité réelle, et non plus supposée, du stablecoin. Une difficulté est que cette transparence impose un comportement procyclique car les liquidations vont en général intervenir au moment d'une baisse du cours, aggravant ainsi celle-ci.

Il ressort de notre analyse que la décentralisation, en permettant à tout un chacun de vérifier la composition du portefeuille d'actifs, restreint grandement une des sources fondamentales de fragilité des stablecoins. Ce bénéfice n'est toutefois pas sans contrepartie. La décentralisation s'accompagne d'un nouvel ensemble de contraintes et de risques afférents :

1. Aléas technologiques : la complexité des smart contracts engendre des risques d'exécution et crée une surface d'attaque pour des acteurs mal intentionnés. Ces menaces sont exacerbées par le manque de maturité de la technologie (cf. New-York Times, 2022) d'une part, l'irréversibilité des transactions rendant le plus souvent impossible de récupérer les fonds perdus ou subtilisés d'autre part.
2. Manque de flexibilité : la logique de gestion d'un stablecoin décentralisé est complètement encodée dans son smart contract. Ce pré-engagement réduit grandement le besoin de confiance puisqu'il éradique tout aléa moral quant à l'exécution des transactions. Le revers de la médaille est qu'il est difficile, voire impossible, d'amender le fonctionnement du stablecoin en réponse à des circonstances imprévues au moment de sa création. En effet, même si des procédures de vote sur-chaîne sont prévues, elles seraient compliquées à mettre en place rapidement en périodes de stress.
3. Volatilité des actifs : Les réserves d'un stablecoin décentralisé sont, par définition, uniquement constituées de cryptoactifs. Ces derniers étant extrêmement volatiles, les stablecoins décentralisés, lorsqu'ils sont garantis, sont exposés à un risque de réserve nettement plus élevé que les stablecoins centralisés. De plus, une baisse trop rapide de la valeur des garanties peut générer une dette que les protocoles devront purger pour rester solvables.

ARCHITECTURE DES STABLECOINS DECENTRALISES

Tandis que les stablecoins hors-chaîne comme Tether sont gérés de façon relativement traditionnelle, les stablecoins sur-chaîne, en tant que protocole blockchain, doivent mettre en place de nouvelles formes de gouvernance et de gestion des risques. Cette section met en évidence les enjeux liés à la gouvernance et aux mécanismes de liquidation automatisés, puis décrit certains exemples concrets de stablecoins.

Gouvernance des stablecoins sur-chaîne

Quand le mécanisme de stabilisation du prix du stablecoin est géré par un protocole, ce dernier propose en général au moins un jeton de gouvernance en plus du stablecoin lui-même. Les détenteurs de ce jeton de gouvernance, librement échangeable, ont un droit de participation à la gouvernance décentralisée du protocole. Cette gouvernance est qualifiée de décentralisée en ce sens qu'elle tend en principe vers un processus démocratique dans lequel les détenteurs des jetons de gouvernance ont la possibilité de soumettre des propositions de modification ou de voter sur des propositions existantes. En plus du smart contract gérant le stablecoin lui-même, un ensemble de smart contracts dédiés à l'administration du protocole sont déployés sur la blockchain, et permettent de définir sur quels paramètres les propositions de modifications peuvent porter ainsi que le processus de vote et d'approbation.

Un des enjeux de la gouvernance est d'assurer que les évolutions du protocole sont votées par les détenteurs de jetons de gouvernance. Il y a donc un double enjeu : avoir suffisamment de participation aux votes pour la gouvernance et avoir suffisamment de propriétaires de jetons de gouvernance pour assurer un niveau de décentralisation significatif du protocole. Cependant, de tels projets peuvent avoir des évolutions à faire passer en urgence, soit pour des raisons techniques, soit pour des raisons économiques. La plupart des protocoles laissent donc du temps pour les votes des évolutions fondamentales, mais certains choisissent de centraliser la prise des décisions urgentes alors que d'autres travaillent à des mécanismes décentralisés également pour ce sujet.¹⁰ La question de la gouvernance adaptée à un stablecoin algorithmique reste ouverte en 2022.

En général, les paramètres modifiables par proposition de modification sont l'acceptation d'un nouvel actif en tant que garantie du stablecoin ou le niveau de garantie pour les stablecoins garantis. Tandis que certains protocoles permettent aux détenteurs de jetons de gouvernance de voter sur un large éventail de paramètres (comme MakerDAO), d'autres protocoles (comme Frax) préfèrent circonscrire les modifications envisageables afin de limiter les divergences potentielles de la communauté et garantir un niveau de sécurité suffisant. De la même façon, il est possible de donner des droits particuliers (par exemple un droit de veto) à certains utilisateurs, comme les fondateurs, ou à certains membres élus au sein de la communauté (comme le fait Aave avec les Aave Guardians). Cette solution permet d'éviter des discussions trop stériles au sein de la communauté et de s'assurer que les évolutions du protocole iront dans une certaine direction.

Par opposition aux stablecoins, les jetons de gouvernance ont une valeur qui fluctue. Comme des droits de vote sont attachés à ces jetons de gouvernance, il est nécessaire que le niveau de concentration de leur détention soit faible pour limiter la possibilité de manipulation des votes par un détenteur majoritaire. Pour inciter des investisseurs, qu'ils soient utilisateurs du stablecoin associé ou non, à acheter des jetons de gouvernance et à participer activement à la gouvernance, il est donc nécessaire de lier directement ou indirectement la valeur des jetons de gouvernance au succès du stablecoin associé.

Sans rentrer dans les détails de l'économie des jetons de gouvernance, il nous semble important de mentionner qu'il existe plusieurs façons de rendre ces jetons attractifs. En plus de collecter des frais de transactions, la quantité de jetons de gouvernance en circulation est souvent automatiquement ajustée en fonction du niveau de risque global du protocole. Lorsque le stablecoin connaît un certain succès, le

¹⁰ Voir par exemple la gouvernance du protocole Aave : <https://docs.aave.com/aavenomics/governance>

protocole peut acheter des jetons de gouvernance et les détruire dans un processus appelé “burning”, de façon très similaire à une entreprise qui ferait un rachat d’actions. Ceci a pour effet de réduire la quantité de jetons de gouvernance en circulation et donc tend à en augmenter la valeur. Le processus inverse de création de jetons de gouvernance peut avoir lieu si le succès du stablecoin s’amointrit, bien que cela puisse poser des problèmes sur la gouvernance du protocole. Les mécanismes exacts des différents stablecoins sur-chaîne varient mais ils proposent généralement des variations du principe décrit ci-dessus. Dans le cas des stablecoins algorithmiques ou fractionnaires, le jeton de gouvernance est explicitement utilisé comme partie intégrante de la contrepartie du stablecoin et sa quantité est alors gérée de façon proactive par le protocole.

Mécanismes de liquidation

Dans le cadre d’un stablecoin décentralisé, la gestion du risque lié à une garantie volatile est un élément central du protocole. Lorsque de nouvelles unités de stablecoins sont créées, la position est sur-garantie d’un facteur au moins égal à ce qui est appelé le “ratio de liquidation” à l’aide d’actifs risqués comme Bitcoin ou Ether. La gestion du risque de garantie est alors assurée de manière automatique par un smart contract dédié qui est capable de connaître le prix de marché de la garantie grâce à des oracles.¹¹ Si la valeur des garanties, relativement à la quantité de stablecoins adossée à celles-ci, baisse sous le ratio de liquidation de la position, le protocole déclenche leur mise en vente. En pratique, le ratio dépend du niveau de risque de chacune des garanties.

Si nous prenons l’exemple de MakerDAO présenté plus bas, les positions sont regroupées dans des “coffres” ou “Vaults” qui permettent aux utilisateurs de créer de nouvelles unités du stablecoin Dai en échange de garanties. Dans le cadre d’un Vault avec un Liquidation Ratio de 150%, chaque USD de Dai créé va nécessiter un minimum de 1.50 USD de collatéral ; une liquidation est déclenchée si la valeur de la garantie baisse sous ce niveau. Un élément clé du processus est la sécurité des oracles qui fournissent en temps réel les valeurs de marché des garanties, apportant la donnée qui, le cas échéant, déclenche des liquidations.¹²

Le processus de liquidation consiste en une mise aux enchères sur-chaîne de l’actif liquidé. L’enchère est généralement ouverte à tout le monde. Son produit est utilisé pour clore la position et détruire la quantité équivalente de stablecoins. Une pénalité de liquidation est en général appliquée puis utilisée pour acheter et détruire des jetons de gouvernance.

Bien que la sur-garantie serve de coussin de sécurité pour des baisses modérées de la valeur des garanties, il est également nécessaire de se prémunir contre des événements de marché extrêmes. En effet, si cette valeur baisse de façon trop forte et trop rapide, le temps que l’enchère se mette en place, il est fort possible

¹¹ Un oracle est un service tiers qui permet à des smart contracts sur blockchain d’accéder à des données externes à leur blockchain.

¹² Pour la sécurité des utilisateurs, il est nécessaire d’utiliser un ou plusieurs oracles difficilement manipulables afin de prévenir le déclenchement de liquidations qui ne seraient pas justifiées.

que les garanties mises en vente ne soient pas d'un montant suffisant pour couvrir en totalité la position à liquider. Les protocoles gèrent ce risque de différentes manières mais ils comportent tous un mécanisme d'urgence qui peut servir soit à bloquer temporairement le système d'enchères pour éviter que les pertes soient trop importantes, soit à allouer les pertes aux détenteurs de jetons de gouvernance ou à différents groupes d'utilisateurs qui auraient accepté de prendre ce risque extrême contre une rémunération adaptée.

Exemples

MakerDAO, le grand-père de la DeFi

MakerDAO a créé un produit financier appelé Dai, qui est un stablecoin sur-garanti basé sur Ethereum. Les utilisateurs de MakerDAO peuvent emprunter une valeur en Dai en fournissant une garantie sous la forme d'autres jetons ou crypto-monnaies. Les positions des emprunteurs doivent être sur-garanties afin de maintenir un risque de contrepartie faible.¹³

Le smart contract qui régit MakerDAO connaît le prix de la garantie via un service d'oracle. Lorsque sa valeur devient trop faible, le smart contract déclenche une liquidation de la position. Le processus de liquidation contient plusieurs étapes qui, outre l'exigence de sur-garantie de la position, visent à réduire le risque de contrepartie même dans le cas d'un krach des cryptos important. Les taux de sur-collatéralisation peuvent aller de 130% à 170% pour les collatéraux très volatils.

Le taux d'intérêt payé par les emprunteurs ainsi que le montant de la garantie à partir duquel la liquidation a lieu (et plusieurs autres paramètres) sont fixés par le smart contract de gouvernance de MakerDAO. Les droits de gouvernance dans MakerDAO sont portés par le jeton de gouvernance MKR. Les détenteurs du jeton MKR peuvent voter directement sur la blockchain Ethereum pour les modifications du protocole, y compris, mais sans s'y limiter, l'ajustement des règles de garantie et l'ajout de nouveaux types de garanties. Le remboursement du prêt déclenche le rachat et la destruction de jetons MKR, ce qui augmente en principe la valeur des MKR restant en circulation.

En termes financiers, MakerDAO crée un actif numérique, Dai, qui est garanti par d'autres actifs numériques et dont la valeur est indexée de manière décentralisée sur 1 USD. Par opposition à Tether, le tiers de confiance est remplacé par le smart contract MakerDAO, qui empêche une mauvaise gestion, mais introduit d'autres risques comme des risques de marché ou des risques opérationnels tel que des bugs, ou des failles de sécurité.

GHO stablecoin by Aave

Pendant l'été 2022, une équipe contribuant au développement d'Aave a proposé un stablecoin décentralisé et générateur de rendement, le GHO. Il s'agit d'un stablecoin algorithmique indexé sur le dollar américain qui sera créé par les utilisateurs d'Aave et produira un rendement sous forme d'intérêts pour les détenteurs. Ce stablecoin sera entièrement natif à l'écosystème Aave et disponible initialement sur le réseau Ethereum.

¹³ Pour une analyse des mécanismes de stabilité de MakerDAO, voir Kozhan et Viswanath-Natraj (2022).

Il devrait être proposé sur d'autres blockchains prises en charge par Aave en fonction des futurs votes de la communauté.

Toujours à l'état de proposition, Aave devrait permettre aux utilisateurs de frapper des jetons GHO contre leurs garanties. Le GHO serait soutenu par un panier de crypto-monnaies choisies à la discrétion des utilisateurs, tandis que les emprunteurs continueraient à gagner des intérêts sur les garanties sous-jacentes.

GHO est censé fonctionner de la même manière que les stablecoins sur-garantis en créant 1 USD de jetons lorsque les utilisateurs fournissent des garanties en cryptomonnaie. Dans le cas de GHO, un utilisateur doit fournir une garantie (à un ratio de garantie spécifique) pour créer un GHO. De même, lorsqu'un utilisateur rembourse une position emprunteuse (ou que celle-ci est liquidée), le protocole GHO brûle le GHO de cet utilisateur. Toutes les décisions relatives au GHO seront entre les mains de la gouvernance d'Aave. GHO devrait générer des revenus supplémentaires pour la DAO d'Aave en envoyant 100 % des intérêts perçus sur les emprunts du GHO au DAO.

Une équipe contribuant au développement d'Aave a proposé que le stablecoin GHO s'appuie sur des "facilitateurs". Seul un facilitateur tel qu'un autre protocole pourra générer ou brûler des jetons GHO. Les facilitateurs devront être approuvés par la gouvernance d'Aave. Différents animateurs pourront appliquer différentes stratégies à leur génération de GHO. Les facilitateurs, cependant, seront soumis à des limites suivant la gouvernance d'Aave, pour s'assurer qu'ils n'abusent pas de leurs pouvoirs. Pour chaque facilitateur, la gouvernance devra également approuver un sceau représentant la limite supérieure de GHO qu'un facilitateur donné peut créer.

Suite à l'introduction de GHO, le DAO sera également en mesure de décider du taux d'intérêt natif de GHO et de le modifier au fil du temps grâce à un processus de gouvernance, qui sera décrit dans une proposition à venir. Cela signifie qu'en principe la politique de taux d'intérêt du GHO sera contrôlée par la gouvernance d'AAVE.

FRAX Finance

Cherchant à combiner les avantages des stablecoins décentralisés et algorithmiques, Frax introduit un stablecoin dit fractionnaire. L'écosystème Frax est composé d'un stablecoin, le FRAX, et d'un jeton de gouvernance ou de réserve, le Frax Share ou FXS. Ce dernier possède en réalité plusieurs fonctions : outre permettre aux propriétaires du FXS de voter sur des modifications du protocole, il leur permet d'être rémunérés grâce aux frais payés par les utilisateurs, aux revenus liés au seigneurage ainsi qu'à l'excès de garanties. En partie garanti, la valeur d'un Frax est aussi maintenue à travers un mécanisme similaire à celui d'un stablecoin algorithmique.

La particularité de Frax est que le taux de collatéralisation dépend de la demande pour le stablecoin. Au lancement, le taux de collatéralisation était de 100%, c'est-à-dire que pour créer 1 stablecoin FRAX, il fallait mettre en réserve l'équivalent d'1 USD. Si la demande pour le stablecoin augmente et que sur une certaine période (par exemple, 1h) la valeur moyenne d'un FRAX est supérieure à une limite (ex: 1 USD), le taux de garantie, diminue par palier successif (ex: 0,25%). Le phénomène inverse se produit si la valeur moyenne d'un FRAX est inférieure à la limite. Lorsque le taux de garantie baisse trop, la confiance se

détérioré, les utilisateurs vendent le FRAX, sa valeur baisse par rapport à la valeur de référence et le taux de garantie augmente pour restaurer la confiance.

Le jeton de gouvernance FXS entre en jeu lorsque le taux de garantie est inférieur à 100%. Pour créer 1 FRAX il faut alors déposer des garanties et compléter par un dépôt en FXS qui est détruit par le protocole. Si, par exemple, le taux de collatéralisation est de 80%, pour créer 1 FRAX, il sera nécessaire de déposer 0.8 USD en collatéral ainsi que 0.2 USD en FXS. L'idée sous-jacente est, qu'à mesure que le stablecoin devient populaire, le taux de garantie baisse et plus de FXS sont détruits, ce qui devrait entraîner une hausse de la valeur des FXS. Ce mécanisme de destruction est donc un moyen de lier directement la valeur des jetons de gouvernance au succès du stablecoin.

Il est important de noter qu'au moment de la rédaction de cet article, la seule garantie acceptée au sein de Frax est l'USDC, un stablecoin centralisé et garanti. L'acceptation de nouveaux types de garanties, vraisemblablement quand les différents mécanismes du protocole auront été éprouvés, pourra être soumise au vote des détenteurs de FXS.

SOLVABILITE ET PANIQUES BANCAIRES

Luna et le spectre des paniques bancaires

Luna, le jeton de la blockchain Terra, revendiquait pour objectif de soutenir un stablecoin dollar nommé TerraUSD. La spécificité de ce projet est qu'il était purement algorithmique et n'avait donc pas de garanties externes au protocole.

Puisque le prix d'un TerraUSD est déterminé sur le marché secondaire, un oracle décentralisé a été mis en place pour l'estimer. Ce prix est obtenu par le mécanisme suivant :

- Les contributeurs ("stakers") de la blockchain Terra soumettent un vote sur ce qu'ils pensent être le prix pertinent en dollar. Chaque n blocs, les moyennes pondérées des votes sont choisies comme prix pertinent. Des récompenses en Luna sont données à ceux qui ont voté à moins d'un écart-type du prix finalement choisi. Ceux qui n'ont pas voté dans cet intervalle peuvent, en guise de punition, perdre une partie des jetons qu'ils ont mis en dépôt.
- Quand un désarrimage du taux de conversion est identifié, un ajustement de la quantité de Luna en circulation doit permettre de rétablir la parité. Plus précisément, si le prix du TerraUSD est inférieur à 1 USD, chacun peut envoyer 1 TerraUSD vers le smart contract et recevoir en échange 1 USD de valeur en Luna. Si en revanche le prix est supérieur à 1 USD, chacun peut envoyer 1 LUNA pour 1 USD de valeur et recevoir 1 TerraUSD en retour.

L'arbitrage est donc le moyen de maintenir l'arrimage du stablecoin. Mais, comme expliqué dans la section 2, un tel mécanisme comporte un risque dit de "spirale de la mort" au cours duquel le prix du LUNA baisse si vite que les émissions de jetons ne permettent pas de stabiliser les prix au niveau attendu. Ce risque s'est matérialisé le 5 mai 2022. Alors que le cours du Luna était de 87 USD à cette date, il s'est mis à chuter

vertigineusement pour atteindre 0.0005 USD le 13 mai 2022.¹⁴ Dans la même période, le prix du stablecoin TerraUSD est passé d'environ 1 USD à 0.03 USD, et tout espoir de restauration de l'arrimage semble désormais perdu pour ce projet.¹⁵ Ce krach a entraîné l'évaporation en quelques jours d'une soixantaine de milliards de dollars et a vraisemblablement sonné le glas des expériences autour des stablecoins purement algorithmiques, même si quelques initiatives, comme USDD sur la blockchain Tron, continuent à s'inspirer de LUNA.

Tokenisation d'actifs réels

La qualité et la liquidité des garanties utilisées étant très importantes pour le calcul du ratio de liquidation, une évolution attendue de l'écosystème est l'émergence d'actifs réels, ou « Real World Assets » (RWA), tokenisés sur blockchain et utilisés comme garanties.

Un exemple récent est RealT qui propose sur Aave des jetons correspondant à des actifs immobiliers.¹⁶ Leur introduction devrait permettre de mieux diversifier le risque, l'immobilier étant assez décorrélé des cryptoactifs disponibles jusqu'ici sur Aave. Cependant, ces jetons seront sûrement considérés comme des « securities » par la SEC et comme des titres financiers par l'AMF. Il est donc fort probable qu'ils seront réglementés, avec des contraintes spécifiques liées à l'obligation de recourir à un agent de transfert pour réaliser des échanges de titres. Pour cette raison, certains membres de la communauté de Maker s'opposent à l'ajout des RWA comme garanties, si bien qu'à ce jour aucun RWA n'a été accepté par la gouvernance de MakerDAO.

Gestion algorithmique optimale

La débâcle de Luna a convaincu de nombreux observateurs du caractère chimérique des stablecoins purement algorithmiques. Dans le même temps, la résilience de MakerDAO a démontré la viabilité des stablecoins sur-garantis, y compris en période de correction sévère des marchés. Ce contraste frappant suggère que le modèle intermédiaire des stablecoins fractionnaires repose sur l'identification d'une ligne de crête assez étroite. Une approche naïve, basée uniquement sur l'intuition, risque fort d'être inadaptée à un tel projet. C'est pourquoi des articles de recherche récents se proposent d'approfondir le sujet en identifiant les tensions économiques générées par les stablecoins ainsi que les solutions algorithmiques permettant d'y remédier.

Li et Mayer (2020) proposent un modèle dynamique dont l'objectif est de rendre compte du fonctionnement des stablecoins sur-garantis. L'unique source de risque dans leur modèle provient des fluctuations du prix des actifs déposés en réserve : un mouvement de panique se déclenche dès que la valeur totale des réserves devient inférieure à celle des stablecoins en circulation. Autrement dit, le protocole est définitivement liquidé dès que sa position globale devient sous-garantie. Cette hypothèse conservatrice peut être justifiée en s'appuyant sur un modèle de jeux globaux (Goldstein et Pauzner, 2005). Elle implique que l'objectif des

¹⁴ L'historique du prix de Terra-Luna disponible à l'adresse : <https://coinmarketcap.com/currencies/terra-luna/>

¹⁵ Pour plus de détails sur la panique engendrée par Terra-Luna, le lecteur peut se référer à l'article de Vivien Levy-Garboua (2022) dans cette revue.

¹⁶ <https://decrypt.co/40679/defi-meets-real-estate-as-aave-readies-crypto-mortgages>

gestionnaires du protocole est de préserver autant que faire se peut la sur-garantie afin d'éviter la liquidation.

Li et Mayer (2020) démontrent que la règle optimale de gestion consiste à ne verser des dividendes aux détenteurs du protocole que quand le niveau de sur-garantie atteint un seuil endogènement déterminé par leur modèle. En dessous de ce seuil, la seule source de revenus pour le protocole est prélevée sous forme de frais auprès des détenteurs des stablecoins, ce qui est équivalent à l'imposition d'un taux d'intérêt négatif.

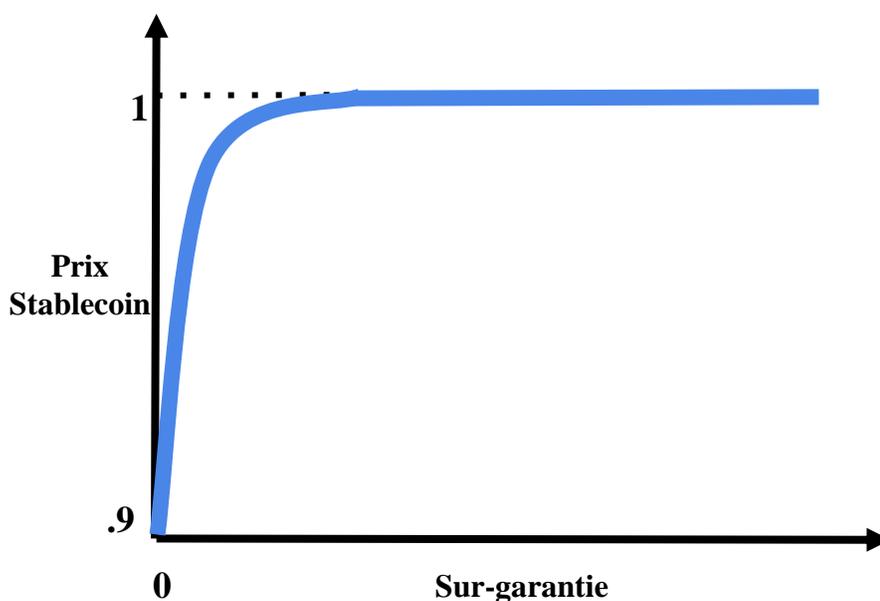


Figure 4 : Prix du stablecoin en fonction du niveau de sur-garantie (Li et Mayer)

Leur résultat le plus frappant est qu'il n'est pas optimal de défendre coûte que coûte l'arrimage du stablecoin à sa valeur de référence (voir figure 4). Au contraire, il est préférable d'abandonner la convertibilité un pour un avant que le seuil de liquidation ne soit atteint. Ce désarrimage volontaire peut sembler contre-intuitif. Ne risque-t-il pas de précipiter le mouvement de panique et par conséquent la liquidation des réserves? Au contraire, en laissant son stablecoin se dévaluer, le protocole utilise son pouvoir de seigneurage au maximum afin de reconstituer ses réserves et, si possible, d'éviter le seuil fatidique de sous-garantie.

D'Avernas et al. (2022) aboutissent à une conclusion similaire en s'appuyant sur un modèle adapté à l'analyse des stablecoins fractionnaires. La différence principale¹⁷ entre leur approche et celle proposée par Li et Mayer (2020) est que d'Avernas et al. (2022) n'imposent plus l'hypothèse selon laquelle le protocole doit rester sur-garanti pour éviter d'être liquidé. Par contraste, d'Avernas et al. (2022) analysent les stablecoins fractionnaires en introduisant explicitement le pouvoir de seigneurage dans le bilan comptable

¹⁷ Les deux modèles diffèrent dans d'autres dimensions moins cruciales. Par exemple, la source d'incertitude dans d'Avernas et al. (2022) provient des variations exogènes de la demande pour le stablecoin et non plus de la valeur des garanties qui sont considérées comme sûres.

du protocole, lui permettant de rester solvable tant que la valeur de son pouvoir de seigneurage excède l'insuffisance de ses réserves.

La contribution fondamentale de d'Avernas et al. (2022) par rapport à Li et Mayer (2020) est donc de démontrer qu'il est possible de construire un modèle théorique au sein duquel les stablecoins fractionnaires sont viables. Leur analyse indique que la règle optimale de stabilisation est similaire à celles adoptées en pratique puisqu'elle prescrit de défendre l'arrimage du stablecoin en diluant les parts des détenteurs du jeton de gouvernance, comme mis en place par FRAX ou Luna. Par ailleurs, les stablecoins purement algorithmiques ne sont viables que si leur demande croît continuellement dans le temps, ce qui les rend effectivement assimilables à des systèmes de Ponzi.¹⁸

Pour conclure, ces recherches récentes montrent comment les stablecoins fractionnaires doivent ajuster le niveau de leurs garanties afin de trouver un équilibre entre pouvoir de stabilisation et efficacité du capital. Bien que les modèles fournissent un cadre quantitatif pour la résolution optimale de ce compromis, ils sont aussi porteurs de mises en garde puisqu'ils mettent en évidence la coexistence d'un mauvais équilibre avec mouvements de panique. Il est probable que cette ligne de recherche progresse rapidement dans les années à venir, en approfondissant les modèles décrits ci-dessus afin de les rendre plus opérationnels et, qui sait, peut-être un jour d'encoder leurs solutions au sein d'un smart contract.

CONCLUSION

De nombreux stablecoins ont émergé au cours de ces huit dernières années, avec des échecs retentissants mais aussi des succès. Nous entrons désormais dans une phase de consolidation. Le volume attirant le volume, il est probable que, pour chaque monnaie légale, un oligopole de stablecoins émerge, avec quelques leaders regroupant une forte majorité des encours et devenant des acteurs importants de la souveraineté numérique des Etats. Une nouvelle période charnière est sur le point de démarrer. Les lancements de MNBC par les banques centrales vont créer les conditions d'une concurrence directe avec les stablecoins. Les années à venir décideront donc des formes de stablecoins et de MNBC qui seront durablement adoptés.

BIBLIOGRAPHIE

Aave, 2022. [Introducing: GHO - Governance - Aave.](#) (2022)

Alexander, Carol, 2021. "Tether and Bitcoin Ponzi-Ecosystem. "
<https://www.coalexander.com/post/the-bitcoin-ponzi-ecosystem>

Coindesk, 2022. "Stablecoin Issuer Tether Ordered to Produce Documents Showing Backing of USDT."

¹⁸ Voir aussi l'article de Levy-Garboua et Maarek (2022) publié dans ce recueil.

<https://www.coindesk.com/markets/2022/09/21/stablecoin-issuer-tether-ordered-to-produce-documents-showing-backing-of-usdt/>

d'Avernas, Adrien, Vincent Maurin et Quentin Vandeweyer, 2002. "Can Stablecoins be Stable?" Document de travail.

Berentsen, Aleksander et Fabian F. Schär, 2019. *The Economics of Fintech and Digital Currencies*. CEPR Press.

Bullmann, Dirk, Klemm, Jonas et Andrea Pinna, 2019. "In search for stability in crypto-assets: are stablecoins the solution?" ECB Occasional Paper, (230).

Cochrane, John, 2014. "Toward a Run-Free Financial System", in M. N. Baily and J. B. Taylor (ed.), *Across the Great Divide : New Perspectives on the Financial Crisis*, chapitre 10, Hoover Institution, Stanford University.

Griffin, John M. et Amin Shams, 2020. "Is Bitcoin really untethered?" *The Journal of Finance*, 75, no. 4: 1913-1964.

Goldstein, Itay et Ady Pauzner, 2005. "Demand–deposit contracts and the probability of bank runs." *The Journal of Finance* 60(3): 1293–1327.

Gorton, Gary B. et Jeffery Zhang, 2022. "Taming wildcat stablecoins." A paraitre dans la *University of Chicago Law Review*, Vol. 90.

Kozhan, Roman et Ganesh Viswanath-Natraj, 2021. "Decentralized Stablecoins and Collateral Risk." WBS Finance Group Research Paper.

Levy-Garboua, Vivien et Gérard Maarek, 2022. "Les fausses promesses de Terra-Luna." Référence Ouvrage??

Li, Ye et Simon Mayer, 2020. "Money Creation in Decentralized Finance: A Dynamic Model of Stablecoin and Crypto Shadow Banking." Document de travail, Fisher College of Business Working Paper No. 2020-03-030.

Lipton, Alexander, 2019. "Towards a Stable Tokenized Medium of Exchange." *Cryptoassets: Legal, Regulatory, and Monetary Perspectives*, Oxford University Press.

Lipton, Alexander, Sardon, Aetienne, Schär, Fabian et Christian Schüpbach, 2020. "Stablecoins, Digital Currency, and the Future of Money." *Building the New Economy*, PubPub Edition.

Lyons, Richard K. et Ganesh Viswanath-Natraj, 2020. "What keeps stablecoins stable?" Document de travail, National Bureau of Economic Research, WP27136.

Nakamoto, Satoshi, 2008. "Bitcoin: A peer-to-peer electronic cash system." *Decentralized Business Review*: 21260.

Pfister, Christian et Anastasia Melachrinou, 2021. "Stablecoins: A Brave New World?" *Stanford Journal of Blockchain Law and Policy*, 4(2), 113-138,

New-York Times, 2022. "The Crypto World Is on Edge After a String of Hacks."
<https://www.nytimes.com/2022/09/28/technology/crypto-hacks-defi.html>