

Le système Dai Stablecoin

Livre blanc

<https://makerdao.com/>

Par l'équipe Maker

Décembre 2017

Présentation du système Dai Stablecoin 3

Contrats intelligents de positions adossées à des créances 3

Le processus d'interaction des CDP 5

Dai à garantie simple et Dai à garanties multiples 5

Ether regroupé (mécanisme temporaire pour le Dai à garantie simple) 6

Mécanismes de stabilité des prix 6

Prix d'objectif 6

Mécanisme de rétroaction pour le prix d'objectif 6

Paramètre de sensibilité 7

Règlement global 8

Règlement global : Pas à pas 8

Gestion des risques de la plate-forme Maker 9

Paramètres de risque 10

Gouvernance des jetons MKR 11

MKR et Dai à garanties multiples 12

Liquidations automatiques des CDP à risques 12

Contrat de fourniture de liquidités (mécanisme temporaire pour le Dai à garantie simple)
13

Enchères de créance et de garantie (Dai à garanties multiples) 13

Acteurs externes clés 14

Gardiens 14

Oracles 14

Régleurs globaux 15

Exemples 15

Marché adressable 18

Les risques et leur atténuation 18

Attaque pirate malveillante contre l'infrastructure de contrat intelligent 19

Évènement Cygne noir dans un ou plusieurs actifs de garantie 19

Compétition et importance de la facilité d'utilisation 20

Erreurs de prix, irrationalité et événements non prévus 20

Échec d'infrastructure centralisée 21

Conclusion 21

Glossaire 22

Liens 23

Présentation du système Dai Stablecoin

Certains actifs numériques répandus tels que le Bitcoin (BTC) et l'Ether (ETH) ont une volatilité trop forte pour servir de monnaie au quotidien. Le cours du bitcoin connaît souvent d'importantes fluctuations : ses variations à la hausse ou à la baisse peuvent atteindre 25 % en une seule journée et il peut parfois augmenter de plus de 300 % en un mois.¹

Le Dai Stablecoin est une crypto-monnaie adossée à une garantie et dont la valeur est stable par rapport au dollar US. Nous estimons que l'existence d'actifs numériques stables comme le Dai Stablecoin est essentielle pour exploiter pleinement le potentiel de la technologie de la blockchain.

Maker est une plate-forme de contrats intelligents sur l'Ethereum, qui soutient et stabilise la valeur du Dai grâce à un système dynamique de positions adossées à des créances (CDP), à des mécanismes de rétroaction autonomes et à des acteurs externes bénéficiant d'incitations appropriées.

Maker permet à tous ses utilisateurs d'exploiter leurs actifs en Ethereum pour créer du Dai sur sa plate-forme. Une fois généré, le Dai peut être employé de la même manière que toutes les autres crypto-monnaies : il peut être transmis gratuitement à des tiers afin de servir de moyen de paiement pour des biens et des services, ou être utilisé comme une épargne de long terme. Point important : la création de Dai génère également les composants indispensables pour une plate-forme robuste et décentralisée de trading sur marge.

Contrats intelligents de positions adossées à des créances

Toute personne possédant des actifs en garantie peut les utiliser pour créer du Dai sur la plate-forme Maker par le biais de contrats intelligents proposés exclusivement par Maker et appelés « positions adossées à des créances » (CDP).²

Les CDP détiennent les actifs en garantie déposés par un utilisateur et lui permettent de générer du Dai. Cette création s'accompagne toutefois de l'accroissement de la créance. Celle-ci bloque de manière effective les actifs en garantie déposés dans le CDP, jusqu'à ce qu'elle soit couverte ultérieurement par le remboursement d'une somme équivalente en Dai.

À ce stade, le détenteur des actifs en garantie peut encore les retirer. Les CDP actifs sont toujours sur-garantis, ce qui signifie que la valeur de la garantie est toujours supérieure à celle de la créance.

¹ David Ernst [Hard Problems in Cryptocurrency \(difficultés liées aux crypto-monnaies\)](#)

² <https://github.com/makerdao>

Le processus d'interaction des CDP

- **Étape 1 : Création du CDP et dépôt de la garantie**

L'utilisateur du CDP envoie une transaction à Maker pour créer le CDP, puis envoie une autre transaction pour le financer avec le montant et le type de la garantie qui servira à créer du Dai. À ce stade, le CDP est considéré comme garanti.

- **Étape 2 : Création de Dai à partir du CDP garanti**

L'utilisateur du CDP envoie ensuite une transaction pour récupérer le montant de Dai souhaité sur ce CDP. En retour, le CDP cumule un montant équivalent de créance, en bloquant l'accès à la garantie jusqu'au paiement de la créance à récupérer.

- **Étape 3 : Paiement de la créance et des frais de stabilité**

Lorsque l'utilisateur souhaite récupérer sa garantie, il doit payer sa créance dans le CDP ainsi que les frais de stabilité qui se cumulent au fil du temps et s'ajoutent à la créance. Ces frais de stabilité doivent être réglés uniquement en MKR. Une fois que l'utilisateur a réglé sa créance et les frais de stabilité en envoyant le montant requis en Dai et en MKR, le CDP est libéré de sa dette.

- **Étape 4 : Retrait de la garantie et clôture du CDP**

Après avoir réglé la créance et les frais de stabilité, l'utilisateur du CDP peut transférer tout ou partie de sa garantie dans son porte-monnaie en envoyant une transaction à Maker.

Dai à garantie simple et Dai à garanties multiples

Le Dai sera initialement proposé avec la prise en charge d'un seul type de garantie appelé « Ether regroupé ». Nous prévoyons de passer dans les 6 à 12 mois du Dai à garantie simple au Dai à garanties multiples. La principale différence entre ces deux systèmes réside dans le fait que le Dai à garanties multiples prend en charge tous les types de CDP.

3

³ Les mécanismes temporairement mis en place dans le système pendant la phase du Dai à garantie simple sont décrits dans ce livre blanc

Ether regroupé (mécanisme temporaire pour le Dai à garantie simple)

Dans un premier temps, l'Ether regroupé (PETH) sera le seul type de garantie accepté sur Maker. Les utilisateurs souhaitant ouvrir un CDP et créer du Dai pendant la première phase de la plate-forme Maker devront en premier lieu obtenir du PETH. Ils pourront le faire immédiatement et simplement sur la blockchain, en déposant des ETH dans un contrat intelligent spécifique, qui regroupe les ETH de tous les utilisateurs et leur donne en retour un montant correspondant en PETH.

Si un krach boursier affecte subitement l'ETH, et si un CDP se termine en contenant une créance d'un montant supérieur à sa garantie, la plate-forme Maker dilue automatiquement le PETH pour recapitaliser le système. Cela se traduit par une diminution de la demande de remboursement proportionnel de chaque PETH.

Après la mise à niveau de la plate-forme Maker en vue de prendre en charge les types de garanties multiples, le PETH sera supprimé et remplacé par l'ETH associé aux autres nouveaux types de garanties.

Mécanismes de stabilité des prix

Prix d'objectif

Le prix d'objectif du Dai remplit deux fonctions principales sur la plate-forme Maker :

1) Il sert à calculer le ratio garantie/créance d'un CDP ; 2) Il permet de déterminer la valeur des actifs en garantie reçus par les détenteurs de Dai en cas de règlement global.

Le prix d'objectif est libellé à l'origine en USD et sa valeur initiale est de 1 (ce qui signifie une parité de 1 pour 1).

Mécanisme de rétroaction pour le prix d'objectif

Dans l'hypothèse d'une forte instabilité du marché, le mécanisme de rétroaction pour le prix d'objectif (TRFM) peut être mis en œuvre. Le déclenchement du TRFM met fin à la parité fixe du Dai mais permet de conserver sa valeur nominale.

Le TRFM est le mécanisme automatique par lequel le système Dai Stablecoin ajuste le taux d'objectif de manière à ce que les forces du marché maintiennent la stabilité du cours du Dai autour de son prix d'objectif. Le taux d'objectif détermine le taux de change du prix d'objectif au fil du temps, afin que ce prix constitue une incitation à détenir du Dai (si le taux d'objectif est positif) ou à en emprunter (s'il est négatif). Lorsque le TRFM n'est pas mis en œuvre, le taux d'objectif est défini à 0 % afin de stabiliser le prix d'objectif sur la durée et de fixer le cours du Dai.

Lorsque le TRFM est pas mis en œuvre, le taux d'objectif et le prix d'objectif varient de manière dynamique afin d'équilibrer l'offre et la demande de Dai, en ajustant automatiquement les incitations poussant l'utilisateur à créer et à détenir du Dai. Le mécanisme de rétroaction amène le cours du Dai vers le prix d'objectif variable, amortissant ainsi sa volatilité et fournissant des liquidités en temps réel lors des chocs de demande.

Avec le déclenchement du TRFM, le taux d'objectif augmente lorsque le cours du Dai est inférieur au prix d'objectif. Cela provoque une augmentation plus rapide du prix d'objectif et entraîne une création de Dai avec des CDP orientés à la hausse. Dans le même temps, l'augmentation du taux d'objectif entraîne celle des gains en capital issus de la détention de Dai et se traduit par une augmentation correspondante de la demande de Dai. La diminution de l'offre combinée à l'accroissement de la demande provoque l'augmentation du cours du Dai et l'entraîne à la hausse vers son prix d'objectif.

Le même mécanisme fonctionne en sens inverse si le cours du Dai est plus élevé que son prix d'objectif : le taux d'objectif diminue, avec à la clé une hausse de la demande de création de Dai et une baisse de la demande de détention de cette crypto-monnaie. Cela provoque la diminution du cours du Dai et l'entraîne à la baisse vers son prix d'objectif.

Ce mécanisme constitue une boucle de rétroaction négative, dans la mesure où l'écart par rapport au prix d'objectif dans un sens accroît la force dans le sens opposé.

Paramètre de sensibilité

Le paramètre de sensibilité du TRFM permet de déterminer l'amplitude de la variation du taux d'objectif en réponse à l'écart du prix d'objectif/du cours du Dai. Le taux de rétroaction peut ainsi s'ajuster à l'échelle du système. Les votants MKR peuvent définir le paramètre de sensibilité. Cependant, lorsque le TRFM est mis en œuvre, le prix d'objectif et le taux d'objectif sont déterminés par la dynamique du marché et ne sont pas sous le contrôle direct des votants MKR.

Le paramètre de sensibilité permet également de déclencher ou d'interrompre le TRFM. Si

le paramètre de sensibilité et le taux d'objectif sont tous les deux égaux à zéro, le cours du Dai est fixé par rapport à la valeur actuelle du prix d'objectif.

Règlement global

Le règlement global est un processus qui peut être utilisé en dernier ressort pour garantir de manière cryptographique le prix d'objectif pour les détenteurs de Dai. Il interrompt et dénoue avec élégance la plate-forme Maker tout en garantissant que l'ensemble des utilisateurs (détenteurs de Dai et utilisateurs du CDP) recevront la valeur nette des actifs à laquelle ils peuvent prétendre. Ce processus est entièrement décentralisé, et les votants MKR en gèrent l'accès afin de vérifier qu'il est utilisé uniquement dans les cas d'extrême urgence (irrationalité des marchés à long terme, piratage ou failles de sécurité, mise à niveau des systèmes).

Règlement global : Pas à pas

- **Étape 1 : Le règlement global est activé**

Si certains acteurs (nommés « régulateurs globaux » par l'instance de gouvernance de Maker) sont assez nombreux pour estimer que le système fait l'objet d'une attaque grave, ils peuvent activer la fonction de règlement global. Ils peuvent également le faire si un règlement global est planifié dans le cadre d'une mise à niveau technique. L'activation de cette fonction interrompt la création et la manipulation de CDP et gèle le flux de prix sur une valeur fixe qui est ensuite utilisée pour traiter les demandes de remboursement proportionnel de tous les utilisateurs.

- **Étape 2 : Les demandes de règlement global sont traitées**

Après l'activation du règlement global, un délai est nécessaire pour permettre aux gardiens de traiter les demandes proportionnelles de tous les détenteurs de Dai et de CDP sur la base de la valeur fixe du flux de prix. Une fois ce traitement effectué, tous les détenteurs de Dai et de CDP pourront demander un montant fixe d'ETH en contrepartie de leur Dai et leurs CDP.

- **Étape 3 : Les détenteurs de Dai et de CDP demandent leur garantie en contrepartie de leur Dai et de leurs CDP**

Tous les détenteurs de Dai et de CDP peuvent utiliser une fonction de remboursement sur la plate-forme Maker pour échanger leur Dai et leurs CDP en contrepartie d'un montant fixe d'ETH correspondant à la valeur calculée de leurs actifs, sur la base du prix d'objectif du Dai.

- g. Si le prix d'objectif du Dai est de 1 USD, si la parité ETH/USD est de 200 et si un utilisateur détient 1 000 Dai lors de l'activation d'un règlement global, cet utilisateur pourra demander la somme exacte de 5 ETH sur la plate-forme Maker. Il n'existe aucune limite quant au moment où effectuer sa demande finale.

Gestion des risques de la plate-forme Maker

Le jeton MKR permet aux détenteurs de voter pour effectuer les opérations de gestion des risques suivantes :

- **Ajout d'un nouveau type de CDP** : Création d'un nouveau type de CDP avec une liste spécifique de paramètres de risque. Il peut s'agir d'un nouveau type de garantie ou d'une nouvelle liste de paramètres de risque associés à un type de garantie existant
- **Modification des types de CDP existants** : Modification des paramètres de risque associés à un ou plusieurs types de CDP ajoutés précédemment
- **Modification du paramètre de sensibilité** : Modification de la sensibilité du mécanisme de rétroaction pour le prix d'objectif
- **Modification du taux d'objectif** : L'instance de gouvernance peut modifier le taux d'objectif. En pratique, le taux d'objectif doit être modifié uniquement lorsque les votants MKR souhaitent fixer le cours du Dai par rapport à son prix d'objectif actuel. Cette modification doit toujours être effectuée en parallèle avec la modification du paramètre de sensibilité. Un paramètre de sensibilité et un taux d'objectif égaux à 0 % permettent de désactiver le TRFM et de fixer le prix d'objectif du Dai par rapport à sa valeur actuelle.

- **Choix de l'ensemble des oracles fiables** : La plate-forme Maker recherche ses prix internes de garantie ainsi que les cours du Dai dans d'une infrastructure d'oracle décentralisée, qui consiste en un vaste ensemble de nœuds d'oracle individuels. Les votants MKR contrôlent le nombre et l'identité des nœuds contenus dans l'ensemble des oracles fiables. La proportion d'oracles corrompus ou défectueux peut atteindre 50 % sans que le bon fonctionnement du système n'en soit perturbé.
- **Modification de la sensibilité du flux de prix** : Le changement des règles permettant de déterminer la modification la plus importante alimentée par le prix peut affecter les valeurs des prix internes dans le système.
- **Choix de l'ensemble des régleurs globaux** : Le règlement global est un mécanisme essentiel qui permet à la plate-forme Maker de résister aux attaques touchant les oracles ou la procédure de gouvernance. Celle-ci sélectionne un ensemble de régleurs globaux et détermine le nombre de régleurs requis pour activer le règlement global.

Paramètres de risque

Les CDP possèdent de nombreux paramètres de risque qui garantissent leur mode d'utilisation. Chaque CDP possède un ensemble spécifique de paramètres de risque définis sur la base du profil de risque de la garantie utilisée par le type de ce CDP. Les détenteurs de MKR contrôlent directement ces paramètres par le biais de leur vote (chaque MKR détenu donne droit à une voix).

Les principaux paramètres de risque des CDP sont les suivants :

- **Limite de créance** : La limite de créance est le montant maximum de dette pouvant être créée par un type spécifique de CDP. Une fois qu'une dette suffisamment élevée a été créée par un CDP d'un type donné, il devient impossible d'en créer davantage sauf en cas de clôture de CDP existants. La limite de créance vise à assurer une diversification suffisante du portefeuille de garantie.
- **Ratio de liquidation** : Le ratio de liquidation est le ratio garantie/dette qui marque la limite de l'exposition au risque d'un CDP. Un ratio de liquidation faible signifie que les votants MKR s'attendent à une faible volatilité du prix de la garantie. À l'inverse, un ratio de liquidation élevé est le signe d'une importante volatilité attendue.

- **Frais de stabilité** : Les frais de stabilité sont des frais réglés par tous les CDP. Ils représentent un pourcentage annuel du rendement, qui vient s'ajouter à la créance existante du CDP. Ils doivent être réglés par l'utilisateur du CDP. Les frais de stabilité sont libellés en Dai, mais peuvent être réglés uniquement au moyen du jeton MKR. Le montant de MKR à régler est calculé sur la base d'un flux de prix du cours du MKR. Après le règlement, le MKR est brûlé, ce qui le supprime définitivement du stock d'approvisionnement.
- **Ratio de pénalité** : Le ratio de pénalité permet de déterminer le montant maximum de Dai recueilli lors d'une enchère de liquidation et servant à acheter et à retirer le MKR du stock d'approvisionnement, avec la garantie en excès retournée à l'utilisateur du CDP qui détenait celui-ci avant sa liquidation. Le ratio de pénalité permet également de couvrir l'inefficacité du mécanisme de liquidation. Lors de la phase du Dai à garantie simple, la pénalité de liquidation sert à acheter et à brûler du PETH, au profit du ratio PETH/ETH.

Gouvernance des jetons MKR

En plus de régler les frais de stabilité sur les CDP actifs, le jeton MKR joue un rôle important dans la gouvernance de la plate-forme Maker.

La gouvernance est pilotée au niveau du système, via l'élection d'une proposition active par les votants MKR. Une proposition active est un contrat intelligent qui, à l'issue du vote MKR, dispose d'un accès total pour modifier les variables internes de gouvernance de la plate-forme Maker.

Les propositions actives existent sous deux formes : Les contrats de proposition d'action unique (SAPC) et les contrats de proposition de délégation (DPC).

Les SAPC sont des propositions qui peuvent être exécutées uniquement après l'obtention de l'accès total et qui, après exécution, modifient les variables internes de gouvernance de la plate-forme Maker. Après avoir été exécutées une seule fois, les SAPC s'auto-détruisent et ne peuvent pas être réutilisées. C'est ce type de proposition qui sera employé au cours des premières phases du système car il est simple à utiliser (mais moins flexible).

Les DPC sont des propositions qui utilisent en permanence leur accès total via une logique de gouvernance de seconde couche. Cette logique est codifiée dans le DPC. La logique de gouvernance de seconde couche peut être relativement simple (définition d'un protocole pour l'organisation d'un vote hebdomadaire sur les paramètres de risque actualisés, par exemple). Elle peut également mettre en œuvre une logique plus avancée, consistant par exemple à limiter l'étendue des actions de gouvernance sur des périodes

définies, ou encore à déléguer tout ou partie des autorisations à un ou à plusieurs DPC de troisième couche, avec ou sans restrictions.

Tout compte Ethereum peut déployer des contrats de proposition intelligents. Les votants MKR peuvent utiliser leurs jetons MKR pour approuver une ou plusieurs propositions qu'ils souhaitent sélectionner en tant que « proposition active ». Le contrat intelligent ayant obtenu le plus grand nombre de suffrages obtient le statut de « proposition active ».

MKR et Dai à garanties multiples

Après la mise à niveau vers le Dai à garanties multiples, MKR jouera un rôle encore plus significatif dans le système Dai Stablecoin en se substituant à PETH comme ressource de recapitalisation. Si les CDP ne sont plus garantis à la suite de krachs boursiers, l'offre de MKR sera automatiquement diluée et liquidée afin de recueillir suffisamment de fonds pour recapitaliser le système.

Liquidations automatiques des CDP à risques

Afin qu'il y ait toujours un montant de garantie suffisant pour couvrir la valeur de toutes les créances à récupérer (sur la base du prix d'objectif), un CDP peut être liquidé s'il est jugé trop risqué. La plate-forme Maker détermine le moment opportun pour liquider un CDP, en comparant le ratio de liquidation avec le ratio actuel garantie/dette du CDP.

Chaque CDP possède un ratio de liquidation spécifique, contrôlé par les votants MKR et établi sur la base du profil de risque de l'actif en garantie spécifique pour ce type de CDP.

La liquidation a lieu lorsqu'un CDP atteint son ratio de liquidation. La plate-forme Maker achète automatiquement la garantie du CDP et liquide celui-ci par la suite. Un mécanisme temporaire, appelé contrat de fourniture de liquidités, a été mis en place pour le Dai à garantie simple. Un mécanisme d'enchères sera utilisé pour le Dai à garanties multiples.

Contrat de fourniture de liquidités (mécanisme temporaire pour le Dai à garantie simple)

Pendant la phase de Dai à garantie simple, le mécanisme de liquidation est un contrat de fourniture de liquidités, à savoir un contrat intelligent qui effectue directement des transactions avec les gardiens et les utilisateurs d'Ethereum, sur la base du flux de prix du système.

Lorsqu'un CDP est liquidé, il est immédiatement acquis par le système. Le titulaire du CDP reçoit la valeur du restant de la garantie, diminué de la créance, des frais de stabilité et de la pénalité de liquidation.

La garantie ETH est mise en vente dans le contrat de fourniture de liquidités, et les gardiens peuvent acheter le PETH de manière individuelle en payant en Dai. Tout le Dai payé de cette manière est immédiatement supprimé du stock d'approvisionnement en Dai, jusqu'à ce qu'un montant égal à la créance du CDP soit retiré. Si du Dai est payé plus cher que le manque à gagner de la créance, le surplus de Dai est utilisé pour acheter du PETH auprès du marché et le brûler, ce qui change le ratio ETH/PETH de manière positive. Cela entraîne un gain de valeur net pour les détenteurs de PETH.

Si la vente de PETH ne génère pas assez de Dai initialement pour couvrir tout le manque à gagner de la créance, plus de PETH est créé en continu et vendu. Le nouveau PETH créé de cette manière change de manière négative le ratio ETH/PETH, ce qui entraîne une perte de valeur pour les détenteurs de PETH.

Enchères de créance et de garantie (Dai à garanties multiples)

Lors d'une liquidation, la plate-forme Maker achète la garantie d'un CDP et le vend ensuite lors d'une enchère automatique. Le mécanisme d'enchère permet au système de régler les CDP même lorsque les informations sur le prix ne sont pas disponibles.

Afin de récupérer la garantie du CDP pour qu'il puisse être vendu, le système a d'abord besoin de générer assez de Dai pour couvrir la créance du CDP. Ceci est appelé une enchère de créance et fonctionne en diluant l'approvisionnement du jeton MKR et en le vendant aux offrants sous la forme d'une enchère.

En parallèle, la garantie du CDP est vendue lors d'une enchère de garantie où tous les bénéficiaires (aussi en Dai) jusqu'au montant de la créance du CDP plus une pénalité de liquidation (un paramètre de risque déterminé par vote MKR) sont utilisés pour acheter du MKR et le retirer de l'approvisionnement. Ceci contrebalance directement la dilution du MKR qui survient lors de l'enchère de créance. Si le volume de Dai offert est suffisant pour couvrir entièrement la créance CDP plus la pénalité de liquidation, l'enchère de garantie passe à un mécanisme d'enchère inversée et essaie de vendre aussi peu de garantie que possible. Toute garantie restante est renvoyée au propriétaire d'origine du CDP.

Acteurs externes clés

En plus de son infrastructure de contrat intelligent, la plate-forme Maker se repose sur certains acteurs externes pour la gestion des opérations. Les gardiens sont des acteurs externes qui tirent profit des incitations économiques présentées par la plate-forme Maker. Les oracles et les régleurs globaux sont des acteurs externes avec des autorisations spéciales au niveau du système, qui leur sont affectées par les votants MKR.

Gardiens

Un gardien est un acteur indépendant (en général automatisé) qui est incité par des opportunités de profit à contribuer à des systèmes décentralisés. Dans le contexte du système Dai Stablecoin, les gardiens participent aux enchères de créance et aux enchères de garantie lorsque les CDP sont liquidés.

Les gardiens échangent aussi du Dai environ au prix d'objectif. Les gardiens vendent du Dai lorsque le prix du marché est supérieur au prix d'objectif et achètent du Dai lorsque le prix du marché est inférieur au prix d'objectif, pour profiter de la convergence à long terme attendue vers le prix d'objectif.

Oracles

La plate-forme Maker nécessite des informations en temps réel sur le prix du marché des actifs utilisés comme garantie dans les CDP afin de savoir quand déclencher les liquidations. La plate-forme Maker a également besoin d'informations sur le prix du marché du Dai et de son écart par rapport au prix d'objectif afin d'ajuster le taux cible lorsque le TRFM est engagé. Les votants MKR choisissent un ensemble d'oracles fiables pour fournir ces informations à la plate-forme Maker via les transactions Ethereum.

Pour protéger le système contre un pirate qui prendrait le contrôle d'une majorité d'oracles, et contre toute autre forme de collusion, une variable globale existe, qui détermine le changement maximum de la valeur du flux de prix autorisé par le système. Cette variable est appelée paramètre de sensibilité du flux de prix.

Pour donner un exemple de la façon dont le paramètre de sensibilité du flux de prix fonctionne, si le paramètre est défini sur « 5 % dans 15 minutes », les flux de prix ne peuvent pas changer de plus de 5 % dans une période de 15 minutes. Une variation d'environ 15 % prendrait 45 minutes. Cette restriction garantit qu'il y a assez de temps pour déclencher un règlement global en cas de prise de contrôle d'une majorité d'oracles par un pirate.

Régleurs globaux

Les régulateurs globaux sont des acteurs externes semblables aux oracles de flux de prix et sont la dernière ligne de défense du système Dai Stablecoin en cas d'attaque. Le groupe de régulateurs globaux, sélectionnés par les votants MKR, ont le droit de déclencher un règlement global. À part ce droit, ces acteurs n'ont aucun autre accès ni contrôle spécial au niveau du système.

Exemples

Le système Dai Stablecoin peut être utilisé par tout le monde sans restriction ou processus d'inscription.

- **Exemple 1** : Bob a besoin d'un prêt et décide de générer 100 Dai. Il verrouille un montant d'ETH d'une valeur bien supérieure à 100 Dai dans un CDP et l'utilise pour générer 100 Dai. Les 100 Dai sont instantanément envoyés directement sur son compte Ethereum. En supposant que les frais de stabilité sont de 1 % par an, Bob aura besoin de 101 Dai pour couvrir le CDP s'il décide de récupérer son ETH un an plus tard.

L'un des cas d'utilisation principaux des CDP est la transaction de marge par les utilisateurs CDP.

- **Exemple 2** : Bob souhaite une longue marge sur la paire ETH/Dai et génère donc 100 USD de Dai en publiant 150 USD d'ETH sur un CDP. Il achète ensuite de nouveau 100 USD d'ETH avec son Dai nouvellement généré, ce qui lui donne 1,66 fois d'exposition ETH/USD nette. Il est libre de faire ce qu'il veut avec les 100 USD d'ETH qu'il a obtenus en vendant le Dai. La garantie ETH d'origine (d'une valeur de 150 USD) reste verrouillée dans le CDP jusqu'à ce que la créance plus les frais de stabilité soient couverts.

Bien que les CDP ne sont pas fongibles les uns avec les autres, la propriété d'un CDP est cessible. Cela permet d'utiliser les CDP dans des contrats intelligents qui ont des méthodes plus complexes de génération de Dai (par exemple, en impliquant plus d'un acteur).

- **Exemple 3** : Alice et Bob collaborent en utilisant un contrat OTC Ethereum pour émettre 100 USD de Dai sécurisés par ETH. La contribution d'Alice s'élève à 50 USD d'ETH tandis que celle de Bob s'élève à 100 USD. Le contrat OTC prend les fonds et crée un CDP, générant ainsi 100 USD de Dai. Les Dai nouvellement générés sont automatiquement envoyés à Bob. Du point de vue de Bob, il achète 100 USD de Dai en payant la valeur équivalente en ETH. Le contrat transfère alors la propriété du CDP à Alice. Elle termine avec une créance d'une valeur de 100 USD (en Dai) et une garantie d'une valeur de 150 USD (en ETH). Ayant commencé avec seulement 50 USD d'ETH, elle est à présent dans une position avec un effet de levier 3 fois plus long d'ETH/USD.

Les liquidations garantissent que dans le cas d'un krach du prix d'une garantie soutenant un type de CDP, le système pourra automatiquement fermer les CDP qui deviennent trop risqués. Ceci permet de s'assurer que l'approvisionnement de Dai restant reste entièrement garanti.

- **Exemple 4** : Supposons qu'il y a un type de CDP en Ether avec un ratio de liquidation de 145 %, un ratio de pénalité de 105 % et que nous avons un CDP en Ether avec un ratio de garantie/créance de 150 %. Le prix en Ether perd maintenant 10 % par rapport au prix d'objectif, entraînant une chute du ratio garantie/créance du CDP d'environ de 135 %. Lorsqu'il passe en dessous du ratio de liquidation, les traders peuvent déclencher sa liquidation et commencer à enchérir avec du Dai pour acheter du MKR lors de l'enchère de la créance. Simultanément, les traders peuvent commencer à enchérir avec du Dai pour acheter environ 135 Dai de garantie lors de l'enchère de garantie. Une fois qu'il y a au moins 105 Dai enchéris sur la garantie en Ether, les traders inversent l'enchère pour prendre le volume le plus bas de garantie pour 105 Dai. Toute garantie restante est retournée au propriétaire de CDP.

Marché adressable

Comme mentionné dans l'introduction, une crypto-monnaie avec stabilité de prix est une condition de base pour la majorité des applications décentralisées. Dans ces conditions, le marché potentiel du Dai est au moins aussi vaste que celui de toute l'industrie de la blockchain. La petite liste suivante, non exhaustive, répertorie certains marchés immédiats (dans la blockchain et l'ensemble de l'industrie) qui s'ouvrent au système Dai Stablecoin, grâce à son profil de crypto-monnaie avec stabilité de prix et utilisation en tant que plateforme de transaction de marge décentralisée.

- **Marchés de prédiction et applications de pari** : Dans le cadre d'une prédiction non associée, il est évident qu'on ne va pas vouloir accroître le risque en utilisant une crypto-monnaie volatile pour le pari. Les paris à long terme deviennent particulièrement irréalisables si l'utilisateur doit aussi parier sur le futur prix de l'actif volatile utilisé. À la place, une crypto-monnaie avec une stabilité de prix comme le Dai sera le choix naturel pour le marché de prédiction et les parieurs.
- **Marchés financiers ; couverture, dérivés, effet de levier** : Les CDP permettront des transactions avec effet de levier sans autorisation. Le Dai sera aussi utilisé en tant que garantie stable et fiable dans les contrats intelligents dérivés personnalisés, tels que les options ou les CFD.
- **Reçus de commerçant, transactions transfrontalières et remises** : L'atténuation de la volatilité des devises étrangères et l'absence d'intermédiaires signifient que les coûts de transaction de commerce international peuvent diminuer significativement en utilisant le Dai.
- **Systèmes de comptabilité transparents** : Les organismes caritatifs, les ONG et les gouvernements constateront tous davantage d'efficacité et moins de corruption en utilisant le Dai.

Les risques et leur atténuation

La réussite du développement, du déploiement et du fonctionnement de la plate-forme Maker ne va pas aller sans risques. Il est essentiel que la communauté Maker prenne toutes les mesures nécessaires pour atténuer ces risques. Ci-dessous se trouve une liste énumérant certains des risques identifiés et le plan d'accompagnement pour les atténuer :

Attaque pirate malveillante contre l'infrastructure de contrat intelligent

Le plus grand risque du système en phase initiale est qu'un programmeur malveillant utilise une faille dans un contrat intelligent déployé pour rentrer dans le système, ou y commettre un vol, avant que la vulnérabilité ne soit corrigée. Dans le pire des cas, tous les actifs numériques décentralisés qui sont conservés comme garantie dans la plate-forme Maker, comme Ether (ETH) ou Augur Reputation (REP), pourraient être dérobés sans qu'il soit jamais possible de les récupérer. *La partie du portefeuille de garantie qui n'est pas décentralisée, comme les IOU Digix Gold, ne serait pas dérobée dans une telle situation car elle peut être gelée et contrôlée via une porte dérobée centralisée.*

Atténuation : La sécurité de contrat intelligent et de bonnes pratiques de sécurité sont la priorité numéro 1 dès le début du développement du Dai. Le code base a déjà subi trois audits de sécurité indépendants par certains des meilleurs chercheurs en sécurité de l'industrie de la blockchain.

Sur le très long terme, le risque d'être piraté peut théoriquement être presque complètement atténué grâce à une vérification formelle du code. Cela implique de prouver mathématiquement que le code fait exactement ce qu'il est censé faire. Tandis que la vérification formelle complète est un objectif à très long terme, un travail considérable a déjà été effectué, y compris l'implémentation de référence complète du système Dai Stablecoin dans le langage de programmation fonctionnel Haskell, qui sert de première étape vers des formalisations plus sophistiquées actuellement en cours de recherche et de développement.

Évènement Cygne noir dans un ou plusieurs actifs de garantie

Un autre risque à impact élevé est un évènement Cygne noir potentiel sur une garantie utilisée pour le Dai. Cela pourrait arriver lors des phases initiales du système Dai Stablecoin, avant que le MKR soit assez robuste pour prendre en charge les dilutions inflationnistes, ou après que le système Dai Stablecoin prenne en charge un portefeuille diversifié de garanties.

Atténuation : La garantie CDP sera limitée à l'ETH au début, avec un plafond de créance initialement restreint et augmentant graduellement dans le temps.

Compétition et importance de la facilité d'utilisation

Comme mentionné précédemment, des efforts et investissements financiers considérables sont consacrés à une crypto-monnaie avec stabilité de prix. De par sa « vraie décentralisation », le système Dai Stablecoin est de loin le modèle le plus complexe envisagé par l'industrie de la blockchain. Un des risques possibles est que les utilisateurs de crypto-monnaie préfèrent le leurre de la simplicité et la commercialisation d'actifs numériques centralisés aux idéaux de décentralisation.

Atténuation : Nous pensons que le Dai sera très facile à utiliser pour un utilisateur de crypto-monnaie classique. Le Dai sera un jeton Ethereum standard adhérant à la norme ERC20 qui sera facilement disponible avec une liquidité élevée sur l'ensemble de l'écosystème. Le Dai a été conçu de telle manière que l'utilisateur moyen n'a pas besoin de comprendre les mécanismes sous-jacents du système pour l'utiliser.

Les complexités du système Dai Stablecoin devront être comprises principalement par les gardiens et les sociétés d'investissement de capital qui utilisent le système Dai Stablecoin pour les transactions de marge. Ces types d'utilisateurs disposent d'assez de ressources pour s'engager tant que la documentation sur tous les aspects des mécanismes du système reste suffisamment claire et étoffée. La communauté Maker s'assurera que ce sera le cas.

Erreurs de prix, irrationalité et évènements non prévus

Un nombre d'évènements imprévus peuvent potentiellement survenir, comme un problème avec le flux de prix émanant des oracles, ou une dynamique de marché irrationnelle qui entraîne un écart de valeur du Dai pour une durée prolongée. Si la confiance dans le système est perdue, les ajustements TRFM ou même la dilution MKR pourraient atteindre des niveaux extrêmes tout en n'apportant pas assez de liquidité ou de stabilité sur le marché.

Atténuation : La communauté Maker devra motiver un capital de démarrage suffisamment important pour fonctionner comme gardiens du marché afin d'optimiser la rationalité et l'efficacité du marché, et permettre que l'approvisionnement du Dai se développe à un rythme régulier sans chocs du marché importants.

Échec d'infrastructure centralisée

L'équipe Maker joue un rôle majeur dans le développement et la gouvernance de la plate-forme Maker à ses débuts : budgétisation pour les dépenses, embauche de nouveaux développeurs, recherche de partenariat et d'utilisateurs institutionnels, et interfaçage avec des régulateurs et d'autres parties prenantes externes clés. Si l'équipe Maker échoue dans une certaine mesure, pour des raisons juridiques ou à cause de problèmes internes de gestion, le futur de Maker pourrait être compromis sans plan de sauvegarde approprié.

Atténuation : La communauté Maker existe en partie pour agir comme contrepartie décentralisée face à l'équipe Maker. Il s'agit d'un collectif informel d'acteurs indépendants qui ont tous la même finalité en étant détenteurs du jeton MKR, ce qui les motive beaucoup à vouloir la réussite de la plate-forme Maker. Lors de la phase initiale de la distribution de MKR, tout a été fait pour s'assurer que les principaux développeurs les plus importants reçoivent un intérêt en MKR significatif. Si l'équipe Maker n'est plus capable de développer la plate-forme Maker, les détenteurs de MKR seront motivés pour financer les développeurs (ou simplement pour effectuer le développement eux-mêmes) afin d'essayer de protéger leur investissement.

Conclusion

Le système Dai Stablecoin a été conçu pour résoudre le problème crucial de stabilité de valeur d'échange dans l'écosystème Ethereum et dans l'économie de la blockchain en général. Nous pensons que le mécanisme par lequel le Dai est créé, échangé et mis hors service, en plus du rôle de gestion de risque direct des détenteurs de MKR, permettra aux gardiens eux-mêmes intéressés de maintenir efficacement la stabilité du prix du Dai sur le long terme. Les fondateurs de la communauté Maker ont défini un plan de route de gouvernance prudent, parfaitement approprié aux besoins en développement agile sur le court terme, et tout aussi cohérent avec des idéaux de décentralisation dans le temps. Le plan de route de développement est quant à lui agressif, et axé sur l'adoption globale du Dai de manière raisonnable.

Glossaire

- **Position adossée à des créances (CDP)** : Un contrat intelligent dont les utilisateurs reçoivent un actif (Dai), qui fonctionne efficacement comme un instrument de créance avec un taux d'intérêt. L'utilisateur du CDP a publié une garantie dépassant la valeur du prêt afin de garantir sa position d'endettement.
- **Dai** : La crypto-monnaie avec une stabilité de prix qui est l'actif d'échange dans le système Dai Stablecoin. Il s'agit d'un jeton (token) Ethereum standard respectant la norme ERC20.
- **Enchère de dette** : L'enchère inversée vendant du MKR pour du Dai afin de couvrir la créance d'urgence lorsqu'un CDP n'est plus garanti.
- **Enchère de garantie** : L'enchère vendant la garantie d'un CDP subissant une liquidation. Elle est conçue pour donner la priorité à la couverture de la créance due par le CDP et ensuite donne au propriétaire du CDP le meilleur prix possible pour son remboursement de garantie excessif.
- **La Fondation Dai** : Une équipe décentralisée de développeurs de contrats intelligents, dédiés au développement et au lancement réussi de la plate-forme Maker.
- **Gardiens** : Acteurs économiques indépendants qui négocient du Dai, des CDP et/ou MKR, qui créent du Dai ou ferment des CDP, et qui cherchent un arbitrage sur le système Dai Stablecoin. Au final, les gardiens aident à maintenir la rationalité du marché du Dai et la stabilité des prix.
- **MKR** : Le jeton ERC20 utilisé par les votants MKR pour voter. Il sert aussi de soutien en cas de CDP insolubles.
- **Votants MKR** : Les détenteurs de MKR qui gèrent activement le risque du système Dai Stablecoin en votant sur les paramètres de risque.
- **Maker** : Le nom de l'organisation autonome décentralisée qui est constituée de l'infrastructure technique de la plate-forme Maker et de la communauté de votants MKR.

- **Oracles** : Comptes Ethereum (contrats ou utilisateurs) sélectionnés pour fournir des flux de prix dans les divers composants de la plate-forme Maker.
- **Paramètres de risque** : Les variables qui déterminent (entre autres) quand la plate-forme Maker juge automatiquement un CDP comme risqué, permettant aux gardiens de le liquider.
- **Paramètres de sensibilité** : La variable qui détermine le niveau d'agressivité auquel le système Dai Stablecoin change automatiquement le taux d'objectif en réponse aux écarts du prix du marché du Dai.
- **Mécanisme de rétroaction pour le prix d'objectif (TRFM)** : Le mécanisme automatique par lequel le système Dai Stablecoin ajuste le taux d'objectif afin d'entraîner les forces du marché à maintenir la stabilité du prix du marché du Dai aux environs du prix d'objectif.

Liens

- **Chat** : <https://chat.makerdao.com/> — Plate-forme principale d'interaction de la communauté
- **Forum** : <https://forum.makerdao.com/> — Pour les débats et les propositions
- **Subreddit** : <https://reddit.com/r/makerdao/> — Le meilleur site pour obtenir les dernières nouvelles et des liens
- **GitHub** : <https://github.com/makerdao/> — Référentiel du code Maker public
- **TeamSpeak** : <https://ts.makerdao.com/> — Pour les réunions (conference calls) sur la gouvernance
- **SoundCloud** : <https://soundcloud.com/makerdao/> — Enregistrements des réunions sur la gouvernance
- **Oasis** : <https://oasisdex.com/> — Échange décentralisé du MKR et du Dai
- **Sai** : <https://sai.makerdao.com/> — Stablecoin expérimental