“ Maximal Extractable Value ” ou la Tragédie des Blockchains en tant que Communs

Primavera de Filippi, Philémon Poux, Bruno Deffains

« Maximal Extractable Value » ou la Tragédie des Blockchains en tant que Communs

Primavera de Filippi
CNRS
CERSA, Université Paris 2
pdefilippi@gmail.com

Philémon Poux*
CRED&CERSA, Université Paris 2
ENPC
philemon.poux@gmail.com
CRED, 21 rue Valette 75005 Paris

Bruno Deffains
CRED, Université Paris 2
bruno.deffains@gmail.com

Résumé
Dans cet article nous montrons comment certaines pratiques de Maximal Extractable Value (MEV) qui conduisent à l'accaparement, par certains acteurs des réseaux blockchains, de la valeur produite par d'autres utilisateurs s'apparentent à du parasitisme (freeriding). Nous montrons que ces comportements de passagers clandestins sont d'un nouveau genre, rendu possible par la conception algorithmique et économique, des blockchains qui éliminent pourtant les pratiques classiques de "free-riders". Ces MEV réduisent notamment l'assurance (confidence) que les utilisateurs de la blockchain portent au réseau.
La théorie des jeux non-coopératifs qui sous-tend les relations sur les blockchains ne sont donc pas en mesure de prévenir les MEV inéquitables. Nous nous tournons donc vers les jeux coopératifs, et en particulier dans le contexte des biens communs pour éclairer la situation. La théorie ostromienne des biens communs, en particulier, ses 8 principes permettent de proposer une nouvelle lecture des pratiques iniques de MEV, de leurs conséquences sur les utilisateurs du réseau mais également des solutions existantes.
Nous proposons également de nouvelles pistes, reposant sur une participation communautaire et réintroduisant les enjeux de confiance (trust) afin de préserver la fiabilité du réseau.
Mots clefs : Blockchains, Biens communs, MEV, Passagers Clandestins

Maximal Extractable Value or the Tragedy of the Blockchains Commons

Abstract
This paper shows how some MEV practices, resulting in unfair appropriation of the value created by all users by a small set of blockchains actors is similar to free-riding. In particular we demonstrate that this a new form of free-riding is made possible precisely by the design of blockchains that aims at preventing classical forms of free-riding. This also entails that non-cooperative game theory is not adequate to solve the issues raised by such MEV practices. We thus turn to cooperative games, in particular in the case of commons goods. After recalling that blockchains are a specific type of commons goods we dwell on Ostrom's theory of the governance of the commons, in particular on her design principles to analyze MEV practices and their impact on users confidence in the network. We then go on proposing new avenues for possible solutions, based on collective participation and we note that a trust-based solution may be efficient to sustain confidence.

Keywords: blockchains, Commons, MEV, Freeriding

« Maximal Extractable Value » ou la Tragédie des Blockchains en tant que Communs

Résumé
Dans cet article nous montrons comment certaines pratiques de Maximal Extractable Value (MEV) qui conduisent à l'accaparement, par certains acteurs des réseaux blockchains, de la valeur produite par d'autres utilisateurs s'apparentent à du parasitisme (freeriding). Nous montrons que ces comportements de passagers clandestins sont d'un nouveau genre, rendu possible par la conception algorithmique et économique, des blockchains qui éliminent pourtant les pratiques classiques de "free-riders". Ces MEV réduisent notamment l'assurance (confidence) que les utilisateurs de la blockchain portent au réseau.
La théorie des jeux non-coopératifs qui sous-tend les relations sur les blockchains ne sont donc pas en mesure de prévenir les MEV inéquitables. Nous nous tournons donc vers les jeux coopératifs, et en particulier dans le contexte des biens communs pour éclairer la situation. La théorie ostromienne des biens communs, en particulier, ses 8 principes permettent de proposer une nouvelle lecture des pratiques iniques de MEV, de leurs conséquences sur les utilisateurs du réseau mais également des solutions existantes.
Nous proposons également de nouvelles piste, reposant sur une participation communautaire et réintroduisant les enjeux de confiance (trust) afin de préserver la fiabilité du réseau.
Mots clefs : Blockchains, Biens communs, MEV, Passagers Clandestins

Introduction

Contrairement aux bases de données centralisées, dont les données sont stockées sur un serveur ou un centre de données centralisé géré par une entité unique, une blockchain est un entrepôt décentralisé dont les données sont répliquées sur plusieurs nœuds du réseau. Il existe deux grandes catégories d'acteurs impliqués dans une blockchain : les utilisateurs et les opérateurs. Les utilisateurs du réseau sont ceux qui soumettent des messages au réseau afin d'exécuter une transaction particulière. Les opérateurs peuvent, à leur tour, être divisés en deux sous-catégories : ceux chargés d'enregistrer les nouvelles transactions dans la blockchain (producteurs ou mineurs de blocs) et ceux chargés de vérifier la validité de ces blocs (validateurs de blocs). Si le travail des validateurs est relativement simple, celui des producteurs de blocs peut être très coûteux en temps et en énergie. C'est pourquoi les producteurs de blocs y sont incités par des récompenses de blocs : un montant fixe de crypto-monnaie est automatiquement accordé au producteur de chaque nouveau bloc. Cependant, pour tenir compte du fait que la récompense de bloc diminue avec le temps (par exemple, dans le cas du bitcoin, la récompense attribuée aux mineurs est divisée par deux tous les 210 000 blocs minés), les producteurs de blocs sont également dédommagés par la collecte de frais de transaction. C'est-à-dire que les utilisateurs souhaitant utiliser le réseau joignent à leur transaction une commission pour inciter les producteurs de blocs à inclure ladite transaction dans leur nouveau bloc.

Ainsi, divers producteurs de blocs sont en concurrence, incités par des mécanismes fondés sur la théorie des jeux conçus pour garantir la sécurité de l'ensemble du réseau. Cependant, le système ne fonctionne que si un nombre suffisant de producteurs de blocs participe au réseau, de sorte qu'aucun acteur ne contrôle plus de 50 % des ressources totales utilisées pour produire de nouveaux blocs. Aujourd'hui, dans les principales blockchains, telles que Bitcoin ou Ethereum, le nombre d'opérateurs - à la fois producteurs et validateurs de blocs - est en déclin. Cela ne pose pas seulement des problèmes en termes de gouvernance du réseau, mais fait également peser un risque sur sa sécurité. La plupart des blockchains sont actuellement gouvernées par quelques opérateurs disposant d'une grande part des ressources (par exemple, des "mining pools"). Si ces opérateurs décidaient d'agir de manière concertée, afin de contrôler plus de 50% des ressources impliquées dans le réseau, ils seraient en mesure de produire des blocs plus rapidement que le reste du réseau. Ils leur serait donc possible, potentiellement, de réécrire l'historique de la blockchain, en allant effacer certaines transactions qui ont déjà été enregistrées dans la blockchain, et en re-calculant ensuite tous les blocs successifs jusqu'à obtenir une nouvelle chaîne de blocs qui réplique les transactions de chaîne de bloc originale, à l'exception de celles qui ont voulu été effacées. Puisque les validateurs s'accordent pour toujours suivre la chaîne la plus longue, ils vont automatiquement adopter cette nouvelle chaîne dès que sa longueur dépassera celle de la chaîne de bloc originale. Cela permet ainsi à ces opérateurs de pratiquer la "double dépense" que la blockchain était précisément destinée à empêcher. Pourtant, malgré ce risque avéré, la probabilité de collusion reste faible, car toute tentative d'effectuer une attaque à 51 % mettrait potentiellement en péril l'ensemble du réseau. Cela soulèverait des inquiétudes, tant au niveau de la sécurité que de la durabilité à long terme du réseau, et entraînerait probablement une baisse significative de la valeur marchande de la cryptomonnaie associée. Les opérateurs, qui visent à maximiser leurs profits économiques, sont donc incités à se comporter comme le prévoit le protocole du réseau, ce qui favorise l'assurance dans le réseau et la valeur de la cryptomonnaie associée.

Si les mécanismes d'incitation conçus pour cadrer les comportements des différents acteurs de la blockchain peuvent apparaître comme efficaces, de nouveaux problèmes ont émergé ces dernières années. Certains opérateurs ont commencé à développer un nouveau mécanisme d'accaparement de la valeur du réseau, actuellement appelé "Maximum Extractable Value" ou MEV. Alors qu'une attaque à 51% est facilement détectable par les autres opérateurs du réseau et est généralement condamnée, la MEV est beaucoup plus difficile à détecter car elle ne viole aucune des règles du protocole. En effet, la MEV consiste simplement, pour les opérateurs (tels que les producteurs de blocs ou d'autres acteurs du réseau ayant accès aux transactions soumises via la mempool), à extraire de la valeur des transactions proposées par des utilisateurs en manipulant l'ordre des transactions enregistrées dans la blockchain. En particulier, certaines MEV reposent sur le fait de profiter des efforts d'un autre utilisateur pour identifier une transaction rentable et en capturer la valeur. Le problème de la MEV est qu'il n'est actuellement pas possible de la distinguer de l'activité commerciale légitime, car elle repose souvent sur les mêmes mécanismes de marché. Il est par conséquent difficile d'évaluer son impact économique, et encore plus difficile de concevoir des stratégies qui en atténueraient les effets négatifs. Nous disposons toutefois des premiers résultats de recherches et des efforts de la communauté permettant de donner une première image du phénomène et de son ampleur. Ces travaux permettent de conceptualiser techniquement et économiquement le MEV mais, comme nous le montrons dans le premier chapitre de cet article, de nombreux aspects du problème restent encore à élucider. Il est à cet égard essentiel de souligner que la littérature existante est principalement de nature

technique et ne fournit pas de cadre analytique pour comprendre les enjeux socio-économiques et juridiques associés à cette pratique.

Une façon de voir la MEV est de la considérer comme une taxe sur les utilisateurs du réseau, capturant la valeur de transactions spécifiques qui, autrement, bénéficieraient à ces utilisateurs. En tant que tel, la MEV représente effectivement un transfert de richesse des utilisateurs du réseau vers certains opérateurs. Ce transfert de richesse n'est généralement pas pris en compte par les utilisateurs du réseau, car il se produit "en coulisses" et n'est souvent pas facilement détectable. Par conséquent, la MEV représente un défi économique important, qui peut potentiellement conduire à une concentration de la richesse et, à terme, à une baisse de l'adoption du réseau et donc de sa valeur.

Dans cet article, nous analysons la question de la MEV à la lumière des théories économiques traditionnelles de la maximisation de l'utilité et du parasitisme, aussi appelé passager clandestin (free-riding). En nous appuyant sur les théories existantes des biens communs, nous proposons de considérer les réseaux publics de blockchains comme des ressources communes, qui, malgré les efforts déployés en matière de théorie des jeux et de “mechanism design”, restent soumises à la tragédie des communs. Nous examinons ensuite comment la théorie des communs peut nous aider à identifier des solutions potentielles à la question de la MEV qui affecte de plus en plus de blockchains.

1. Blockchains et biens communs

1.1 Présentation de la théorie des communs

Les économistes distinguent habituellement 3 types de ressources, associées à des formes de gestion différente : les ressources publiques, typiquement gérées par un acteur central contrôlant l'accès et l'utilisation des ressources (gestion publique) ; les ressources privées, généralement associées à des droits de propriété individuels et régies par une dynamique de marché ; et les ressources communes, qui font l'objet d'une propriété collective (par opposition à la propriété publique ou privée) et doivent donc également être gouvernées collectivement. Dans le contexte des blockchains, étant donnée l’impossibilité d’établir des droits de propriété et comme aucune autorité unique n'a la capacité de réglementer et de contrôler le fonctionnement du réseau ou le comportement des acteurs, les approches publiques (basées sur un système centralisé) ou privées (basées sur le marché) sont peu adaptées pour conceptualiser la manière dont les blockchains sont gouvernées. La théorie des biens communs semble donc constituer une approche plus appropriée.

Elinor Ostrom est une des pionnières dans ce domaine : grâce à l'analyse de centaines de communautés gérant différents types de biens communs, elle a développé des outils conceptuels pour analyser la gouvernance des biens communs dans une large variété de contextes (Ostrom, 1990, 2010). Parmi ces outils figurent les 8 Principes (Design Principles) d'Ostrom. Ces principes, résumés Table 1, sont des indicateurs de la soutenabilité et la qualité d’un système de gouvernance d’une ressource commune.

Principe DP1 : Des limites bien définies Il faut que la communauté concernée (**1A**) soit bien identifiée et que la ressource (**1B)** le soit également	**Principe DP5 : Sanctions graduées** Les infractions sont punies et les mécanismes de sanctions sont graduels.
Principe DP2 : Concordance entre les règles et le contexte local Il faut que les contraintes locales soit compatibles avec les règles de la gouvernance	**Principe DP6 : Mécanismes de résolution des conflits** Il existe des instances de résolution de conflits qui sont accessibles rapidement et à bas coût
Principe DP3 : Participation ouverte La plupart des membres de la communauté peuvent participer à l'élaboration des règles	**Principe DP7 : Légitimité externe** La légitimité du groupe à gérer la ressource avec ses propres règles est reconnue par les institutions extérieures (le plus souvent, l'État)
Principe DP4 : Mécanismes de surveillance interne Il y a des membres qui contrôlent les actions des participant·e·s (**4A**). Ils sont responsables devant les autres (**4B**)	**Principe DP8 : Un système imbriqué à plusieurs échelles** L'ensemble des règles, institutions et groupes est organisé à différentes échelles s'imbriquant les unes dans les autres et fonctionnant ensemble

Table 1 Les 8 principes d'Ostrom (Cox et al., 2010; Ostrom, 2010)

Pour comprendre la façon dont ces principes peuvent être atteints, Ostrom (2005) a identifié un ensemble d'aspects clés à examiner dans les systèmes de gouvernance. Elle indique notamment que l'accent ne doit pas être mis uniquement sur les "règles opérationnelles" utilisées pour gérer la ressource au quotidien. En effet, si ces règles opérationnelles peuvent fonctionner au jour le jour, elles ne suffisent pas à faire face à des situations exceptionnelles ou à des crises qui pourraient en révéler les limites, et donc nécessiter leur modification ou leur encadrement. Les règles et normes qui définissent les façons dont ces règles opérationnelles peuvent être modifiées ont été définies par Ostrom comme des "règles constitutionnelles". Qu'elles soient formellement écrites ou non, ces règles sont essentielles car elles ont la capacité d'influencer l'ensemble du niveau opérationnel. Dans le contexte des blockchains, les règles opérationnelles peuvent être assimilées aux règles "on chain", par exemple le protocole de la blockchain ou le code des smart contracts,

tandis que les règles constitutionnelles sont plus difficiles à définir précisément car elles se situent principalement “off-chain”.

Développée à l'origine pour analyser la gouvernance des ressources naturelles, la théorie des biens communs (Ostrom, 1990, 2010) a ensuite été étendue à la gouvernance des ressources numériques (Fuster Morell, 2014; Hess, 2008; Hess & Ostrom, 2007). Bien que les difficultés auxquelles les ressources digitales sont confrontées soient différentes de celles des ressources naturelles (en particulier, le risque n'est pas l'épuisement et la surconsommation de la ressource mais plutôt le manque de contribution), les deux types de ressources doivent trouver des moyens de faire face aux passagers clandestins (free-riders).

Certains auteurs ont déjà analysé les blockchains sous l'angle de la théorie des biens communs. Par exemple, Shackelford & Myers, (2016) ont montré que les blockchains respectent, pour l’essentiel, les 8 principes d’Ostrom, même si ces conclusions sont tempérées par les travaux de Howell & Potgieter (2019) qui soulignent le risque de la concentration du pouvoir dans les mains de certains acteurs. Rozas et al. (2018) ont ensuite été parmi les premiers à appliquer le cadre théorique des biens communs au monde de la blockchain, montrant que les blockchains étaient des outils appropriés pour la gouvernance des biens communs. Poux et al. (2020) ont approfondi la question, en étudiant comment la gouvernance de et par la technologie blockchain peut apporter un changement de paradigme par rapport à la gouvernance traditionnelle en raison des spécificités en termes d'application *ex ante* et de vérifiabilité *ex post* de la blockchain, notamment sur les questions de la surveillance et des sanctions.

La section suivante analyse les blockchains au regard d’un type spécifique de communs.

1.2 Les blockchains comme Commons-Based Peer-Production

Le concept de Commons-Based Peer-Production (CBPP) est souvent attribué à Yochai Benkler. Dans son livre *The Wealth of Networks*, Benkler (2006) montre que l'essor d'Internet et d'autres technologies numériques a permis l'émergence d'une nouvelle forme de production sociale, qu'il appelle la "production par les pairs basée sur les biens communs" (CBPP). Benkler définit les CBPP comme un nouveau modèle économique dans lequel la production d'information et de connaissances est basée sur l'action collective décentralisée et l'échange, plutôt que sur le travail de quelques individus. Le concept a été inventé dans le contexte du mouvement des logiciels libres, mais il a depuis été appliqué à d'autres domaines tels que les œuvres libres, la science ouverte et le matériel libre (Papadimitropoulos, 2018).

Plus généralement, les CBPP peuvent être décrits comme une nouvelle forme d'activité économique qui repose sur les efforts de collaboration d'un réseau distribué d’individus. Sa caractéristique principale est qu'elle ne repose pas sur les logiques du marché ou de l'État, mais sur la coopération volontaire d'un grand nombre d'individus qui fonctionnent selon un ensemble de règles basées sur les biens communs. Le succès de ce modèle a été attribué au fait qu'il permet de produire des biens et des services de haute qualité sans avoir besoin d'un contrôle ou d'une coordination centralisés.

Les CBPP ont été étudiés par des chercheurs, tels que Bauwens & Pantazis (2018), Benkler & Nissenbaum (2006), Morell et al. (2016) ou Siefkes, (2013). Bien qu'il n'existe pas de définition communément admise de ce qui constitue ou non une CBPP, il est généralement admis qu'elle

fonctionne selon quatre composantes ou critères distincts (Morell et al., 2015) : deux se rapportent au résultat de la production et deux au processus par lequel la production est réalisée. Enn ce qui concerne le résultat, la CBPP génère toujours une ressource partagée qui est détenue en commun par un groupe d'individus ou par le public en général. Une telle ressource est généralement caractérisée par un certain degré de reproductibilité ou de dérivabilité. S'agissant du processus, la CBPP implique toujours une participation distribuée, ou ce que l'on appelle communément la collaboration entre pairs, en ce sens qu'elle utilise généralement des moyens de production collaboratifs. Ces méthodes collaboratives ont également tendance à s'appuyer sur des structures de gouvernance décentralisées, plutôt que sur des structures centralisées ou hiérarchiques.

Le fonctionnement de la plupart des blockchains peut être considéré comme une nouvelle forme de CBPP, tant en ce qui concerne le processus que la production. En ce qui a trait au premier aspect, ces réseaux reposent sur la collaboration d'un grand nombre d'individus, responsables du développement du code logiciel (c'est-à-dire le protocole) et de la maintenance du réseau (c'est-à-dire les mineurs et les validateurs). En ce qui concerne le second aspect, les blockchains permettent la production d'un bien public, le registre distribué, qui est le composant central de la technologie. Cette caractérisation des réseaux de blockchains en tant que ressources communes est étayée par le fait que la plupart des principales blockchains, telles que Bitcoin et Ethereum, sont open-source, décentralisées et sans permission, c'est-à-dire ouvertes à la participation de chacun.

Cependant, les blockchains diffèrent des CBPP en plusieurs points. Tout d'abord, les blockchains sont souvent conçues pour être sans confiance (trustless), c'est-à-dire qu'elles ne reposent sur aucune autorité centrale ou tiers de confiance. Les blockchains sont conçues pour avoir une structure de gouvernance décentralisée, de sorte qu'aucune autorité centrale ne puisse influencer les opérations du réseau. Cela contraste avec la production par les CBPP traditionnelles, qui dépendent souvent d'une autorité centrale, telle qu'une fondation ou une entreprise, pour gérer la communauté et les ressources.

Ensuite, les blockchains ont généralement un token natif qui est utilisé pour alimenter le réseau. Le token natif d'une blockchain donne aux utilisateurs une participation dans le réseau et permet d'aligner les intérêts des utilisateurs sur ceux du réseau. Ces tokens natifs sont destinés à réduire les possibilités de parasitisme, tant en ce qui concerne la surconsommation que le manque de contribution. Premièrement, ils permettent d'établir des incitations économiques pour encourager la participation au réseau. En effet, la plupart des blockchains ont un mécanisme intégré pour distribuer des récompenses à ceux qui contribuent au réseau. Par exemple, Bitcoin récompense les mineurs avec des bitcoins nouvellement minés (créés) pour valider les transactions sur le réseau. Comme les mineurs ont un intérêt direct dans le réseau et sont rétribués en bitcoins, ils sont incités à contribuer au bon fonctionnement du réseau et à s'assurer que celui-ci reste sécurisé. Ces incitations économiques sont à l'opposé de la production par les pairs traditionnelle basée sur les biens communs, qui repose souvent sur le travail volontaire. Deuxièmement, le token natif d'une blockchain est souvent utilisé pour payer les ressources nécessaires à l'utilisation du réseau : les utilisateurs qui souhaitent bénéficier des services d'une blockchain doivent généralement verser une contribution à ceux qui en assurent la maintenance. Dans le cas de Bitcoin, les utilisateurs doivent dépenser des bitcoins pour payer les frais de transaction, qui seront distribués aux mineurs chargés de faire fonctionner le réseau, au prorata de leur contribution. Le réseau peut ainsi s'autofinancer, en payant les coûts de fonctionnement du réseau et garantissant un niveau de sécurité suffisant. Cela contraste avec les CBPP traditionnelles, qui dépendent généralement des contributions volontaires des membres de la communauté.

Malgré ces puissants mécanismes d'incitation, le problème du parasitisme n'est pas complètement éliminé dans la plupart des réseaux blockchain. Comme nous le verrons dans la section suivante, le token natif d'une blockchain introduit de nouvelles opportunités de parasitisme, qui n'ont pas été correctement prises en compte par les concepteurs de ces systèmes.

2. MEV et la tragédie des communs

2.1 Typologie des MEV

Le problème de la *Miner Extractable Value* a été originellement identifié à l'origine par pmcgoohan (2014) qui a remarqué que les mineurs ont la possibilité de *frontrun*[1] les transactions les plus rentables soumises au mempool[2] public car ils sont en charge de la sélection des transactions à inclure dans les blocs. Plus précisément, alors que les mineurs choisissent généralement les transactions à inclure dans un bloc en fonction des frais de transaction (ou commission) qui leur sont versés, ils peuvent également manipuler l'ordre des transactions, en insérant leurs propres transactions dans le bloc afin d'en tirer des profits. Ce type particulier de MEV a été initialement défini comme "la valeur qui peut être extraite par un mineur en manipulant l'ordre des transactions dans les blocs qu'il crée" (Judmayer et al., 2021, p. 1). Cependant, comme le processus concerne également d'autres acteurs que les mineurs, le terme a finalement été généralisé à *Maximal Extractable Value*, pour garder le même acronyme.

Avant de décrire les acteurs de la MEV, caractérisons d'abord les différentes formes de MEV existantes, que nous présentons selon leur impact sur le réseau et ses participants. Nous analysons ces impacts selon deux dimensions : la première évalue si la MEV contribue à la réalisation des objectifs du système tel qu'il a été conçu à l'origine, par exemple en améliorant l'efficacité du réseau. Cette dimension peut être analysée de manière relativement objective, et ne concerne que les coûts et la congestion du réseau. La seconde dimension concerne la légitimité perçue de ces pratiques MEV, c'est-à-dire si les participants les considèrent ou non comme "équitables". Cette question est intrinsèquement subjective, car elle repose sur des considérations personnelles des participants, qui peuvent se rapporter à une définition spécifique de l'équité qui peut ne pas faire l'objet d'un consensus universel.

Dans le cadre de cet article, nous proposons une approche de l'équité fondée sur la légitimité de l'appropriation de la valeur : la MEV est considéré comme "équitable" lorsque la valeur extraite du réseau est le résultat de l'effort réel d'une personne pour identifier l'opportunité d'extraction de la valeur, par opposition à l'extraction de la valeur à partir de l'effort des autres. En d'autres termes, lorsque la MEV est "équitable", elle n'empêche pas les utilisateurs de récolter les fruits de leurs efforts. Cette approche est inspirée du deuxième principe d'Ostrom. Cox et al. (2010) écrivent que "certains chercheurs ont souligné l'importance, pour les utilisateurs, de percevoir l'adéquation entre

[1] Frontrun signifie inclure une transaction avant une autre, notamment pour la copier, voir plus bas.
[2] Dans une blockchain, la mempool publique est le recueil de toutes les transactions possibles soumises au réseau, avant qu'elles ne soient incluses dans un bloc. Les mineurs choisissent généralement les transactions à inclure dans un bloc en fonction des frais de transaction. Cependant, ils peuvent également introduire leurs propres transactions dans le bloc qu'ils produisent dans un ordre particulier, afin d'anticiper ou de retarder certaines transactions.

les règles d'appropriation et les règles de contribution comme “équitable”, en reliant cette condition à un principe d'équité que l'on retrouve dans la littérature" (p38). Cela signifie que, dans un bien commun, l'équité est liée à la juste récompense des efforts des participants. En d’autres termes, une appropriation privant les utilisateurs de leur gain peut être considérée comme inique.

Forts de ces deux dimensions, nous pouvons maintenant proposer une typologie des pratiques de MEV :

MEV améliorant l’efficacité

Nous recensons ici les pratiques MEV qui augmentent l'efficacité du réseau et qui sont en adéquation avec les objectifs initiaux du système. Nous distinguons celles qui reposent sur des récompenses explicites (codées en dur) de celles qui reposent sur des mécanismes d’incitation.

Récompenses par le code :

Elles sont fréquentes pour encourager certaines actions. L'exemple le plus évident est celui des mineurs qui reçoivent des cryptomonnaies lorsqu'ils minent un bloc. Ces récompenses existent non seulement au niveau du protocole mais aussi au niveau des dApps et conduisent à des opportunités de MEV. Prenons l’exemple des Cryptokitties. Alors que la vie des Cryptokitties repose sur des mécanismes de marché, leur création requiert une intervention *ex-nihilo*. Pour inciter les utilisateurs à les créer, une récompense est distribuée à ceux que Zargham a surnommé " Crypto Sages Femmes" (Koch, 2018) qui envoie une transaction pour les faire naître. Cet exemple illustre comment l'exécution de certaines actions rémunèrent, automatiquement ceux qui les font.

En ce qui concerne les MEV, l’exemple le plus fréquent de ces récompenses par le code sont les ordres de liquidation (*liquidation calls*). Les systèmes de prêt décentralisés tels que Aave ou DyDx exigent des emprunteurs qu'ils déposent des cautions pour couvrir leurs opérations. Lorsque la valeur de la caution tombe en-deçà d'un seuil, n'importe qui est autorisé à liquider la position en rachetant la caution à un prix fixe, généralement inférieur au prix du marché, de manière à rembourser le prêteur. Ce faisant, le liquidateur (qui envoie l'ordre de liquidation) réalise un profit garanti, tout en assurant au prêteur que la caution ne se dévalue pas (Qin, Zhou, Gamito, et al., 2021). Dans cette forme de MEV, il existe une récompense codée en dur pour le liquidateur qui a un profit garanti lorsqu'il envoie l'ordre.

Récompenses par le marché :

Dans cette forme de MEV essentielle à l’équilibre du marché, les récompenses interviennent pour garantir le fonctionnement efficace d'un système de marché décentralisé. Le type MEV le plus courant dans cette catégorie est l'arbitrage :

Les plateformes d’échange décentralisées (DEX) ont chacune des stratégies différentes pour fixer le taux de change entre deux tokens. Il peut donc arriver qu'il y ait un écart important entre les taux de change des mêmes tokens sur deux DEX différentes. Les utilisateurs peuvent tirer profit de cette situation en effectuant des opérations d’arbitrage, en achetant à bas prix sur une plateforme et en vendant à prix élevé sur l'autre, contribuant ainsi à égaliser les taux de change. Dans ce cas, le profit ne résulte pas de l'exécution de la transaction elle-même mais de l'état du marché à un

moment donné. Si le marché s'appuie délibérément sur ces incitations, elles sont fondamentalement différentes des précédentes car elles dépendent davantage du contexte.

Ces deux types de MEV participent de la finance décentralisée (DeFi). Ils font partie de la conception du système et sont en phase avec ses objectifs (par exemple, fournir un marché décentralisé efficace ou créer des Cryptokitties). En effet, des opportunités d'arbitrage se présentent car il n'y a pas de mécanismes centralisés pour harmoniser les taux de change entre les plateformes. L'arbitrage contribue au bon fonctionnement du système en incitant les utilisateurs à rechercher des opportunités de profit pour rétablir l'équilibre entre les taux de change des plateformes. De même, dans le cas des protocoles de prêt, les liquidateurs font le travail nécessaire de détection des prêts dont les garanties sont trop basses, et sont rémunérés pour ce travail.

MEV détériorant l'efficacité

Nous recensons ici les pratiques de MEV qui ont des conséquences néfastes sur le réseau et ses participants. Elles découlent notamment d'une asymétrie de pouvoir et d'information qui permet à certains acteurs de s'approprier la valeur des transactions émises par d'autres. Notre typologie démontre que non seulement ces pratiques réduisent l'efficacité du réseau mais qu'elles sont également inéquitables.

Frontrunning :

Cette forme de MEV repose sur la possibilité, pour certains acteurs, d'insérer certaines transactions avant les autres. D'une part, les mineurs peuvent réorganiser les transactions parce qu'ils sont responsables de la création des blocs. D'autre part, les utilisateurs (appelés *searchers*) qui identifient des opportunités de MEV sont en compétition avec d'autres utilisateurs du réseau pour s'assurer que leurs transactions seront prioritaires dans la file d'attente. Le système PGA (*Price Gas Auction*) repose sur le fait que les mineurs incluent en premier les transactions dont le prix du gaz, qui rétribue les mineurs, est le plus élevé dans leurs blocs. Par conséquent, lorsqu'un utilisateur détecte une opportunité MEV, il peut soumettre la même transaction avec des prix du gaz légèrement supérieurs afin de la devancer. Quand cette pratique se généralise, elle entraîne des guerres d'enchères, et une hausse du prix du gaz qui, en fin de compte, nuit à tous les utilisateurs du réseau. Le *frontrunning* permet à ceux qui le pratiquent de "voler" des transactions rentables, en les reproduisant (à leur bénéfice) pour inclure ces transactions modifiées plus tôt dans le bloc. En particulier, les ordres d'arbitrage ou de liquidation sont des cibles courantes du frontrunning.

MEV par attaque sandwich :

Dans une Attaque Sandwich (AS), une transaction (classiquement une commande sur un DEX) est enveloppée entre deux transactions supplémentaires, conçues pour extraire de la valeur de la transaction originale, aux dépens de l'auteur original et au profit de l'attaquant (voir figure 1). L'AS utilise le fait que les ordres sur les DEX incluent un "slippage" pour tenir compte de la possibilité d'un changement dans le marché entre le moment où l'ordre a été envoyé et celui où il sera ajouté à la chaîne. Les AS modifient le marché de manière à ce que les conditions se situent dans la fourchette de slippage de l'ordre mais soient suffisamment défavorables pour que le searcher puisse réaliser un bénéfice (et réduire le celui de l'utilisateur initial). Un aspect négatif des AS sur

le réseau (en plus de contribuer à la PGA) est qu'ils augmentent le nombre de transactions et utilisent plus d'espace de bloc, réduisant ainsi l'efficacité de la chaîne.

MEV par agression :

Ce type de MEV vise à effectuer une transaction afin de créer une opportunité de profit au détriment d'un autre utilisateur. Cela est rendu possible par l'asymétrie de pouvoir qui permet aux mineurs et aux chercheurs de manipuler l'ordre des transactions. Ce type de MEV repose principalement sur les front ou backrunning mais également sur les flashloans. Les flashloans dépendent de la faculté, propre à la blockchain, d'inverser certaines transactions atomiques si certaines conditions ne sont pas réunies. Ainsi, grâce au recours aux smart contracts, le prêt, l'opération pour laquelle l'argent est utilisé et le remboursement du prêt (avec intérêts) peuvent être regroupés en une seule transaction. Si, à la fin de cette transaction, l'emprunteur n'est pas en mesure de rembourser le prêt, aucune de ces opérations n'est exécutée. Cela garantit que le prêteur sera remboursé et que l'emprunteur n'a pas besoin d'avoir de garantie (Qin, Zhou, Livshits, et al., 2021).
En voici quelques exemples :

- Manipulation de marché : ce type de MEV provient de la possibilité de modifier temporairement les taux de change en émettant une transaction à large échelle et en profitant de la distorsion temporaire du marché qui en résulte pour vendre en position longue ou courte. Ces attaques entraînent une perte nette pour les autres acteurs de la blockchain (soit les utilisateurs ciblés, soit les DEX directement). Ces attaques sont facilitées par les *flashloans* qui permettent un accès instantané à la grande quantité d'argent nécessaire pour biaiser le marché.
- Liquidation forcée : Parfois, une transaction n'est pas rentable en tant que telle, mais le changement d'état de la blockchain qui en résulte conduit à une opportunité de MEV (ici, une liquidation). Le searcher peut donc effectuer un backrun de la transaction, en incluant un ordre de liquidation juste après cette transaction, pour bénéficier du profit garanti par le code. Alors que le frontrunning se traduit généralement par des opportunités de profit manquées pour les émetteurs de la transaction initiale, le backrunning se traduit généralement par des pertes réelles. Supposons qu'Alice remarque que la caution associée à un de ses emprunts risque d'être sous-dotée (et est donc susceptible d'être liquidée) et envoie un ordre pour renflouer sa position et éviter la liquidation. Quelqu'un détecte cette transaction et inclut un ensemble de transactions qui vont modifier le marché, rendre la position liquidable et la liquider[3]. Les flashloans facilitent également ce type de transactions puisqu'ils permettent de modifier le marché sans fonds propres.

Attaques par "Time-Bandit" :

Lorsqu'un bloc contient suffisamment d'opportunités MEV, il est dans l'intérêt d'un mineur d'essayer de reminer le bloc (c'est-à-dire d'essayer de miner un nouveau bloc, incorporant ces opportunités MEV à la même hauteur pour le remplacer) plutôt que de miner un nouveau bloc à la fin de la chaîne. Ce type de MEV est extrêmement problématique car une tentative réussie conduirait à réécrire l'histoire de la blockchain. Qui plus est, cela peut menacer la stabilité de l'ensemble du réseau blockchain, car il pourrait être dans l'intérêt économique de chaque mineur de ré-exploiter les transactions les plus rentables des blocs précédents, plutôt que de continuer la

[3] Dans ce cas, c'est parce qu'Alice a remarqué un risque sur son emprunt et a essayé de le prévenir qu'elle a été attaquée. Cela la met dans une situation intenable : si elle ne fait rien, elle risque la liquidation, mais si elle essaie d'y remédier, elle signale cette opportunité et se fait attaquer. C'est ce qu'on appelle "Dark Forest" (Robinson & Konstantopoulos, 2020)

chaîne et d'inclure de nouvelles transactions. Combinées au risque de “selfish mining” (Eyal, 2015), ces attaques de type time-bandits mettent en péril la sécurité et la durabilité de la blockchain. Ce type d'attaques est fondamentalement différent des précédentes car elles ne se font pas uniquement par une réorganisation des transactions mais par une réécriture réelle de l’histoire de la blockchain. Si elles sont intrinsèquement plus nuisibles que les autres pratiques MEV, elles sont également beaucoup plus coûteuses à mettre en œuvre, car elles nécessitent une part importante de puissance de calcul (similaire à celle requise pour une attaque à 51%). Par conséquent, le reste de notre discussion ne portera pas sur les attaques de type "time-bandit".

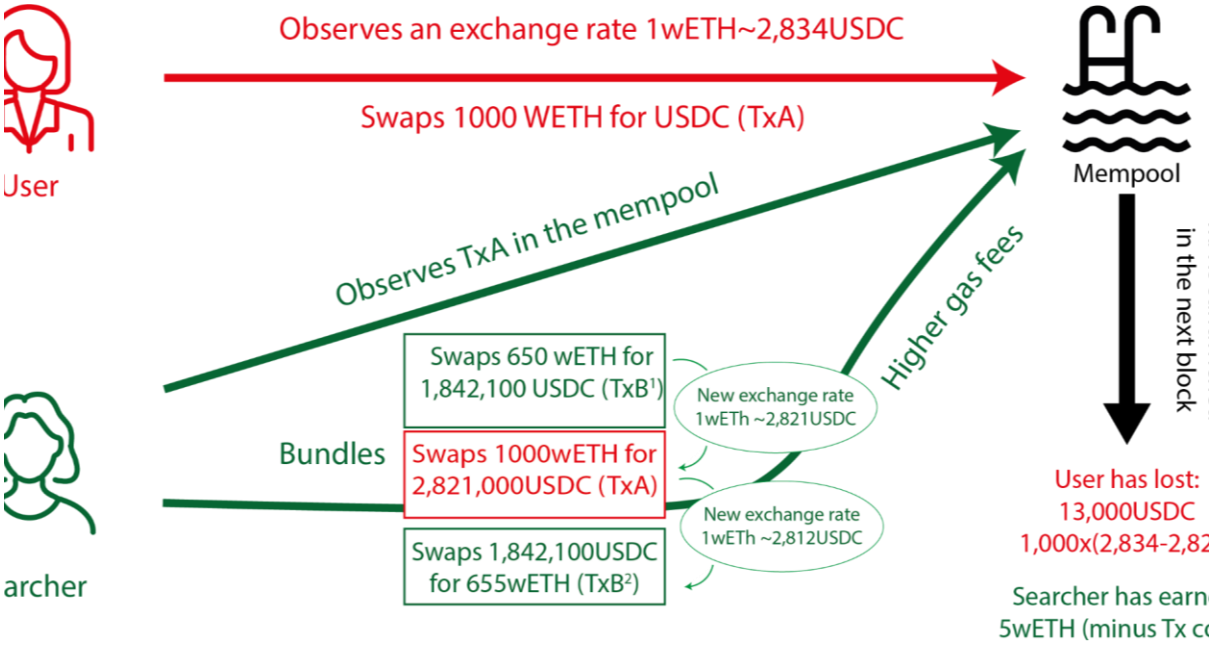

Figure 1 : Exemple d’une attaque sandwich

Adapté de https://eigenphi-1.gitbook.io/classroom/arbitrage-types/sandwich-arbitrage

Il apparaît donc que ces deux grandes catégories de MEV sont très différentes dans leur nature et dans leurs conséquences. D'une part, les MEV positives sont nécessaires au maintien de l'équilibre des marchés de DeFi, car elles permettent une détection efficace des prix dans un contexte décentralisé. D'autre part, les MEV négatives sont préjudiciables au réseau, car elles entraînent une augmentation des frais de gaz et occupent plus d'espace dans les blocs.

Qui plus est, elles permettent à un ensemble de participants au réseau (producteurs ou searchers) de monopoliser la valeur qui peut être tirée du réseau. Piet et al. (2022) ont notamment pu estimer qu’au moment de la parution de leur étude, les mineurs s’accaparaiennt l’essentiel de la MEV en raison de leur pouvoir et de l'asymétrie de l'information. Selon notre définition de l’équité, reposant sur l’adéquation entre l’effort fourni et la redistribution de la valeur, ces pratiques sont donc inéquitables.

2.2 Une nouvelle tragédie des communs

Les économistes différencient les types de ressources sur la base de deux paramètres : l'exclusivité et la non-rivalité. Un bien est excluable si son accès peut être interdit à des individus.

Un bien est rival s'il ne peut être utilisé que par une seule personne à la fois, empêchant les autres de l'utiliser également. Le problème des passagers clandestins concerne principalement les biens non excluables, qu'il s'agisse de biens publics ou de ressources communes. Puisqu'il est impossible d'exclure des personnes, des individus peuvent être tentés, — de manière égoïste — de consommer plus que ce à quoi ils ont droit et/ou de contribuer moins que ce qu'ils doivent. Ces individus comptent sur les autres pour faire le travail de maintien et d'exploitation de la ressource, sans en assumer eux-mêmes la responsabilité. Quand trop d'acteurs se mettent à agir de la sorte, cela conduit à la surexploitation (dans le cas de biens rivaux) ou à un manque de contribution (dans le cas de biens non rivaux) de la ressource. Ce dilemme est généralement appelé la "tragédie des communs" (Hardin, 1968).

Malgré l'introduction d'incitations fondées sur les cryptomonnaies, les blockchains, comme de nombreuses autres ressources communes, souffrent de problèmes similaires. Comme expliqué ci-dessus, les concepteurs des blockchains ont introduit différents types de solutions basées sur l'économie des cryptomonnaies et des tokens pour résoudre le problème de parasitisme. Cependant, le risque de comportements opportunistes n'est pas totalement éliminé de ces réseaux, car, paradoxalement, ces mêmes mécanismes d'incitation créent de nouvelles possibilités de parasitisme, qui ne sont plus fondées sur la surconsommation ou la sous-contribution, mais plutôt sur une appropriation injuste de la valeur. Cela produit alors des effets négatifs lorsqu'il s'agit de la répartition des ressources entre les opérateurs du réseau. Un tel comportement opportuniste consiste à "profiter" du travail des autres, précisément en s'appropriant la valeur générée par leurs transactions. En d'autres termes, ce comportement n'enfreint pas les règles du réseau, mais il nuit aux intérêts de l'ensemble de ses utilisateurs. Le problème résulte ici d'une appropriation "inéquitable" de la valeur dans le sens où ceux qui parasitent profitent du surplus généré par le travail des autres, qui ne sont plus rémunérés pour leurs efforts. Même si cette appropriation ne peut pas être qualifiée "juridiquement" de vol, l'acte en question est une forme d'externalité négative qui nuit largement à l'ensemble du réseau.

Nous savons que la technologie blockchain a été conçue comme une solution potentielle à l'érosion de la confiance envers les institutions traditionnelles et plus généralement dans les intermédiaires en ligne, car elle vise à éliminer le besoin de confiance entre les acteurs. Le principe sous-jacent à cette technologie et de ses diverses applications est que les utilisateurs se soumettent à l'autorité d'un système technologique dont ils ont l'assurance qu'il est immuable, plutôt qu'à des institutions centralisées considérées comme peu fiables. Les blockchains visent à réduire les problèmes de principal-agent tels que l'aléa moral ou la sélection adverse qui caractérisent la plupart des relations de confiance. Cela a conduit de nombreux chercheurs à décrire la blockchain comme une "*trustless technology*" (Werbach, 2018). Cependant, comme le notent De Filippi et al. (2020), cette approche ne considère cette propriété des blockchains que sous un angle négatif (la technologie blockchain n'a pas besoin de confiance pour fonctionner). Les auteurs suggèrent une perspective positive en considérant ce que la technologie blockchain produit pour fonctionner, c'est-à-dire reconnaître que "la technologie blockchain reconfigure la confiance dans la société, en soutenant que la technologie ne se qualifie pas comme une 'machine à confiance' [*trust machine*] mais plutôt comme une 'machine à assurance' [*confidence machine*]" (p. 2). Cette distinction entre confiance et assurance, empruntée à Luhmann (2000), est cruciale car elle nous permet de comprendre que la question porte moins sur les propriétés distinctives de la confiance (*trust*), caractérisée par un risque et une incertitude, que sur le sentiment d'assurance (*confidence*) qui ne présente pas ces caractéristiques : "l'état d'assurance existe implicitement chaque fois qu'une personne s'engage avec une autre sans avoir besoin de réfléchir à l'existence d'un risque ou d'une incertitude, éliminant ainsi la nécessité de choisir parmi des alternatives. En

ce sens, l'assurance, contrairement à la confiance, apparaît lorsqu'un individu croit que la personne ou le système avec lequel il interagit n'a pas la possibilité de trahir ses attentes" (De Filippi et al., 2020, p. 4). En tant que telle, l'assurance découle de la prévisibilité des événements futurs et elle est définitivement différente du risque qui est inhérent à la confiance.

Les blockchains génèrent une forme d'assurance pour leurs utilisateurs grâce aux incitations économiques et la théorie des jeux qui les sous-tendent. Combinées aux propriétés mathématiques des fonctions de hachage et de la cryptographie à clé publique-privée, les utilisateurs peuvent prévoir avec un haut degré de certitude le comportement des acteurs sur le réseau. L'automatisation et l'impartialité inhérente au protocole d'un réseau basé sur la blockchain devient une source d'assurance. Comme l'infrastructure technologique n'est pas gérée (ni contrôlée) par une institution (sociale ou politique), les systèmes basés sur les blockchains sont souvent considérés comme une alternative préférable à bon nombre de nos institutions actuelles dirigées par des humains et donc corruptibles.

Lorsque l'on considère les blockchains comme "machine à assurance" (confidence machine), le principal problème consiste à définir dans quelle mesure le risque d'appropriation déloyale (telles que les MEV de second type) a un impact négatif sur les attentes (et donc l'assurance) des utilisateurs du réseau, car il devient difficile d'avoir l'assurance qu'il n'y aura pas de "vol" de la valeur créée. En d'autres termes, la machine à assurance va partiellement s'effondrer et le recours au réseau peut s'en trouver affecté.

Du côté des utilisateurs, nous pouvons distinguer deux types d'attentes. La première concerne le fonctionnement des blockchains, notamment en termes d'immuabilité, de sécurité et de résilience. La seconde concerne les services que les blockchains peuvent offrir et l'assurance que les transactions de chacun seront effectivement ajoutées aux blockchains. Dans le contexte du MEV, l'assurance d'immuabilité n'est pas affectée alors que la seconde est rompue, ce qui fait apparaître une nouvelle "tragédie des blockchains en tant que communs".

Cette approche, reposant sur la distinction entre confiance et assurance, trouve un écho dans la théorie des jeux. En effet, il apparaît que les blockchains reposent essentiellement sur la théorie des jeux non coopératifs qui fonde la nature même du lien entre les opérateurs de la blockchain. Cependant, pour résoudre les problèmes provoqués par ce *mechanism design*, il peut être utile de mobiliser les jeux coopératifs. Un aspect central qui apparaît, notamment de la théorie des communs, est que, pour que les intérêts collectifs et individuels s'alignent une véritable coopération peut être nécessaire. Cela fait notamment référence au problème susmentionné de la "tragédie des communs" de Hardin, tel qu'il est conventionnellement compris en termes de théorie des jeux.

En effet, les travaux d'Ostrom (1990, 2010) ont souligné que la conclusion de Hardin était, à maints égards, trop simpliste, car il existe de nombreux exemples empiriques de gestion par les communs réussies et durables. En particulier, cette gestion collective s'appuie sur le fait, prouvé à la fois en économie expérimentale et empirique, que les acteurs agissent souvent au-delà de leur intérêt immédiat afin de collaborer et préserver une ressource. C'est par ce recours à la coopération que les biens communs sont en mesure de résoudre les problèmes de passagers clandestins. En outre, dans de nombreuses expériences, où l'intérêt personnel devrait théoriquement conduire à une contribution nulle à un bien public, de nombreuses personnes contribuent en fait de manière significative. Pour citer Ostrom (2000): "Dans tous les régimes de gouvernance auto-organisés connus qui ont survécu pendant plusieurs générations, les

participants investissent des ressources dans la surveillance et la sanction des actions des autres afin de réduire la probabilité de resquillage." (p.138).

Cela nous incite donc à nous pencher vers une solution basée sur les communs pour résoudre les problèmes de passagers clandestins causés par les MEV.

3. Vers une solution basée sur les biens communs

Au cours des dernières années, différentes solutions ont été proposées pour résoudre le problème des MEV, principalement sur Ethereum. Nous les passons brièvement en revue, avant de les analyser sous l'angle de la théorie des biens communs. Cette analyse nous permet d'identifier de nouvelles pistes, inspirées des biens communs, que nous discutons également.

3.1 Solutions existantes

La plupart des solutions actuelles consistent à éviter la publication des transactions sur la mempool publique, afin de réduire les risques de surenchères par la PGA. Cela implique généralement d'ajouter une couche supplémentaire entre les utilisateurs proposant une transaction et l'inclusion de cette transaction dans un bloc. Des relais privés (comme le réseau Taichi) peuvent être utilisés pour envoyer la transaction directement à un mineur, dont on sait qu'il ne fera pas de MEV déloyale. Les "Request for Quotes" (RFQ) sont des transactions qui comprennent certaines métadonnées (telles que l'adresse de la transaction et le prix convenu à l'avance). C'est un moyen de sécuriser un ordre sur une DEX pour éviter d'inclure un "slippage" et réduire ainsi le risque de frontrunning ou de SA.

Les services d'ordonnancement équitable (fair sequencing services) proposent de séparer la création des blocs et leur validation. La création des blocs se fait alors de manière "équitable" afin d'éviter une MEV "inéquitable". Chainlink est le plus avancé de ces services avec une approche en deux temps (Breidenbach et al., 2021). Tout d'abord, il s'appuie sur un réseau décentralisé pour ordonner les transactions avant d'envoyer les blocs de transactions aux mineurs. Dans la phase 2, un protocole d'ordonnancement équitable, Aequitas, basé sur le principe First-In/First-Out, empêche la manipulation de l'ordre des transactions.

Actuellement, la solution la plus populaire au MEV est fournie par Flashbots, une société qui se consacre à la recherche et au développement de solutions aux problèmes liés à la MEV. Ses fondateurs, en particulier Phil Daian, ont été parmi les premiers à sensibiliser à la question (Daian et al. 2020) et restent à ce jour une référence influente dans la discussion sur la MEV. Le service principal de Flashbots est MEV-gETH, un logiciel qui permet aux utilisateurs du réseau ou aux searchers de proposer des « paquets de transactions » (bundles) aux producteurs de blocs en partageant la valeur extraite avec les mineurs. Les « paquets » sont une façon de proposer un ensemble de transactions dans leur ensemble plutôt qu'individuellement. L'exécution devient alors "tout ou rien", empêchant les mineurs d'exécuter des MEV basées sur l'ordre des transactions.

Les mineurs sélectionnent alors les paquets en fonction de l'efficacité du gaz plutôt que de son prix, ce qui permet de réduire le prix du gaz sur le réseau. De plus, le processus est transparent et tout le monde peut participer et devenir un searcher. Pour aider les mineurs à trier les paquets en fonction de qui les a proposés, le système d'enchères est également complété par un système de réputation. Flashbots est un relais privé très spécifique qui, en plus d'établir un canal de communication privé entre les utilisateurs du réseau et les producteurs de blocs, offre également

des services de regroupement et de classement des transactions en paquet. En plus de proposer ce logiciel, Flashbots collecte et publie également des données qui servent à estimer la quantité de MEV se produisant au fil du temps sur Ethereum, fournissant ainsi à la communauté de précieuses informations.

Ces différentes solutions ont été conçues à des fins distinctes. D'une part, l'objectif de Flashbots est de démocratiser la MEV, mais pas de la prévenir. Il n'empêche pas les utilisateurs de s'engager dans le frontrunning ou le backrunning des transactions, ou les AS ; il leur permet simplement de le faire d'une manière plus transparente et ouverte. D'autre part, Chainlink vise à éliminer toute sorte de réorganisation des transactions et à séparer la proposition de bloc et sa validation. Cela empêche toute possibilité de manipulations, y compris celles qui peuvent augmenter l'efficacité (comme l'inclusion de l'arbitrage au sommet d'un bloc) et ne distingue pas parmi les pratiques de MEV, y compris celles qui peuvent être considérées comme "équitables". Un autre problème est que l'ordre repose sur le moment où une transaction a été reçue par les nœuds et non émise. La raison est technique, car un ordre d'envoi équitable "nécessiterait un horodatage côté client fiable ou vérifiable" (Kelkar et al., 2020) et donc un acteur centralisé. Toutefois, des chercheurs ont montré que des agents malveillants pourraient manipuler le réseau pour différer l'arrivée de certaines transactions permettant ainsi un autre type de manipulation (Tang et al., 2022). Cela reste hypothétique, notamment tant qu'Aequitas n'est pas généralisé mais ces questions doivent être débattues en termes de risques et d'opportunités par l'ensemble de la communauté.

La partie 1.2 a montré que les blockchains sont des CBPP, or il est intéressant de remarquer qu'aucune de ces solutions ne s'appuie sur la communauté pour régler la question de la MEV. Flashbots adopte une approche basée sur le marché qui résout les problèmes d'efficacité présentés dans la section 3 mais n'aborde pas la question de l'équité. Chainlink adopte une position radicale en empêchant toute réorganisation des transaction, équitable ou non. Nous suggérons qu'il pourrait y avoir une autre voie, basée sur la communauté, bénéficiant des apprentissages des biens communs, en particulier basée sur la théorie des jeux coopératifs.

3.2 MEV et principes ostromiens

Pour comprendre ce qu'une solution basée sur les biens communs peut apporter, examinons d'abord les MEV, en particulier celles détériorant le réseau, au regard des 8 principes d’Ostrom.

Cette évaluation présentée en Table 3 révèle que certaines pratiques de MEV sapent la gouvernance collective de la blockchain en tant que bien commun. Les quatre premiers principes sont notamment remis en cause par ces pratiques. En ce qui concerne le DP1, les searchers qui explorent la mempool pour identifier les transactions rentables assurent un nouveau rôle qui modifie la définition standard des limites de la communauté. Ostrom et al. (1994) ont montré comment la gouvernance durable des biens communs nécessite une identification claire des différents rôles possibles pour les membres de la communauté, ainsi qu'une définition claire de ce que ces rôles impliquent (en termes de droits et d'obligations) et de qui peut les occuper. Actuellement, le rôle des searchers et la légitimité de leurs activités ne font pas l'objet d'un consensus collectif, comme en témoigne le fait que certains considèrent leur comportement comme injuste (Zhang & Jie, 2022). Le DP2 est particulièrement mis en cause car il repose sur la proportionnalité entre les coûts et les bénéfices associés aux différentes actions entreprises par les membres de la communauté. Les utilisateurs victimes de MEV "inéquitable" ont fourni des efforts coûteux pour identifier des opportunités de profit, mais n'en tirent pas les bénéfices

attendus. Comme nous l'avons mentionné ci-dessus, l'approche de l'équité que nous avons proposée est un indicateur de ce principe ostromien, car nous suggérons qu'aucune situation dans laquelle la MEV laisse des efforts sans récompenses ne saurait être considérée comme équitable. La question de la participation ouverte (DP3) sera abordée plus spécifiquement dans la section suivante, qui propose une approche participative pour résoudre la MEV. Alors que la surveillance (DP4) est généralement aisée en raison de la transparence d'une blockchain, il demeure difficile de détecter des transactions de MEV, et ce malgré des efforts conséquents de la communauté (Flashbots et d'autres chercheurs notamment), notamment parce que les transactions de MEV ne diffèrent en rien des transactions normales.[4] Les sanctions (DP5) ne peuvent pas être facilement réalisées sur la chaîne parce que le design même de la blockchain les rend difficiles ; cependant des mécanismes de sanctions sociales (basés sur la réputation) pourraient s'avérer efficaces. De tels mécanismes sont néanmoins confrontés aux problèmes causés par le côté pseudonyme des blockchains. Enfin, les mécanismes de résolution des conflits (DP6), la légitimité externe (DP7), et l'imbrication des règles (DP8) ne sont pas affectés par les pratiques MEV.

DP1 Des limites bien définies Si la ressource est bien définie (la blockchain), les différents rôles, en particulier la question des searchers, ne font pas l'objet d'un accord collectif.	**DP5 Sanctions graduelles** Nécessite un changement de paradigme
DP2 Concordance entre les règles et le contexte local La règle d'appropriation n'est pas proportionnelle aux coûts	**DP6 Mécanisme de résolution des conflits** NA
DP3 Participation ouverte Pour l'instant, la plupart des utilisateurs n'ont pas voix au chapitre	**DP7 Application locale des règles** Garantie par l'automatisation et la distribution
DP4 Mécanisme de surveillance interne Le contrôle de la MEV est difficile car les transactions apparaissent comme normales.	**DP8 Plusieurs couches d'entreprises imbriquées** La gouvernance des blockchains se fait nécessairement par couches imbriquées.

Table 2 : Evaluation de la MEV au regard des 8 principes ostromiens

Adapté de Cox et al., 2010; Ostrom, 2010

[4] Il est notamment possible de détecter les types de MEV les plus répandus (comme les AS ou les liquidations) mais il existe également de nombreuses variations ou pratiques bien plus difficiles à identifier.

Cette analyse permet d'identifier les aspects clefs de la gouvernance des communs qui sont le plus menacés par la pratique inéquitable des MEV. En particulier, on peut noter que tant que ces pratiques subsistent, le deuxième principe ostromien ne peut être respecté. Pour trouver des solutions susceptibles de résoudre ces problèmes, il faut donc parvenir à une participation collective via un processus ouvert.

3.3 Une nouvelle piste

En examinant les solutions existantes, nous constatons qu'elles se concentrent sur les règles opérationnelles et proposent avant tout une solution technique. Par exemple, alors que Flashbots et Chainlink peuvent techniquement résoudre certains problèmes associés au MEV et en particulier ceux associés aux principes DP1 et DP4, ils ne peuvent pas résoudre, par la technique seule, les DP2 et DP3 qui nécessitent l'implication et l'adoption par la communauté. De plus, comme cet article le souligne, ces deux solutions peuvent entraîner de nouvelles formes d'opportunités de profit pour certains acteurs (soit en généralisant la MEV pour Flashbots, soit pour les personnes ayant la capacité infrastructurelle d'envoyer leurs transactions avant les autres), et n'éliminent donc pas tout risque de passagers clandestins.

La théorie de la gouvernance des biens communs nous informe que l'adoption et la prise de décision collective doivent se faire en adéquation avec les "règles constitutionnelles" de la communauté. Dans notre cas, cela signifie en particulier répondre aux attentes de l'ensemble des utilisateurs quant à ce qu'est une blockchain afin de préserver la "machine à assurance".
Bien que Chainlink et Flashbots identifient tous deux explicitement les prémisses et les interprétations de ces attentes, ces deux approches ne sont pas complètement identiques, singulièrement sur certains aspects clés tels que la notion "d'équité" (voir le blog Daian, 2021).

Nous conjecturons que la communauté dans son ensemble pourrait bénéficier d'un engagement explicite dans une consultation participative sur les raisons pour lesquelles elle considère la MEV comme néfaste. Cela pourrait ensuite servir à éclairer une solution qui bénéficierait d'une forte légitimité de la part des utilisateurs et serait donc plus susceptible de satisfaire les 8 principes ostromiens.

Cette solution pourrait notamment s'appuyer sur la théorie des jeux coopératifs inspirée de la théorie des biens communs. Parce que les blockchains disposent d'une communauté active prête à collaborer pour réduire les effets néfastes sur le réseau (que ce soit en termes d'efficacité ou en termes d'équité), les enseignements tirés de la CBPP et d'autres communs démontrent que la coopération peut fournir une solution efficace à un coût relativement faible. Parce que les échanges sur une blockchain forment un jeu répété et qu'il est dans l'intérêt de tous de ne pas conduire à une dépréciation de système, la théorie des jeux coopératifs et la collaboration peuvent s'avérer prometteuses.

La communauté blockchain dispose déjà d'un exemple récent d'un tel processus : les attaques de type time-bandit ont été unanimement condamnées comme mettant en danger la stabilité du réseau dans son ensemble. Par conséquent, bien que ne disposant pas de solution technique pour les empêcher, la communauté Ethereum dans son ensemble (y compris les puissants *mining pools* qui avaient la capacité de les réaliser) s'est engagée à ne pas le faire, afin de préserver la blockchain. Bien qu'il ne soit pas certain qu'un engagement similaire puisse émerger pour d'autres types de MEV, nous encourageons la communauté à explorer cette direction.

Les approches fondées sur les communs reposent généralement sur la confiance, ce qui peut sembler incompatible avec la logique de la blockchain. Cependant, les solutions existantes telles que les relais privés et même Flashbots (par le biais de leur mécanisme de réputation) ont réintroduit la confiance pour pallier le manque d'assurance envers l'inclusion des transactions. Loin de considérer cela comme une vulnérabilité du système, nous estimons que c'est un indicateur que les solutions basées sur la confiance sont une direction prometteuse à explorer.

C'est dans cette perspective que nous avons proposé une contribution pour définir ce que nous considérons comme équitable. Notre approche semble se distinguer de celles Flashbots ou de Chainlink, et nous espérons qu'elle suscitera un débat constructif et qu'elle permettra d'aborder la question du MEV dans le cadre plus large de la gouvernance des communs. Bien que particulièrement décentralisées, les blockchains peuvent s'appuyer sur leur communauté pour concevoir des solutions coordonnées dans un système polycentrique sans s'appuyer uniquement sur les mécanismes de marché ou des solutions techniques.

Par définition, cette approche doit être participative et nous ne pouvons pas fixer d'autorité la direction qu'elle devrait prendre. Nous pouvons toutefois recommander de s'inspirer de la littérature ostromienne pour adopter les meilleures pratiques.

Conclusion

Les blockchains telles qu' Ethereum ont été conçues pour permettre à leurs utilisateurs de se fier à la qualité de leurs mécanismes d'incitation et de sécurité en assurant un réseau sûr, immuable et transparent ne nécessitant aucun acteur de confiance. À ces fins, elles reposent sur des jeux non coopératifs qui encouragent des acteurs à entretenir et faire évoluer le réseau en échange de récompenses. Ce système, en intégrant dans ses paramètres les risques de parasitisme et de passagers clandestins, a permis d'éliminer ces derniers par l'élaboration de protocoles inviolables.

Toutefois, cette codification très forte des blockchains a aussi permis l'émergence d'autres types de pratiques, respectant les termes de ces protocoles, mais s'apparentant néanmoins à du parasitisme. En particulier, la Maximal Extractable Value (MEV) a récemment fait couler beaucoup d'encre en raison de l'ampleur du phénomène. Bien que de nombreuses solutions soient en cours de développement ou de déploiement, la recherche autour de la MEV reste relativement rare en raison de la nouveauté du sujet et se concentre souvent sur ses aspects techniques. Nous proposons une approche centrée sur la théorie des communs pour comprendre si elle pourrait déboucher sur une nouvelle forme de solution aux problèmes causés par la MEV.

Tout d'abord, nous avons proposé une typologie des pratiques de MEV qui distingue leurs conséquences sur le réseau (objectives) et celles sur les utilisateurs (subjectives). Afin de caractériser ces dernières, nous avons proposé une approche en termes d'équité fondée sur la juste rétribution des efforts. Cela nous a permis de définir explicitement les pratiques inéquitables de la MEV. Cette première étape de définition nous a ensuite permis de développer nos contributions à ce champ de recherche qui sont de deux ordres.

La première a consisté à démontrer que la MEV constituait une nouvelle forme de parasitisme. Cette forme, propre à la blockchain, a été rendue possible par le fait que les blockchains s'affranchissent du recours à la confiance, la remplaçant par de l'assurance envers le fonctionnement du réseau. Ce nouveau type de parasitisme, bien que distinct de ceux

classiquement redoutés par des gestionnaires de ressources collectives, menace également la stabilité du réseau et constitue un vrai enjeu pour le futur.

Notre seconde contribution fut de relier cette remarque à la théorie des communs. Ce champ de recherche analyse et explique comment des communautés gouvernant collectivement une ressource parviennent à limiter les comportements opportunistes notamment par le biais de coopération et de l'instauration de valeurs sociales telles que la confiance ou la réputation. Fort de cette théorie, nous avons identifié les principaux enseignements qu'elle pouvait apporter à la situation actuelle concernant la MEV.

En particulier, le co-développement d'une solution communautaire, réintroduisant une forme de confiance, pourrait être prometteur. Cette approche est d'autant plus porteuse de sens que les blockchains sont elles-mêmes des communs. La nécessité de s'emparer de la question des communs et d'autant plus prégnante que les solutions proposées actuellement requièrent une forme de confiance sans l'énoncer explicitement, ce qui pourrait provoquer des asymétries de pouvoirs qui viendront à terme déstabiliser l'ensemble du système.

Afin d'étayer nos propos, nous avons également évalué la MEV au regard des principes ostromiens de bon fonctionnement de la gouvernance d'un commun. Cela nous a permis de mettre en évidence que la gouvernance des blockchains comme commun décentralisé était ébranlée par ces pratiques et qu'aucune des solutions disponibles aujourd'hui ne permettaient, en l'état actuel, de résoudre ces questions.

Nous proposons donc une piste reposant explicitement sur la coopération et des mécanismes sociaux (et non plus économiques), pour apporter des éléments de réponses. A défaut de recommandations définitives, nous avons démontré qu'il existait de nombreuses raisons d'explorer cette piste. La difficulté principale réside dans le fait que nous ne pouvons pas faire de recommandations sur la forme qu'une telle solution pourrait prendre puisqu'elle doit émaner de la communauté et répondre à ses attentes envers la blockchain afin de restaurer l'assurance (*confidence*) des utilisateurs envers le réseau.

Bibliographie

Bauwens, M., & Pantazis, A. (2018). The ecosystem of commons-based peer production and its transformative dynamics. *The Sociological Review*, *66*(2), 302–319. https://doi.org/10.1177/0038026118758532

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale Univ. Press.

Benkler, Y., & Nissenbaum, H. (2006). Commons-based Peer Production and Virtue. *Journal of Political Philosophy*, *14*(4), 394–419. https://doi.org/10.1111/j.1467-9760.2006.00235.x

Breidenbach, L., Cachin, C., Coventry, A., Ellis, S., Juels, A., Miller, A., Magauran, B., Nazarov, S., Topliceanu, A., Zhang, F., Chan, B., Koushanfar, F., Moroz, D., & Tramer, F. (2021). Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks. *Chainlink Whitepaper*.

Cox, M., Arnold, G., & Villamayor Tomás, S. (2010). A Review of Design Principles for Community-based Natural Resource Management. *Ecology and Society*, *15*(4). https://doi.org/10.5751/ES-03704-150438

Daian, P. (2021, April 15). *Phil Does Security | MEV… wat do?* https://pdaian.com/blog/mev-wat-do/

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*, 101284. https://doi.org/10.1016/j.techsoc.2020.101284

Eyal, I. (2015). The Miner's Dilemma. *2015 IEEE Symposium on Security and Privacy*, 89–103. https://doi.org/10.1109/SP.2015.13

Fuster Morell, M. (2014). *Governance of Online Creation Communities for the Building of Digital Commons: Viewed Through the Framework of the Institutional Analysis and Development* (SSRN Scholarly Paper ID 2842586). Social Science Research Network. https://papers.ssrn.com/abstract=2842586

Hardin, G. (1968). The Tragedy of the Commons. *Science*, *162*(3859), 1243–1248. https://doi.org/10.1126/science.162.3859.1243

Hess, C. (2008). *Mapping the New Commons* (SSRN Scholarly Paper No. 1356835). Social Science Research Network. https://doi.org/10.2139/ssrn.1356835

Hess, C., & Ostrom, E. (2007). *Understanding knowledge as a commons: From theory to practice* (1st MIT Press pbk. ed). MIT Press.

Howell, B. E., & Potgieter, P. H. (2019). *Governance of Blockchain and Distributed Ledger Technology Projects: A Common-Pool Resource View*. 25.

Judmayer, A., Stifter, N., Schindler, P., & Weippl, E. (2021). Estimating (Miner) Extractable Value is Hard, Let's Go Shopping! *Cryptology EPrint Archive*, *Paper 2021/1231*, 29.

Kelkar, M., Zhang, F., Goldfeder, S., & Juels, A. (2020). Order-Fairness for Byzantine Consensus. In D. Micciancio & T. Ristenpart (Eds.), *Advances in Cryptology – CRYPTO 2020* (Vol. 12172, pp. 451–480). Springer International Publishing. https://doi.org/10.1007/978-3-030-56877-1_16

Koch, M. B. (2018, August 19). Exploring CryptoKitties — Part 2: The CryptoMidwives. *BlockScience*. https://medium.com/block-science/exploring-cryptokitties-part-2-the-cryptomidwives-a0df37eb35a6

Luhmann, N. (2000). Familiarity, confidence, trust: Problems and alternatives. *Trust: Making and Breaking Cooperative Relations*, *6*(1), 94–107.

Morell, M. F., Salcedo, J. L., & Berlinguer, M. (2016). Debate About the Concept of Value in Commons-Based Peer Production. In F. Bagnoli, A. Satsiou, I. Stavrakakis, P. Nesi, G. Pacini, Y. Welp, T. Tiropanis, & D. DiFranzo (Eds.), *Internet Science* (pp. 27–41). Springer International Publishing. https://doi.org/10.1007/978-3-319-45982-0_3

Morell, M. F., Salcedo, J. L., De Filippi, P., Delong de Rosnay, M., Musiani, F., Capdevila, I., Caliandro, A., Gandini, A., & Rozas, D. (2015). *Value in Commons-Based Peer Production*. https://p2pvalue.eu/wp-content/uploads/2016/09/Doc2-Findings-1-72.pdf

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge University Press.

Ostrom, E. (2000). Collective Action and the Evolution of Social Norms. *Journal of Economic Perspectives*, *14*(3), 137–158. https://doi.org/10.1257/jep.14.3.137

Ostrom, E. (2005). *Understanding institutional diversity*. Princeton Univ. Press.

Ostrom, E. (2010). The Institutional Analysis and Development Framework and the Commons. *Cornell Law Review*, *95*, 807.

Ostrom, E., Gardner, R., & Walker, J. (1994). *Rules, Games, and Common-Pool Resources*. The University of Michigan Press.

Papadimitropoulos, V. (2018). Commons-Based Peer Production in the Work of Yochai Benkler. *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *16*(2), 835–856. https://doi.org/10.31269/triplec.v16i2.1009

Piet, J., Fairoze, J., & Weaver, N. (2022). Extracting Godl [sic] from the Salt Mines: Ethereum Miners Extracting Value. *ArXiv:2203.15930 [Cs]*. http://arxiv.org/abs/2203.15930

pmcgoohan. (2014, August 11). *Miners Frontrunning* [Reddit Post]. R/Ethereum. www.reddit.com/r/ethereum/comments/2d84yv/miners_frontrunning/

Poux, P., de Filippi, P., & Ramos, S. (2020). Blockchains for the Governance of Common Goods. *Proceedings of the 1st International Workshop on Distributed Infrastructure for Common Good*, 7–12. https://doi.org/10.1145/3428662.3428793

Qin, K., Zhou, L., Gamito, P., Jovanovic, P., & Gervais, A. (2021). *An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities*. https://doi.org/10.1145/3487552.3487811

Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2021). Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. In N. Borisov & C. Diaz (Eds.), *Financial Cryptography and Data Security* (pp. 3–32). Springer. https://doi.org/10.1007/978-3-662-64322-8_1

Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S., & Hassan, S. (2018). When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3272329

Shackelford, S., & Myers, S. (2016). *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace* (SSRN Scholarly Paper ID 2874090). Social Science Research Network. https://papers.ssrn.com/abstract=2874090

Siefkes, C. (2013). The Boom of Commons-Based Peer Production. In D. Bollier & S. Helfrich, *The Wealth of the Commons: A World Beyond Market and State* (pp. 289–294). Levellers Press.

Tang, W., Kiffer, L., Fanti, G., & Juels, A. (2022). *Strategic Latency Reduction in Blockchain Peer-to-Peer Networks* (arXiv:2205.06837). arXiv. https://doi.org/10.48550/arXiv.2205.06837

Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.

Zhang, L., & Jie, L. B. (2022, January 25). MEV — A Deep Dive, Part 1. *Medium*. https://medium.com/@liamzhang/mev-a-deep-dive-part-1-3f389ef16d32