Exploitation des amendes dans Ethereum PoS

Ulysse Pavloff, Yackolley Amoussou-Guenou, Sara Tucci-Piergiovanni

Exploitation des amendes dans Ethereum PoS †

Ulysse Pavloff[1] et Yackolley Amoussou-Guenou[2] et Sara Tucci-Piergiovanni[1]

[1] *Université Paris-Saclay, CEA, List, Palaiseau, France*
[2] *Université Paris-Panthéon-Assas, CRED, Paris, France*

En mai 2023, la blockchain Ethereum a connu son premier *drainage des inactifs* (inactivity leak), un mécanisme conçu pour rétablir la finalisation de la chaîne en cas de perturbations persistantes du réseau. Ce mécanisme vise à réduire le pouvoir de vote des validateurs qui sont injoignables au sein du réseau via des amendes, en réallouant ce pouvoir aux validateurs actifs. Cet article examine les implications du drainage des inactifs sur la sécurité de la blockchain Ethereum. Notre analyse révèle des scénarios où les actions de validateurs Byzantins accélèrent la finalisation de deux branches conflictuelles cassant ainsi la sécurité. La proportion de Byzantins a aussi la possibilité de dépasser le seuil d'un tiers de pouvoir de vote dans des conditions particulières. Nos découvertes démontrent comment la pénalisation des nœuds inactifs peut casser la sécurité du système, de surcroît lorsqu'elle est couplée à des actions malveillantes de validateurs Byzantins.

Mots-clefs : Ethereum, Drainage des Inactifs, Sécurité, Vivacité, Blockchain

1 Introduction

Ethereum a basculé vers son protocole de preuve d'enjeu (Proof-of-Stake, PoS) en septembre 2022, passant de la preuve de travail à un système plus économe en énergie. Le PoS d'Ethereum mélange un consensus classique tolérant aux fautes Byzantines (BFT) avec un protocole au style Nakamoto. Les blockchains au style Nakamoto peuvent bifurquer (fork) mais restent toujours *disponibles*. À l'inverse, les blockchains de consensus BFT sont toujours *sécurisées*, sans bifurcation, mais peuvent cesser de croître pendant des perturbations réseau.

Ethereum PoS combine une chaîne finalisée sans bifurcation, un préfixe sécurisé, et une partie bifurcable, un suffixe avec bifurcation, pour équilibrer sécurité et croissance. Néanmoins, la finalisation dans Ethereum PoS, basée sur des quorums Byzantins, est limitée par la problématique des validateurs injoignables. Il n'y aura pas de finalisation si un trop grand nombre de validateurs semblent inactifs. Pour atténuer cela, le mécanisme de *drainage des inactifs* rédistribue la puissance de vote en réduisant petit à petit le pouvoir de vote des inactifs. Ce mécanisme vise à maintenir l'activité du réseau mais pose un risque théorique pour la sécurité. Notre travail propose une description formelle du drainage des inactifs et son impact sur Ethereum PoS, évaluant la perte de sécurité et les conditions sous lesquelles elle se produit. Nous considérons notre analyse essentielle pour comprendre les mécanismes de pénalité dans les blockchains PoS.

État de l'art. Bien que des mécanismes similaires au drainage des inactifs d'Ethereum, punissant le manque d'activité des validateurs, existent ailleurs (e.g., Polkadot, Tezos), à notre connaissance, il n'y a pas eu d'analyse du risque associé au drainage potentiel des honnêtes dans un environnement Byzantin.

Des efforts initiaux ont été faits pour analyser les effets des incitations sur les propriétés de vivacité et de sécurité du protocole Ethereum [BRLP20]. Cependant, cette exploration préliminaire discute d'une version antérieure du protocole et n'a pas inclus d'analyse du drainage des inactifs. D'autres études du protocole ont analysé des attaques sur la vivacité de la dernière version du protocole à ce jour [SNM$^+$, PAT23] mais sans prise en compte des incitations.

Une étude liant les pénalités d'attestation aux actions des validateurs Byzantins est présentée dans [ZLD23]. Bien que similaire dans l'entreprise, notre travail diffère puisque nous nous concentrons sur les pénalités

† Une présentation étendu de ces travaux est à paraître à DSN2024.

prédominantes pendant le drainage des inactifs, c'est-à-dire les pénalités d'inactivité et la sanction (slashing). En effet pendant cette période, les pénalités d'attestation tendent à être moins significatives. Notre travail vise à combler cette lacune d'analyse de l'effet du drainage des inactifs sur le protocole en prenant en compte la dernière version du protocole.

2 Modèle du Système et Propriétés de la Blockchain

Nous considérons un système composé d'un ensemble fini Π de processus appelés *validateurs*, possédant chacun une *mise* (stake). La mise, exprimée en crypto-monnaie (ETH), sert de métrique de leur influence dans le protocole de consensus. Les validateurs possèdent une paire de clés publique/privée unique pour la signature cryptographique et sont identifiés par leur clé publique, supposant que les signatures numériques ne peuvent être falsifiées. Le temps est mesuré par des périodes de 12 secondes appelées *slots*, une période de 32 slots constituant une *époque*.

Réseau. Les validateurs communiquent par passage de messages dans un modèle partiellement synchrone, où le système devient synchrone après un Temps de Stabilisation Global (`GST`) a priori inconnu. Avant le `GST`, la période est asynchrone sans limite de délai de transfert des messages Δ, et après le `GST`, une limite finie connue sur Δ est établie.

Modèle de Faute. Les validateurs sont catégorisés en *honnêtes* et *Byzantins*. Les validateurs honnêtes suivent le protocole, tandis que les validateurs Byzantins peuvent s'en écarter arbitrairement. Nous notons β_0 la proportion initiale de la mise des validateurs Byzantins, avec $\beta_0 < 1/3$.

Le protocole PoS d'Ethereum vise à atteindre la Tolérance aux Fautes Byzantines (BFT), assurant la préservation des propriétés de sécurité et de vivacité pour toute proportion initiale de mise Byzantine (β_0) strictement inférieure à 1/3.

Propriétés PoS d'Ethereum. Les validateurs maintiennent une structure de données locale sous forme d'arbre contenant tous les blocs perçus, puis un protocole de consensus aide à choisir une chaîne unique dans l'arbre. Ethereum a la particularité d'avoir une chaîne *finalisée* comme préfixe d'une chaîne sujette à des bifurcations.

La propriété de sécurité d'Ethereum stipule que la chaîne finalisée n'est pas bifurcable, tandis que la propriété de *vivacité* indique que la chaîne finalisée croît toujours. L'existence d'une propriété de *disponibilité* sur l'ensemble de la chaîne garantit une croissance constante de la chaîne malgré les défaillances et les partitions réseau. Les définitions simplifiées des propriétés PoS formelles d'Ethereum sont présentées pour une plus claire compréhension.

Propriété 1 (Sécurité) *Une blockchain atteint la **sécurité** si pour deux validateurs honnêtes avec une chaîne finalisée, alors une chaîne est nécessairement le préfixe de l'autre.*

Propriété 2 (Disponibilité) *Une blockchain est **disponible** si les deux conditions suivantes sont remplies : (1) tout validateur honnête peut ajouter un bloc à sa chaîne en un temps fini, indépendamment des défaillances d'autres validateurs et des partitions du réseau ; (2) les chaînes de tous les validateurs honnêtes croissent après un temps fini.*

Propriété 3 (Vivacité) *Une blockchain est **vivace** si la chaîne finalisée croît après un temps fini.*

3 Description du Protocole et du Drainage des Inactifs

Dans ce travail, nous étudions le drainage des inactifs dans le protocole Ethereum PoS. La structure temporelle repose sur des *slots* et des *époques*, avec des rôles de proposants et attestants pour les validateurs.

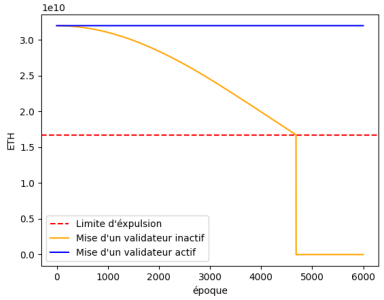
Structure et Consensus. Le protocole mesure le temps en *slots* et *époques*, facilitant le consensus sur les points de contrôle (checkpoints). Les points de contrôle sont des pairs bloc-époque qui aide à la finalisation. Les validateurs alternent entre les rôles de proposant et attestant. Être proposant signifie proposer un bloc, tandis qu'attestant signifie voter pour un bloc et un point de contrôle au début de l'époque.

Incitations. Ethereum PoS utilise des récompenses et pénalités pour encourager les validateur à atteindre un consensus efficacement. Les pénalités comprennent les sanctions (slashing) qui éjectent les validateurs sanctionnés ; les pénalités d'attestation qui pénalisent les validateurs qui retardent l'envoi de leur attestation ; et les pénalités d'inactivité, ces dernières augmentant avec le score d'inactivité des validateurs et sont l'objet de notre étude.

Drainage des inactifs. Le drainage des inactifs est un mécanisme activé à la suite de quatre époques sans finalisation. Il vise à drainer les mises des validateurs inactifs. Les pénalités augmentent avec le temps d'inactivité. Un point important est qu'un validateur est jugé inactif pour une chaîne spécifique. En effet, lors d'une bifurcation quand deux chaînes coexistent, être actif sur une seule des chaînes signifie être inactif sur l'autre.

Score et Pénalités d'Inactivité. Le score d'inactivité est crucial car c'est ce qui ajuste les pénalités en fonction de l'activité du validateur. Le score d'inactivité I pour un validateur i évolue ainsi : $I_i(t) = I_i(t-1)+4$, si i est inactif durant l'époque t et $I_i(t) = I_i(t-1)-1$ sinon. La mise s et le score d'inactivité I déterminent les pénalités subies par les validateurs. Au cours du temps la mise varie ainsi : $s'(t) = -I(t) \cdot s(t)/2^{26}$.

Modélisation de la Mise. Nous modélisons la mise des validateurs comme une fonction continue. Nous pouvons ainsi analyser l'évolution de la mise selon différents comportements de validateurs durant le drainage des inactifs. À savoir (i) Mise d'un validateur actif au cours du temps : $s(t) = s_0 = 32$; et (ii) Mise d'un validateur inactif au cours du temps : $s(t) = s_0 e^{-t^2/2^{25}}$.



(a) Évolution de la mise d'un validateur au cours du temps en fonction de leur activité.

β_0	t
0	**4685**
0,1	4066
0,15	3622
0,2	3107
0,33	502

(b) Époque de finalisation conflictuelle en fonction de la proportion initiale de la mise des Byzantins B_0

4 Analyse

Dans cette section, nous étudions la robustesse de la propriété de sécurité dans le contexte du drainage des inactifs. Nos résulats montrent qu'en cas de partition prolongée, deux chaînes distinctes peuvent être finalisées, menant à des blocs finalisés conflictuels, ce qui est une violation de la propriété de sécurité.

Limite Supérieure pour la Sécurité. Nous cherchons une borne supérieure sur la durée où le réseau est synchrone (`GST`) avant laquelle la sécurité ne peut pas être cassée (aucune finalisation conflictuelle ne peut se produire). En cas d'événements catastrophiques, une grande partie des validateurs honnêtes pourrait devenir injoignable.

Deux chaînes finalisées. Nous montrons qu'un scénario remarquable survient pendant les périodes asynchrones. Durant ces périodes une partition du réseau peut entraîner la finalisation de deux chaînes distinctes. Si cette partition persiste pendant une période prolongée, les deux chaînes drainent indépendamment les mises des validateurs qu'elles considèrent inactifs jusqu'à ce qu'elles finalisent à nouveau.

Nous évaluons ensuite le temps nécessaire pour finaliser les deux branches de la bifurcation. Supposons que l'ensemble des validateurs est honnêtes mais qu'ils soient partitionnés sur deux branches. Une finalisation conflictuelle subviendra lorsque les deux branches auront finalisé. Pour trouver le temps que mettra à finaliser chaque branche, il suffit de regarder l'évolution du ratio d'actif au cours du temps, et de déterminer

quand celui-ci sera supérieur ou égal à 2/3. En donnant la proportion initiale d'actif sur une branche, nous pouvons déterminer le ratio d'actif au cours du temps, car on sait que la mise des actifs sera constant tandis que celui des inactifs va baisser en suivant le fonction $s(t) = s_0 e^{-t^2/2^{25}}$. Ainsi, on trouve que peu importe les proportions initiales d'actif sur les branches, la finalisation conflictuelle adviendra lorsque les validateurs inactifs seront expulsés.

On trouve alors qu'avec uniquement des validateurs honnêtes, il faut exactement 4685 époques pour obtenir une finalisation conflictuelle (temps à partir duquel les inactifs seront expulsés) et ainsi casser la propriété de sécurité.

Diminution de la Limite Supérieure à cause des Validateurs Byzantins. Nous étudions également comment la présence de validateurs Byzantins accélère la rapidité avec laquelle une finalisation conflictuelle apparaît. Les validateurs Byzantins exploitant la période asynchrone du réseau peuvent manipuler les délais de transmission des messages entre les validateurs honnêtes. En contrôlant le temps de délai, les validateurs Byzantins peuvent séparer efficacement le réseau en plusieurs sous-ensembles qui ne communiquent pas entre eux et se considèrent ainsi inactifs. Pour obtenir un conflit de bloc finalisé sur des chaînes différentes, le plus rapide est de créer seulement deux sous-ensembles. Le tableau (b) montre comment la proportion de la mise détenue par les Byzantins dans le réseau, β_0, peut avoir un impact sur le temps t auquel on finalise. Plus la proportion initiale β_0 est proche de 0, plus le temps t nécessaire avant une nouvelle finalisation conflictuelle sera court.

Cette attaque met en lumière les vulnérabilités inhérentes aux protocoles blockchain dans des conditions de réseau asynchrone et souligne l'importance de concevoir des mécanismes de défense robustes contre de telles manipulations par les acteurs Byzantins. Dans l'attaque présentée les actions des validateurs Byzantins sont sanctionnables mais nous montrons une attaque avec des effets équivalents où les actions des validateurs Byzantins ne sont pas sanctionnables (car non observables).

Plus d'un tiers de Byzantins. Un autre problème créé par le drainage de validateurs inactifs est que durant une période asynchrone les Byzantins peuvent augmenter la proportion de leur mise en expulsant des honnêtes pour lesquels ils augmentent le délai de leurs messages et créent des pénalités. Ainsi, si leur proportion initiale est assez proche de la limite d'un tiers, un drainage peut leur permettre de dépasser ce seuil symbolique. Nous montrons que les validateurs Byzantins peuvent créer un tel scénario si la proportion de leur mise initial est 0,2421.

5 Conclusion

Cette étude approfondit les complexités du drainage des inactifs du protocole Ethereum PoS, conçu pour restaurer la finalisation lors d'une défaillance catastrophique du réseau.

Notre exploration, à travers divers scénarios, révèle des situations où les actions Byzantines accélèrent l'apparition de bifurcations irréconciliables. Nos découvertes soulignent le rôle critique des mécanismes de pénalité dans l'analyse BFT. En éclairant les problèmes de conception du protocole, nous offrons des perspectives pour des améliorations futures et fournissons des outils pour les étudier.

Références

[BRLP20] Vitalik Buterin, Daniël Reijsbergen, Stefanos Leonardos, and Georgios Piliouras. Incentives in ethereum's hybrid casper protocol. *Int. J. Netw. Manag.*, 30(5), 2020.

[PAT23] Ulysse Pavloff, Yackolley Amoussou-Guenou, and Sara Tucci Piergiovanni. Ethereum proof-of-stake under scrutiny. In *38th ACM/SIGAPP Symposium on Applied Computing, SAC 2023*, 2023.

[SNM+] Caspar Schwarz-Schilling, Joachim Neu, Barnabé Monnot, Aditya Asgaonkar, Ertem Nusret Tas, and David Tse. Three attacks on proof-of-stake ethereum. In *26th Financial Cryptography and Data Security, FC 2022*.

[ZLD23] Mingfei Zhang, Rujia Li, and Sisi Duan. Max attestation matters : Making honest parties lose their incentives in ethereum pos. *IACR Cryptol. ePrint Arch.*, page 1622, 2023.