ZOC : Identification et Quantification des Contrats Intelligents "Zombie On Chain" pour la Durabilité de la Blockchain

Résumé (Abstract)

Le caractère immuable et persistant des blockchains conduit à l'accumulation exponentielle de code obsolète sur le registre. Des analyses montrent que jusqu'à **70% des projets crypto** finissent par échouer, laissant derrière eux un volume massif de débris numériques.

Cet article propose une nouvelle taxonomie pour adresser ce problème : le concept de **Contrat Intelligent ZOC** (*Zombie On Chain*).

Un ZOC est défini comme un contrat déployé qui présente une inactivité externe continue d'une période initiale de **neuf mois** — seuil choisi par analogie à un cycle d'incubation — et une valeur économique négligeable.

Ce délai, ainsi que les seuils de valeur, sont établis comme hypothèse de travail initiale et sont sujets à validation et ajustement par les données recueillies par le *ZOC Tracker* et le consensus communautaire futur.

Nous détaillons la méthodologie pour un outil (*ZOC Tracker*) capable de quantifier et de classifier ces entités numériques. L'identification précise des ZOC est essentielle pour affiner les métriques d'activité, sécuriser les appels erronés, et améliorer l'audit et la durabilité des écosystèmes décentralisés.

---

1. Introduction : Le Paradoxe de la Persistance et la Nécessité d'une Nouvelle Taxonomie

La promesse des blockchains repose sur l'**immuabilité** et la **résistance à la censure**. Toutefois, cette permanence engendre une conséquence structurelle : l'accumulation massive de **code mort** ou **abandonné**. Le problème est aggravé par le taux d'échec élevé dans l'écosystème : les analyses montrent qu'environ **50% à 70% des projets crypto finissent par cesser leurs activités**, laissant derrière eux des vestiges non fonctionnels.

La racine du problème est structurelle et repose sur trois vérités fondamentales des contrats intelligents :

- Un contrat mal conçu **ne peut pas être corrigé** après son déploiement.
- Il **reste immuable et public** sur le registre, parfois même avec des fonds bloqués (Contrats ZOC Verrouillés).
- Il devient un exemple tangible à ne pas suivre, mais aussi un **objet d'étude précieux** pour la recherche et l'éducation des développeurs.

Ces leçons structurelles confirment la nécessité d'une classification. Ce travail introduit et définit formellement le concept de **Contrat Intelligent Zombie On Chain (ZOC)**.

De manière imagée, quand un *smart contract* est déployé mais ne sert à rien : il est là, visible, consomme de l'espace, mais est sans vie fonctionnelle.

Un ZOC erre dans la blockchain sans jamais réagir.

Lien vers le site : zoctracker.com
Contact : contact@zoctracker.com

2. Définition Formelle : Le Concept ZOC (Zombie On Chain)

Le terme **ZOC** désigne les contrats intelligents qui sont jugés **non-opérationnels et économiquement insignifiants**.

2.1. Les Critères de Classification d'un ZOC

Pour qu'un contrat soit catégorisé comme **ZOC**, il doit satisfaire simultanément les deux critères suivants :
$$\text{Contrat} = \text{ZOC IFF } (\text{Critère Temporel X}) \wedge (\text{Critère de Valeur Y})$$

Critère Temporel (Inactivité - X) : Période Initiale de 9 Mois

Le seuil d'inactivité est fixé à une période initiale de **neuf mois (9 mois)**. Ce délai est choisi comme **hypothèse de travail** en s'appuyant sur l'analogie d'un cycle complet de gestation, confirmant l'abandon ou l'obsolescence fonctionnelle.

Le contrat ne doit avoir enregistré **aucune interaction externe** pendant cette période continue. Sur un réseau comme Ethereum, ce critère représente environ **2 millions de blocs** consécutifs sans activité.

Critère de Valeur (Insignifiance Économique - Y)

Le contrat doit présenter une valeur économique totale **négligeable**. Ces seuils sont établis comme **base de travail initiale** pour le *ZOC Tracker* :

1. **Balance Native Insignifiante :** La balance du contrat est **inférieure à 0.001** unité native du réseau (ex : 0.001 ETH).
2. **Actifs Secondaires Minimes :** La valeur marchande totale des actifs secondaires détenus par le contrat est **inférieure à 10 USD**.

Note méthodologique : Les seuils monétaires et la période de neuf mois sont sujets à des ajustements futurs. Le déploiement du *ZOC Tracker* permettra, par l'analyse statistique des populations de contrats, d'optimiser ces critères pour qu'ils restent pertinents face à l'évolution de l'économie des blockchains et du coût des transactions.

2.2. Classification des Types de ZOC

Type de ZOC	Description	Potentiel de Sécurité / Exploitation
🧠 **Inerte**	Contrat déployé sans logique active, souvent des librairies ou des tests.	Étude pédagogique, audit de conception de code.
🔒 **Verrouillé**	Contrat contenant des fonds qui sont inaccessibles en raison d'un bug de retrait.	Documentation de bug critique, analyse de *honeypots* involontaires.
🧨 **Dangereux**	Contrat avec une vulnérabilité connue non corrigée, mais inactif.	Exploitation *White Hat* pour sécuriser ou documenter l'exploit.
🧳 **Abandonné**	Contrat d'un projet mort ou migré, mais encore référencé par des entités externes.	Récupération de trafic et migration douce via contrat proxy.

3. Vers le "ZOC Tracker" : Méthodologie et Stratégie d'Exploitation

La classification ZOC est implémentée via l'outil analytique **ZOC Tracker**.

3.1. Architecture et Acquisition des Données

1. **Accès aux Données Brutes :** L'outil s'interface avec un **Nœud d'Archive** (via des services API comme Alchemy ou Infura) pour garantir un accès non limité à l'historique de la blockchain.
2. **Pipeline d'Indexation :** Un pipeline de données est responsable de la lecture séquentielle des blocs. Ce pipeline (développé par exemple **en langage tel que Python** avec la librairie Web3.py, ou en **Go** avec des outils natifs) filtre et extrait les événements critiques nécessaires à l'analyse ZOC.
3. **Stockage :** Les données indexées sont stockées et optimisées dans une base de données analytique (ex : **PostgreSQL** ou **ClickHouse**), préparant le terrain pour des requêtes complexes et rapides.

3.2. Stratégie d'Exploitation et Récupération de Trafic

L'outil applique la logique Booléenne du ZOC pour générer un index d'adresses ZOC et mettre en lumière les opportunités.

- **Récupération de Trafic (🧳) :** Pour les ZOC Abandonnés, le **ZOC Tracker doit utiliser des méthodes d'identification des appels résiduels** (transactions call, delegatecall ou références d'interfaces) qui persistent vers l'adresse inactive. L'outil **propose ensuite des solutions telles que l'implémentation d'un nouveau contrat proxy (wrapper)** pour simuler l'interface du ZOC, absorber les appels erronés et les rediriger vers un contrat sain ou un service d'information.
- **Audit et Sécurité (🧨 🔒) :** Les ZOC Dangereux et Verrouillés fournissent une base de données essentielle pour la **documentation des vulnérabilités** et l'amélioration des outils d'audit de sécurité automatisés.

3.3. Bénéfices et Valeur Ajoutée

Le ZOC Tracker offre des bénéfices concrets pour l'écosystème : hygiène de la chaîne, sécurisation des appels erronés, et valorisation potentielle des adresses abandonnées.

3.4. Critères d'Exclusion Avancés : La Distinction entre ZOC et Contrats en Dormance Stratégique.

La persistance inhérente à la blockchain exige une approche rigoureuse de la classification. L'inactivité seule ne suffit pas à qualifier un contrat intelligent de ZOC (Zombie On Chain). Certains contrats sont conçus pour présenter des périodes d'inactivité prolongées pour des raisons fonctionnelles ou stratégiques légitimes (par exemple, l'attente de l'expiration d'un verrouillage temporel ou d'un consensus).

Le ZOC Tracker intègre un ensemble de critères d'exclusion avancés afin d'identifier et de filtrer ces faux positifs, garantissant ainsi la précision et la fiabilité de la métrique ZOC.

Catégorie d'exclusion	Objectif et justification technique
Mécanismes de gouvernance et de sécurité	Ces contrats, tels que les portefeuilles multisignatures (comme Gnosis Safe) ou les coffres-forts des organisations autonomes décentralisées (DAO), restent souvent inactifs pendant de longues périodes, en attendant qu'un quorum soit atteint sur une proposition stratégique. Si l'état interne du contrat (emplacements de stockage) indique une transaction en attente non exécutée, le contrat est marqué comme stratégiquement inactif (et n'est donc pas un contrat ZOC).
Contrats à durée déterminée (acquisition/verrouillage temporel)	Les contrats conçus pour détenir et libérer des actifs selon un calendrier prédéfini (par exemple, l'acquisition de jetons pour les employés ou le déblocage différé de fonds) sont soumis à une période d'inactivité. Cette période est normale jusqu'à l'atteinte d'un bloc ou d'une date ultérieure spécifique. Une exclusion est appliquée si le contrat détient encore des jetons non acquis ou si la période de blocage n'est pas entièrement écoulée.
Composants d'infrastructure (proxies/bibliothèques)	Les contrats déployés uniquement comme dépendances internes, tels que les proxys de mise à niveau (par exemple, les modèles UUPS ou de proxy transparent) ou les bibliothèques logiques, ne sont pas destinés à être appelés par les utilisateurs finaux. Leur fonction principale est d'être appelés par d'autres contrats intelligents. Ils doivent être totalement exclus des critères d'inactivité, car l'absence d'appels externes relève de leur fonctionnement normal.

Méthodologie d'exclusion : L'identification de ces exceptions est réalisée par **l'analyse des signatures de bytecode du contrat** (identification des modèles de contrat connus) et par la **vérification active de l'état interne du contrat** via des API améliorées (comme celles fournies par Alchemy) afin de déterminer si une condition d'activité est en attente (par exemple, vérifier si le quorum Multisig est atteint ou si la date de verrouillage temporel a expiré).

Ce mécanisme garantit que le ZOC Tracker fournit une mesure reflétant un véritable abandon de projet plutôt qu'une quiétude stratégique intentionnelle.

---

4. Conclusion et Perspectives 🚀

L'immuabilité des registres distribués est à la fois leur plus grande force et leur plus grand défi structurel.

Ce travail a permis de formaliser l'une des conséquences inévitables de cette permanence : la prolifération silencieuse des contrats intelligents abandonnés. En introduisant la taxonomie **ZOC** (*Zombie On Chain*), nous avons fourni la première grille d'analyse rigoureuse pour distinguer le code persistant du code fonctionnel.

Le **ZOC Tracker** n'est pas seulement un outil de diagnostic ; c'est un pas vers une **hygiène de la chaîne** plus mature et responsable. En reconnaissant et en mesurant l'existence des ZOC, la communauté technologique se donne les moyens de mieux gérer, d'auditer avec plus de précision, et d'assurer une meilleure durabilité de l'infrastructure décentralisée.
