

## ZOC (Zombie On Chain)

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

#### **Abstract (Version 1.2.0)**

La nature immuable et persistante des blockchains conduit à une accumulation exponentielle de code obsolète dans le registre. Les analyses indiquent 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 aborder 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** sur une période initiale de **neuf mois** – un seuil choisi par analogie à un cycle d'incubation complet – et une **valeur économique négligeable** (Critère Y).

Ce délai et les seuils de valeur sont établis comme une hypothèse de travail initiale et sont soumis à la validation et à l'ajustement par les données collectées par le **ZOC Tracker** et le consensus futur de la communauté.

Nous détaillons la méthodologie pour un outil (**ZOC Tracker / Z-Terminal**) capable de quantifier et de classer ces entités numériques. L'identification précise des **ZOCs** est essentielle pour affiner les métriques d'activité, sécuriser les appels erronés et améliorer l'audit et la durabilité des écosystèmes décentralisés. Le **ZOC Tracker** est une **Plateforme d'Ingestion de Données Analytiques (PIDA)**.

#### **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**. Cependant, cette permanence génère 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.**

## 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 :

Contrat = ZOC IFF (Critère Temporel X)  $\wedge$  (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 **dérisoire**. Ces seuils sont établis comme **base de travail initiale** pour le *ZOC Tracker* :

- Balance Native Insignifiante** : La balance du contrat est **inférieure à 0.001** unité native du réseau (ex : 0.001 ETH).
- 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                                  |
|---|--|---|
|  <b>Inerte</b>     | Contrat déployé sans logique active, souvent des librairies ou des tests.          | Étude pédagogique, audit de conception de code.                       |
|  <b>Verrouillé</b> | Contrat contenant des fonds qui sont inaccessibles en raison d'un bug de retrait.  | Documentation de bug critique, analyse de honeypots involontaires.    |
|  <b>Dangereux</b>  | Contrat avec une vulnérabilité connue non corrigée, mais inactif.                  | Exploitation <i>White Hat</i> pour sécuriser ou documenter l'exploit. |
|  <b>Abandonné</b>  | Contrat d'un projet mort ou migré, mais encore référencé par des entités externes. | Récupération de trafic et migration douce via contrat proxy.          |

### 3. L'Architecture du ZOC Tracker : La Plateforme d'Ingestion de Données Analytiques (PIDA)

Le **ZOC Tracker** est plus qu'un simple *dashboard* ; c'est une **Plateforme d'Ingestion de Données Analytiques (PIDA)** haute performance conçue pour traiter l'intégralité de l'historique de l'EVM de manière efficace et rigoureuse. Cette architecture est justifiée par la nécessité de valider la taxonomie **ZOC** à l'échelle du *Big Data*.

#### 3.1. Le Pipeline d'Ingestion Go (Z-Terminal Core)

Le cœur du système est un pipeline écrit en **Go (Golang)**. Le choix de Go est stratégique pour sa gestion supérieure de la concurrence (*goroutines*), essentielle pour gérer l'importation massive des blocs historiques d'Ethereum (le "ratrapage historique") et maintenir le suivi en temps réel.

- **Source de Données :** Utilisation des Enhanced APIs d'**Alchemy** pour accéder à l'historique complet et aux traces de transactions.
- **Traitements :** Le pipeline Go applique la logique de la Taxonomie **ZOC V1.1.0** en temps réel, filtrant les exceptions et enrichissant les métadonnées des contrats.

#### 3.2. Stockage et Analyse : ClickHouse

Les données structurées sont écrites dans **ClickHouse**, une base de données analytique orientée colonnes (OLAP).

- **Raison Stratégique :** ClickHouse est conçu pour l'agrégation et les requêtes analytiques sur des pétaoctets de données, ce qui est parfait pour calculer le **ZOC Score** (le pourcentage de contrats ZOC par bloc, par jeton, ou par protocole) rapidement.
- **Sécurité des Données :** L'utilisation de cette architecture permet de séparer les secrets d'API et de garantir une intégrité des données traçable.

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

La logique explicite des faux positifs est essentielle :

- Cette section détaille l'analyse des **signatures de bytecode** et des états internes de contrats afin d'identifier les **contrats stratégiquement inactifs** (par exemple, les contrats multisignatures et les contrats à verrouillage temporels)
- Cette étape garantit que le ZOC Tracker fournit une mesure précise de **l'abandon réel d'un projet** (et non d'une simple inactivité).

| Catégorie d'exclusion                           | Objectif et justification technique  |
|---|--|
| <b>Mécanismes de gouvernance et de sécurité</b> | 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). |

| Catégorie d'exclusion  | Objectif et justification technique   |
|--|---|
| <b>Contrats à durée déterminée (acquisition/verrouillage temporel)</b> | 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.                  |
| <b>Composants d'infrastructure (proxies/bibliothèques)</b>             | 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 formalisé l'une des conséquences inéluctables de cette permanence : la prolifération silencieuse des contrats intelligents abandonnés. En introduisant la taxonomie **ZOC (Zombie On Chain)**, nous fournissons le premier cadre d'analyse rigoureux pour distinguer le code persistant du code fonctionnel.

Le **ZOC Tracker** n'est pas seulement un outil de diagnostic ; c'est une étape vers une hygiène de chaîne plus mature et responsable.

En reconnaissant et en mesurant l'existence des **ZOCs**, 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.