ZOC (Zombie On Chain) White paper (Version 2.0 – L'Ere de la Prédiction)

Dormant Echoes: The Exiled Code & The Logic of Systemic Decay

Strategic Alert: The adoption of blockchain technologies, much like AI, is following a much steeper adoption curve than any technology of the past. This is precisely why we need predictive risk management.

Abstract (Version 2.0 - Predictive Risk Vector)

The persistent and immutable nature of blockchains leads to an exponential accumulation of obsolete code on the ledger. This silent proliferation of **Digital Debris** creates a systemic health crisis: The **Blockchain's Bad Cholesterol**.

This paper proposes a taxonomy and methodology to address this threat: the concept of the **ZOC (Zombie On Chain)** Smart Contract. The ZOC Tracker is the first tool to perform **Negative Space Auditing**, focusing on the latent risk residing in forgotten code.

Key Innovation: The **ZOC Score** is now a **Predictive Risk Encoding Vector**, derived from a **Transformer Encoder-Decoder** architecture. This approach allows us to move from simple classification to **probabilistic modeling** of the occurrence of a systemic disaster.

The ZOC Tracker is architected as an **Analytical Decentralized Risk Platform (ADIP)**, built on Go/ClickHouse, designed to transform this taxonomy into a continuous, verifiable audit metric.

---

1. Introduction: The Paradox of Persistence and the ZOC Crisis

The promise of immutability generates a structural consequence: the massive accumulation of dead or abandoned code. The problem is aggravated by the high failure rate in the crypto ecosystem (50% to 70% of projects cease operations). These visible, yet functionally inert, remnants constitute the ZOC.

---

2. ZOC Taxonomy: Negative Space Auditing

The term ZOC refers to smart contracts deemed non-operational and economically insignificant.

2.1. Classification Criteria (V1.2.2 Data Baseline)

To be categorized as ZOC, a contract must simultaneously satisfy:

- Temporal Criterion (Inactivity - X): The contract must have recorded no external interaction for a continuous period of nine months (i.e., approximately 2 million consecutive blocks on Ethereum).
- Value Criterion (Economic Insignificance - Y): The contract exhibits negligible total economic value, defined by a Native Balance below 0.001 native unit (e.g., 0.001 ETH) and total Secondary Assets below $10 USD.

2.2. ZOC Taxonomy V2.0: The Four Factors of Systemic Risk

The classification integrates four factors to evaluate the latent risk of exiled code, moving away from simple Inert/Dangerous classification to focus on structural interdependence.

Risk Factor	Analysis Description	Justification (Attention Logic)
1. Code Reachability	Measures the probability of accidental or malicious re-activation of obsolete code.	Maintains the role of the former **Code Complexity** as a foundational factor.
2. Vulnerability Signatures	Correlation with known, unpatched but inactive vulnerabilities (Dormant Bug).	Core risk factor integrating **Vulnerability Signatures.**
3. State Dependency	Measures whether the obsolete code impacts critical variables or UTXOs.	Obsolete code is classified by its ability to corrupt network state.
4. Architectural Decay (Nouveau)	**New :** Measure the risk associated with **weak logical dependecies** and Off-Chain links specific to distributed architecture (eUTXO/Cardano).	**Target Complexity (Cardano) :** ZOC risk shifts to subtle state dependencies, making this audit essential for resilient architectures.

3. ZOC Score and Predictive Modeling (AI Architecture)

The ZOC Tracker establishes its credibility by transforming the Taxonomy risk factors into a predictive metric.

3.1. The ZOC Score as a Hidden Representation

The ZOC Score (0-100) is the output of a **Sequence-to-Sequence (Seq2Seq)** architecture inspired by **Transformers**.

- **The Encoder (Go/ADIP):** Ingests the Taxonomy criteria (the "tokens") and uses an **Attention Mechanism** (Multi-Head Attention) to weigh the importance of the factors. The result is a **Hidden Representation** of the risks, called the **ZOC Risk Vector**.
- **The Decoder (ClickHouse/Statistics):** Takes the ZOC Risk Vector and translates it into two structured outputs, based on the **Marginalization** model and **Bayesian Calibration**:
    1. **The Final ZOC Score (0-100)**.
    2. **Probabilistic Modeling:** Uses statistical models (Poisson/Exponential) to provide the **Probability of Occurrence of a Systemic Disaster** within a given timeframe (DDM Justification).

3.2. ADIP Architecture and Performance (ADIP V2.0)

The ADIP (Analytical Data Ingestion Platform) is designed for the scalability and reliability of an enterprise solution.

- **Stack and Pipeline:** Go (Goroutines) for ingestion, ClickHouse (OLAP) for analysis. Uses **Protocol Buffers (Protobufs)** for binary serialization and network optimization (TCP Keep-Alive, HTTP/2 Multiplexing).
- **Security and Reliability (Production-Grade):**
    - **Data Persistence:** Uses **Docker Volumes** to secure the massive historical dataset.
    - **Latency and Uptime:** Implements **Caching (Redis)** for the final *ZOC Score* (Cache-Aside) and **Load Balancing** to ensure **High Availability (HA)** of the API service.
    - **Observability (M&O):** Defines **SLOs** and integrates monitoring for the predictive detection of anomalies.
    - **API Security:** Protects requests with **JWT** (JSON Web Tokens) and manages access via **RBAC** (Role-Based Access Control).

---

4. Case Study: The Cardano Split

The Cardano Split incident (mainnet bifurcation due to a dormant deserialization bug) is the most recent empirical validation of the ZOC threat. It confirms that Cardano's resilience was tested not by its consensus, but by the fragility of its underlying code base.

- **Implication:** The ZOC Tracker is designed to audit these millions of forgotten contracts that could hide such a dormant bug.

---

5. Conclusion and Perspectives

By recognizing and measuring the existence of ZOCs, the ZOC Tracker establishes itself as a **predictive diagnostic tool**. Our approach, based on Negative Space Auditing and validated by a **Transformer AI architecture** and enterprise-grade reliability foundations, represents the next step toward the maturity and sustainability of decentralized infrastructures.
