Enhancing Blockchain Integrity Using Dual-Reference Validation: Proof of Work and Model-Based Anomaly Detection

Abstract

Blockchain systems have traditionally relied on cryptographic mechanisms such as Proof of Work (PoW) to ensure the integrity and immutability of data. However, these mechanisms do not account for behavioral anomalies or contextual deviations within the network. This paper introduces a novel architecture that integrates an anomaly detection model into the blockchain structure. Each block in the chain references the previous one using both a PoW-based hash and a behaviorally-informed model hash. This dual-reference validation enhances tamper resistance and enables early detection of potentially malicious activity within the network, while also addressing vulnerabilities such as the 51% attack.

1 Introduction

Blockchain is a decentralized ledger technology where each block contains a cryptographic hash of the previous block, linking them in a tamper-evident chain. Traditional implementations, especially those based on Proof of Work (PoW), achieve consensus by requiring nodes to solve computational puzzles before adding a new block. This provides security through economic and computational cost.

However, PoW alone cannot detect behavioral anomalies, such as data patterns that indicate tampering, insider attacks, or violations of expected network behavior. In contexts where trust and behavioral consistency are critical—such as healthcare data, critical infrastructure, or internal organizational chains—PoW needs to be supplemented with semantic or behavioral validation.

2 Traditional Proof of Work Blockchain

In a PoW blockchain, each block B_n contains the hash of the previous block B_{n-1}, computed as:

$$\text{prev\_hash}_n = H(B_{n-1})$$

Typically, H is a cryptographic hash function (e.g., SHA-256), and is applied over a structured combination of:

$$H(B_{n-1}) = \text{SHA256}(\text{data}_{n-1} \,\|\, \text{timestamp}_{n-1} \,\|\, \text{nonce}_{n-1})$$

This process ensures that any alteration in the contents of a previous block will invalidate the hash in subsequent blocks, thereby breaking the chain.

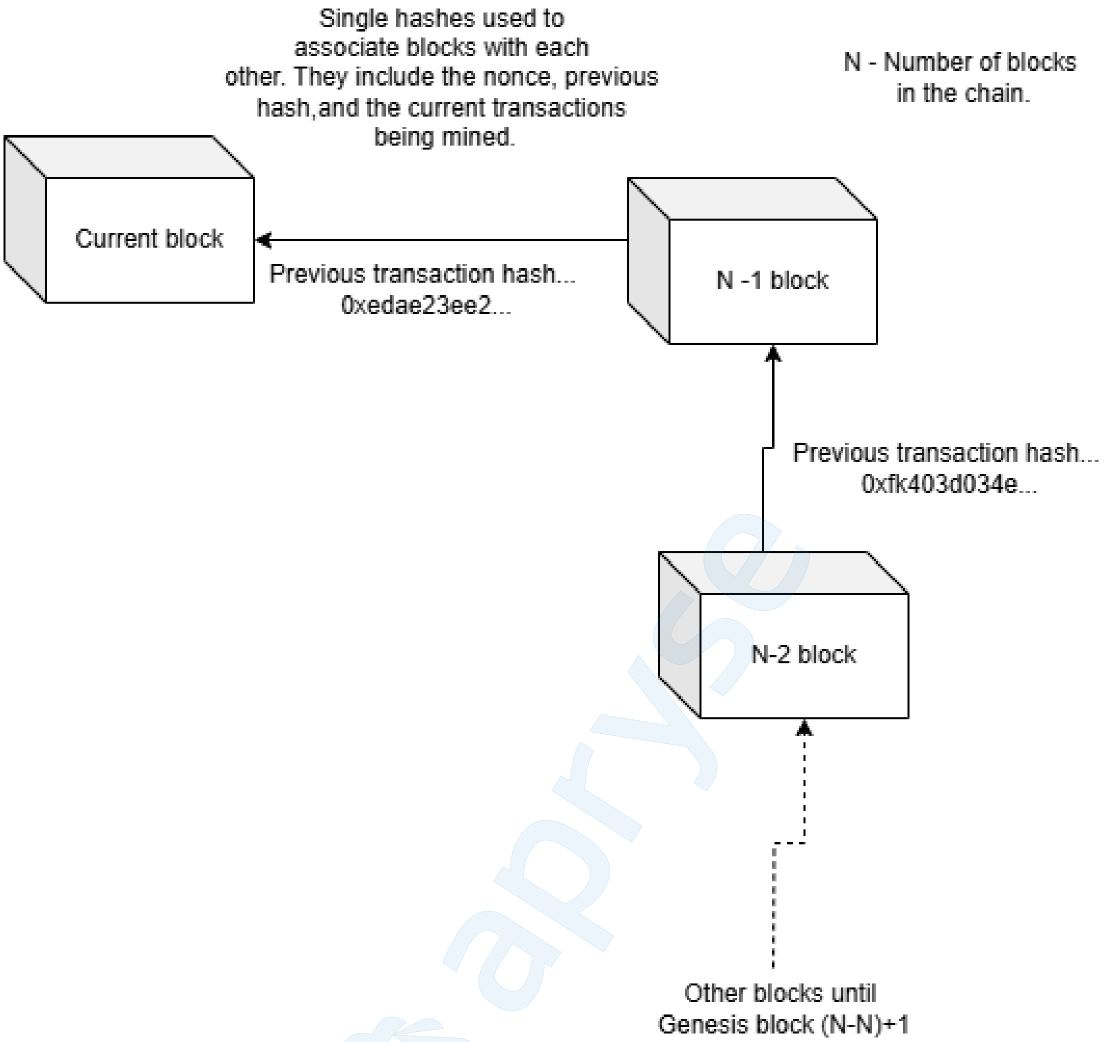

Single hashes used to associate blocks with each other. They include the nonce, previous hash,and the current transactions being mined.
N - Number of blocks in the chain.
Current block
Previous transaction hash... 0xedae23ee2...
N -1 block
Previous transaction hash... 0xfk403d034e...
N-2 block
Other blocks until Genesis block (N-N)+1

Figure 1: Structure of a Traditional Proof of Work Blockchain

3 Dual-Reference Blockchain Model

We propose an extension of this structure by including a second reference to the previous block. This reference is not derived from the usual data fields, but from the output of a machine learning-based anomaly detection model applied to the previous block.

3.1 Structure

Each block B_n includes:

- **Proof-of-Work Hash** (prev_pow_hash_n): The conventional hash of B_{n-1}, required to satisfy PoW difficulty.
- **Model-Based Hash** (prev_model_hash_n): The cryptographic hash of the output of an anomaly detection model applied to B_{n-1}.

The model-based hash is computed as:

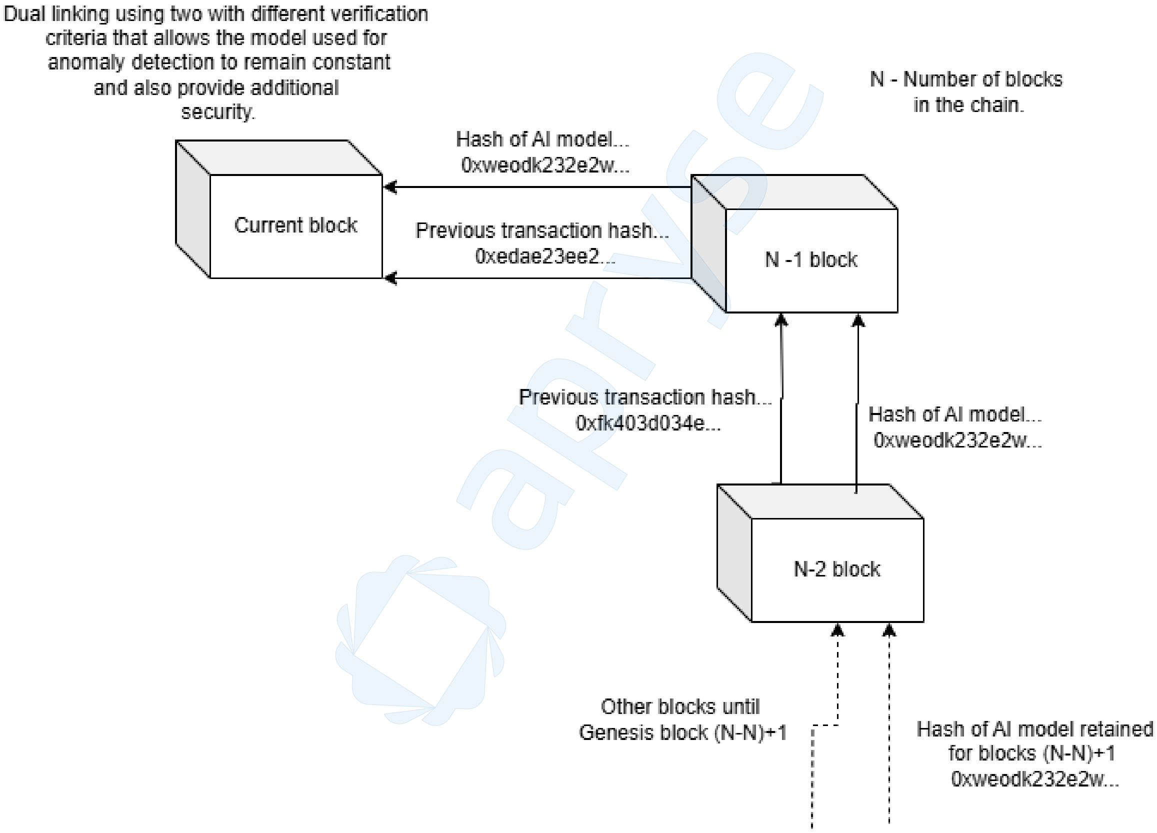
$$\text{prev\_model\_hash}_n = H(\text{Model}(B_{n-1}))$$

where Model(·) represents a behavioral or anomaly detection model that encodes key statistical and behavioral properties of the block.

3.2 Validation Criteria

For a block B_n to be considered valid, both conditions must be satisfied:

$$\text{prev\_pow\_hash}_n = H(B_{n-1})$$
$$\text{prev\_model\_hash}_n = H(\text{Model}(B_{n-1}))$$



Dual linking using two with different verification criteria that allows the model used for anomaly detection to remain constant and also provide additional security.
N - Number of blocks in the chain.
Hash of AI model...
0xweodk232e2w...
Current block
Previous transaction hash...
0xedae23ee2...
N -1 block
Previous transaction hash...
0xfk403d034e...
Hash of AI model...
0xweodk232e2w...
N-2 block
Other blocks until Genesis block (N-N)+1
Hash of AI model retained for blocks (N-N)+1
0xweodk232e2w...

Figure 2: Structure of a Dual-Reference Blockchain with Anomaly Detection

4 Mitigation of the 51% Attack via Dual-Reference Validation

In traditional PoW blockchains, a **51% attack** occurs when an entity gains control over a majority of the network's hashing power. This enables malicious actors to create longer chains, overwrite history, and perform double-spending attacks.

In the dual-reference blockchain model, such an attack becomes infeasible due to the requirement of behavioral conformity:

- The attacker may control the majority of mining power and generate valid PoW hashes.

- However, they cannot generate *valid model hashes* without replicating the behavioral patterns expected by the anomaly detection model.
- Any attempt to alter, replay, or rapidly manipulate block behavior would result in a model output that deviates from the expected pattern and is immediately flagged.
- Honest nodes verify both the PoW and model hash. If either check fails, the block is rejected.

Behavioral Consistency as a Trust Filter

The anomaly model acts as a filter, ensuring that only blocks generated by nodes exhibiting consistent, legitimate behavior are accepted. Unlike PoW, which is susceptible to brute force, the model hash requires **semantic compliance**, which is resistant to computational domination.

Effectively Eliminating 51% Attack Risk

- The attacker must not only out-mine the network, but also match behavioral signatures perfectly.
- The model acts like a cryptographic behavior certificate, effectively enforcing a whitelist of legitimate behavior.
- Therefore, control over hash rate alone is insufficient to corrupt the chain.

5 Advantages of Dual-Reference Design

The inclusion of a model-based hash provides several benefits:

- **Behavioral Integrity:** Even if the data in a block remains unchanged, behavioral anomalies (e.g., suspicious timing, abnormal patterns) can be detected.
- **Early Warning:** Malicious blocks can be flagged before they propagate widely.
- **Defense in Depth:** Tampering now requires both PoW manipulation and consistency with model outputs.
- **Resistance to 51% Attacks:** A major improvement over traditional PoW-based systems.

6 Comparison with Traditional Blockchain

Feature	**Traditional PoW Blockchain**	**Dual-Reference Blockchain**
Reference Method	Single hash of previous block	Two hashes: PoW + model output
Security Focus	Data immutability	Data + behavioral consistency
Anomaly Detection	None	Built-in via model
Tamper Resistance	High	Very high (dual-layer)
51% Attack Risk	High	Extremely low
Computational Cost	Moderate (hashing + PoW)	Higher (PoW + model + hash)
Validation Complexity	Simple hash check	Dual-condition verification
Best Use Case	Public cryptocurrency networks	Secure or behavior-sensitive systems

Table 1: Comparison of Blockchain Architectures

7 Use Cases and Applications

The dual-reference model is particularly useful in scenarios that require high integrity and behavioral validation:

- **Secure Medical Records:** Detect tampering or unusual access patterns in health data.
- **Critical Infrastructure Monitoring:** Log and verify device behaviors across smart grids or industrial systems.
- **Permissioned Blockchains:** Identify rogue actors in enterprise environments.
- **Financial Auditing:** Ensure transaction blocks follow statistically expected patterns.

8 Conclusion

The dual-reference blockchain structure introduces a powerful enhancement to existing blockchain security models. By incorporating an anomaly detection model as a behavioral validator alongside traditional Proof of Work, this approach mitigates both structural and semantic risks. It strengthens chain immutability, resists 51% attacks, and introduces a modular, AI-driven mechanism for identifying malicious behavior — all while preserving compatibility with existing consensus mechanisms.