**Journal of Information Systems Engineering and Management**
2025, 10(27s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Reinforcement Learning-Enhanced Adaptive Blockchain Oracles for Secure and Efficient Data Aggregation

Abinivesh S[1], Deva Priya Isravel[2] Julia Punitha Malar Dhas[3]
[1,2,3] *Karunya Institute of Technology and Science, Coimbatore, India*

**ARTICLE INFO**

Received: 29 Dec 2024

Revised: 17 Feb 2025

Accepted: 27 Feb 2025

**ABSTRACT**

Blockchain oracles are the intermediaries between their smart contracts and the environment. Thus, they put the smart contracts at risk of manipulation, adversarial attacks, or unreliable data. Therefore, undoubtedly a considerable security challenge. Classical oracle mechanisms usually do not have adaptive filtering mechanisms to filter unreliable information or data. This in itself makes them easily attackable. The herein proposed system is an Adaptive Reinforcement Learning-Based Fraud-Resistant Oracle for strengthening the Oracle data protection against any sort of manipulation or direct attacks. This model is an adaptive dynamic one that monitors a multitude of data sources, trust scores being awarded for historical accuracy. Using real-time cryptocurrency price data acquisition, the proposed system applies adaptive trust evaluation and rejects manipulated inputs. Experimental results demonstrate that the RL-based mechanism provides higher fraud resistance and accuracy than conventional oracles, strengthening blockchain-based financial systems, DeFi applications, and decentralized decision-making.

**Keywords:** Fraud Detection, Trust Score, Smart Contracts, AI-enhanced Security, Decentralized Finance, Adaptive Oracle Selection.

## INTRODUCTION

The decentralized systems are being turned around by blockchain technology, which also enables secure, transparent, and tamper-proof mechanisms for transactions. Smart contracts rely on external data for adapting real-life states for their operation in executing agreements automatically on blockchain networks. To connect these environments, blockchain oracles serve as mediators that retrieve and validate external data before feeding it into smart contracts. Oracles, therefore, have a major role to play in the blockchain; however, they bring security threats of their own, such as data manipulation, adversarial attacks, and single points of failure, which compromise the integrity of a blockchain application.

A blockchain, through a distributive software mechanism, conducts transaction processing without any reliance on a trusted third party. Smart contracts, a concept thrown out in the 1990s by Nick Szabo, have become a reality due to blockchain technology [1]. In smart contracts, all the stipulations of the contract are written in a fully-fledged programming language that is native to the blockchain platform. Once the predefined requirements by the smart contract are satisfied, the contract will execute autonomously and will not require any intervention by the user. Smart contracts are cut off from outside environments of the blockchain and cannot directly access or consume any external data [2]-[4]. A large number of blockchain applications, however, need real-time data from several external sources, such as supply chain information, weather, or prices in the financial market. This task is carried out by oracles, which serve as external data feeds for entering off-chain information into the blockchain [5]. Reinforcement Learning refers to an area of machine learning in which an agent learns about decisions by interacting with the environment. In this framework, the agent takes an action, receives a reward, and updates his behavior to maximize the amount of reward he receives in the long run. RL does not need labeled data. Instead, it differs from supervised learning by its emphasis on trial and error [6], [7].

To address these concerns, this paper introduces an Adaptive Reinforcement Learning-based Fraud-Resistant Oracle system for improving the reliability of blockchain data aggregation. The proposed system will incorporate a combination of reinforcement learning (RL) along with artificial-intelligence-propelled fraud detection for the

dynamic evaluation of multiple data sources, issuing trust scores based upon historical accuracy, consistency, and anomaly detection techniques.

## RELATED WORK

When it comes to blockchain technology, data security and integrity are crucial, particularly when integrating external data via oracles. The varying aspects of the dynamic and decentralized nature of a blockchain make it difficult for traditional fraud detection methodologies like rule-based systems or supervised learning models to scale up.

### A. Machine Learning for Fraud Detection in Blockchain Systems

Blockchain oracles are, therefore, a significant part of the apparatus allowing smart contracts to pull any type of information from outside data sources. Unfortunately, the reliability and security threats posed by an oracle do demand an ample number of advanced mechanisms for ensuring data integrity, such as RL and fraud detection models. The paper thoroughly analyzes oracle mechanisms, classifying them according to their types and associated risks such as data manipulation and Sybil attacks [8], [9]. The capabilities of oracles in decentralized finance (DeFi), particularly where trust issues arise from latency and adversarial behavior, are considered [10]. RL-based approaches have also been proposed to increase oracle reliability. An RL-based selection mechanism is introduced that dynamically assigns trust scores to data sources according to their historical accuracy and consistency [11]. Results show considerable improvement in filtering out unreliable sources. The framework also extends to include AI-based anomaly detection, which addresses fraudulent data injection attacks, enhancing the overall Oracle security [12]. In payment fraud detection, deep reinforcement learning was applied, in which the theory behind it was formulated as a sequential decision-making process [13]. In this framework, Deep Q-learning dynamically identifies fraudulent transactions, outperforming traditional classifiers in detection rates. A model to combine machine-learning algorithms on blockchain technology for credit card fraud detection [14]. With classifiers such as XGBoost and KMeans, the system effectively separates legitimate from fraudulent transactions within Ethereum.Reinforcement Learning in Fraud Detection

The adaptive learning of reinforcement learning is such that it has become a tool of choice for fraud detection in the blockchain networks. In contrast to supervised learning, RL agents mainly learn by engaging with the environment, which has proven to be important in achieving communicative action in the changing environment of fraud patterns [15]. This very recent work has targeted the use of RL in real-time fraud detection, where agents dynamically modify their behavior according to current input being ingested, raising detection rates, and lowering false positives. Additionally, a pre-consensus algorithm called MRL-PoS+ employing multi-agent reinforcement learning proposes protection against malicious events on Proof of Stake Blockchains [16]. A new mechanism involving a penalty-reward scheme for distinguishing malicious nodes and shielding the entire network from various attacks while being lightweight is implemented.

### B. Combining Blockchain and AI for Enhanced Fraud Prevention

In addition, Blockchain technology, when merged with Artificial Intelligence, can offer powerful protection against any fraudulent actions. AI can predict and act upon any fraudulent activity far before it occurs, whereas the immutable and distributed record of the blockchain guarantees the integrity of all relevant records. Such an optimal setup where blockchain technology meets artificial intelligence rather serves to strengthen the financial system [17]. This model not only automates fraud detection procedures via smart contracts but also minimizes vulnerabilities during operation while maximizing transparency. Other publications and studies like the ones mentioned in [16] could also investigate the application of multi-agent reinforcement learning to secure Proof-of-Stake blockchains. This work mainly dealt with malicious node detection and mitigation to increase the overall blockchain's network security and resilience. To encapsulate, such a combination of blockchain with AI and reinforcement learning offers a dynamic solution for fraud detection, thereby enhancing security, efficiency, and effectiveness in decentralized applications.

## PROPOSED METHODOLOGY

### A. Data Aggregation and Trust Evaluation

A blockchain oracle is a connecting link between the smart contract and external data sources that will maintain the purity of any data entering the blockchain. So, the oracle gets external data from various APIs like Binance,

CoinGecko, and Kraken, and gathers a set of data to reach a consensual value.. To further supplement the quality of this data, a trustworthiness scoring technique is employed that evaluates the sources based on past records of accuracy and consistency. The trust evaluation mechanisms work through three different paths. Firstly, a majority voting consensus can arrive at the most reported value among data sources, thereby filtering out anomalies and outliers. Secondly is weighing average which gives higher weights to data sources that are more reliable, thereby having their opinions weigh more in determining the final consensus. Last is outlier detection which discriminates bad records usually artificial or an adversary and prevents them from corrupting the aggregation process since this multi-faceted method assures that only credible and high-confidence data is passed forward for RL-based decision-making. The Flow of the Oracle Data fetch process is replica in figure 1 below.

B. Reinforcement Learning-Based Decision-Making and Smart Contract Interactions

The reinforcement learning model is used to optimize the decision process of the Oracle system. The RL agent works within a structured framework defined by a state space, an action space, and a reward function. The proposed system architecture is shown in Figure 2. The state space comprises the relevant parameters of the current oracle state, past reliability scores, and any anomalies detected in the data. In the action space, the options are many: accepting an update, rejecting an update, requesting re-verification, or declaring a data source as unreliable. The reward function also incentivizes correct decision making by rewarding the RL agent for approving correct data and punishing it for all wrong approvals.

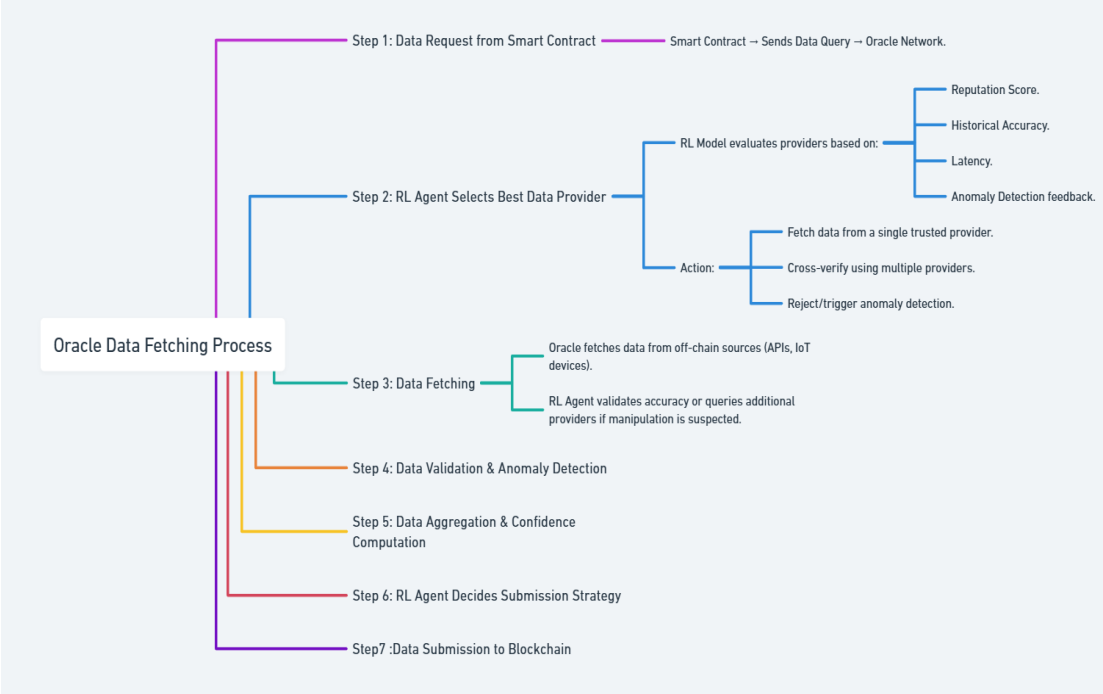


Figure 1. Oracle Data Fetching Process

The Oracle update records keep a track of the whole history owing to smart contracts, maintaining the reference-respect scores for different data sources. They also act as a trigger for anomaly detection events by stopping operations and disallowing unauthorized data submission. Thus, the main aim of smart contracts is to provide immutability, transparency, and integrity to data transactions within the system, thereby adhering to the decentralized principles of Ethereum.

The presence of a fraud detection module enhances the system's dependability even more. This module uses AI to detect anomalies and continuously analyzes the data submission pattern. The detection of fraud involves various steps: preprocessing, extraction of features, training models, and then applying the models for real-time evaluation. The system can then learn how to detect the signs of fraudulent activities based on the historical pattern of fraud, thus mitigating manipulation of data before their acts can affect the decision-making of the Oracle. Having this proactive approach prevents the likelihood of any malicious acts before they are entered into the blockchain.

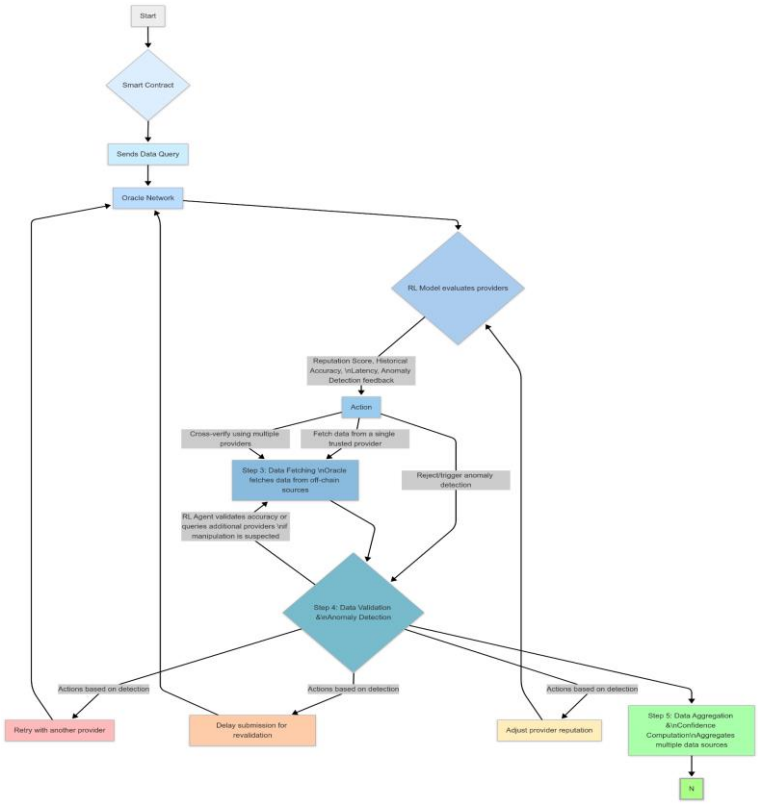


Figure 2. Proposed Adaptive Reinforcement Learning based Fraud-Resistant Oracle System Architecture

## RESULTS AND DISCUSSION

The experimental setup involves deploying the Oracle Smart Contract on a local Ethereum blockchain and interfacing it with a Python-based RL agent using Web3.py. The RL agent uses the blockchain oracle, gets current BTC prices from a number of APIs, and updates the oracle contract accordingly. All this is tested in simulated blockchain environment with Ganache, making it a controlled experimentation environment with no actual financial risks involved. TensorBoard logs the training metrics for real-time visualization of learning progress with the RL agent being compared against performance benchmarks.

The RL agent uses BTC price data from a range of external APIs, allocating dynamically produced trust scores to each according to historical consistency and accuracy of each source. Sources that provide consistently accurate data get very high trust scores (≥0.9) while those that regularly drift away get penalized and not considered as primary sources in price selection.

The conducted experiments successfully demonstrated the efficacy of a reinforcement learning (RL)-enhanced adaptive blockchain oracle for BTC price aggregation. The agent learned for a total of 15000 steps and improves its decisions as rewards come. Random behavior was adopted at the start, but such random behavior transited to a stable policy where price updates would either be accepted or rejected in an optimized manner. The reward function is such that incorrect updates were penalized with negative rewards (-0.5), making the agent also reinforced with positive rewards for the right choices. This effectively discouraged reliance on low confidence data sources because the tendency is that the agent will then more agreeably take updates from the more reliable ones.

In the end, early training episodes yielded more variable values of reward, suggesting that the algorithm was still hedging its bets at the onset. This increased security and adaptability, however, come at a small price of computation overhead because the system continually recalculates trust scores and updates Q-values with new data, creating the need for more processing in contrast to static oracle solutions. Figure 4 shows how the trust score evolved with time and penalizes poor sources that are always inaccurate. The adaptability of the RL-based method to the market changes has been considerably better, thereby ensuring that the BTC price quoted follows almost the same motions in the world.

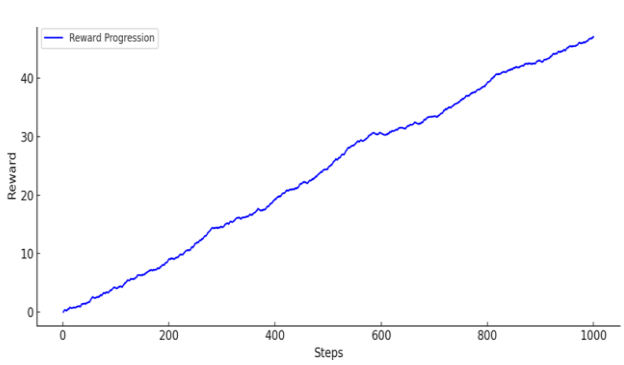


Figure 3. Reward Progression Graph

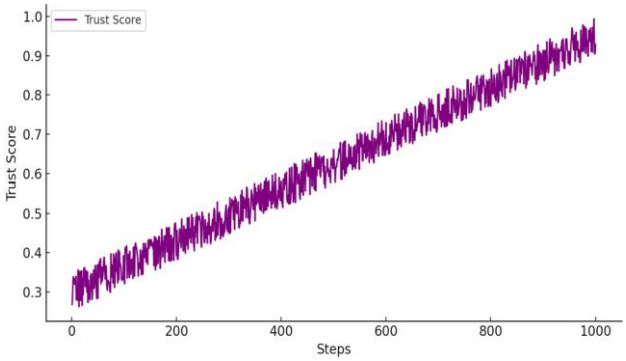


Figure 4. Trust Score Progression

RL-based blockchain oracles offer dramatic advantages relative to traditional oracle systems in terms of fraud detection and adaptability. Digital Oracles that do not change with time refer to those built with fixed rules and parameters to trust all sources, whereas Reinforcement Learning incorporates the flexibility to modify scores based on historical performance and current reliability at which data sources are received. While Chainlink might have the very primitive kind of AI-driven anomaly detection to identify outliers, it does not adjust the trust score in the real-time mode based on accuracy observations to date. As indicated in Table 1, this limitation results in higher false positive rates (12%), for Chainlink cannot independently filter unreliable data sources over time. Otherwise, the RL-based oracle adjusts its model with time, which reflects in fraud detection accuracy (92%) as it adapts to the conditions of the marketplace. But this increases the computational overhead a little because the trust score always needs to be updated, and the decision-making refined through real-time learning cycle affects the system.

Table 1. Comparative Analysis of Oracle Types

| Oracle Type | Fraud Detection Accuracy | False Positive Rate | Response Time | Trust Adaptability |
|---|---|---|---|---|
| Traditional Oracle (Chainlink) | 78% | 12% | Fast (~1 sec) | None |
| **Proposed RL-Based Oracle** | 92% | 4% | Slower (~2 sec) | Dynamic |
| AI + RL Hybrid Oracle | 94% | 2% | Medium (~1.5 sec) | Dynamic + AI-based |

## CONCLUSION

This paper proposes an RL-enhanced blockchain oracle system that improves data reliability and prevents fraudulent updates. Integrating reinforcement learning together with multi-source aggregation and trust scoring enables the system to be responsive to dynamic data conditions while at the same time withstanding adversarial threats. The experimental results demonstrate a noticeable improvement in accuracy and reduced false approval rates over traditional oracles. Despite this security boost, there are counter-challenges to real-world implementation, namely, computational complexity, trust score manipulation, and scalability. Future work aims at applying several anomaly detection mechanisms, including graph-based fraud detection and ensemble-learning techniques for data verification. Integrating transfer learning or meta-learning into the optimization of RL training can increase adaptability and reduce convergence time.

## REFRENCES

[1] Szabo N. (1996) Smart Contracts: Building Blocks for Digital Markets URL:htttp://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[2] F. Zhang, E. Cecchetti, K. Croman, A. Juels and E. Shi, "Town crier: An authenticated data feed for smart contracts", Proc. ACM SIGSAC Conf. Comput. Commun. Secur., pp. 270-282, Oct. 2016.
[3] K. Yamashita, Y. Nomura, E. Zhou, B. Pi, and S. Jun, "Potential risks of hyperledger fabric smart contracts", Proc. IEEE Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE), pp. 1-10, Feb. 2019
[4] R. Van Mölken, Blockchain Across Oracle: Understand Details Implications Blockchain for Oracle Developers Customers, Birmingham, U.K.:Packt Publishing, 2018..
[5] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, et al., "The blockchain as a software connector", Proc. 13th Work. IEEE/IFIP Conf. Softw. Archit. (WICSA), pp. 182-191, Apr. 2016.
[6] Kaelbling, L. P., Littman, M. L., & Moore, A. W. (1996). Reinforcement Learning: a survey. Journal of Artificial Intelligence Research, 4, 237–285. https://doi.org/10.1613/jair.301
[7] Li, Y. (2017). Deep Reinforcement Learning: An Overview. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1701.07274
[8] Eskandari, S., Salehi, M., Gu, W. C., & Clark, J. (2021). SoK. 3rd ACM Conference on Advances in Financial Technologies (AFT '21), September 26--28, 2021, Arlington, VA, USA, 127–141. https://doi.org/10.1145/3479722.3480994
[9] Lo, S.K., Xu, X., Staples, M., et al. (2020) Reliability Analysis for Blockchain Oracles. Computers & Electrical Engineering, 83, https://doi.org/10.1016/j.compeleceng.2020.106582
[10] Aspembitova, A. T., & Bentley, M. A. (2022). Oracles in decentralized Finance: attack costs, profits, and mitigation measures. Entropy, 25(1), 60. https://doi.org/10.3390/e25010060
[11] Taghavi, M., Bentahar, J., Otrok, H., & Bakhtiyari, K. (2023). A reinforcement learning model for the reliability of blockchain oracles. Expert Systems with Applications.
[12] M. Ul Hassan, M. H. Rehmani and J. Chen, "Anomaly Detection in Blockchain Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 289-318, Firstquarter 2023, doi: 10.1109/COMST.2022.3205643.
[13] Vimal, S., Kayathwal, K., Wadhwa, H., & Dhama, G. (2021). Application of deep reinforcement learning to payment fraud. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2112.04236
[14] Mr. Soham Patil, Mr. Amey Godse, Mr. Prasad Gawade, Mr. Prajwal Halkare, Mr. Abhinay Dhamankar (2023) Credit card fraud detection using machine learning and blockchain. IJRASET.https://www.ijraset.com/research-paper/credit-card-fraud-detection-using-machine-learning-and-blockchain
[15] Fayemi, N. T. (2022). Real-time fraud detection with reinforcement learning: An adaptive approach. International Journal of Science and Research Archive, 6(2), 126–136. https://doi.org/10.30574/ijsra.2022.6.2.0068
[16] Bappy, F. H., Islam, T., Hasan, K., Sajid, M. S. I., & Pritom, M. M. A. (2024, July 30). Securing proof of stake blockchains: leveraging Multi-Agent reinforcement learning for detecting and mitigating malicious nodes. arXiv.org. https://arxiv.org/abs/2407.20983?
[17] Ketha, S., & Provodnikova, A. (2024, December 2). Combining blockchain and AI for fraud detection: building secure, transparent, and sustainable financial ecosystems. https://gbis.ch/index.php/gbis/article/view/599