Chapter 10
The Critical Role of Blockchain Oracles in Web 3

Vijaya Killu Manda

https://orcid.org/0000-0003-2938-838X

GITAM School of Science, GITAM University (Deemed), India

Vedavathi Katneni

GITAM School of Science, GITAM University (Deemed), India

ABSTRACT

Blockchain networks often require data to and from the outside world, especially when offering services such as in the financial domain. Blockchain oracles are critical infrastructure layers that bridge the blockchain network so that smart contracts get rich data to process transactions or execute business logic. Blockchain oracles are classified into various types depending on the data facility offered. Some popular oracle networks include chainlink, brand protocol, and provable. This chapter explains how oracles work, such as fetching and delivering data, data verification and aggregation, and reward mechanisms. It also briefly discusses on their applications, such as price feeds for DeFi applications, event triggers used in insurance and gambling contracts, identity/reputation management for NFTs, and aggregating of IoT sensor data. Security and decentralization are discussed. The chapter ends with a discussion of future research trends and the integration of artificial intelligence and machine learning, event-driven architectures, and recent advancements.

WHAT ARE ORACLES?

The burgeoning blockchain landscape has witnessed a proliferation of heterogeneous blockchain platforms, each with a unique architecture and protocol. Unfortunately, these platforms remain mostly isolated, hindering seamless communication and interoperability. Two popular approaches currently famous for this are – the relay approach and the oracle approach.

An "Oracle", according to Greek mythology, is a person who can communicate with God. Because ordinary people sometimes cannot make decisions independently, they used to turn to oracles to help

communicate with God and get insights. In blockchain, "Oracles" are considered infrastructure tools and layers through which off-chain data is accessed, sourced, and verified for use by the blockchain. They are essential in blockchains such as Decentralized Finance (DeFi) because of the necessary interactions with the real world when offering financial services. No wonder they are called the 'invisible backbone' of DeFi and blockchain-based applications (Wintermeyer, 2021). Oracles are conceptual solutions offered as services. However, they are not explicit programs, codes, or data sources. They use trusted third parties that collect data from data sources, verify it, and then transmit it to the blockchain so that the smart contracts get exogenous data (data/information from the outside world) (Hassan et al., 2023). Because oracles are centralized, the dependency of blockchain on them could pose problems because they bring back the concepts of centralization and trust them back to blockchains.

Definition and Purpose of Oracles

Oracles are intermediaries that facilitate communication between a distributed application (dApps) and some external real-world data sources. They serve as trusted third-party entities that verify and validate external data, ensuring its accuracy and authenticity. Applications can get rich real-world data such as price feeds (as in stock markets or for an online store), weather updates, or event notifications (such as from an IoT sensor or a CCTV camera). dApps and blockchain networks need external data to enhance the functionality and decision-making processes as per the business logic.

There are five main advantages of using blockchain oracles:

1. **Decentralized Data Access**: Blockchain oracles will make secure and reliable external data, resources, and events available. With this, dApps can make more informed decisions and improve their functionality.
2. **Increased Trust and Security**: Oracles ensure the accuracy and authenticity of data by validating and verifying external information. Reduced risk of fraud and manipulation will hence become possible. Also, the blockchain nodes will be de-stressed because of the shift in part of their processing load.
3. **Interoperability**: Interaction with external systems and networks will be possible through blockchain oracle-enabled dApps. This promotes interoperability and collaboration between various elements and stacks of the blockchain ecosystems. This became even more important because typical blockchain systems have several fragmented and heterogeneous blockchain platforms. Blockchains implement interoperability using Naive relay and Oracle solutions (Sober et al., 2021).
4. **Feeding off-chain data to smart contracts**: The Oracle Problem is an open practical problem involving off-chain data to and from blockchains and their smart contracts. According to the oracle problem, or oracle paradox, as it is referred to in some literature, the dilemma lies in the fact that the reliability of blockchain data is threatened and compromised when data/information is introduced from the outside world. The paradox is believed to be a prime reason some businesses hesitate about smart contracts. Some mitigation strategies were proposed to counter this (Albizri & Appelbaum, 2021). "Trust, but Verify" and "from trust to truth" (Hassan et al., 2023) remain famous mantras. One example of this happens is when oracles are used to observe occurrences and provide this information to smart contracts. Researchers insist that oracles should be viewed as service organizations under the auditing standards of the AICPA and PCAOB (Sheldon, 2021).

Related Content

Real-Time Unspecified Major Sub-Events Detection in the Twitter Data Stream That Cause the Change in the Sentiment Score of the Targeted Event
Ritesh Srivastavaand M.P.S. Bhatia (2017). *International Journal of Information Technology and Web Engineering (pp. 1-21).*
www.irma-international.org/article/real-time-unspecified-major-sub-events-detection-in-the-twitter-data-stream-that-cause-the-change-in-the-sentiment-score-of-the-targeted-event/188379

A Novel Method to Dynamically Fix Threshold for Node Neighbourhood Based Link Prediction Techniques
Anand Kumar Guptaand Neetu Sardana (2020). *International Journal of Information Technology and Web Engineering (pp. 17-34).*
www.irma-international.org/article/a-novel-method-to-dynamically-fix-threshold-for-node-neighbourhood-based-link-prediction-techniques/241774

Integrity of E-Health Record Ensured With Context-Based Merkle Tree Through Temporal Shadow in Blockchain
 Charanya R.and Saravanaguru R. A. K. (2020). *International Journal of Information Technology and Web Engineering (pp. 72-87).*
www.irma-international.org/article/integrity-of-e-health-record-ensured-with-context-based-merkle-tree-through-temporal-shadow-in-blockchain/264476

The Role of Electronic Commerce in the Global Business Environments
Kijpokin Kasemsap (2016). *Web Design and Development: Concepts, Methodologies, Tools, and Applications (pp. 1014-1034).*
www.irma-international.org/chapter/the-role-of-electronic-commerce-in-the-global-business-environments/137385

Energy-Aware Manufacturing Using Information Technology Tools: A Knowledge Based System Approach
Mohammed A. Omar, Ahmad Mayyasand Qilun Zhou (2014). *International Journal of Information Technology and Web Engineering (pp. 70-77).*
www.irma-international.org/article/energy-aware-manufacturing-using-information-technology-tools/113322