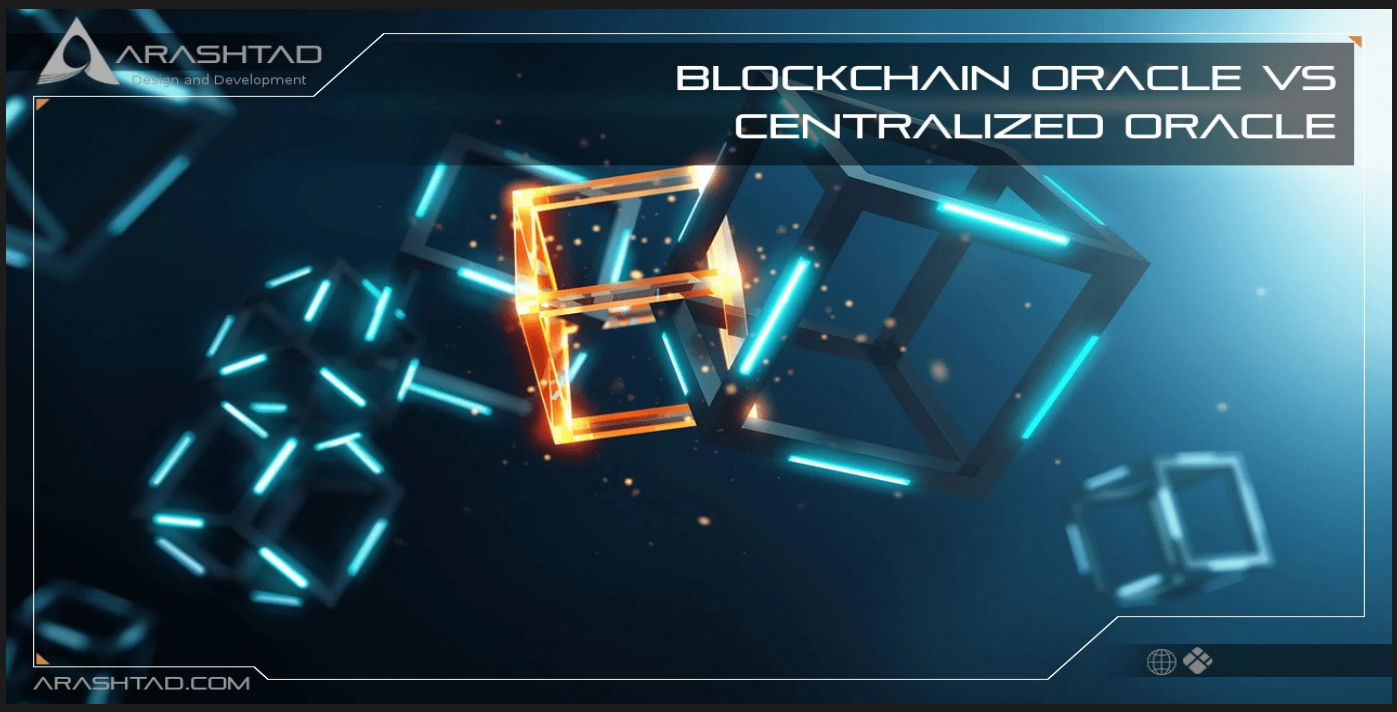
Title	DECENTRALIZAED ORACLE VS. CENTRALIZED ORACLE
Description	Intro
Date	2022 26 Augus
Author	Arashtad
Author URI	https://Arashtad.com



The blockchain oracle connects blockchains to external systems, enabling smart contracts to execute based on real-world inputs and outputs. Oracles allow decentralized Web3 ecosystems to access existing data sources, legacy systems, and advanced computations. With decentralized oracle networks (DONs), advanced decentralized applications (dApps) can interact with traditional systems by combining on-chain code with off-chain infrastructure. In this article, we will see how a blockchain oracle works, how it makes blockchain systems more secure, and also compare it with a non-blockchain or centralized oracle.

THE PROBLEM WITH APIS IN A BLOCKCHAIN ECOSYSTEM:

Due to the distributed nature of the blockchain, each node in the network needs to be able to get the same result given the same input. otherwise, when a node looks to validate a transaction another node makes, it will get the same result. This architecture is purposefully deterministic.

If you want to create a smart contract in which a person pays an online shop 10 Dollars to purchase the software. And he wants to pay it in Ethereum, the smart contract uses an API call to first retrieve the Ethereum/USD pair. And then do the rest of the job. Now, in this scenario, we might face an issue. What if the nodes that fetch the Ethereum price from the API get different results? Because of many reasons such as being hacked, deprecated, or a lag in the time of getting data. As a result, the nodes will return results, and consequently, they cannot agree on the state of the blockchain.

HOW CAN BLOCKCHAIN ORACLES SOLVE THIS ISSUE?

A blockchain oracle is any device that connects to off-chain data from a deterministic blockchain. Oracles enter all data inputs through external transactions. In this way, we can be sure that the blockchain contains all of the information it needs to verify itself. This is why oracles are referred to as blockchain middleware: They provide a link between two worlds.

THE PROBLEM WITH BLOCKCHAIN ORACLES

The blockchain oracle problem outlines a fundamental limitation of smart contracts. They cannot inherently interact with data and systems existing outside their native blockchain environment. Resources external to the blockchain are considered “off-chain,”. While data already stored on the blockchain is on-chain. Blockchains obtain their most valuable properties like strong consensus on the validity of user transactions, prevention of double-spending attacks, and mitigation of network downtime. Securely interoperating with off-chain systems from a blockchain requires an additional piece of infrastructure. This infrastructure is called oracle and its job is to connect the two environments.

WHAT IS A DECENTRALIZED ORACLE?

A decentralized oracle network is a group of independent blockchain oracles that provide data to a blockchain. Each independent node or oracle in the decentralized oracle network retrieves and brings data from an off-chain source independently. In order to arrive at a deterministic value of truth for that data point, the data is aggregated. Decentralized oracles solve the problem of oracles. In order to avoid data manipulation, inaccuracy, and downtime, decentralized oracles are necessary to overcome the Oracle Problem. For end-to-end decentralization, Decentralized Oracle Networks, or DONs, combine multiple independent Oracle nodes and multiple reliable data sources. One of the most famous oracles which are very popular is ChainLink. In the next section, we will talk about it in more detail.

WHAT IS CHAINLINK?

Smart contracts can reach their full potential by connecting the real world's data to the blockchain with Chainlink's independent network of nodes. At ChainLink, developers are building a blockchain oracle using the same reliable decentralized infrastructure concept as the blockchain. In case of hacks, depreciations, or deletions, Chainlink will continue to operate.

BLOCKCHAIN ORACLE USE CASES

The use of oracles in smart contract development allows developers to build more advanced decentralized applications across a broader range of blockchain use cases. Here are the main blockchain use cases that are currently in use.

DYNAMIC NFTS AND GAMING

The Oracle platform also supports non-financial use cases for smart contracts, such as dynamic NFTs (Non-Fungible Tokens) that change appearance, value, or distribution based on external factors. The compute oracle also generates verifiable randomness that projects can then use to assign random traits to NFTs or to select random winners in high-demand NFT drops. Verifiable randomness is useful for creating engaging and unpredictable gameplay experiences in on-chain games, such as random loot boxes and randomized matchmaking during tournaments.

DEFI

For decentralized finance (DeFi) to function, it relies on oracles to access financial data about assets and markets; a decentralized money market, for example, uses price oracles to check if users' positions are undercollateralized or subject to liquidation by determining their borrowing capacity; In a similar manner, synthetic asset platforms use price oracles to equate token values with real-world assets, and automated market makers (AMMs) use price oracles to concentrate liquidity at the current market price.

ENTERPRISE

Using cross-chain oracles, enterprises can secure their backend systems from any blockchain network and connect them to it. Using the same oracle network, enterprise systems can perform complex logic on how to deploy assets and data across chains and with counterparties. By doing so, institutions can join blockchains in high demand by their counterparties and create support for smart contract services quickly without having to spend time and development resources integrating with each blockchain.

SUSTAINABILITY

Through advanced verification techniques around green initiatives' true impact, hybrid smart contracts contribute to environmental sustainability by encouraging participation in green practices. As a result of sensor readings, satellite imagery, and advanced machine learning computation, Oracles provide smart contracts with environmental data that allows them to distribute rewards to people who practice reforestation or consume responsibly. In addition, Oracles support a variety of new carbon credits as a way of offsetting climate change's impacts.

INSURANCE

In insurance smart contracts, input oracles verify that insurable events occur during claims processing, allowing access to sensors, web APIs, satellite imagery, and legal information. Insurance smart contracts can also use output oracles to make payouts on claims using other blockchains or traditional payment networks.

WRAPPING UP

In this article, you learned about centralized oracles, their problems and issues in addition to the blockchain oracles, and decentralized oracles. These technologies have enhanced blockchain networks beyond simple tokenization by providing access to all the external resources necessary for the use of hybrid smart contracts beyond simple tokenization. A hybrid smart contract powered by Oracle is redefining how society exchanges value and enforces contractual agreements, similar to the Internet, which revolutionized the way information was exchanged.