Offchain Reporting

Offchain Reporting (OCR) is a significant step towards increasing the decentralization and scalability of Chainlink networks. See theOCR Protocol Paper for a technical deep dive.

For Offchain Reporting aggregators, all nodes communicate using a peer to peer network. During the communication process, a lightweight consensus algorithm runs where each node reports its data observation and signs it. A single aggregate transaction is then transmitted, which saves a significant amount of gas.

The report contained in the aggregate transaction is signed by a quorum of oracles and contains all oracles' observations. By validating the report onchain and checking the quorum's signatures onchain, we preserve the trustlessness properties of Chainlink oracle networks.

What is OCR?

A simple analogy

Imagine ordering 10 items from an online store. Each item is packaged separately and posted separately, meaning postage and packaging costs must be applied to each one, and the carrier has to transport 10 different boxes.

OCR, on the other hand, packages all of these items into a single box and posts that. This saves postage and packaging fees and all effort the carrier associates with transporting 9 fewer boxes.

The OCR protocol allows nodes to aggregate their observations into a single report offchain using a secure P2P network. A single node then submits a transaction with the aggregated report to the chain. Each report consists of many nodes' observations and has to be signed by a quorum of nodes. These signatures are verified onchain.

Submitting only one transaction per round achieves the following benefits:

- Overall network congestion from Chainlink oracle networks is reduced dramatically
- Individual node operators spend far less on gas costs
- Node networks are more scalable because data feeds can accommodate more nodes
- Data feeds can be updated in a more timely manner since each round needn't wait for multiple transactions to be confirmed before a price is confirmed onchain.

How does OCR work?

Protocol execution happens mostly offchain over a peer to peer network between Chainlink nodes. The nodes regularly elect a new leader node that drives the rest of the protocol.

The leader regularly requests followers to provide freshly signed observations and aggregates them into a report. It then sends this report back to the followers and asks them to verify the report's validity. If a quorum of followers approves the report by sending a signed copy back to the leader, the leader assembles a final report with the quorum's signatures and broadcasts it to all followers.

The nodes attempt to transmit the final report to the aggregator contract according to a randomized schedule. The aggregator verifies that a quorum of nodes signed the report and exposes the median value to consumers as an answer with a block timestamp and a round ID.

All nodes watch the blockchain for the final report to remove any single point of failure during transmission. If the designated node fails to get their transmission confirmed within a determined period, a round-robin protocol kicks in so other nodes can also transmit the final report until one of them is confirmed.