Ojo Network

An Economically-Aligned, Decentralized, Intelligent Oracle

Adam Wozniak

1.0 Abstract

Due to many factors such as server latency, regionally differing information, and difference of opinion, it is difficult to build an efficient decentralized system for determining the truth around information that originates off-chain. This is referred to as the Oracle Problem, and this is the problem which the Ojo Network aims to solve.

The Ojo Network is a Cosmos SDK blockchain using tendermint BFT for the consensus layer, which specializes in aggregating data from decentralized sources on the blockchain in a permissionless manner and relaying that information to other blockchains via cross-chain smart contracts and the Inter-Blockchain Communication Protocol (IBC). Validators will be able to proactively provide data feeds approved via governance, and are rewarded for their work.

1.1 Introduction

Existing Oracle networks do not solve the immediate need of the DeFi landscape. With more fast-finality DeFi protocols coming to fruition, protocols need to access accurate pricing information, as well as information that allows them to make automated decisions for the safety of the protocol.

Existing solutions provide data that is out-of-date; in a PoW world, this is reasonable, as consensus for a given block takes minutes to hours. As fast-finality PoS becomes the dominant consensus method, data must be quicker on both sides. Users are able to transact faster on AMMs and Lending Protocols, meaning dramatic price change happens at a much higher rate. Oracles must be reactive to this, while also giving context around the health of the market.

Existing oracles are also often controlled by centralized entities. This centralization tends to bleed into the consensus layer, with hand-picked network operators becoming the source of information for a supposedly decentralized oracle. This lack of competitiveness can lead to lazy implementations and slow timing. In order to be aligned with the PoS thesis, this process must be trustless and also buy-in; validators need to have enough skin in the game to actively compete with one another to provide the best information possible.

The implications of a network which is trustless, economically secure, intelligent, and decentralized go far beyond what was previously attainable.

With these ideas in mind, we present the Ojo Network - an economically-aligned, decentralized, intelligent oracle solution designed for high-stakes fast-finality protocols which need the ability to make informed decisions.

2.0 Economically-Aligned

DeFi protocols are incredibly sensitive products; swings in asset pricing can cause entire markets to collapse. In order to have the most accurate pricing, network participants need to be incentivized to act in accordance with the protocol. This aligns with the PoS thesis; validators with a stake in the network are incentivized to act in good faith. For an oracle protocol, this must be a focal point; consuming protocols need to trust that Ojo's validator set is economically aligned; otherwise, the integrity of the product is in question. In addition to these incentives, Ojo will also have an Oracle Treasury which is designed to make the cost of manipulating Ojo's price feeds more than the potential gain of an attacker.

2.1 Decentralized

An oracle protocol's foundation, or the top 10 validators, should not be able to collude to alter pricing information. In a PoS system, this is especially fragile; oracle pricing information can be set by a 2/3rds majority, which allows validators to choose which information they'd like to relay. If 1/3rd of the voting power goes down, the validator set is able to halt information coming to other validators. Taking this into consideration, we must focus on incentivizing delegations to lower-power validators in order to be as robust as possible. In order to promote decentralization we will have a set of rewards dedicated strictly to pricing behavior, which we will go over in more detail.

2.2 Intelligent

Information about the market should not be limited to the current spot price of a given asset; DeFi protocols need access to contextual market data in order to make the right decisions for the health of the protocol. In the real world, legal protections require identification and will lead to jail time for performing exploits against banks and insider-trading. Blockchains are people-agnostic and anonymous, so DeFi protocols must assume that any actor will intend to hurt the system if it is for personal gain. To defend against this, client protocols could take historic market data and trading information in order to design built-in decision making for what users are allowed to do. This kind of information should be simple to understand and robust enough for protocols to draw many different conclusions; specifically, it should allow the protocol to decide whether or not someone is trying to artificially manipulate prices, or if the borrower of a token is intending to leave the position in bad health.

The Ojo Network will have a set of features which grant protocols with access to this kind of data: Smart Oracles. These will enable blockchains to allow different trading strategies, list more tokens, and allow more interoperability with CeFi and institutional banking.

2.3 Oracle Treasury

Oracle protocols are inherently error-prone and difficult to maintain. Latency, miscalculations, hacks, and human error cause immediate and sometimes irreparable exploits on client protocols; especially in the emergent world of fast-finality blockchains and smart contracts. Since blockchains are essentially anonymous, bad actors are not incentivized by good reputation; the driving force always ends up being financial gain. In centralized oracle networks such as Chainlink, there is an authority from which client protocols and their users can demand a repayment. This is another manual and trusted process; and in the world of lawless, borderless blockchains, client protocols are not secured by this promise. Adversely, the Ojo Network is decentralized; no one entity holds the keys to the kingdom to unilaterally determine how much to reward the client with. As a result of this, the Ojo Network will be secured by a protocol treasury, which will hold a certain amount of tokens as an “insurance policy” against these bad actors.

2.4 Client Security

As larger protocols adopt the Ojo Network, the profit which could be gained by disrupting Ojo’s price calculations increases. In the proof of stake model, the cost to influence oracle votes is equal to the fully diluted valuation of the chain; simply put, if an individual or a group of individuals were to buy enough tokens to significantly affect pricing without incurring a penalty, they could alter oracle to their benefit. If at any point the cost does not outweigh the benefit, actors with enough capital will stand to gain. As a measure to increase this cost, payments made to the Ojo Network will be received by the treasury, then measured against the current valuation of the Ojo Network, and either disbursed to validators as payment for services or held in the treasury. Validators will both vote on the cost of exploiting the chain, as well as the collective value of the client chains. Together these will determine how to correctly allocate funds.

3.0 Generalized Implications

Ojo has been defined as an expandable, proactive, intelligent oracle with economics in mind. This architecture will allow us to develop unique solutions for the industry that go past the bounds of cosmos.

3.1 Proof of Reserves

Ojo’s oracle capabilities can be leveraged to relay proof of reserves data to other chains. This is of critical importance to many decentralized applications, as it serves to assure users that their assets are adequately backed by reserves. Validators on the Ojo Network can vote on relevant datapoints related to proof of reserves, such as the amount of assets held in reserve by a particular entity, and securely store and verify this information on-chain. Other chains can then access this data through IBC-enabled queries, enabling them to independently verify the proof of reserves for themselves. This can be incredibly valuable for decentralized exchanges and lending platforms, where trust and transparency are paramount.

3.2 VRF

Verifiable randomness is a key feature of the Ojo Network, implemented as a module on the chain. This technology provides applications that require provably fair, unbiased, and tamper-proof randomness, such as gaming, prediction markets, and distributed lotteries, with an essential tool. With the Ojo Network, verifiable randomness is generated on-chain using a cryptographic function, ensuring its unpredictability and non-manipulability. This module can be easily integrated into smart contracts, allowing developers to build trustless and decentralized applications that rely on random events.

In addition to on-chain verifiable randomness, the Ojo Network's interoperability with other blockchains using IBC-enabled queries enables the relay of this data to other chains. This allows developers to expand the possibilities for cross-chain applications that utilize verifiable randomness. The ability to generate secure and tamper-proof randomness on-chain, combined with the network's interoperability, creates exciting opportunities for developers to build decentralized applications that rely on this technology. Verifiable randomness is an essential feature for a wide range of blockchain applications, including gaming, gambling, prediction markets, and any other application that relies on random events. With the Ojo Network's verifiable randomness module, developers can build trustless and decentralized applications that are transparent and tamper-proof, providing users with a secure and fair experience.

3.3 Multi-chain Vision

The Ojo Network's cross-chain smart contracts and IBC protocol enable it to efficiently relay pricing information to various blockchain environments. Validators on the Ojo Network can provide data feeds on the current prices of different assets approved via governance, which can be aggregated and verified on the blockchain. This data can then be transmitted to other blockchains through the use of cross-chain smart contracts and the IBC protocol. With this approach, pricing information can be efficiently and securely shared across multiple blockchain environments, including Cosmos, Ethereum, Solana, and Celestia, allowing for more accurate and up-to-date pricing information to be available across the decentralized ecosystem. The more protocols which implement IBC, the easier this integration becomes, though the network is robust enough to allow for anyone to deploy cross-chain smart contracts onto client chains and be rewarded for relaying information to the new environment.

3.4 Real-world Vision

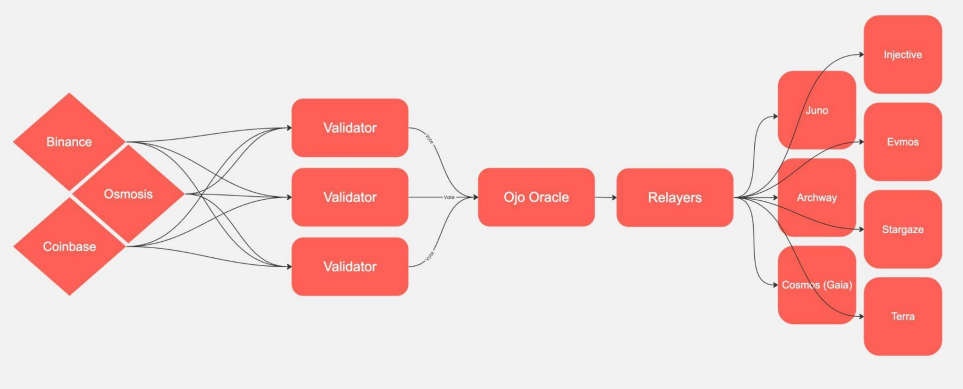
Ojo’s unique features make it an ideal platform to determine the prices of various financial instruments such as stock prices, equity indexes, commodities, interest rates, bond markets, and forex currencies. With the ability to aggregate data from decentralized sources and relay it across blockchains through cross-chain smart contracts and IBC, the network can provide reliable and verified pricing information for these assets. By utilizing governance-approved data feeds and incentivizing validators to provide accurate data, the Ojo Network can help reduce the risk of errors and discrepancies in pricing, increasing confidence in the accuracy of valuations. This makes it an attractive option for bringing larger, non-crypto-native markets onto the blockchain and promoting the adoption of blockchain technology in traditional financial markets.

4.0 Basic Concepts

Ojo validators run the network in a permissionless manner using PoS consensus built on Tendermint BFT (soon to be Comet BFT). Delegated PoS blockchains in the cosmos ecosystem rely on users to delegate their tokens to validators in order to receive governance power and staking rewards; these typically take the form of inflationary rewards in the chain's native token which are granted to stakers at the expense of non-stakers. Validators are rewarded for running the network by earning a percentage commission of these inflationary tokens. Consensus is able to continue by 2/3rds majority. Validators who do not agree with the majority are removed from the validator set, and their delegated tokens are typically slashed by some predefined percentage.

4.1 Basic Architecture

The basic architecture of the Ojo Network is as follows: validators query external providers such as Binance and Coinbase for information on the price of assets. They then submit votes to the Ojo Oracle, which determines a set of canonical data. This is then picked up by relayers, which relay this information over to other IBC-enabled blockchains.



5.0 Off-Chain Price Feeder

We're building an off-chain tool for validators to use to vote on prices. This tool is given to validators to run, and is responsible for querying external price providers and voting on prices. This is referred to as our Price Feeder. This tool has quite a few features; it's proactive, considers stablecoin depeg events, and protects against unstable providers.

5.1 Proactivity

Most oracles are designed to be reactive; once a client needs a piece of information, a bounty is set, and validators respond at their own leisure. This introduces unnecessary latency and, depending on transaction times, can significantly delay the on-chain availability of information. We've reversed this design; once governance has approved a data source to be relayed, validators will be expected to provide up-to-date information originating from the source.

5.2 Stablecoin Security

Stablecoin depegging events have been the death of many protocols; unfortunately, oftentimes DeFi protocols are written under the assumption that stablecoins will always be at or near their intended price. Our price feeder is built with resilience in mind, meaning all stablecoins are treated as if they will not stay at the intended price at any given moment. We aggregate data from many sources to make sure that if the price of a stablecoin changes from what is intended, our oracles react quickly.

5.3 Provider Deviations

Ojo uses several external data providers in order to determine asset prices; however, these providers are often centralized and are susceptible to hacks, downtime, and latency. Our price feeder is designed to consider each of these conditions. Validators can set how tolerant they want to be with a certain asset's providers; if one provider starts to report completely different data, it is assumed to be compromised and filtered out. The price feeder calculates the median price of each asset over a period of time alongside the standard deviation; if a provider reports a price that falls outside of this range, the value is discarded.

5.4 Expandability

This tool is completely open-source, and collaboration is encouraged to expand its use cases. As more decentralized exchanges launch, we'll need to build new APIs and indexers to get this information on-chain for Ojo as liquidity is provisioned across IBC-enabled networks.

Ojo is also capable of providing data feeds far beyond cryptocurrency price feeds. Proof of Reserves, cryptocurrency mining emissions, forex exchange rates, NFT floor prices, and credit rating information are all possible data points to be relayed by Ojo.

6.0 On-Chain Oracle

Our on-chain oracle is a Cosmos SDK module, designed to be a recipient of the price feeder tool. This module aggregates validators' votes on different prices, and is responsible for punishing validators that misbehave. The original implementation was done by Terra Classic.

6.1 Penalties

Network participants that are not validating data in good faith will incur a penalty in the form of slashing. All validators in the active set are required to vote on the price of accepted assets every few blocks; if a validator is unable to do so effectively, the validator will be subject to a penalty.

Let M be the median, σ be the standard deviation of the votes in the ballot, and R be the RewardBand, a governance-determined value for a given asset. The band around the median is set to be ε = max(σ, R/2). All valid (i.e. bonded and non-jailed) validators that submitted an exchange rate vote in the interval [M - ε, M + ε] should be included in the set of winners. All other active validators will incur a "miss count". If these "miss counts" go above a certain threshold, they will be slashed and jailed.

6.2 Rewards

Ojo's reward system is unique; it's based on the aforementioned "miss count". On top of the basic PoS inflation, we set aside an additional "bonus" set of rewards to give to validators. Assuming validators would all start with an equal amount of "bonus" tokens, we can use this graph to determine a given validator's reward multiplier:

$$1 - \log_{m-s+1}(x - s + 1)$$

Given:

- **s -** smallest # of misses a validator had during the slashing window
- **m -** amount of possible misses in a slashing window
- **x -** a given validator's miss count

This equation is necessary since validators' performance must be measured relative to one another. If the entire set of validators has at least 100 "miss counts," only validators with exactly 100 miss counts will receive the full bonus. Any rewards not received by a validator subsequently go into the community fund. After the supply cap is hit, this model will be partially used to reward validators based on customers' payments. See the tokenomics section for more context.

6.3 Risk Metadata - Smart Oracles

Ojo's oracle is designed to accommodate the needs of high-risk protocols like peer-to-peer leverage systems. We've designed a way for protocols to check on the health of positions that users are attempting to take.

For relatively low-volume assets (which applies to the majority of tokens being launched in Cosmos), there is an attack vector for being listed on any peer-to-peer leverage protocol. One of these attack scenarios goes this way:

1. Attacker deposits & collateralizes a large amount FOO, a token with low volume on exchanges.
2. Attacker spikes the price of FOO on the exchanges by buying a large amount.
3. Attacker borrows USDC using their FOO as collateral at its current (spiked) oracle price.
4. The price of FOO returns to normal, and the value of the USDC exceeds the value of the FOO collateral.
5. Attacker exits the market for a profit.

In order to avoid these attacks, and to continue with our goal of allowing users to collateralize and borrow low-volume assets, these protocols need to have a safety net. The oracle module is able to track data on the historic price of assets by "stamping" the current price of an asset every X amount of blocks. After another period of time, the module calculates the median and standard deviation around the median of the price stamps which are currently in storage. This information is then relayed to receiving chains. This leaves us with a relatively efficient way for client chains to determine whether or not the price of an asset is unexpectedly changing, either through a natural swing in the market or through a bad actor attempting to manipulate assets.

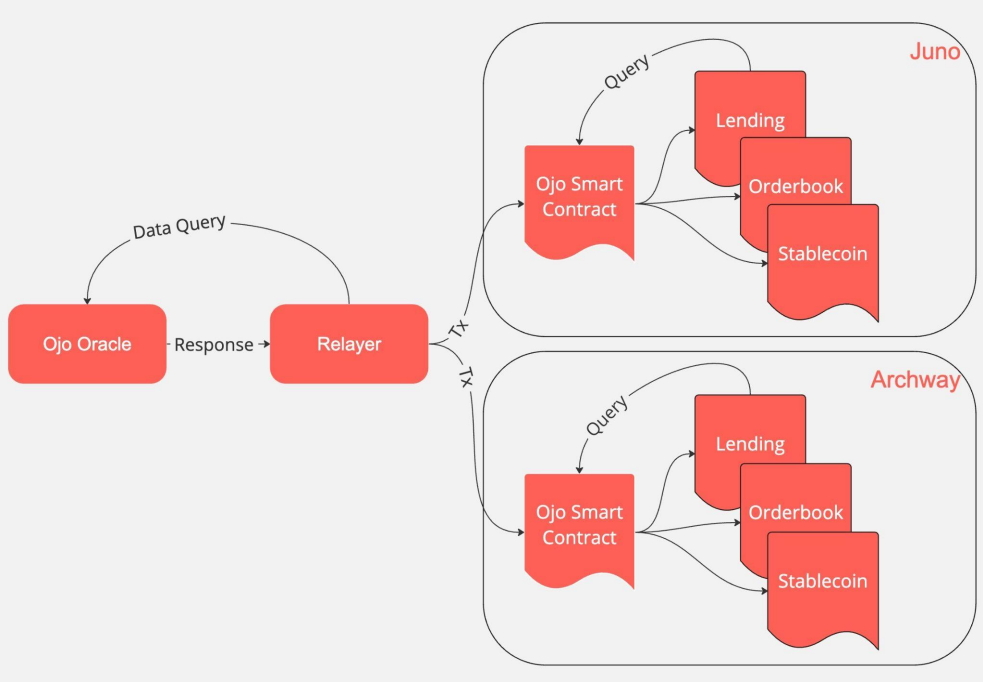
Please see our initial design document to read about the specifics of our implementation and additional attack scenarios for leverage protocols.

7. Data Relaying

For the Ojo Network to be effective in a fast-finality PoS system, relaying must be fast and trustless, and relayers must be rewarded effectively for doing their jobs. For these reasons we've gone with a two-stage approach to our relaying mechanism.

7.1 Centralized Contracts

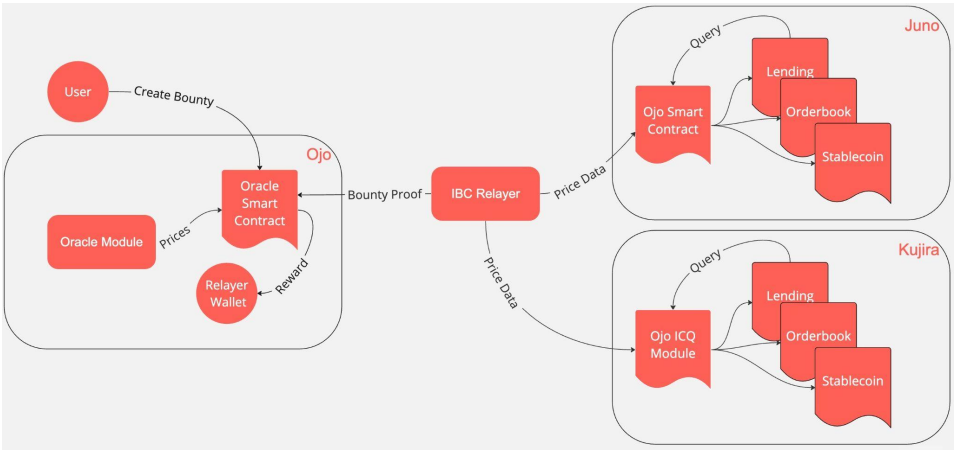
Initially, data relaying to external protocols will be done by a set of centralized smart contracts in order to prioritize speed. These contracts will be deployed to Juno, Archway, and other CosmWasm-enabled chains. Data on these contracts will be reflective of everything available on the oracle module; the risk metadata and pricing information which the recipient chain would like to receive will be configurable. Initially, these services will be completely free to help ease adoption. Eventually, paid whitelists will be implemented. Tokens earned from this model will be used to pay fees and sent back to the validator set as a part of the miss count “bonus" rewards.



Please see our CosmWasm contracts and relayer source code for details.

7.2 Decentralized

Using interchain queries and cross-chain smart contracts, anyone can post a bounty for oracle information to be relayed to a specific chain for a certain duration. The price of these services will be determined by governance, and validators will be rewarded for providing pricing information. The amount of jobs a network participant can take will be limited linearly according to the amount of OJO the participant has staked. Receiving chains can either implement Ojo’s IBC Queries module, or install a cross-chain CosmWasm smart contract.



Please read our initial [design document] for details on our implementation and discussions we've had around it.

8. Tokenomics

OJO is the native token the network will use to incentivize network participants. The network's tokenomics will initially have an inflationary model, which will eventually hit a hard cap of supply. The goal of the tokenomics is to incentivize early stake until Ojo's data relaying model turns into a trustless system where validators need a minimum amount of tokens to be rewarded for relaying information. When customers pay for services, they will be able to pay in any supported IBC asset. Validators will be limited to the amount of "relaying jobs" they can perform based on the amount of OJO they have staked. Once validators can prove that they have relayed information accurately, they will receive a reward.

8.1 Community Fund

A portion of the initial supply will be set aside for a community fund which should be used to improve the Ojo Network, through incentivizing liquidity provisioning on AMMs, putting up bounties for new price feeds, or giving grants for teams that want to build on top of the oracle.

If governance decides to approve an application for funding via the community fund, the assets will initially be subject to a cliff period before disbursement. Once the cliff has passed, the tokens will vest linearly as determined by governance. This ensures that there is not a large influx of assets being introduced to the market at once, and governance also has time to decide on whether or not the grant recipient has delivered on the approved project.

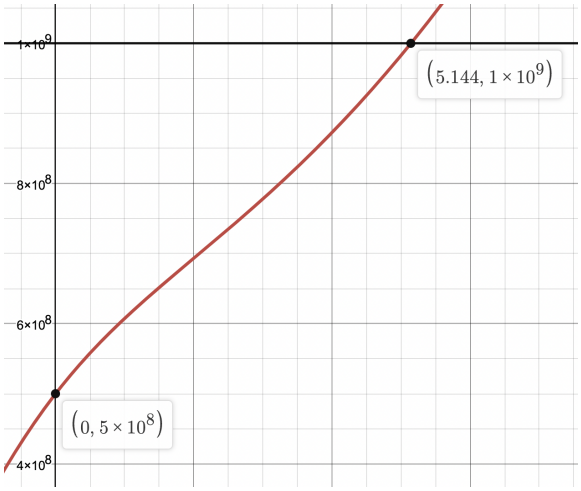
8.2 Inflation Model

Staking emissions act as a self-regulating mechanism to secure the Ojo Network. Validators and delegates will accrue a basis of 7-14% OJO inflation depending on the staking ratio. There will also be a supplemental reward strictly given out based on how accurate a validator supplies pricing info. This latter inflation will be halved each year, until the total supply hits 1B OJO; at this point, no additional tokens will be minted. When the supply cap is hit, there should be enough customers paying for jobs that validators are able to continue running the network profitably.

Our inflation model becomes:

$$P\left(1+\left(s\frac{1}{2}x\right)+g\right)^{x}$$

Where:
P - starting token supply
s - additional reward rate for validators
g - PoS consensus rewards



P = 500,000,000
s = 0.15
g = 0.14

We end up hitting 1B in ~5 years. There are some limitations to **g**, such that we don't want to become deflationary after an initial large gain.