CHARLI3

Cardano’s Decentralized Oracle

Abstract

Blockchain is eating the world. Smart contracts are replacing traditional agreements that require manual functions. However, blockchains are unable to access data from analog systems. Oracles were developed to serve as the abstraction layer between the two systems. Commercially, oracles have provided this service. However, their centralization presents a single point of failure. Decentralized oracle networks are poised as the precise mechanism needed for connectivity to the outside world.

In this paper, we introduce CHARLI3—a decentralized oracle for the Cardano network. We demonstrate how CHARLI3's on-chain smart contracts will connect externally to the world, and how the software will drive the nodes on CHARLI3's network.

We anticipate a rapidly expanding role for oracle networks. Hence, our strategy is to establish a decentralized network of oracles maintained by a council constituting representatives from participating nodes. This network will support any future oracle functions implemented by the council. In summary, CHARLI3 is a powerful intermediary using smart contracts to interface with off-chain data in an efficient and decentralized manner.

Introduction

Finance is dependent on the integrity of the information that allows for informed decisions regarding the market. Traditional finance has data provided by a few organizations, while the world of **De**centralized **Fi**nance (DeFi) has data feeds in a matched decentralized setting. The simplest form of a data feed for DeFi is price information, which can be obtained from multiple independent primary sources. Existing products in DeFi can build their own data feeds or oracles, but due to High-Availability (HA) requirements, many products utilize third-party oracles as a fail-safe. However, these non-HA oracles are not immune to external attacks with false information. The creation of a decentralized—yet trustless—and completely insured system solves one of the largest problems in DeFi.

Specific fears include attacks associated with manipulation of price leading to market exploits. One example includes the use of flash loans to alter the price of one liquidity pair on a decentralized exchange that was weighted heavily for price feeds. This attack exploits the use of inaccurate information to affect market decisions. Being able to avoid market manipulation through both trusted and novel methodologies is the cornerstone of CHARLI3's creation.

Decentralized Oracle Network

CHARLI3 is an open-source decentralized oracle to the Cardano Network. CHARLI3 is the platform that provides and verifies data—initially focused on blockchain economic values—for blockchain applications. CHARLI3 is a firm believer in decentralization and open, safe, and efficient access to accurate information. The contracts and updates will be open to the public. CHARLI3 will utilize blockchain-based rewards for node operators verifying data.

Other services exist on the Ethereum network and report being chain-agnostic. One concern is that cross-platform accessibility and prioritization of parachain applications is likely secondary to Ethereum-based applications. Beyond this, Ethereum has notable issues with scaling and transaction expenses. All three of these issues are solved by having a Cardano-native oracle service to capture the ADA-based application market. ADA is also known to have superior metadata for identity verification.

With the rapid growth of decentralized identity, ADA-based applications are at the forefront of solving these issues. Our discussions with these projects confirm that they will prefer a Cardano-native oracle service.

Oracle Security

Beyond the above applications and benefits of CHARLI3, the initial focus will be on providing data for DeFi applications that have had tremendous success on the Ethereum network but stagnated in 2021 due to high transaction fees and lack of scalability. DeFi platforms such as Compound, Yearn.Finance, and AAVE have been attacked via flash loans and price changes allowing for market manipulation. While redundant oracle services are utilized to prevent this in Ethereum, these are not always attack-proof; it only requires one security data breach for DeFi protocols to lose community trust.

Cardano-based DeFi protocols mimicking these existing applications will utilize CHARLI3 to ensure off-chain oracle services have built-in redundancy and cross-verification. CHARLI3 does this by holding the data providers and node operators responsible with staked tokens. Staked tokens will be removed from inaccurate operators and transferred to accurate—redundant external **and** internal consensus—operators. This will allow CHARLI3 to function as an independently-insured oracle as well as an *oracle aggregator*. If node operators are inaccurate, their node reputation will decrease over time, thereby decreasing the amount of nodes able to be staked in addition to token penalties.

Traditional finance will also be a market for CHARLI3 after its use case is established on blockchain applications. This transition is further aided by the growing number of traditional financial institutions, hedge funds, and centralized financial authorities utilizing digital assets as a store of value. These funds will all require insured and accurate data sources.

Network Consensus

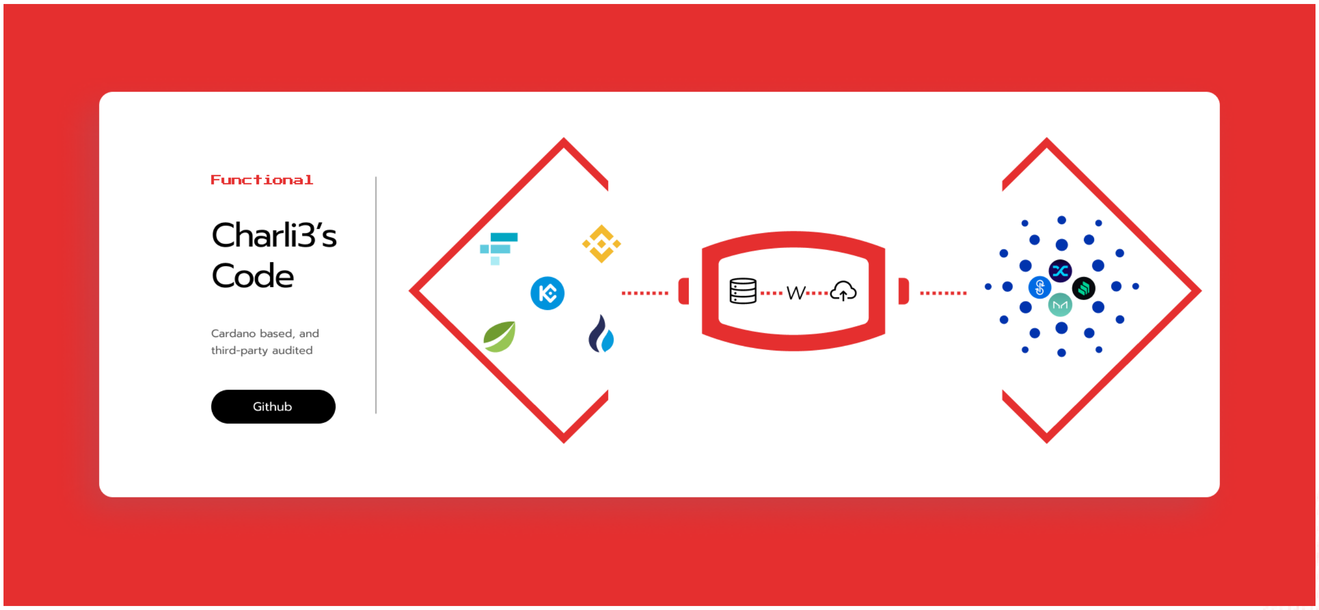
Node operators will stake tokens to allow access to a data request. Larger requests/stakes will be provided to long-standing, reputable node operators. After establishing consensus and covering for insurance, staked nodes are required to complete data retrieval and verification. Only upon completion of these tasks will the reward tokens be paid to the nodes.

Data Sources

The data sources for the CHARLI3 platform will include primary sources weighted over secondary sources and other oracle providers. Primary sources will include decentralized and centralized exchanges (reputation of CEX determined by the CHARLI3 community to avoid false-volume transaction entities), and well-established on-chain tools. Primary/secondary sources are provided rewards for API connection to nodes.

All data sources are evaluated across nodes of all sources and weighted according to each node's stakes—higher stakes will already be associated with a higher existing reputation. Secondary sources will also include other oracle providers allowing for CHARLI3 to act as an oracle aggregator. This will include a fail-safe, whereby node operators not associated with a given request ticket are externally responsible for vetoing the finding, allowing for any response that is associated with a 51% attack or data manipulation to be halted by third-parties that exist in the ecosystem. This allows for multiple internal (alternative node operators) and external (alternative oracles aggregated) fail-safe mechanisms, which are revolutionary in the oracle architecture space.

Finally, CHARLI3 will store data after validation and report it via our partnered reverse oracle service(s). These published data will be accessible for token holders as a token subscription service.



Token Utility Model

Beyond the incentives of the token as a reward, it will also act as an operator-based DAO for data consensus and community changes. Larger stakes are associated with ELO-based reputations and aid in consensus as described above, as well as future platform governance in a decentralized fashion. In the ELO system, gamified reputation is not measured in absolute terms, but is inferred from wins, losses, and draws against other participants. Operator ratings will depend on the ratings of their opponents and the results scored relative to their own. Using the ELO system ensures fairness and accountability. This allows for the integrity of the platform to be maintained long term.

Architectural Overview

On-Chain Framework

CHARLI3's smart contract interaction with client requests is an on-chain contract, termed CHARLI3-SC. CHARLI3-SC's internal architecture comprises 3 sub-contracts: (1) aggregation contract, (2) order-matching contract, and (3) reputation contract. The aggregation contract gathers responses from external data providers and computes the final results of the CHARLI3 query. The order-matching contract organizes the requested service agreements, indexes the parameters requested, and gathers the bids from external data providers. The reputation contract monitors the performance of the external data providers. These three components can each be tailored to suit the users' needs. Hence, the on-chain process consists of the following steps:

1. Selecting an oracle,
2. reporting data, and
3. aggregation results.

Oracle Selection

A client seeking oracle services specifies parameters which compose the service agreement proposal. This proposal will need to include parameters of the query and the quantity of oracles requested by the client. Furthermore, the client needs to specify the reputation level and aggregation smart contracts to be used for the duration of the agreement.

Long Term Strategy

CHARLI3's long term strategy is built on three pillars:

1. Confidentiality of oracle data
2. dynamic infrastructural changes, and
3. computation off-chain.

Oracle confidentiality

Decentralized oracle networks were designed to achieve a high degree of protection against poor performing oracles. The oracle network ideally seeks the optimally-selected truth response with consideration of Byzantine faults. In this instance, trusted hardware is the recommended approach to secure the CHARLI3 network. However, achieving confidentiality in a distributed oracle network is a difficult task by nature of being on a public blockchain. Here again, trusted hardware provides strong confidentiality.

Dynamic infrastructure

The current state of oracles is plagued with the problem that external data sources do not perform digital signatures on their data exports. Without a tamper-proof digital signature, there exists the need for a layer of trust requiring oracles to act in good faith. The team at CHARLI3 strongly believes that a network capable of dynamic infrastructural changes is a promising approach to oracle security.

Off-chain computation

In certain scenarios, oracles are required to perform functions in addition to data transmission. For instance, oracles may be requested to verify credentials or log into databases to retrieve information. CHARLI3 was built with a language that empowers clients to request specific off-chain data processing. Our long term strategy aims to nurture the environment where oracles play vital roles as off-chain computation resources used by the majority of smart contracts. We aim to achieve this vision by cultivating a model of privatized off-chain computation with a generalized availability, feeding results to the smart contracts. Hence, we believe that by incorporating a plan of high confidentiality, infrastructure dynamism, and off-chain computation capabilities, CHARLI3 will reduce costs while increasing data sensitivity and efficiency.

Economics

A strong and stable network is vital to CHARLI3's security as a decentralized entity. It is imperative that nodes act cohesively and in accordance with their mandate to CHARLI3. In this section, we will present the strategies to help enforce such behavior with the deployment of economic incentives or punitive measures if found to be acting in bad faith.

Staking

As a commonly-used method in blockchain technology today, staking in CHARLI3 involves participation through the nodal mechanism that locks tokens as surrogates of participation via delegation of network ownership. Where CHARLI3's staking protocol differs is in the mechanism of achieving consensus agreement. In traditional permissionless blockchains, staking consensus agreement is achieved if the block data is agreed upon by the majority of nodes. With CHARLI3, participating network nodes will need to achieve consensus agreement on the data external to the blockchain. Using an external data-based interactive protocol, we have deployed a staking mechanism for CHARLI3 validator nodes.

Conclusion

In conclusion, we introduced CHARLI3—the first decentralized oracle network for the Cardano network. While oracles on other chains are either incapable of, or need significant upgrades to allow interacting with assets outside of the blockchain, CHARLI3 offers this capability right from the start. After describing the traditional approach to oracles, we defined CHARLI3's multi-level decentralization mechanism and security measures for the oracle and the network. We illustrated the abstraction of data from the resources external to the blockchain and we demonstrated the utility of the CHARLI3 token in this function. We presented the architecture of both on- and off-chain components of CHARLI3's architectural design, and we presented the long term strategy for how CHARLI3 will harness its technological advancements to solve the oracle problem today. Finally, we offered CHARLI3's approach to economics and its tokenomics in the Cardano ecosystem.