Clarity Protocol - Whitepaper

Version: 1.0
Authors: Paul Nesteruk, Armin Ranjbar, Marina Khaustova

Abstract

Clarity Protocol is a decentralized tool for the Web 3.0 economy. It allows dApps and their users to control what types of participants are welcome in their communities. This paper introduces the protocol, including design, token economics, and future roadmap.

Summary

Clarity Protocol aims to reduce risk for users of decentralized applications by providing analysis of on-chain behavior based on wallet addresses. Use cases include anti-money laundering [AML] checks, the identification of black hat hackers, as well as information about the risk levels of the decentralized applications themselves.

Such a service is already available to centralized institutions via analytics firms and other such providers, but has not been to the applications generating the source data. Clarity Protocol is a decentralized marketplace that allows providers to send risk-related blockchain data directly to consumer smart contract-based applications without the latter requiring centralization of data around any one service provider.

Contents

Overview

Motivation

The decentralized economy keeps growing, with billions of USD in value being settled across an increasing number of Level 1 and Level 2 chains on a daily basis. One of the key strengths is the open, permissionless, and borderless nature of these systems, but there are instances where participants' actions have damaged or hurt the on-chain community.

Most individuals and businesses from the financial services space are familiar with the concepts of Anti-Money Laundering [AML], but public blockchains provide a much richer source of data allowing us to analyze and understand behaviors at a deeper level than with the traditional economy. Has the address been associated with a hack or an exploit? Has the entity engaged with other protocols in the ecosystem? Was this engagement of a nature that the community using Clarity Protocol wants to encourage, eg. Does it participate in governance procedures or use tokens for core utilities within the protocol - such as staking?

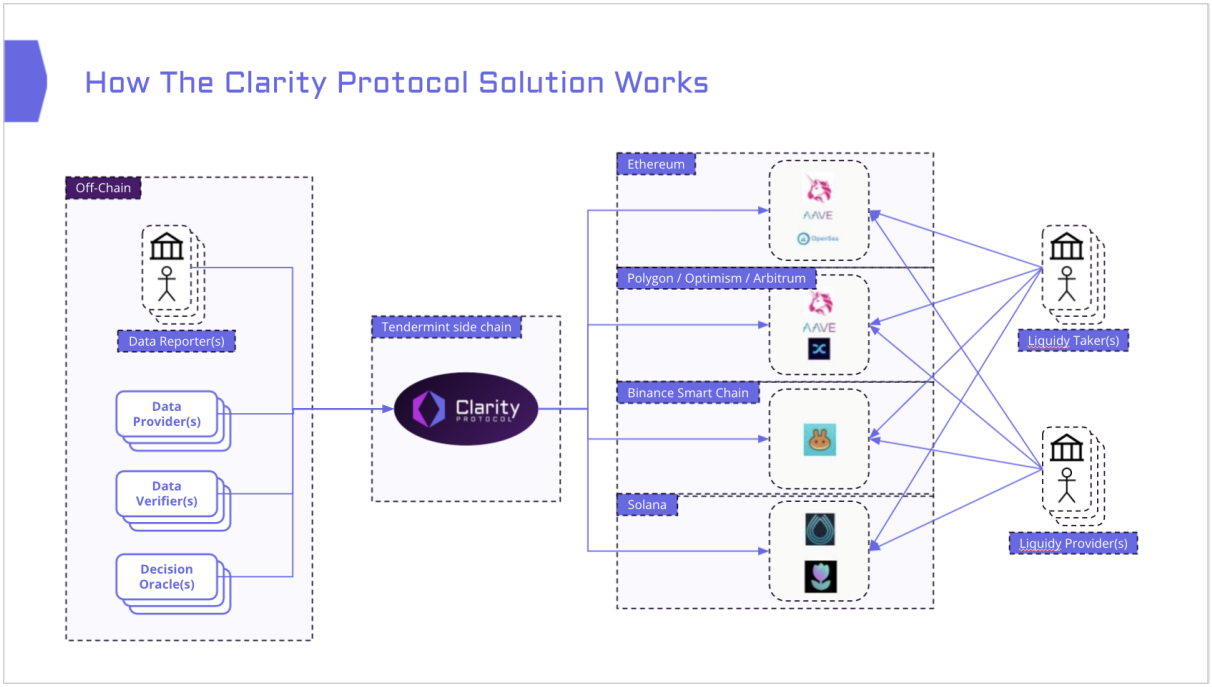
All of this data currently exists but is held off-chain in proprietary databases and is reported via their APIs, Twitter, or other online channels. Clarity Protocol will source this information by providing a market framework and required incentives to bring this data back to the on-chain economy, including the decentralized applications [dApps] that originally generated it and their governing decentralized autonomous organizations [DAOs] or communities.

Clarity Protocol addresses this problem by bringing blockchain analytics data to decentralized applications, allowing communities to define and enforce appropriate behaviors from participants without having to rely on centralized parties to act as gatekeepers.

This solution will not only allow communities to reduce the risk of their on-chain protocols, it will also enable them to grow usage and volumes by attracting institutional capital from entities that couldn't otherwise participate without having AML controls in place first.

Design

Overview



Clarity Data

To support multiple blockchain networks, data is stored in an independent blockchain based on the Tendermint consensus engine [Clarity Chain], which uses a Delegated Proof of Stake [DPoS] consensus algorithm to govern and maintain the chain.

The actual data is stored in logical RocksDB powered database tables and can be queried by multiple parties as needed; data can also be encrypted on chain to protect the privacy of data providers.

Validators

Validators are required to make updates to the Clarity Chain to protect the integrity of the network. For this, they earn fees in CLRTY tokens. DPoS allows token holders to delegate their tokens to any node validators, and then the Top 20 Validators are allowed onto the network.

Number of Validators

The protocol sets the number of active Validators. This will start at 20 but is expected to change over time if approved by protocol governance.

Smart Contract Bridge

DApps can call Clarity from their native chain (e.g. Ethereum) by using a bridge contract and paying CLRTY tokens. Each network supported will have its bridge connecting the dApp to Clarity data.

Key Features

Decentralized

Clarity Protocol is decentralized because it wants to serve a decentralized economy and to allow dApps to remain decentralized; being a decentralized DAO entity increases transparency and makes it easier for dApps to accept and integrate.

Neutral Marketplace

Having a decentralized marketplace is the only way to have different data providers competing under the same roof, which will add value to the ecosystem.

Data providers themselves will also monetize their data in a micro-transaction economy and predictable cash flow.

DApps can integrate with the protocol without falling into a vendor lock with each individual data provider.

Incentive System

All parties need to utilize CLRTY tokens; data providers will stake in and receive rewards, dApps will buy tokens to pay for data queries and different parties running nodes, and oracles will help with scalability of the network.

Crowd-Sourced Data

While crowdsourced data might not have significant accuracy, at least compared to corporate-generated data- it is a great tool to easily allow casual market participants to monetize their on-chain insights.

Verification

Crowdsourced information from reporters is considered lower quality than that of providers. The verification process takes into account the number of similar reports and confirmations from certified providers in assessing the trust level assigned to crowdsourced information.

In the case of split data, eg. reports of a hack as both black hat and white hat, a Decision Oracle will be required to provide a consensus view of the data.

Disputes

Ethics around certain on-chain actions such as exploits are complex with communities often coming to very different conclusions about the actors and their actions. Furthermore, it is possible for macro conditions to change, such as the legal status of activity in a given jurisdiction, or simply for providers to make mistakes when providing analytics.

Because of this, Clarity must have a “disputes” system which allows data within the protocol to be queried. Disputes can be raised by a participant who must stake CLRTY tokens which are held in escrow by the protocol until it is resolved by the Clarity data provider community.

If upheld, the tokens are returned to the raiser of the dispute, if rejected the tokens are burned, in both cases it will be minus a fee that is paid to the verifiers of the dispute.

Multichain

The aim of Clarity is not to create a new level one blockchain where people can create dApps, it is to serve the ecosystems on the existing set of smart contract enabled chains. Clarity is designed to be accessible through any blockchain platform where there is sufficient economic activity and demand from both the data provision and consumption sides.

Data Permissions

Providers can give data in three different classifications. These provide the opportunity to earn income from data while controlling how it can be accessed. This classification is applied when data is submitted to Clarity Chain and can be modified via edits.

Open

Accessible by all participants, either via a bridged consolidated query or direct query from Clarity Chain, anyone can access this data.

Restricted

Included in computational queries but not accessed directly from the data storage. This allows data to be monetized within the protocol without allowing everyone free access to download it in bulk.

Private

Accessible only by the owning data provider or parties they have given explicit access to. This can be used when there is data that can only be made to certain parties but requires extra setup and maintenance by the data provider.

Pricing

All fees payable within Clarity Protocol are distributed to the actors involved, no part of these charges is transferred to the protocol treasury. Data providers and decision oracles set the fees for their services which are then paid by any consumer that uses them.

Decision Oracle Queries

Data providers and decision oracles are free to set fees on the data they provide. This information is published to the data consumers who must then pay the fee to access the data.

If accessed via a decision oracle then that is responsible for both pricing and distribution of the fees to the contributing providers. Providers can exclude themselves from decision oracle queries if they do not agree with the charges.

Direct Access

If a consumer connects directly with a provider's oracle, then fees are set by that provider. As with decision oracles, this is defined in advance so the consumer always knows the cost of the query before executing it.

Governance

ClarityDAO

Clarity Protocol will be governed by the Clarity Decentralized Autonomous Organization [DAO]. Token holders will be able to submit Clarity Improvement Proposals [CIPs] which are then voted on by DAO members. CIPs that pass will be scheduled and implemented alongside other work in the roadmap.

Clarity Improvement Proposals [CIPs]

Clarity Improvement Proposals [CIPs] are a method for DAO members to propose, review, and vote on changes to Clarity Protocol. The mechanism is subject to change and is described in the documentation found on the Clarity website https://www.clarity-protocol.com.

Roles

Clarity Chain

Validators

Update and maintain the data held on-chain, earning rewards from fees.

Stakers

Token holders delegate their assets to validators in order to secure the chain and earn rewards.

Protocol

Data Provider

An expert data provider approved by protocol governance. They are required to stake tokens in order to guarantee a positive contribution to the network.

Data Consumer

DApp requires information on the wallets attempting to access it and whether they fit the risk profile as defined by its community.

Data Reporter

An everyday Web 3.0 user, a non-expert but with some insight into on-chain activity. A lower trust than data providers but a larger number available enabling a greater degree of decentralization

Decision Oracles

Converts datasets into actionable decisions and consolidates data to provide a single access point to multiple providers. In addition to collating information, they also interpret it where various sources have different data dictionaries and standards.

Use Cases

DeFi Exchange Reduces Risk

A decentralized exchange reduces the risk of its pools becoming tainted by integrating with Clarity:

- TokenSwap is a decentralized Automated Market Maker [AMM] that allows liquidity providers to earn fees from liquidity takers when they are converting one token to another.
- The TokenSwap community wants to use Clarity to exclude undesirable actors from training its asset pools:
    - TokenSwap DAO votes to exclude wallets associated with the darknet, illegal services, and those on the OFAC list.
- TokenSwap developers create liquidity pools that check all addresses with Clarity for these risks before they deposit funds to trade with the liquidity pools.

Institutionally Focused Lending

- ChainLend is a decentralized lending protocol that allows liquidity providers to earn fees from lenders borrowing assets via collateralized loans.
- ChainLend has been approached by a group of institutions that want to provide liquidity but require AML checks to be done against lenders to be compliant with their local laws.
- ChainLend development team sets up private pools using Clarity to check risk scores of potential lenders and excludes any deemed too high by the liquidity providing institutions.

Smart Contract Exploit

The Web 3.0 community uses Clarity Protocol to band together and prevent an attacker from liquidating stolen funds.

- BigIdeaDAO has just been hacked with the attacker withdrawing $100M in BID tokens.
- BigIdeaDAO realizes the attack has taken place and releases what they know via social media.
- The attack is now being analyzed in real-time with people posting analysis and reports to both social media and Clarity Protocol.
- The attacker attempts to use the decentralized HNW exchange to swap the BID tokens for ETH but is rejected because the smart contract queries Clarity and gets a match against hack, which the smart contract has been programmed to exclude.
- Other protocols follow suit and the attacker can not do anything with the assets, they return them to the DAO in exchange for a bug bounty.

High-End NFTs

Clarity allows a decentralized NFT marketplace to attract high-end users by checking all sellers wallets and buyers funds before allowing transactions to take place.

- Only transactions from buyers with acceptable risk levels are allowed.
- Seller is alerted and given final say in borderline cases.
- Sellers can liquidate and use CeFi exchanges to convert assets to fiat knowing that they can not be connected to high risk or illicit activities.

Monitise Analytics Data via the Decentralized Economy

Clarity allows centralized analytics firms to further monetize their data by selling to the decentralized economy that can not use its existing centralized API.

- BlockSearchTech has a large database of risk-related analytics which it sells to organizations via its API.
- They have used a decentralized oracle to make it accessible to dApps but it has not been successful because dApps don’t want to introduce a centralized single point of failure.
- BlockSearchTech sends data to Clarity Protocol and it gains income in the form of CLRTY tokens when it is utilized.
- Some data is set to restricted meaning it is protected from other data providers accessing it directly and using it in their own products.

Efficiently Distribute Data on Criminal Activity

A law enforcement agency distributes data on criminals to both dApps and data providers via Clarity.

- A regional law enforcement agency wants to distribute data on wallets linked to criminal activity as broadly as possible.
- They upload the data to Clarity with no privacy settings.
- Is now available for both dApps when they query and for other data providers to download and use by their other clients.

On-Chain Reputation

A decentralized community uses Clarity to ensure members share the same ethos and standards.

- ArtCollectorDAO is set up for buyers of art to support interesting artists.
- It airdrops NFTs to community and DAO members in order to create engagement and build community spirit.
- The ArtCollectorDAO dev team uses Clarity to check that DAO members are not quickly selling their NFTs for a short term profit which is against the ethos of the community.

Smart Contract Risk Ratings

Clarity become a decentralized source for info risks of various smart contracts.

- There are a lot of data points available for smart contracts such as results of audits, operational time, TVL, the status of the team, use of risk management tools, etc.
- Specialist data providers add this info to Clarity.
- Risk ratings are made available to end users either directly or via platforms such as dApp Stores, wallets and portfolios trackers.