Ocelloids Network Specification

The Zone Council, SO/DA

January 9, 2024

Abstract

This document presents the functional specification of the Ocelloids Network, a blockchain protocol designed to facilitate the secure and transparent leasing of software agents. It incorporates a continuous service attestation process to ensure the network's continuous and reliable operation.

Contents

1 Introduction

The Ocelloids Network is a collection of nodes governed by an onchain registry, ensuring vetted access and well-defined roles for providers and auditors.

Operating as a marketplace, the network enables consumers to lease software agents from providers, leveraging blockchain technology for automated leasing and settlement. Continuous Service Attestation, conducted by auditors, ensures the network's ongoing reliable operation.

2 Network

An Ocelloids network is a collection of nodes under a common trust zone with vetted access for participation.

The network is governed through an onchain registry, known as the Network Registry, containing participant information and their Network Roles.

Network participants have well-known identities tied to specific organizations, geolocations, and publicly accessible endpoints.

2.1 Network Registry

The network registry defines a trust zone characterized by designated sovereign and administrative accounts. Each of these accounts is endowed with privileges related to the onboarding and offboarding processes of service providers and auditors. These procedures play a critical role as they establish connections with entities subject to liabilities and potentially involve the establishment of legally binding contractual agreements.

Each participant of the network has an associated Party Record, which includes essential information for locating service providers and verifying the authenticity of digital signatures.

Table 1: Party Record

Property	Description
Accounts	Operator and Treasurer accounts.
Contact Details	E-mail, Organization Name, etc.
Endpoints	URLs[1] of the public endpoints.
Geolocation	Geographic point location[2].
Role	The node role (section 2.2).

2.2 Network Roles

The network encompasses two node roles:

Provider Node
: Negotiates service agreements, hosts agents in accordance with active leases and receives leasing fees.

Auditor Node
: Verifies the execution of the agents involved in active leases and provides attestations to authorize the payment of leasing fees.

3 Service Leasing

The service leasing process involves consumers requesting service offers, depositing funds onto the blockchain for agent execution, undergoing continuous service level attestations, managing periodic payment claims, and facilitating automatic lease renewals.

3.1 Service Agreement

The service agreement process mandates that the consumer commits a deposit before the provider provisions the agent. The high-level steps are as follows:

1. *Request Quote.* The consumer initiates the leasing process by submitting a quote request to the provider, specifying the desired program content identifier for execution.

2. *Service Offer.* The provider responds with a service offer, providing details such as the program content identifier to be executed, the leasing period duration in number of blocks, leasing fee, and minimum deposit required.

3. *Place Deposit.* The consumer submits a deposit to the blockchain, specifying the offer and the transfer amount. The funds for one leasing period are locked, with any remaining funds available for withdrawal by the consumer at any time.

4. *Confirm Deposit.* The blockchain issues a deposit receipt for the offer to the consumer, confirming the deposit. The consumer then sends this receipt to the provider.

5. *Provision Agent.* The provider verifies the deposit and provisions the agent based on the accepted offer.

6. *Confirm Lease.* The provider submits the deposit receipt to the blockchain to formalize the lease, receiving a lease receipt in response.

7. *Activate Lease.* The provider acknowledges the lease activation to the consumer upon receiving the lease receipt.

3.2 Service Attestation

The service attestation process[1] involves auditors continuously verifying the accurate operation and fulfillment of the agents hosted by a providers under the leasing duration. The attestation process operates within the timeframe of a leasing period. During the period, the provider commits a verifiable proof of the processing of each block. Since the blocks could be processed out of order, the provider maintains a local verifiable key-value map independent of the insertion order, such as a sparse Merkle tree[3]. The commitment to the map adds a pair (k, v), where $k = B_{hash}$ and $v = \text{digest}(Log_{out})$. The top hash of the verifiable map must be anchored in the blockchain at the end of the period. The attestation process for each period works as follows:

1. *Request Service Proofs*: The auditor requests service proofs for a random sample[2] of block hashes within the most recent anchored period. $B_{samp} = \{B^0_{hash}, \ldots, B^n_{hash}\}$.

2. *Present Service Proofs*: The provider presents the requested inclusion proofs for the given block hashes. $P_{samp} = \{M_{proof}(x) : x \in B_{samp}\}$.

3. *Verify Service Proofs*: The auditor verifies the inclusion proofs:

   (a) Confirms the inclusion of the proof using the anchored top hash for the period.

   (b) Independently processes the selected blocks to verify that the resulting values align with the given values from the provider.

[1] This process assumes blocks as data sources, necessitating a generalization of the process to support attestations from off-chain data sources.

[2] A simple approach would be to use Yamane's method ($n = \frac{N}{1+Ne^2}$) for N blocks in the period, where $n \approx 400$ for a 1-month period.

4. *Record Attestation*: The auditor submits a signed attestation of the verified period. The attestation authorizes[3] the payment of leasing fees[4] by the provider.

This continuous attestation process ensures the maintenance of verified operational records, serving as a prerequisite for capturing payments during lease periods.

[3]Variations could require signatures from multiple auditors.

[4]The authorized payment should be captured by the provider and could entail the deducation of a managment fee accrued to the auditor/s.

Glossary

agent
: A program instance running on a provider. 3–5, 7

auditor
: Node responsible for verifying the execution of agents involved in active leases and providing attestations to authorize the payment of leasing fees.. 3–6

consumer
: Party that leases the hosting of an agent on a provider within the network. 3–5

program
: Package containing executable bytecode or source code published through vetted catalogues. 7

program content identifier
: Content-addressable location where the program package can be retrieved; e.g., an IPFS CID. 4

provider
: Node responsible for negotiating service agreements, hosting agents according to active leases, and receiving leasing fees.. 3–7

References

[1] Tim Berners-Lee, Roy T. Fielding, and Larry M Masinter. Uniform Resource Identifier (URI): Generic Syntax. RFC 3986, January 2005. URL https://www.rfc-editor.org/info/rfc3986.

[2] Standard representation of geographic point location by coordinates. ISO 6709:2022, September 2022. URL https://www.iso.org/standard/75147.html.

[3] Rasmus Dahlberg, Tobias Pulls, and Roel Peeters. Efficient sparse merkle trees: Caching strategies and secure (non-)membership proofs. Cryptology ePrint Archive, Paper 2016/683, 2016. URL https://eprint.iacr.org/2016/683. https://eprint.iacr.org/2016/683.