Progetto Tecnologie Internet

Smart Contract Astral Objects

Leonardo Fiore

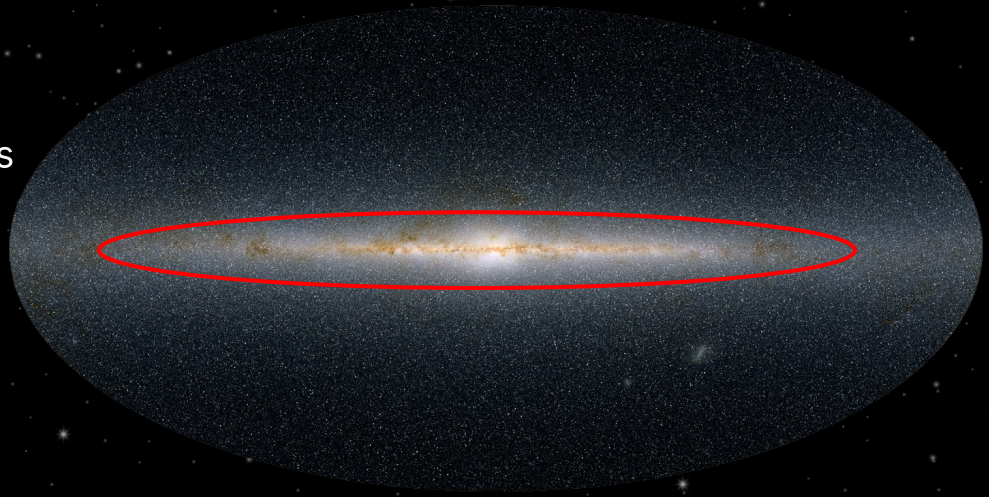
Computer Engineering Student – University of Parma
leonardo.fiore@studenti.unipr.it
Matricola 322767

Table of contents

01
Abstract

Let’s introduce the Zone of Avoidance

The **Zone of Avoidance**, or **Zone of Galactic Obscuration**, is an area in the galactic plane where dust, gas, and stars obstruct the view and sensors of the visible spectrum.



Circled in red, the Zone of Avoidance.

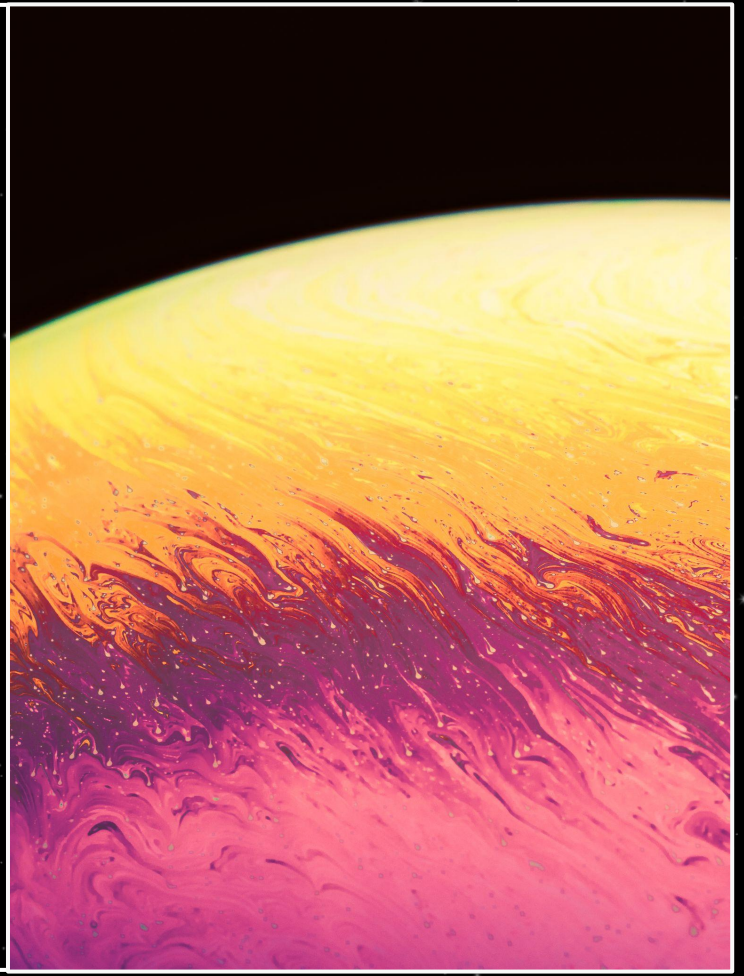
Insufficient resources

Normally, **every** point of the galaxy must be **physically** studied, in order to discover new objects, because there are **very few** operative telescopes and astronomical sensors, compared to the vastity of the galaxy.
At least relatively to the theoretical number of **potential computers.**




A smart contract to solve the problem

The system focuses on **overcoming** this obscuration, by **distributing analyses** of **incomplete** or **unprocessed** data gathered by astronomical sensor, **publicly** among machines, which will have the ability to choose and promote their **own perspective** and classification of celestial areas or bodies.
With such solution, entire space areas can be mapped with the **efficiency** for the astronomical sensor, physically studying only **sufficiently safe** space anomalies.



The two fundamental actors

Master node

Our *virtual* telescope and array of sensor, that **harvest astral datas** in the outer space and inject the smart contract with them.
Then it wait a proposal voted positively by the majority of *peers,* and if it turns empirically true, that proposal is saved, **certifing** a new discovery.

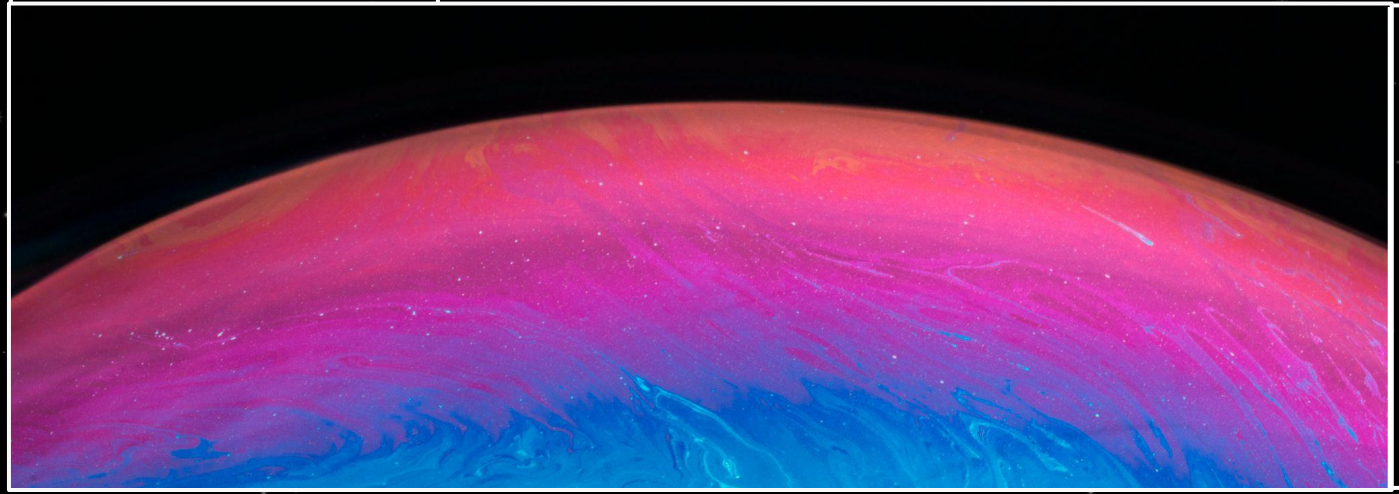
Peer node

It is **whoever connects** itself to the smart contract, able to do **computations** to whatever is the meaning of the astral data extracted.

02

In-depth view

Unfortunately, an astrophysics lesson.



Premise

Being a **one-man-army** project, it's very important to clarify that most theoretic concepts here are **overly simplified**, even **invented** by me, just for the sake of the project.
Nevertheless I will commit myself to highlight those **simplifications** and **fantasies**, as well as provide **references**.

Use cases

Here are given five[1] examples of possible astral object: ***Rocky planet, Gas giant, Star, Supernova*** and ***Black hole***, each with their unique values[2] of ***mass, composition, temperature, difference of spectrum*** and ***microlensing magnitude.***

- The *mass* is calculated by the **Transit method**[1][1], that occurs when the **light** of a space area **dimmer** at constant intervals.
  Here the calculations are made by taking the **luminosity** of our star Sol
  $\mathbf{W_{Sol} = 3.827 \times 10^{26}\ W \approx 4.0 \times 10^{26}\ W = W^{i}_{Sol}}$,
  passed by the Earth
  $\mathbf{W^{f}_{Sol} = 4.0 \times 10^{25}\ W}$.
  So the equation will be
  $\mathbf{W^{i}_{Sol} - W^{f}_{Sol} = 3.6 \times 10^{26}\ W = \Delta W_{Sol\text{-}Earth}}$.
  Now with this simple proportion
  $\mathbf{\Delta W_{Sol\text{-}Earth} : mass_{Earth} = \Delta W_{y} : mass_{x}}$,
  with ΔW_y given by the astral data and $mass_x$ variable, we can find the mass of **any** object.

- The *difference of spectrum* is a value gathered by **Spectroscopic**[2] sensors that will tell us if the body is a **star** or not, if it **fits** in that range[4] (typically from ultraviolet 10^{-8} to radio 10^{3}).

- The *microlensing magnitude* is calculated using the **Gravitational microlensing method**[3], which sates that an object **passing** in front of another, will **bend** the fabric of space-time by **orders of magnitudes** relatively at it's gravitational pull.
  Based on that, our sensors will gather that magnitude[5] of a locked point, after and before the passing of the space anomaly (M_i ; M_f), guessing which **exotic body** it is.

- The *composition* is calculated by analyzing three[6] different radio wavelength measurement taken by the sensor, each corresponding with Hydrogen *H* = 21 cm[4.1], Helium *He*[4.2] = 2.86 cm and Silicium *Si* = 100 cm[2].

- The *temperature* is calculated by the **Wien's displacement law**[5], where harvested peaks of **infrared** wavelength can tell us the temperature of a body.

  $\lambda_{peak} = b / T$, with $b = 2.898 \times 10^{-3}$ **m / K** as **Wien constant**.

Rocky planet

Mass

$\approx 0.1 \cdot mass_{Earth} \leq mass_x \leq 2 \cdot massEarth$

Composition

Must have *Si*; can have *H* and *He*.

Temperature

$\approx 123.15\,K \leq T_x \leq 476.85\,K$

Difference of spectrum

A rocky planet doesn't have it.

Magnitude microlensing

A rocky planet doesn't have it.

Gas Giant

Mass

$\approx 2 \cdot mass_{Earth} < mass_x \leq 0.1 \cdot mass_{Sol}$

Composition

Must not have *Si*;
H and *He* are **strongly** recomended.

Temperature

$\approx 123.15\,K \leq T_x \leq 2500\,K$

Difference of spectrum

A gas giant doesn't have it.

Magnitude microlensing

A gas giant doesn't have it.

Star

Mass

$\approx 0.1 \cdot mass_{Sol} < mass_x \leq 10 \cdot mass_{Sol}$

Composition

Must not have *Si*;
H and *He* are **strongly** recomended.

Temperature

$\approx 2500\,K < T_x \leq 50000\,K$

Difference of spectrum

Border values similar to 10^{-8} and 10^{3}.

Magnitude microlensing

A star doesn't have it.

Supernova

Mass

$\approx 10 \cdot mass_{Sol} < mass_x \leq 50 \cdot mass_{Sol}$

Composition

Absence of *H, He* and *Si* **strongly** recomended.

Temperature

$\approx T_x > 50000\,K$

Difference of spectrum

A supernova doesn't have it.

Magnitude microlensing

Difference must be slightly less.

Black Hole

Mass

$\approx mass_x > 50 \cdot mass_{Sol}$

Composition

Absence of *H, He* and *Si* **strongly** recomended.

Temperature

$\approx 2500\,K < T_x \leq 50000\,K$

Difference of spectrum

Border values similar to 10^{-8} and 10^{3}.

Magnitude microlensing

A star doesn't have it.

03
Code Analysis

Premise

The system is **fully working**, but, for now, only by **automated tests** runned by **JavaScript interfaces** to the smart contract, therefore there's **no human interaction** in the process to choose some data to analyze rather than another, **nor** the generated astral datas have some **physical meaning**, because it's all **pseudo-random generated**.

Solidity contract

All informations are stored in **structs** like these...

```
struct Proposal {
    address proposer;
    uint dataID;
    astralObject object;
    int voteCount;
    bool isAccepted;
    mapping(address => bool) voters;
}
```

```
struct astralData{
    string id;
    int[] position;
    int Dw;
    int[] radioComposition;
    int lambda;
    int[] Ds;
    int[] magnitude;
}
```

```
struct astralObject{
    string id;
    int[] position;
    string tag;
    int T;
    bool[] composition;
    int mass;
}
```

...Through

pretty self-explanatory **functions** like these:

```
function addAstralData( ... ) public onlyAuthorized{
    ...
}
```

```
function addProposal( ... ) public{
    ...
}
```

```
function vote( ... ) public{
    ...
}
```

```
function markProposalAsAccepted( ... ) public onlyAuthorized{
    ...
}
```

Deploying contract

The called constructor will set the **deployer address** as the authorized account or **master node.**
This means that functions and parts of the algorithm that have the ***onlyAuthorized*** keyword, can be *de facto* performed by only our master node.

```
constructor() {
    authorizedAccounts[msg.sender] = true;
    masterNode = msg.sender;
}
```

```
modifier onlyAuthorized() {
    require(authorizedAccounts[msg.sender], "Only authorized accounts can perform this action");
    _;
}
```

JavaScript test

Master node data creation

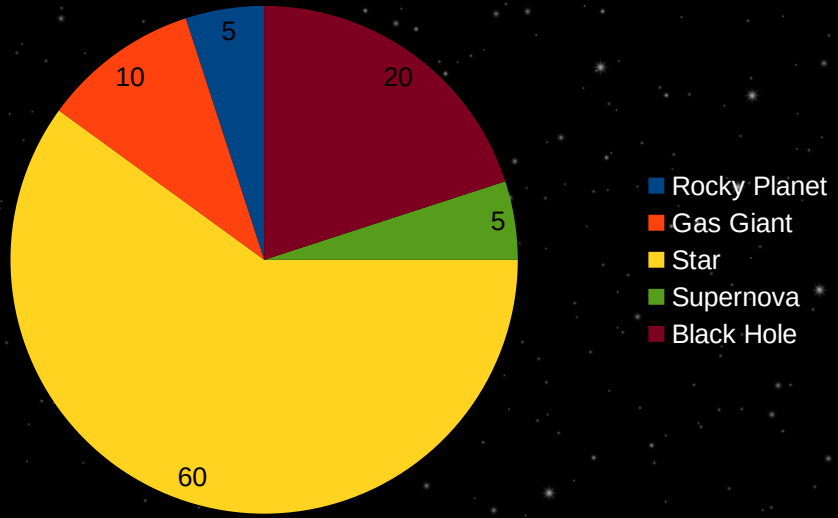
Starting with ***masterNode.js***, the algorithm will *randomly* create **astral data** and inject them to smart contract, ready to be further analyzed.

```
async function createAstralData() {
  //...
}
```




Here, a dice will *roll* in order to simulate the **abundance** of certain types of astral object and the **scarcity** of others

```
var dice = getRandomNumber(0, 100);
```



Taking as example values of *lambda* for *rockyPlanet,*

```
var lambda = getRandomBigNumber(297231, 3361754)
```

These values are just the one that, **replaced** into the *Wien displacement law*, returns **T = [123.15 K ; 473.85 K]** (the **temperature limit** for *Rocky planets)*, **enlarged** both ways by a 30%, and then **multiplied** by 10^{10}.

- The *multiplication* is made to ensure **compatibility** with **Solidity** *BigNumber*, because the language can't directly support decimal numbers, without some variables manipulation;
- The *enlargement* is introduced to achieve some sort of randomness, similar to the *dice roll*;
- Similar concept are made to the other critical variables, as well for other type of astral bodies,

Finally, those generated values are **injected** into the smart contract:

```
const accounts = await web3.eth.getAccounts();
const masterNode = accounts[0];
await contract.methods.addAstralData(id, position, Dw, radioComposition, lambda | 0, Ds, magnitude).send({ from: masterNode, gas: gasLimit });
```

First **two** lines, **fetch** the address of the *masterNode*/deployer, who will be the **first** [0] in the array of the accounts.
Then, an **asynchronous call** for the ***addAstralData()*** contract method will **create** a new variable within the smart contract, sent by the only authorized account.

Peer node analysis and evaluation

About our *peerNode* algorithm, we have two separate **.js* files:

nodeLogic.js for the analysis of *astralData* and dispatching of a *proposal*.
A new proposal is prior created by *processing* and *analyzing* data, relatively at some ***reference values.***

```
function setReferenceValues(){
  refDw = BigNumber( getRandomBigNumber(BigNumber('3.3e26'), BigNumber('3.9e26')) );
  refT = +getRandomNumber(0, 0.15).toFixed(4);
  refComposition = [
    +getRandomNumber(0, 0.15).toFixed(4),
    +getRandomNumber(0, 0.15).toFixed(4),
    +getRandomNumber(0, 0.15).toFixed(4),
  ];
  refDspect = +getRandomNumber(0, 0.15).toFixed(4);
  refDmagnitude = Math.floor(getRandomNumber(2, 5));
  refTreshold = +getRandomNumber(0, 100).toFixed(2);
}
```

These values are unique for each node, as well as (in theory) tuneable.

- *refDw* is the value of $\Delta W_{Sol-Earth}$ stated by the *Transit method*. As previously mentioned, 3.6×10^{26} is the **median** values, but each node can pick a number between **3.3×10^{26}** and **3.9×10^{26}**;
- *refT* is the **percentage** limit that can be tolerable for each astral body range of **temperature**;
- *refComposition* is the **percentage** limit that can be tolerable for each astral body range of element **radio** wavelength;
- *refDspect* is the **percentage** limit that can be tolerable for each astral body range of **spectrum**;
- *refDmagnitude* set the **reference** for difference of order of **magnitude**;
- *refTreshold* set the minimum *quality* a simulation must have to be dispatched as a proposal.

Subsequently, data are extracted at regular intervals…

```
async function extractAstralDatas(){
  //...
}
```

...then are *processed*…

```
async function processAstralDatas(extractAstralDatas){
  //...
}
```

…in order to further *analyze* the *critical values.*

```
async function analysisAstralDatas(processedData){
  //...
}
```

Following the previous example of *lambda,* it's important to note that the value is correctly divided by 10^{10}, ensuring the correct computation of the law.

```
T = (wienConstant.dividedBy(BigNumber(extractedAstralDatas[c].lambda).dividedBy('10e10')));
```

Again, I point out that values are manipulated in order to do calculations and be *Solidity-compatible*.

Inside *analysisAstralData()* function, checks about *critical values* are made, relatively at *reference values* and the standard *critical unique values* for each type of astral body, that will update the corresponding **score**.

Here are stored the *scores* of each guess…

```
objectGuess = [0, 0, 0, 0, 0];
```

...updated by checks like this…

```
if(processedData.mass.isGreaterThan(rockyPlanet.rMass[0]) && processedData.mass.isLessThanOrEqualTo(rockyPlanet.rMass[1])){
  objectGuess[0] += 40;
  objectGuess[1] -= 10;
  objectGuess[2] -= 20;
  objectGuess[3] -= 30;
  objectGuess[4] -= 40;
}
```

Positive for *mass* in range of *rockyPlanet*

Then, if a score is equal or greater than the *refTreshold*, a new proposal is assembled and dispatched, with the data of the guessed *astralObject.*

About ***nodeEvaluationLogic.js***, the algorithm is still pretty the same: the node **extract** the proposal from the pool, then proceed to make the same **computations** of *nodeLogic.js,* and if the result is tolerable, that proposal is **voted** positively, else negatively.

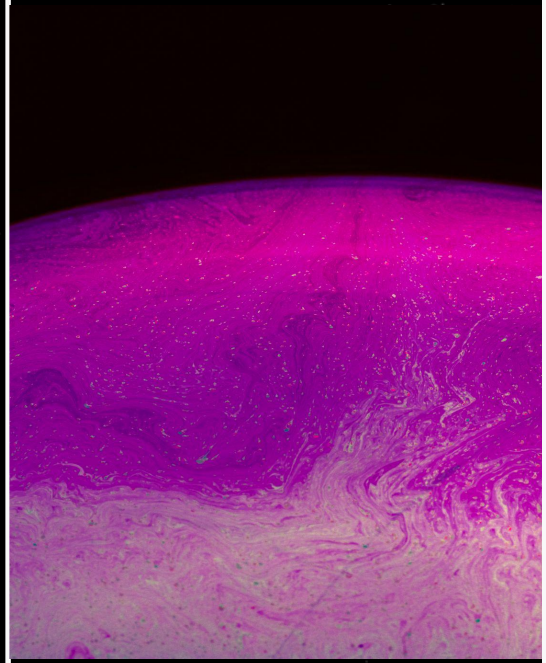
```
    //  If the analyzed proposal return a reasonable guess, then a positive vote will be dispatched
    console.log("This is a good guess! Voting for... ", processedData.id);
    votedPoV = processedData.id
    vote = 1;
    voteProposal(votedPoV, vote);
  }
  else{
    //  If the analyzed proposal return a bad guess, then a negative vote will be dispatched
    console.error("This is a bad guess. Voting against... ", processedData.id);
    votedPoV = processedData.id
    vote = -1;
    voteProposal(votedPoV, vote);
    tag = "unknown";
  }
}
```

Master node validation

The algorithm ***masterNodeValidation.js*** remains pretty similar to the ones concerning peer nodes: here, proposal voted positively by the majority are **empirically** studied, and if the guess turns out *acceptably* true, that proposal are marked as **accepted**, meaning that a new astral body is discovered and his spotter is **certificated.**

```
  //...
  console.log("This is a good guess! We Have WINNER! ", processedData.proposalID);
  acceptedPoV = processedData.proposalID;
  acceptProposal(acceptedPoV);
}
  //...
```

Case of a positive *guess*



04 Conclusions

Problems

Alas, the system is not exempt of theoretic, logical and efficiency failures:

- **Theory:**
  - Concepts are overly **simplified**, **insufficient** and even **invented**;
  - Very **few** use cases and **inadequate** *critical unique values*.

- **Coding:**
  - **No human interaction** is possible;
  - *Master node* generate **meaningless** data and uses the **same logic** of a *peer* to validate the proposal;
  - **Only two** p*eer nodes* available.
  - If there are too much *astralData* in the contract, the **system saturate**, sensibly slowing the machine;
  - **Bad efficiency** in some segments of the code.

Solution

Like most everything, improvements can be made:

- **Theory:**
  - Extend and scientifically verify the concepts;
  - Expand use cases and *critical unique values*.

- **Coding:**
  - *Master node* algorithm only as interface to the contract for the telescopes/sensors, implying no calculation about the proposal, because there will be physical check;
  - Add the ability to publicly connect anyone who wants it, through an interactive web page/app;
  - (?) Save and retrieve *astralData* not directly within the smart contract, but through transaction receipts;
  - Study and deploy new methods to achieve better performance.

Web interface mockup

SCAO

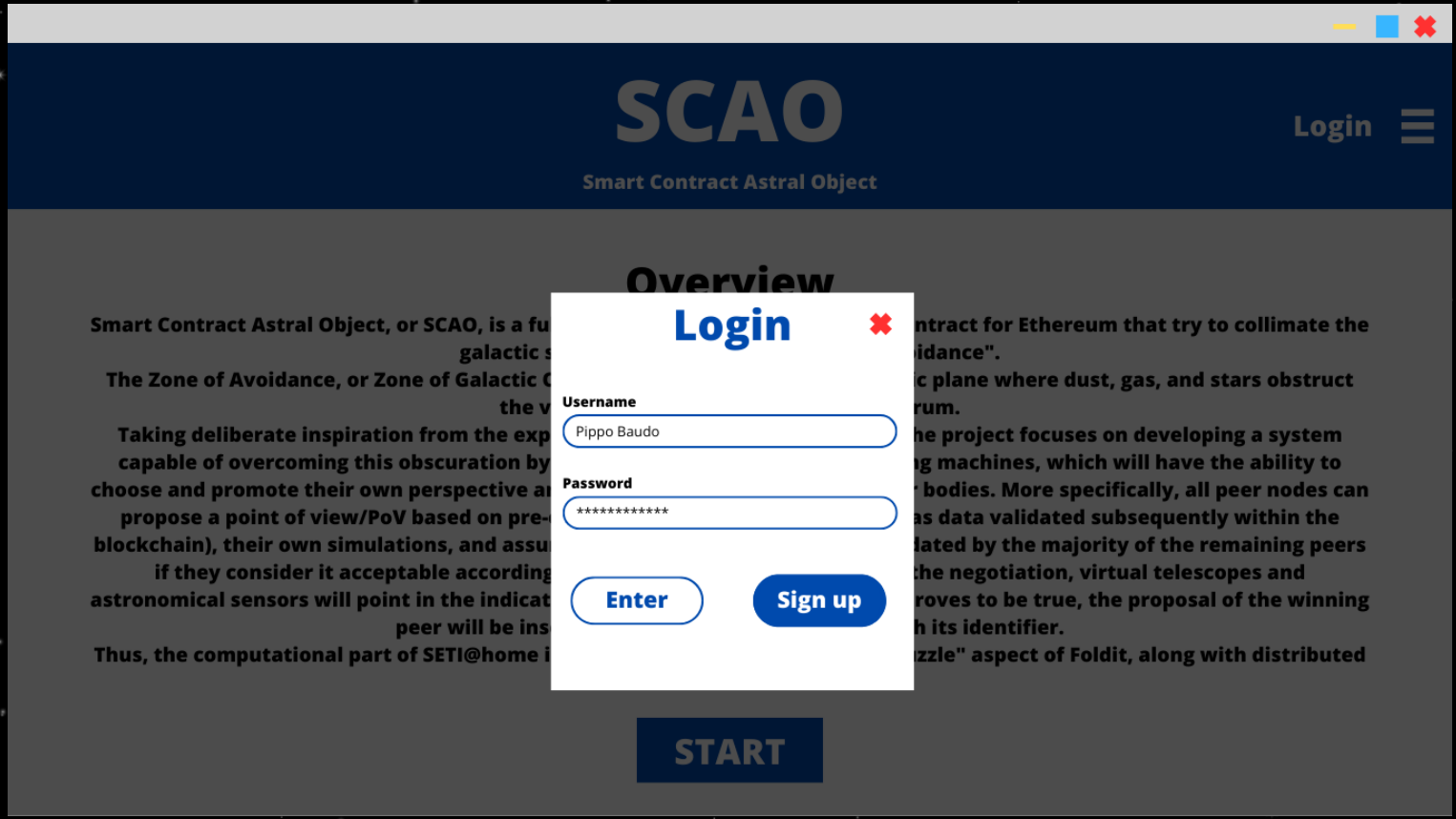
Smart Contract Astral Object

Login

Overview

Smart Contract Astral Object, or SCAO, is a fully independent developed smart contract for Ethereum that try to collimate the galactic space shadowed by the "Zone of Avoidance".
The Zone of Avoidance, or Zone of Galactic Obscuration, is an area in the galactic plane where dust, gas, and stars obstruct the view and sensors of the visible spectrum.
Taking deliberate inspiration from the experiences of Foldit and SETI@home, the project focuses on developing a system capable of overcoming this obscuration by distributing analyses publicly among machines, which will have the ability to choose and promote their own perspective and classification of celestial areas or bodies. More specifically, all peer nodes can propose a point of view/PoV based on pre-existing astronomical data (as well as data validated subsequently within the blockchain), their own simulations, and assumptions. This viewpoint will be validated by the majority of the remaining peers if they consider it acceptable according to their parameters. At the end of the negotiation, virtual telescopes and astronomical sensors will point in the indicated direction, and if the simulation proves to be true, the proposal of the winning peer will be inserted into the blockchain, along with its identifier.
Thus, the computational part of SETI@home is carried forward, as well as the "puzzle" aspect of Foldit, along with distributed assistance for research.

START


SCAO
Smart Contract Astral Object
Login
Overview
Smart Contract Astral Object, or SCAO, is a fu
ntract for Ethereum that try to collimate the
galactic s
idance".
The Zone of Avoidance, or Zone of Galactic C
c plane where dust, gas, and stars obstruct
the v
rum.
Taking deliberate inspiration from the exp
he project focuses on developing a system
capable of overcoming this obscuration by
g machines, which will have the ability to
choose and promote their own perspective a
bodies. More specifically, all peer nodes can
propose a point of view/PoV based on pre-
as data validated subsequently within the
blockchain), their own simulations, and assu
lated by the majority of the remaining peers
if they consider it acceptable according
he negotiation, virtual telescopes and
astronomical sensors will point in the indicat
roves to be true, the proposal of the winning
peer will be ins
h its identifier.
Thus, the computational part of SETI@home i
zzle" aspect of Foldit, along with distributed
Login
Username
Pippo Baudo
Password
Enter
Sign up
START

SCAO

Smart Contract Astral Object

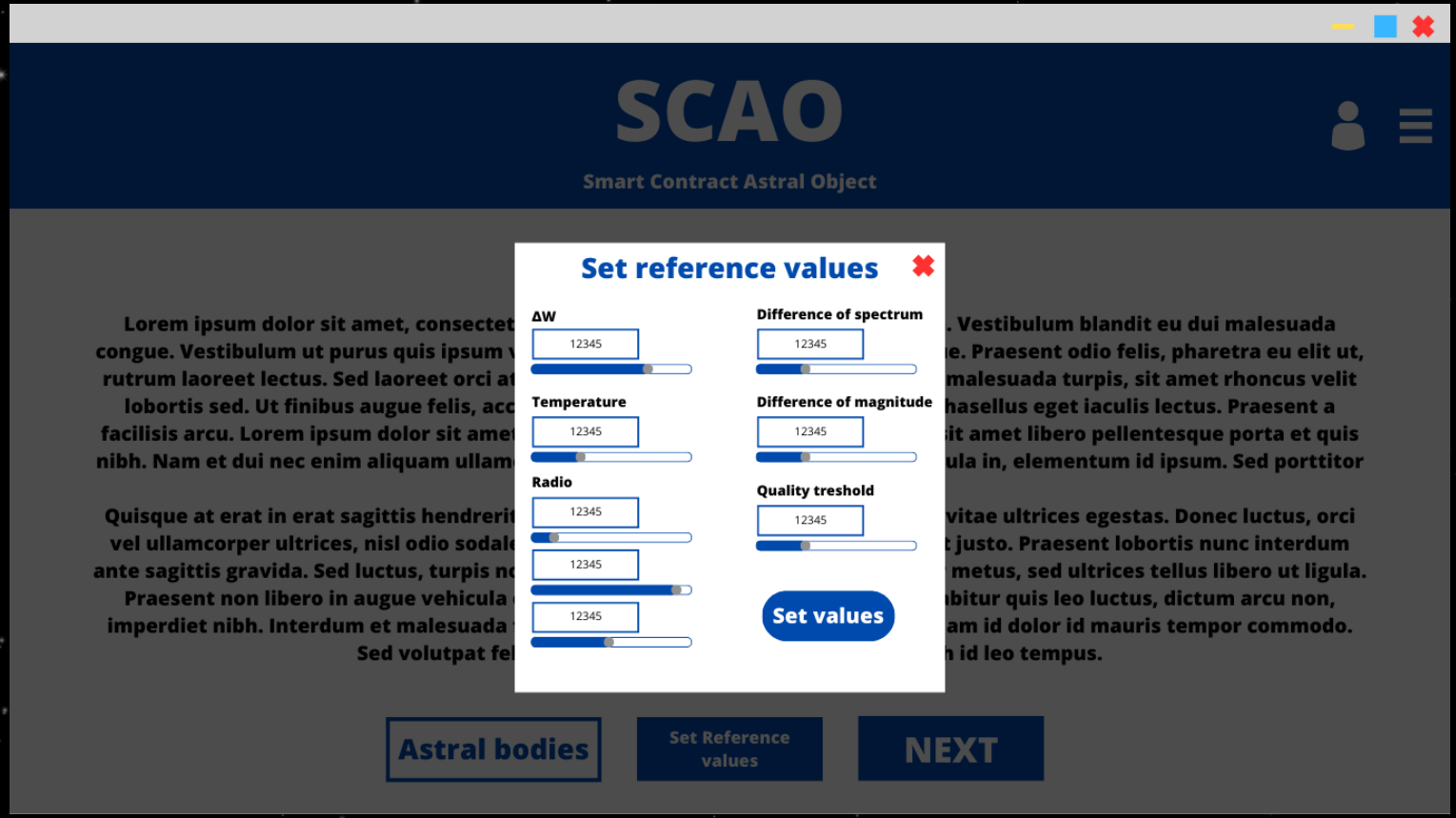
Tutorial

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent a cursus massa. Vestibulum blandit eu dui malesuada congue. Vestibulum ut purus quis ipsum vehicula dictum. Integer quis eleifend augue. Praesent odio felis, pharetra eu elit ut, rutrum laoreet lectus. Sed laoreet orci at justo volutpat tincidunt. Aliquam laoreet malesuada turpis, sit amet rhoncus velit lobortis sed. Ut finibus augue felis, accumsan facilisis nibh vestibulum facilisis. Phasellus eget iaculis lectus. Praesent a facilisis arcu. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi id dui sit amet libero pellentesque porta et quis nibh. Nam et dui nec enim aliquam ullamcorper. Integer lectus elit, facilisis et vehicula in, elementum id ipsum. Sed porttitor sed nisi ornare faucibus.

Quisque at erat in erat sagittis hendrerit eget in felis. Quisque pellentesque turpis vitae ultrices egestas. Donec luctus, orci vel ullamcorper ultrices, nisl odio sodales dui, eget elementum eros purus sit amet justo. Praesent lobortis nunc interdum ante sagittis gravida. Sed luctus, turpis non malesuada consequat, diam arcu auctor metus, sed ultrices tellus libero ut ligula. Praesent non libero in augue vehicula efficitur. Curabitur at pulvinar massa. Curabitur quis leo luctus, dictum arcu non, imperdiet nibh. Interdum et malesuada fames ac ante ipsum primis in faucibus. Etiam id dolor id mauris tempor commodo. Sed volutpat felis quis nisl egestas vulputate. Nunc ut nibh id leo tempus.

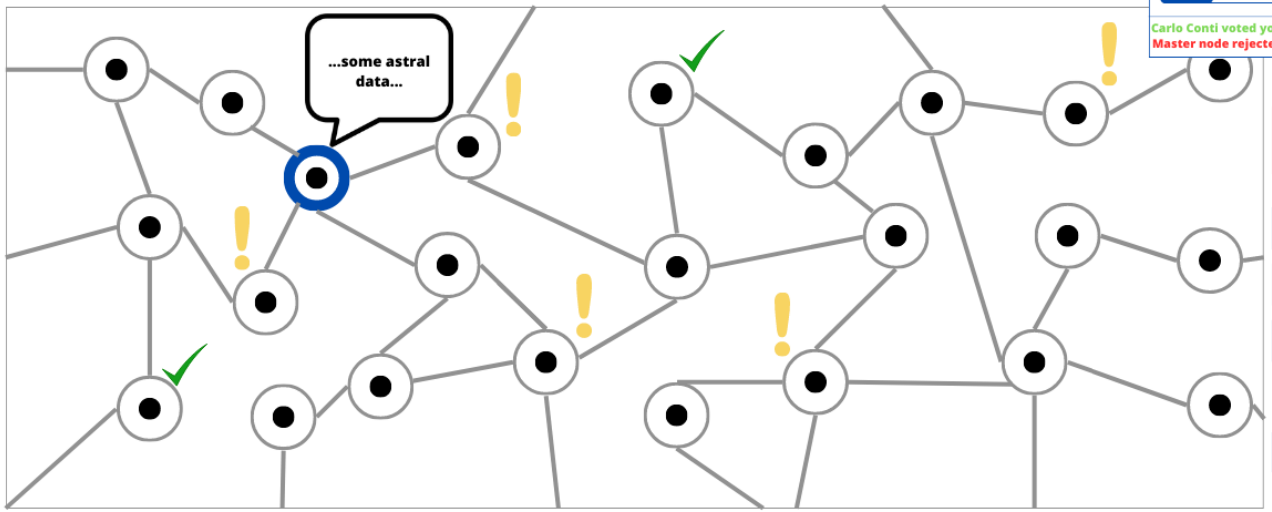
Astral bodies | Set Reference values | NEXT


SCAO
Smart Contract Astral Object
Tutorial
Lorem ipsum dolor sit amet, cons
congue. Vestibulum ut purus quis ip
rutrum laoreet lectus. Sed laoreet o
lobortis sed. Ut finibus augue feli
facilisis arcu. Lorem ipsum dolor sit
nibh. Nam et dui nec enim aliquam u
tibulum blandit eu dui malesuada
aesent odio felis, pharetra eu elit ut,
suada turpis, sit amet rhoncus velit
llus eget iaculis lectus. Praesent a
net libero pellentesque porta et quis
n, elementum id ipsum. Sed porttitor
Quisque at erat in erat sagittis hen
vel ullamcorper ultrices, nisl odio s
ante sagittis gravida. Sed luctus, tur
Praesent non libero in augue vehi
imperdiet nibh. Interdum et malesuada
ultrices egestas. Donec luctus, orci
co. Praesent lobortis nunc interdum
us, sed ultrices tellus libero ut ligula.
r quis leo luctus, dictum arcu non,
id dolor id mauris tempor commodo.
Sed volutpat felis quis nisl egestas vulputate. Nunc ut nibh id leo tempus.
Rocky planet
Mass
Lorem Ipsum
Composition
Lorem Ipsum
Temperature
Lorem Ipsum
Difference of spectrum
Lorem Ipsum
Magnitude microlensing
Lorem Ipsum
1/5
Astral bodies
Set Reference values
NEXT


SCAO
Smart Contract Astral Object
Set reference values
ΔW
12345
Temperature
12345
Radio
12345
12345
12345
Difference of spectrum
12345
Difference of magnitude
12345
Quality treshold
12345
Set values
Astral bodies
Set Reference values
NEXT

SCAO

Smart Contract Astral Object



Proposal progress

Carlo Conti voted your proposal!
Master node rejected you proposal...

Auto

Reference values

Analyzed data

Proposals

Winners

Vote

References

[1] List of astronomical objects.
[2] See relative astronomical object feature.
[4] Stellar spectra.
[5] Gravitational microlensing.
[6] Periodic table.

[1] Transit.
[2] Spectroscopy.
[3] Gravitational microlensing.
[4] Radio wavelenght method.
    [4.1] Hydrogen line
    [4.2.1] Tools of astronomy.
    [4.2.2] Emission at Centimeter Wavelengths; free Helium electron emission in X-band.
[5] Wien's displacement law.

[1] Transit method can't indicate the mass.
[2] Silicon spectrum is not in radio wavelengths