TSR Oráculo

Hackathon web3

Desafio 04: Desenvolvimento de tecnologias para casos de uso de automação de monitoramento, controle e precificação online de títulos públicos (oráculos)

Equipe
Vale das Araucárias

Eduardo Maceira

Fundador da Vitto (adquirida pela Stone em 2022);
Empreendedor tech há 14 anos;
Graduado em Administração pela FAE com especialização em inovação pela Universidade de Stanford.

Luciano Juvinski (líder)

Fundador da Navegg (adquirida pela DENTSU em 2019);
Empreendedor e Desenvolvedor há 20 anos;
Graduado em Engenharia da Computação com MBA em Administração pelo Ibmec.

Felipe Leite

Designer especializado em UX/UI
17 Anos de experiência;
Graduado em Jornalismo com MBA em Marketing Estratégico;
Mestre em Comunicação pela UFT.

Problemas

Falta de transparência na precificação do mercado secundário dos Títulos do Tesouro Nacional no mercado secundário

90% do mercado secundário hoje **acontece manualmente**

Ineficiência no fluxo de informações entre corretoras e Tesouro Nacional

Necessidade de solução on-chain para precificação de títulos públicos

Solução

Uma infraestrutura de dados on-chain orquestrada por um oráculo que organiza três diferentes papéis para esse novo ecossistema

Corretoras Tradicionais e Smart Contracts

Responsáveis por informar os dados de precificação

Função Gestor do Tesouro Nacional

Aprovar participantes, definir regras de distribuição de incentivos financeiros e multar agentes corrompidos

dApp

Exibe para o usuário final de forma amigável e gratuita preço médio por título e na modalidade paga traz valores de última transação, melhor oferta de compra/venda, volume de títulos entre PF e PJ

Público Alvo

Corretoras Tradicionais
Itaú Corretora, XP, Ágora, BTG, Rico, Nu Invest, Modalmais, etc..

Corretoras Cripto
Binance, Mercado Bitcoin, Foxbit, Bybit, OKX, Bitso, etc..

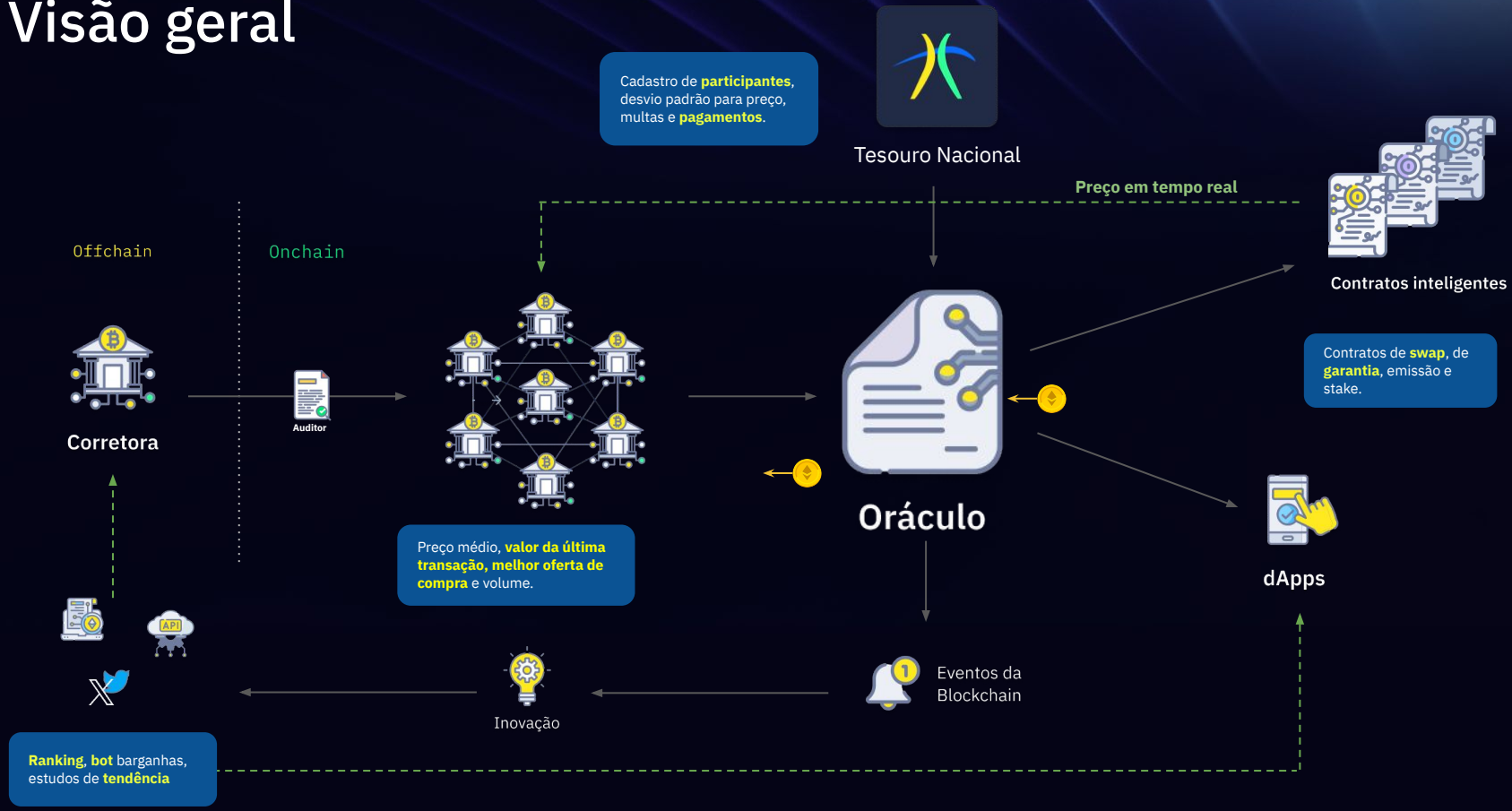
Smart Contracts que recebem Títulos Públicos como garantia

Smart Contracts que negociam Títulos Públicos Tokenizados

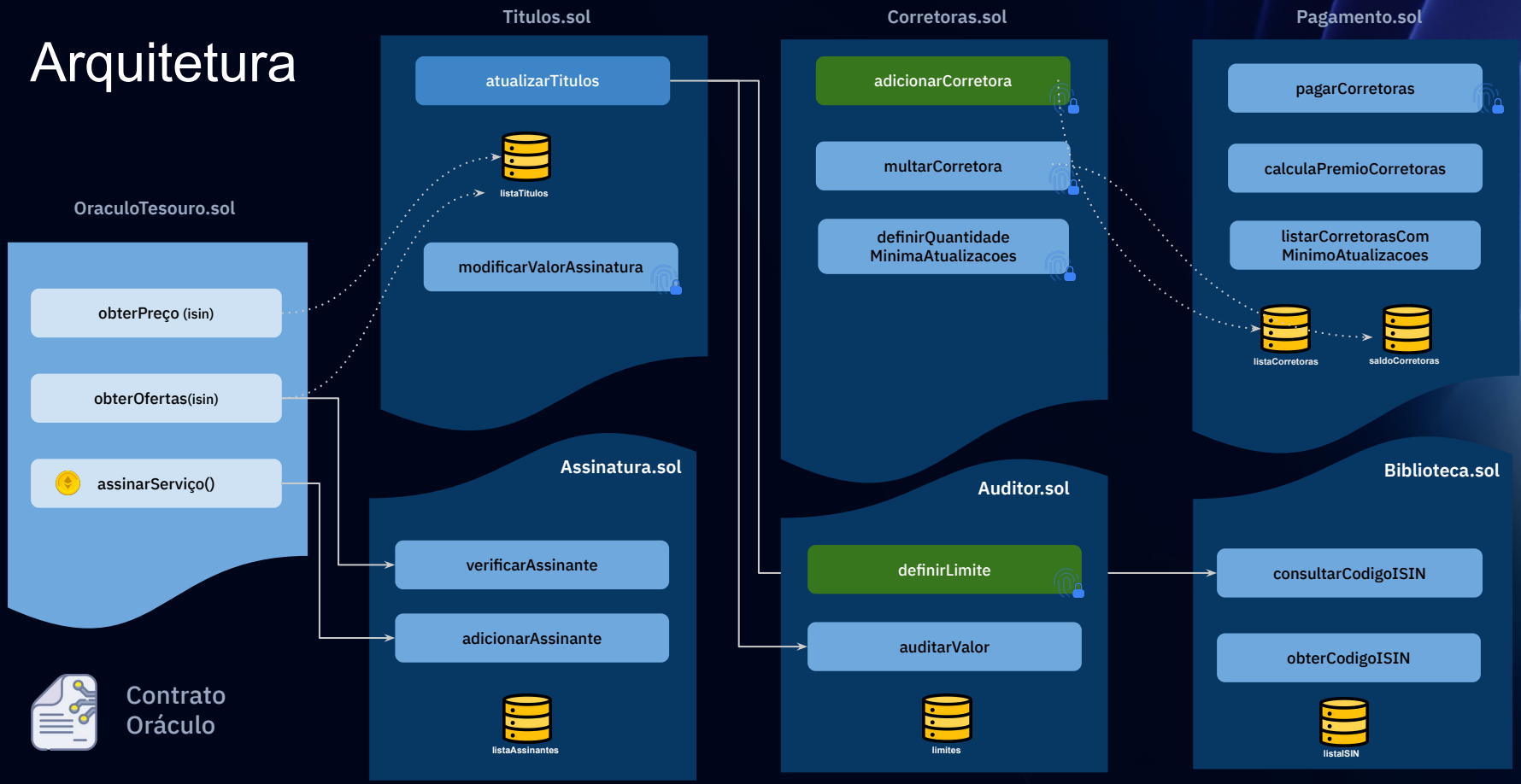
Novas dApps
(Decentralized applications)
Aplicativos descentralizados

Smart Contracts do Governo
Que emitam ou negociem títulos públicos Tokenizados

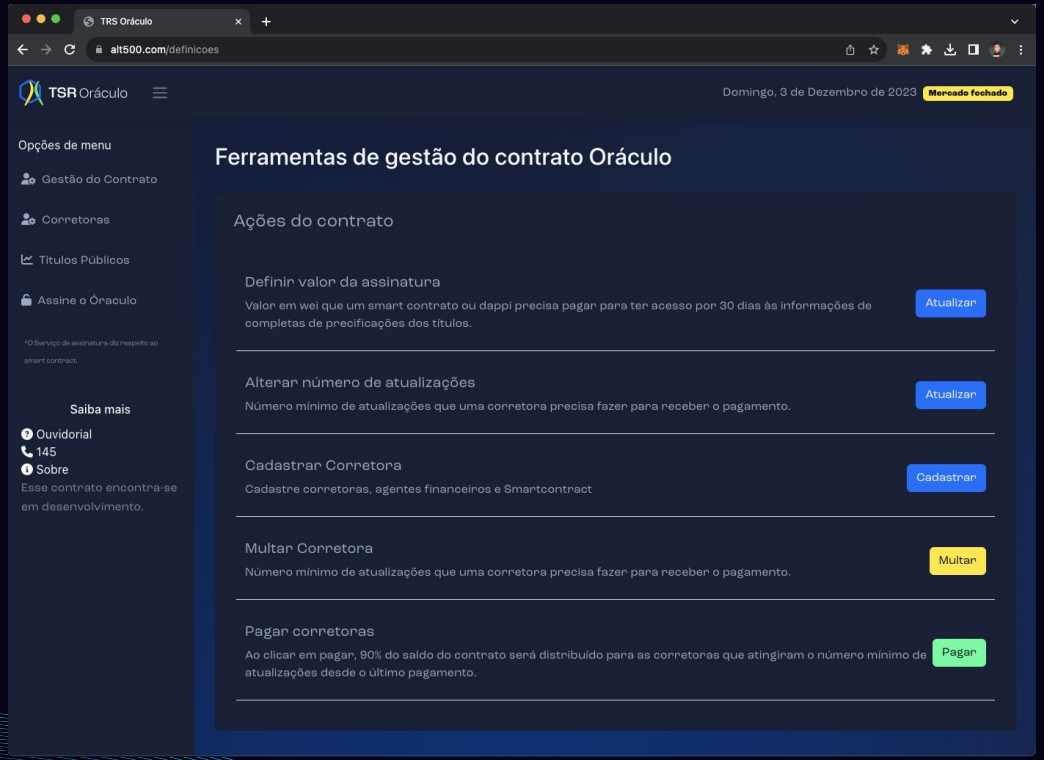
Visão geral


Cadastro de **participantes**, desvio padrão para preço, multas e **pagamentos**.
Tesouro Nacional
Preço em tempo real
Offchain
Onchain
Contratos inteligentes
Contratos de **swap**, de **garantia**, emissão e stake.
Corretora
Auditor
Preço médio, **valor da última transação, melhor oferta de compra** e volume.
Oráculo
dApps
API
Eventos da Blockchain
Inovação
Ranking, **bot** barganhas, estudos de **tendência**

Arquitetura

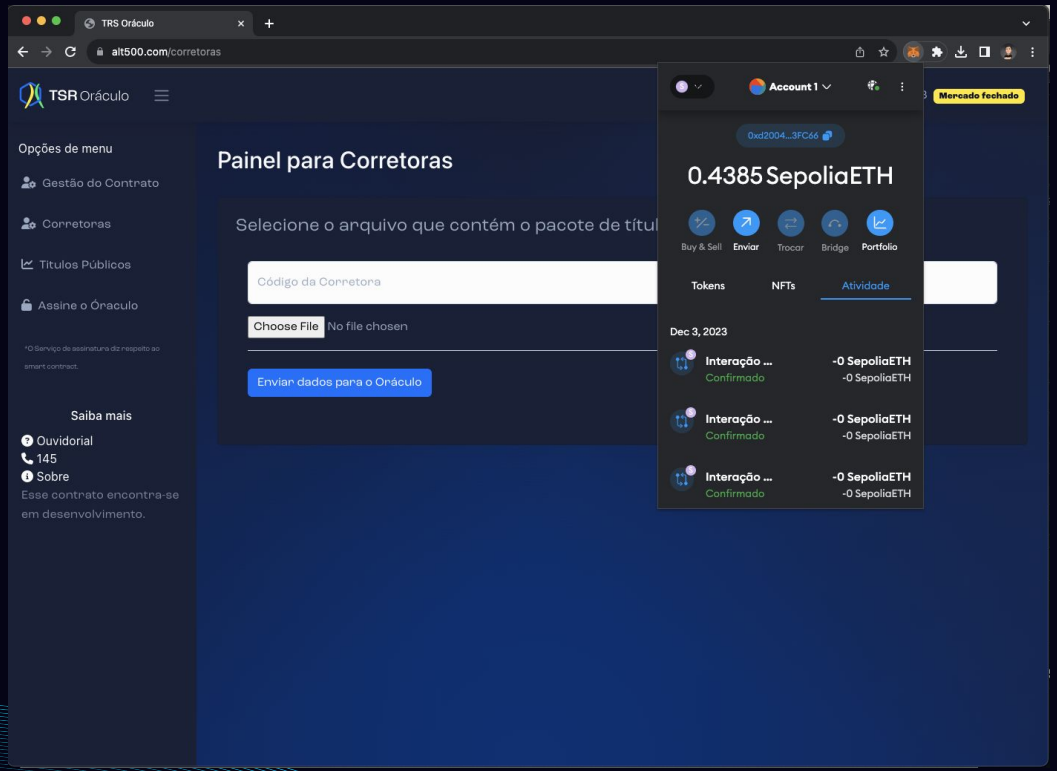


dApp - Gestão do Contrato



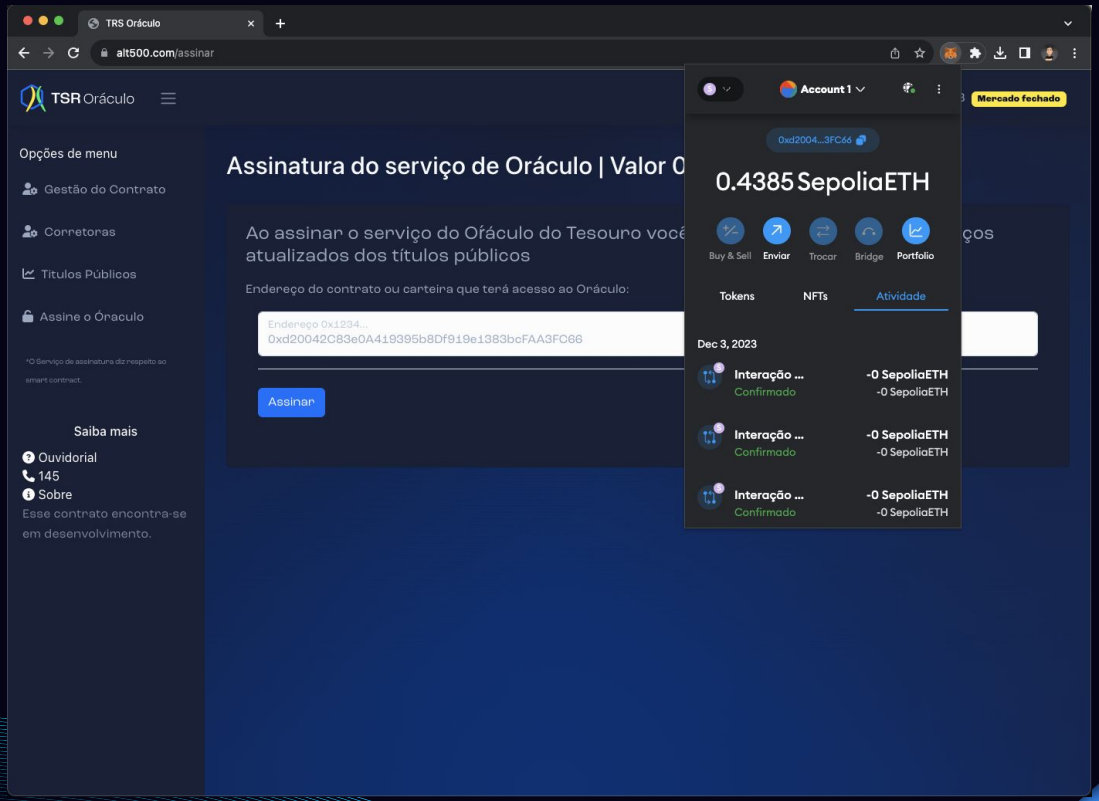
Nessa tela, o Tesouro Nacional adiciona corretoras, define as regras do mecanismo de incentivo e estipula o valor do serviço para smart contracts e dApps

dApp - Corretoras



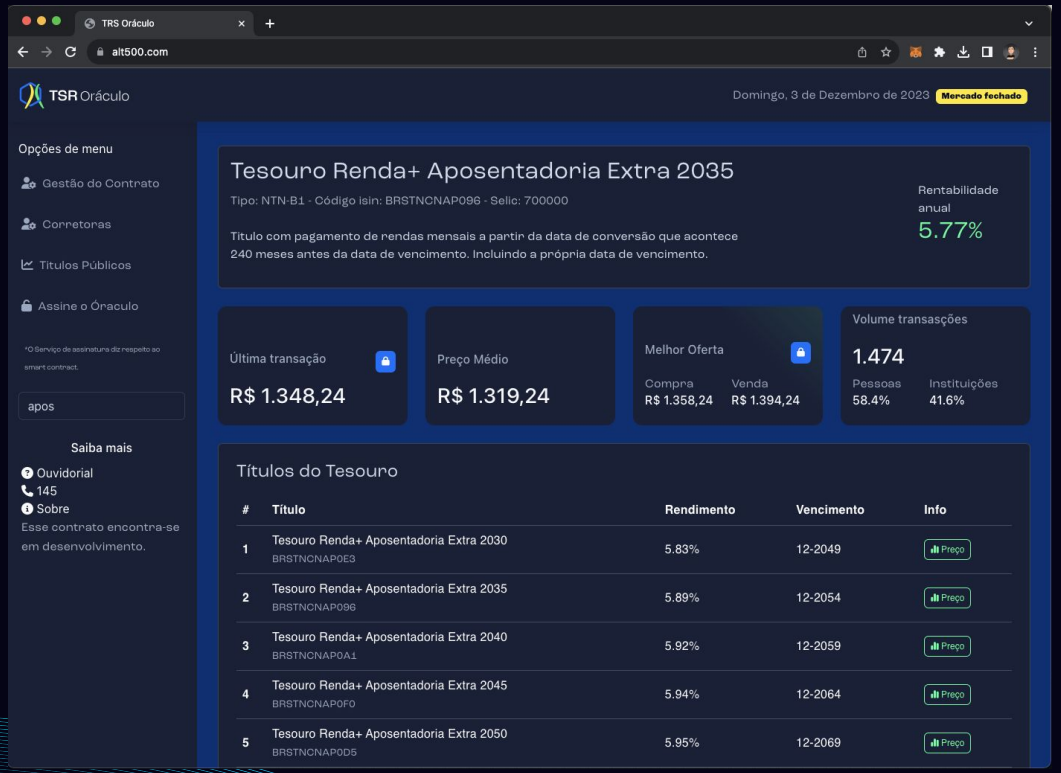
A dApp oferece a opção para que as corretoras iniciem o envio dos preços de títulos a partir do relatório atual que já é enviado para o Tesouro Nacional.

dApp - Assinatura Oráculo



A dApp oferece o recurso de contratação do Oráculo que retorna a informação completa de preços, volumes e divisão entre pessoa física e jurídica.

dApp - Títulos Públicos



A dApp permite que os usuários interajam com o serviço gratuíto de busca de preços médios dos títulos.

Se a carteira conectada, realizar a contratação do Oracle, a Interface exibe as informações completas.

Modelo de Negócio

Desenvolvemos uma infraestrutura inovadora que transmite dados **off-chain para on-chain** por meio de um Oráculo, estabelecendo um sólido **mecanismo de incentivo** financeiro destinado a instituições financeiras que compartilhem informações sobre transações de títulos públicos. Em outras palavras, todas as **corretoras e contratos inteligentes** que atendam aos pré-requisitos, cumprindo a frequência e qualidade estabelecidas pela função de **Gestor, sob controle do Tesouro Nacional**, serão recompensados financeiramente. Esses pagamentos serão **provenientes dos usuários** que consumirem esses dados através de Contratos Inteligente e dApps, possibilitando tomadas de decisão bem informadas nas negociações de tokens do Tesouro.

Diferencial Competitivo

Nossa principal vantagem reside na criação de uma solução personalizada para o Tesouro Nacional, cuidadosamente projetada para atender aos requisitos regulatórios. Simultaneamente, estabelecemos um modelo freemium que não apenas possibilita, mas também incentiva as negociações de títulos públicos, tanto on-chain quanto off-chain.

Eventos do Oráculo

Além de prover dados para Contratos e dApps da Blockchain, a solução desenvolvida **implementou** uma interface para estimular a inovação e aumentar as negociações de títulos públicos.

WebSite

Ranking Melhores corretoras

Estudos de mercado

Liquidez baseado em vencimento por corretora

API

Preço atual

Automatização compra/venda

Melhor corretora compra/venda

Twitter Bot

Tendências (por volume)

Barganha (preço baixo média)

@BondsInsights

Github do Projeto

Contrato Solidity do Smart Contract do Oráculo

https://github.com/juv1nsk1/araucaria

Github do Projeto - Integração

Interface Blockchain em Solidity que permite que desenvolvedores criem contratos utilizando o Oráculo

https://github.com/juv1nsk1/araucaria

Github do Projeto - Integração

Biblioteca Typescript que faz a integração do backend das corretoras com a função enviar dados do Oráculo na Blockchain

Como Usar

1. Clone este repositório: `git clone https://github.com/juv1nsk1/araucaria.git`
2. Siga as instruções detalhadas na documentação para integrar a biblioteca ao seu projeto.
3. Implemente as chamadas necessárias para conectar sua corretora ao Oracle de Dados.

Exemplos

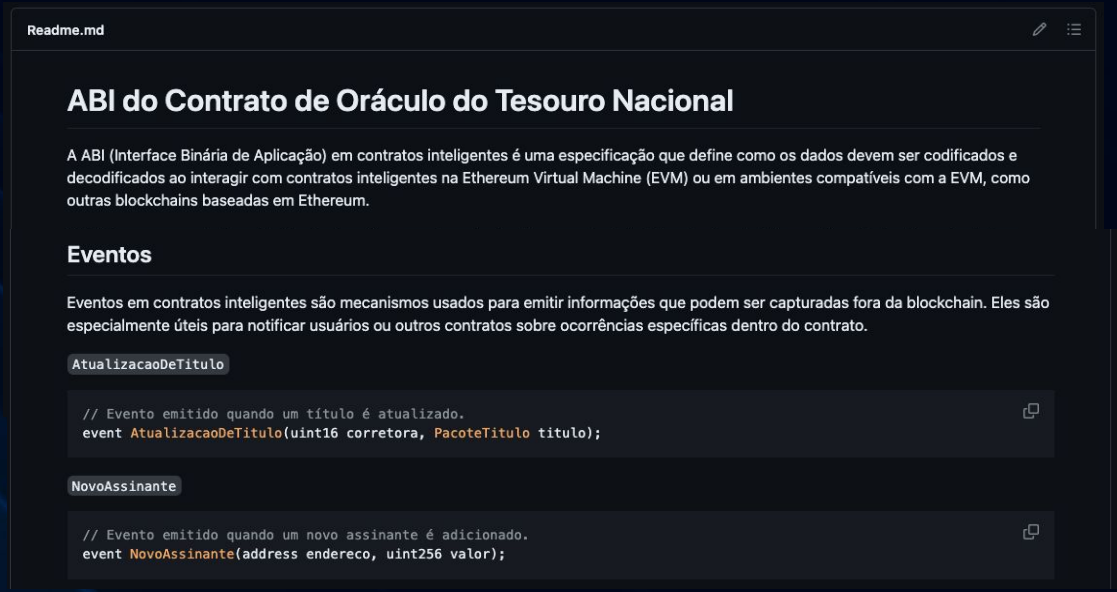
```
// Exemplo de código mostrando como usar a biblioteca para estabelecer uma conexão
// e realizar operações básicas com o Oracle de Dados.

import { EnviarTitulos } from 'importacao-lib';

// Configuração
const CHAVE_CORRETORA = "..";
const ENDERECO_CONTRATO = "...";
```

Name	Last commit message	Last commit date
..		
Readme.md	Rename Read.me to Readme.md	5 days ago
importacao-lib.js	Adicionando referência da LIB para integração	5 days ago

https://github.com/juv1nsk1/araucaria

Github do Projeto - Integração

ABI - Interface e documentação que permite a integração de dApps com as funções e eventos do Oráculo



Readme.md

ABI do Contrato de Oráculo do Tesouro Nacional

A ABI (Interface Binária de Aplicação) em contratos inteligentes é uma especificação que define como os dados devem ser codificados e decodificados ao interagir com contratos inteligentes na Ethereum Virtual Machine (EVM) ou em ambientes compatíveis com a EVM, como outras blockchains baseadas em Ethereum.

Eventos

Eventos em contratos inteligentes são mecanismos usados para emitir informações que podem ser capturadas fora da blockchain. Eles são especialmente úteis para notificar usuários ou outros contratos sobre ocorrências específicas dentro do contrato.

`AtualizacaoDeTitulo`

```
// Evento emitido quando um título é atualizado.
event AtualizacaoDeTitulo(uint16 corretora, PacoteTitulo titulo);
```

`NovoAssinante`

```
// Evento emitido quando um novo assinante é adicionado.
event NovoAssinante(address endereco, uint256 valor);
```

https://github.com/juv1nsk1/araucaria

Github do Projeto - Segurança

Além da documentação das bibliotecas utilizadas, consta no repositório relatório da auditoria realizado.

Auditoria com Mythril

Realizamos uma auditoria abrangente do nosso contrato utilizando a ferramenta Mythril, uma ferramenta de análise de segurança para bytecode da EVM. Essa ferramenta detecta vulnerabilidades de segurança em contratos inteligentes construídos para Ethereum, Hedera, Quorum, Vechain, Roostock, Tron e outras blockchains compatíveis com a EVM. Utiliza técnicas como execução simbólica, solução de SMT e análise de contaminação para detectar uma variedade de vulnerabilidades de segurança.

Relatório da Auditoria com Mythril:

```
==== Dependence on predictable environment variable ====
SWC ID: 116
Severity: Low
Contract: TesouroOracle
Function name: obterOfertas(string)
PC address: 1177
Estimated Gas Usage: 2348 - 2823
A control flow decision is made based on The block.timestamp environment variable.
The block.timestamp environment variable is used to determine a control flow decision. Note that the values of varial
--------------------
In file: contracts/TesouroOracle.sol:43

require(verificarAssinante(), "Acesso negado. Assine esta funcao atraves de assinarServico().")
```

https://github.com/juv1nsk1/araucaria

Github do Projeto - Test

Script de teste unitário, relatório de resultado e arquivo de configuração de bibliotecas externas para auditoria do contrato

Name	Last commit message	Last commit date
..		
Readme.md	informações sobre remap.json do Mythril	4 days ago
TesouroOracle.ts	Script de teste e relatório	5 days ago
remap.json	Script de teste e relatório	5 days ago

Readme.md

```
$ npx hardhat test


  Oráculo Tesouro Nacional
    ✔ Adiciona corretora,verifica endereço e a remove. (1245ms)
    ✔ Adiciona titulos e verifica novo preço médio. (102ms)
    ✔ Adiciona titulos, contrata feed e verifica melhor oferta de compra e venda (65ms)
    ✔ Adiciona auditor e verifica bloqueio. (52ms)
    ✔ Adiciona corretora, define número de atualizacoes minimas e efetua pagameto do prêmio.
    ✔ Teste funções adicionais de governança: Multa corretora e modifica valor da assinatura


  6 passing (2s)
```

https://github.com/juv1nsk1/araucaria

Github do Projeto - dApp

Código React da aplicação que interage com o contrato e realiza as funções de gestão, atualização dos preços e consulta.

Name	Last commit message	Last commit date
..		
public	dApp para demo	17 hours ago
src	Conectando em Sepolia	10 hours ago
README.md	Update README.md	now
Screenshot - dappi 1.png	Adicionando screenshots	16 hours ago
Screenshot - dappi 2.png	Adicionando screenshots	16 hours ago
Screenshot - dappi 3.png	Adicionando screenshots	16 hours ago
package-lock.json	dApp para demo	17 hours ago
package.json	dApp para demo	17 hours ago

README.md

dApp Demo - Oráculo Tesouro

1. Para acessar a dAppi é necessário adicionar a redeSepolia em sua Metamask

Network name: Sepolia

Network URL: https://eth-sepolia.g.alchemy.com/v2/demo

Chain ID: 11155111

https://github.com/juv1nsk1/araucaria

Blockchain sem oráculo é igual a computador sem internet.

@EquipeValeDasAraucárias