BASE BLOCKHAIN ETHEREUM COM SOLIDITY

POR JEFTAR MASCARENHAS

MÓDULO 2

ETHEREUM EVM, SMART CONTRACT

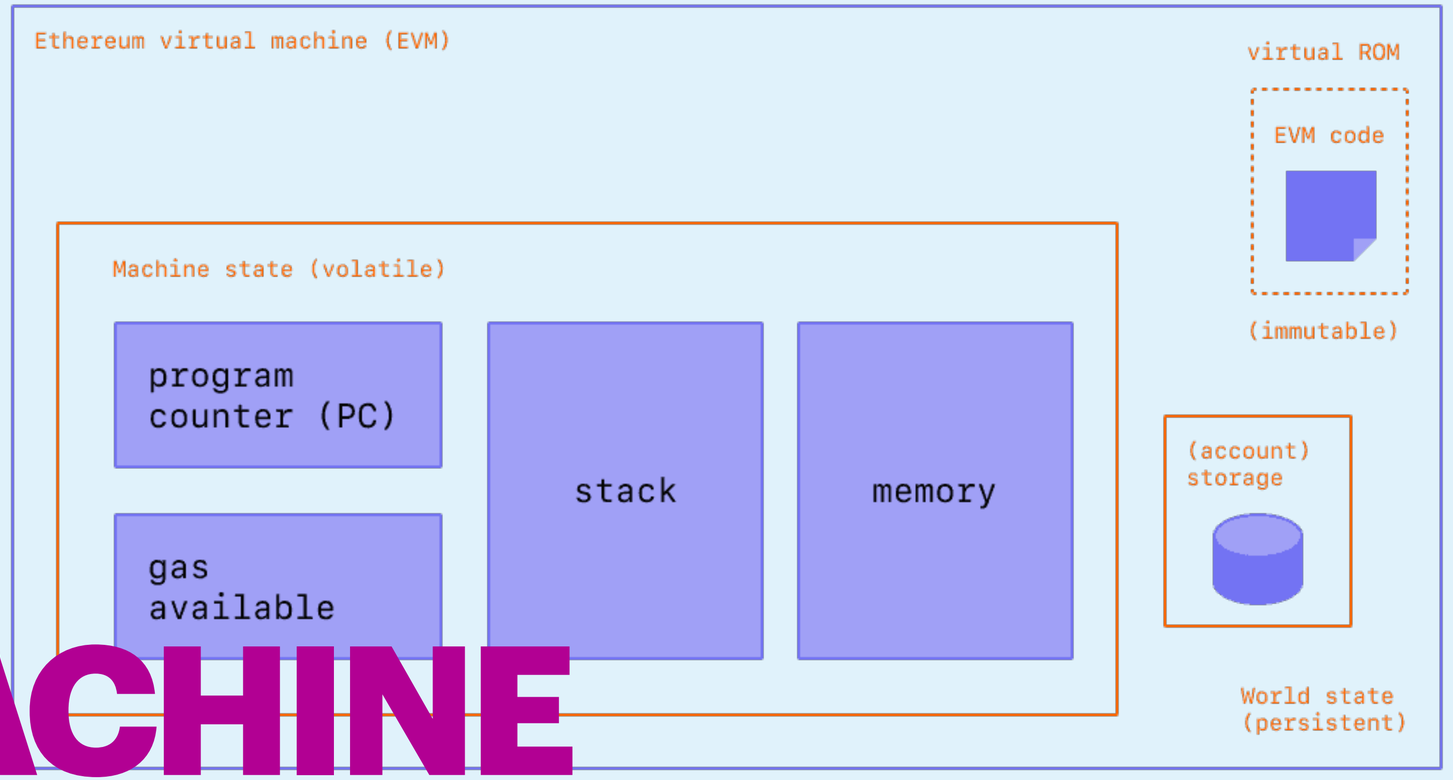
- Aula 1 - Ethereum Virtual Machine
- Aula 2 - Smart Contracts
- Aula 3 - Remix

JEFTAR MASCARENHAS

NFT Choose

MÓDULO 2

AULA 01



ETHEREUM VIRTUALMACHINE

POR JEFTAR MASCARENHAS

O QUE É A EVM?

A MAQUINA VIRTUAL ETHEREUM(EVM) É O AMBIENTE DE EXECUÇÃO PARA CONTRATOS INTELIGENTES NA ETHEREUM.

TODOS OS CONTRATOS E ALTERAÇÕES DE ESTADO NA CADEIA DE BLOCO ETHEREUM SÃO EXCITADOS POR TRANSAÇÕES. O EVM CONTROLA TODOS O PROCESSAMENTO DE TRANSAÇÕES NA REDE ETHEREUM

O EVM É COMO QUALQUER MAQUINA VIRTUAL, ONDE FAZ UMA ABSTRAÇÃO ENTRE O CÓDIGO DE EXECUÇÃO PARA CÓDIGO DE MAQUINA, CHAMADOS ETHEREUM BYTE CODE.

COMO UM DESENVOLVEDOR DAPP, VOCÊ NÃO PRECISA SABER MUITO SOBRE O EVM, APENAS QUE O VEM ALIMENTA DE FORMA CONFIÁVEL TODOS OS APLICATIVOS NA ETHEREUM SEM INTERRUPÇÕES.

NFT Choose

MÓDULO 2

AULA 02

SMART CONTRACTS

POR JEFTAR MASCARENHAS

SMART CONTRACT

UM CONTRATO INTELIGENTE É UM SIMPLESMENTE UM PROGRAMA QUE É EXECUTADO NA CADEIA DE BLOCOS ETHEREUM.

É UMA COLEÇÃO DE CÓDIGO, COM FUNÇÕES E DADOS DE ESTADO QUE RESIDE EM UM ENDEREÇO ESPECIFICO NA BLOCKCHAIN ETHEREUM.

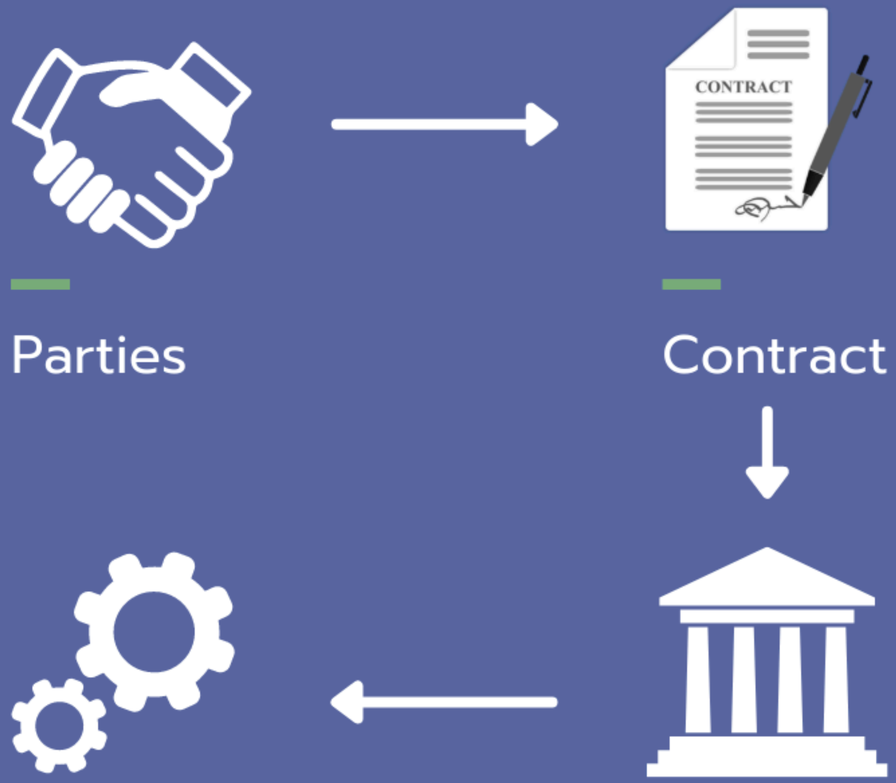
OS CONTRATOS INTELIGENTES TAMBÉM SÃO UM TIPO DE CONTA ETHEREUM.

ISSO SIGNIFICA DIZER QUE ELES TEM UM SALDO, E PODEM ENVIAR TRANSAÇÕES ATRAVÉS DA REDE. NO ENTANTO ELES NÃO SÃO CONTROLADOS POR UM USUÁRIO.

CONTAS DE USUÁRIOS PODE INTERAGIR COM UM CONTRATO ENVIANDO TRANSAÇÕES QUE EXECUTAM UMA FUNÇÃO DEFINIDA NO CONTRATO.

AS ALTERAÇÕES QUE UM CONTRATO FAZ SÃO IRREVERSÍVEIS.

Traditional Contracts



Parties

Contract

3rd Party

Execution

Smart Contracts

Parties

Smart Contract

Execution

SEM PERMISSÃO E COMPONIBILIDADE

QUALQUER UM PODE ESCREVER UM CONTRATO INTELIGENTE E IMPLEMENTA-LO NA REDE.

VOCÊ SÓ PRECISA SABER CODIFICAR EM UMA LINGUAGEM DE CONTRATO INTELIGENTE COMO SOLIDITY OU VYPER E TER ETH SUFICIENTE PARA FAZER O DEPLOY DO CONTRATO PARA REDE PRINCIPAL PAGANDO AS TAXAS NECESSÁRIAS O FAMOSO GÁS.

CONTRATOS INTELIGENTES SÃO PÚBLICOS NA ETHEREUM E PODE SER CONSIDERADOS COMO APIS ABERTAS. ISSO SIGNIFICA QUE VOCÊ PODE CHAMAR OUTROS CONTRATOS EM SEU PRÓPRIO CONTRATO INTELIGENTE AMPLIANDO MUITO O QUE É POSSÍVEL SER FEITO COM CONTRATOS.

OS CONTRATOS PODEM IMPLEMENTAR OUTROS CONTRATOS.

LIMITAÇÕES

POR SÍ SÓ UM CONTRATO INTELIGENTE NÃO CONSEGUE OBTER INFORMAÇÕES SOBRE EVENTOS “NO MUNDO REAL” PORQUE NÃO PODEM ENVIAR SOLICITAÇÕES HTTP.

A NÃO COMUNICAÇÃO COM O "MUNDO REAL” É PARA GARANTIR A SEGURANÇA E A DESCENTRALIZAÇÃO.

ARMAZENAMENTO(STORE)

DADOS: QUAISQUER DADOS DE UM CONTRATO DEVEM SER ATRIBUÍDO A UM LOCAL: ARMAZENAMENTO(STORAGE) OU MEMÓRIA(MEMORY).

É CARO MODIFICAR O ARMAZENAMENTO EM UM CONTRATO.

VOCÊ PRECISA SABER ONDE DEVE ESTÁ OS DADOS NO CONTRATO EVITANDO MAIORES CUSTOS.

STORE: DADOS PERSISTENTES SÃO REFERIDOS COMO ARMAZENAMENTO E SÃO REPRESENTADOS POR VARIÁVEIS DE ESTADO. ESSES VALORES SÃO ARMAZENADOS PERMANENTEMENTE NA BLOCKCHAIN.

```
// Exemplo Solidity
contract SimpleStorage {
    uint storedData; // State variable
    // ...
}
```

MEMÓRIA(MEMORY)

MEMÓRIA: VALORES QUE SÃO ARMAZENADOS APENAS PARA A DURAÇÃO DA EXECUÇÃO DA FUNÇÃO DE UM CONTRATO SÃO CHAMADAS DE VARIÁVEIS DE MEMÓRIA.

COMO NÃO SÃO ARMAZENADAS PERMANENTEMENTE NA BLOCKCHAIN, SÃO MUITO MAIS BARATAS.

VARIÁVEIS DE AMBIENTES

ALÉM DAS VARIÁVEIS DEFINIDAS POR VOCÊ NO SEU CONTRATO, EXISTEM ALGUMAS VARIÁVEIS GLOBAIS ESPECIAIS.

ELAS SÃO USADAS PRINCIPALMENTE PARA FORNECER INFORMAÇÕES SOBRE A CADEIA DE BLOCOS OU TRANSAÇÃO ATUAL.

Prop	Variável de estado	Descrição
`block.timestamp`	uint256	Data/hora de início do bloco atual
`msg.sender`	endereço	Remetente da mensagem (chamada atual)

FUNÇÕES

FUNÇÕES PODEM OBTER INFORMAÇÕES OU UM CONJUNTO DE INFORMAÇÕES EM RESPOSTA A UMA ENTRADA DE TRANSAÇÕES.

EXISTEM DOIS TIPOS DE CHAMADAS DE FUNÇÕES:
INTERNAL - SÓ PODEM SER ACESSADAS DE DENTRO DO CONTRATO ATUAL OU DE CONTRATOS DERIVADOS.
EXTERNAL - NÃO PODE SER CHAMADA INTERNAMENTE POR OUTRA FUNÇÃO, SÓ PODE SER CHAMADA A PARTIR DE OUTRO CONTRATO OU ATRAVÉS DE TRANSAÇÃO

TAMBÉM PODEM SER PÚBLICAS OU PRIVADAS:
FUNÇÕES PÚBLICAS - PODEM SER CHAMADAS INTERNAMENTE A PARTIR DE UM CONTRATO OU EXTERNAMENTE POR MEIO DE MENSAGENS.

FUNÇÕES PRIVADAS - SÃO VISÍVEIS APENAS PARA O CONTRATO NO QUAL ESTÃO DEFINIDAS E NÃO NOS CONTRATOS DERIVADOS.

NFT Choose

MÓDULO 2

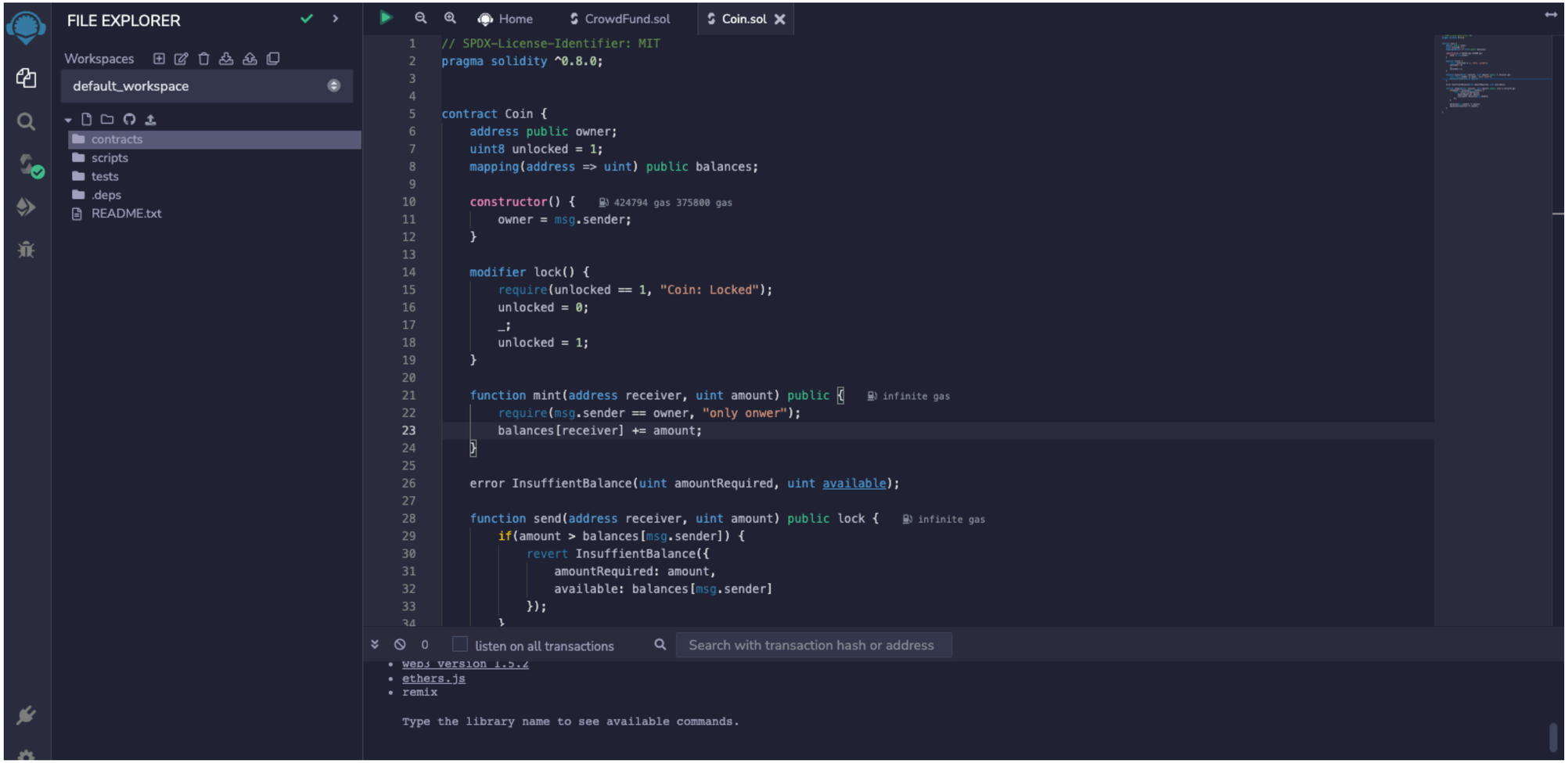
AULA 03

REMIX IDE

POR JEFTAR MASCARENHAS

REMIX IDE

HTTPS://REMIX.ETHEREUM.ORG/



JEFTAR MASCARENHAS

REMIX IDE

HTTPS://REMIX.ETHEREUM.ORG/

O REMIX É UMA IDE QUE RODA NO NAVEGADOR SEM NECESSIDADE DE CONFIGURAÇÃO DO AMBIENTE MUITO ÚTIL PARA ESTUDOS E ATÉ MESMO PARA CONTRATOS PROFISSIONAIS.

ALGUNS PONTOS ONDE O REMIX NOS AJUDA NESSE INICIO COMO DESENVOLVEDORES.

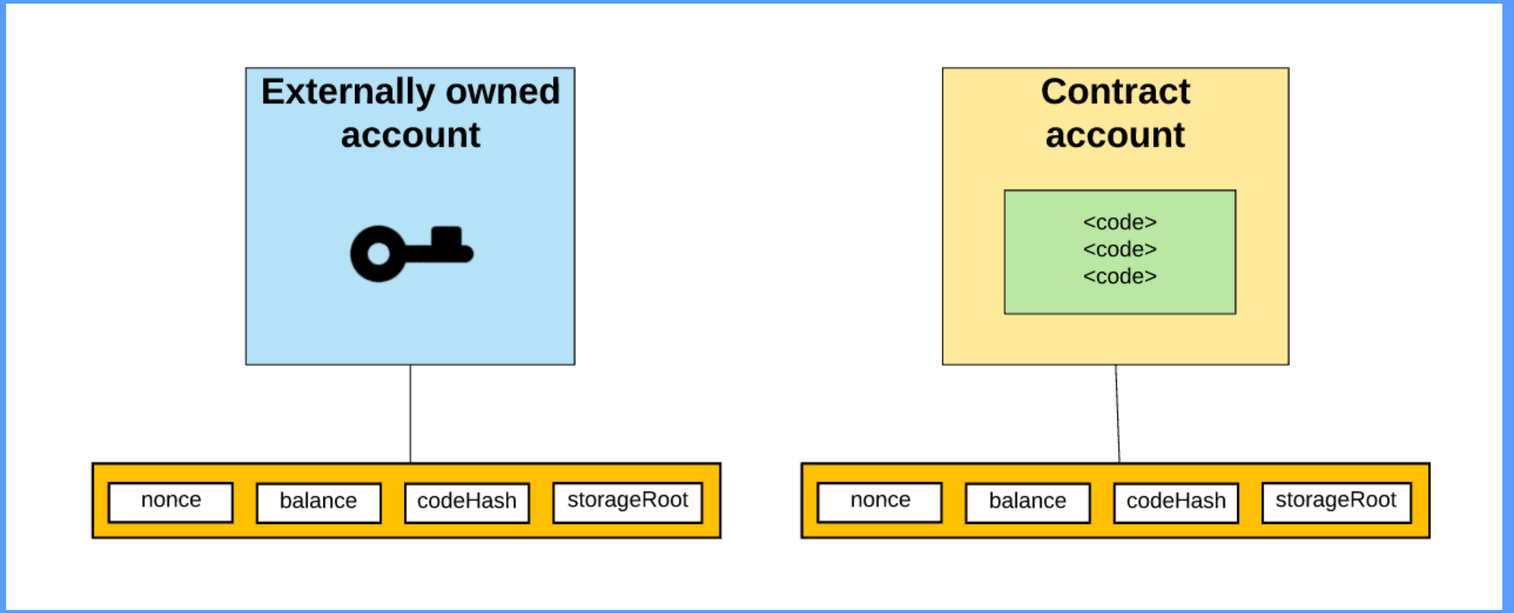
- - SIMULA UMA BLOCKCHAIN NO NAVEGADOR
- - INTERAGE COM OUTRAS BLOCKCHAIN VIA NAVEGADOR
-

- FERRAMENTA FÁCIL PARA TESTAR O CÓDIGO DE CONTRATOS
- EDITOR(IDE - AMBIENTE INTEGRADO DE DESENVOLVIMENTO) PARA SOLIDITY
- COMPILADOR DE CÓDIGO PARA ETHEREUM BYTE CODE
- DEBUGGER(DEPURADOR DE ERROS)

MÓDULO 2

AULA 04

TIPOS DE CONTAS



POR JEFTAR MASCARENHAS

TIPOS DE CONTA NO ETHEREUM

EXISTE DOIS TIPOS DE CONTAS NO ETHEREUM QUE COMPARTILHAM O MESMO ESPAÇO DE ENDEREÇO: CONTAS DE USUÁRIO(CONTAS EXTERNAS) E CONTAS DE CONTRATO.

CONTAS DE USUÁRIO:
SÃO CONTAS CONTROLADAS POR DUAS CHAVES, PÚBLICA E PRIVADA E SÃO CONTROLADOS POR HUMANOS.

CONTAS DE CONTRATO:
SÃO CONTROLADAS PELO PRÓPRIO CONTRATO.

O ENDEREÇO DO USUÁRIO É DERIVADO A PARTI DA CHAVE PÚBLICA ENQUANTO O ENDEREÇO DE CONTRATO É DERIVADO DO ENDEREÇO DO CRIADOR E DO NÚMERO DE TRANSAÇÕES ENVIADAS DESSE ENDEREÇO, O FAMOSO “NONCE".

NFT Choose

ENVIE PERGUNTAS NOS COMENTÁRIOS OU NA ISSUE.

https://github.com/nftchoose/base-blockchain-ethereum-solidity