



PARADIGMA ORIENTADO A CONTRATOS

PROJETO DA DISCIPLINA PARADIGMAS DE LINGUAGENS DE PROGRAMAÇÃO

EQUIPE: DANILO RAFAEL DE LIMA CABRAL E HENRIQUE FERRAZ ARCOVERDE

O QUE É O PARADIGMA ORIENTADO A CONTRATOS?

SURTIU COMO UMA **ESPECIALIZAÇÃO** DO PARADIGMA ORIENTADO A **OBJETOS**, PARA A CRIAÇÃO DE **CONTRATOS INTELIGENTES EM BLOCKCHAINS**.

O QUE É O PARADIGMA ORIENTADO A CONTRATOS?

PARA **ENTENDER O PARADIGMA**, É PRECISO CONHECER O CONCEITO BÁSICO DE **BLOCKCHAIN**.

E O QUE É BLOCKCHAIN?

BLOCKCHAIN PODE SER CONSIDERADA, DE FORMA SIMPLIFICADA, COMO UM **BANCO DE DADOS DESCENTRALIZADO**.

E O QUE É BLOCKCHAIN?

DE FORMA MAIS ESPECÍFICA, UMA BLOCKCHAIN FUNCIONA COMO UM **LIVRO DE REGISTROS DESCENTRALIZADO**, ONDE QUALQUER **INFORMAÇÃO** NELA INCLUÍDA **NÃO PODE SER APAGADA OU MODIFICADA** NO FUTURO.

QUAL A IMPORTÂNCIA DAS BLOCKCHAINS?

A PRIMEIRA BLOCKCHAIN SURTIU **2009** COMO A TECNOLOGIA POR TRÁS DO FUNCIONAMENTO DO **BITCOIN** E É A **BASE** DE TODO ECOSISTEMA DE **CRIPTOMOEDAS** E TECNOLOGIAS RELACIONADAS (JOGOS PLAY-TO-EARN, NFTs, DeFi, etc).

QUAL A IMPORTÂNCIA DAS BLOCKCHAINS?

○ PRINCIPAL OBJETIVO DE UMA BLOCKCHAIN É SER CAPAZ DE ARMAZENAR **INFORMAÇÕES DE VALOR INTRÍNSECO** (NA MAIORIA DOS CASOS, **MONETÁRIO**) DE FORMA INViolÁVEL.

QUAL A IMPORTÂNCIA DAS BLOCKCHAINS?

PARA DAR SENTIDO AO ARMAZENAMENTO DE INFORMAÇÕES COM VALOR INTRÍNSECO, AS BLOCKCHAINS REPRESENTAM AS **ENTIDADES DETENTORAS DE ALGUMA INFORMAÇÃO DE VALOR COMO ENDEREÇOS.**

QUAL A IMPORTÂNCIA DAS BLOCKCHAINS?

MAIS DO QUE SIMPLEMENTE ARMAZENAR INFORMAÇÕES COM VALOR INTRÍNSECO, AS BLOCKCHAINS REGISTRAM O **HISTÓRICO DE TODAS AS TRANSAÇÕES** ENTRE ENTIDADES DETENTORAS DE INFORMAÇÕES DE VALOR.

QUAL A IMPORTÂNCIA DAS BLOCKCHAINS?

Pessoa 1



Pessoa 1 transfere 20 para Pessoa 2.

Pessoa 2



A blockchain armazena o valor associado a cada entidade,
pelo registro das transações.

QUAL A IMPORTÂNCIA DAS BLOCKCHAINS?

AS BLOCKCHAINS FUNCIONAM COMO UM **LIVRO DE REGISTROS DE UM CARTÓRIO**, ONDE A **PROPRIEDADE** DE UM DETERMINADO BEM É **RASTREADA** ATRAVÉS DE SUAS **TRANSAÇÕES**.

QUAL A IMPORTÂNCIA DAS BLOCKCHAINS?

DIFERENTEMENTE, DOS LIVROS-RAZÃO DE CARTÓRIOS CONVENCIONAIS, UMA BLOCKCHAIN **DISPENSA A EXISTÊNCIA DE UMA AUTORIDADE CENTRAL** PARA GARANTIR QUE AS TRANSAÇÕES SÃO REAIS E INVOLÁVEIS.

QUAL A IMPORTÂNCIA DAS BLOCKCHAINS?

AS BLOCKCHAINS CONSEGUEM GARANTIR A **INVIOLABILIDADE** DE SEUS DADOS ATRAVÉS DA COMBINAÇÃO DE CONCEITOS COMO **CRİPTOGRAFIA** E **PROTOCOLO DE CONSENSO**.

BITCOIN SCRIPT

QUANDO O BITCOIN FOI LANÇADO (JUNTAMENTE COM A SUA BLOCKCHAIN), ELE TROUXE CONSIGO O CONCEITO DE **BITCOIN SCRIPT**, COMO UMA **LINGUAGEM DE PROGRAMAÇÃO BASEADA EM PILHA.**

BITCOIN SCRIPT

○ BITCOIN SCRIPT FOI PROJETADO PARA PROVER **CONDIÇÕES DE PAGAMENTO** ENTRE ENDEREÇOS DA SUA BLOCKCHAIN, DERIVANDO-SE DAÍ OS CHAMADOS **CONTRATOS INTELIGENTES**.

BITCOIN SCRIPT

Pessoa 1



Pessoa 1 transfere 20 para Pessoa 2,
se a Pessoa 2 atender as seguintes condições...

Pessoa 2



A blockchain armazena o valor associado a cada entidade,
pelo registro das transações.

SOLIDITY

APESAR DA REVOLUÇÃO TRAZIDA PELO BITCOIN, FOI O **ETHEREUM** QUE POPULARIZOU O CONCEITO DE **CONTRATOS INTELIGENTES**.

SOLIDITY

○ ETHEREUM INTEGROU A SUA BLOCKCHAIN COM UMA MÁQUINA VIRTUAL CAPAZ DE EXECUTAR UMA **LINGUAGEM TURING COMPLETA**, CHAMADA DE **SOLIDITY**.

SOLIDITY

A SOLIDITY UTILIZA UMA **ESPECIALIZAÇÃO DO PARADIGMA ORIENTADO A OBJETOS**, UMA VEZ QUE ELE NÃO PERMITE A DECLARAÇÃO DE CLASSES GENERICAMENTE.

SOLIDITY

AO INVÉS DE PERMITIR A DECLARAÇÃO DE CLASSES GENERICAMENTE, A SOLIDITY
ESPECIALIZOU O CONCEITO DE CLASSES PARA CONTRATOS.

SOLIDITY

A BLOCKCHAIN DA ETHEREUM SUPORTA **DOIS TIPOS DE ENDEREÇOS: ENTIDADES EXTERNAS** (SIMILAR AO BITCOIN) E **CONTRATOS INTELIGENTES.**

SOLIDITY

UM **CONTRATO INTELIGENTE** PODE TER UMA INFORMAÇÃO DE **VALOR INTRÍNSECO ASSOCIADO** A ELE, ASSIM COMO ACONTECE COM UMA ENTIDADE EXTERNA.

O NOSSO PROJETO

ESTENDER A LINGUAGEM ORIENTADA A OBJETOS 1 PARA SUPORTAR ALGUMAS DAS PRINCIPAIS CARACTERÍSTICAS DO PARADIGMA ORIENTADO A CONTRATOS.

O NOSSO PROJETO

O FOCO SERÁ ADICIONAR FUNCIONALIDADES QUE ASSOCIEM ALGUMA **INFORMAÇÃO DE VALOR INTRÍNSECO** AOS **CONTRATOS INTELIGENTES E ENTIDADES EXTERNAS.**

O NOSSO PROJETO

UM **CONTRATO** DEVERÁ SER **DECLARADO** DE FORMA SIMILAR A UMA CLASSE, PORÉM FAZENDO USO DA PALAVRA-CHAVE **CONTRACT**.

O NOSSO PROJETO

TODO **CONTRATO** SERÁ **INSTANCIADO COM UM VALOR ASSOCIADO** A ELE (QUE PODE SER ZERO) VINDO DE ALGUMA **ENTIDADE EXTERNA** (USUÁRIO).

O NOSSO PROJETO

TODO **CONTRATO SERÁ INSTANCIADO** COM A EXIGÊNCIA DE **DOIS PARÂMETROS** (USUÁRIO E VALOR), NA SEGUINTE ORDEM: **NEW** NOME DO CONTRATO (USUÁRIO, VALOR);

O NOSSO PROJETO

UM **USUÁRIO** PODERÁ SER DECLARADO COMO UM **TIPO INTEIRO** DA LINGUAGEM E O SEU VALOR SERÁ O SEU SALDO.

O NOSSO PROJETO

UM **CONTRATO** PODERÁ TER DOIS TIPOS DE **ATRIBUTOS: NATIVOS E NÃO NATIVOS** (DEFINIDOS PELO USUÁRIO).

O NOSSO PROJETO

TODO **CONTRATO** TERÁ UM **ATRIBUTO** CHAMADO **BALANCE**, QUE ARMAZENARÁ O SEU SALDO.

O NOSSO PROJETO

UM **CONTRATO** PODERÁ TER DOIS TIPOS DE **MÉTODOS: NATIVOS E NÃO NATIVOS**
(**DEFINIDOS PELO USUÁRIO**).

O NOSSO PROJETO

OS **MÉTODOS** (NATIVOS E NÃO NATIVOS) SERÃO REPRESENTADOS COMO **PROCEDIMENTOS GENÉRICOS** E PODERÃO DEFINIDOS COMO PAGOS (**PAYABLE**) OU NÃO PAGOS (**PROC**).

O NOSSO PROJETO

UM MÉTODO PAGO (**PAYABLE**) HABILITARÁ O **ENVIO** DE ALGUM **VALOR PARA O CONTRATO**, JUNTAMENTE COM A SUA CHAMADA.

O NOSSO PROJETO

TODO **MÉTODO PAGO SERÁ CHAMADO** COM A EXIGÊNCIA DE **DOIS PARÂMETROS** (USUÁRIO E VALOR), NA SEGUINTE ORDEM: NOME DO MÉTODO (USUÁRIO, VALOR);

O NOSSO PROJETO

TODO CONTRATO TERÁ UM **MÉTODO NATIVO NÃO PAGO** CHAMADO **TRANSFER**(USUÁRIO, VALOR).

O NOSSO PROJETO

○ **MÉTODO TRANSFER IRÁ ENVIAR** UM DETERMINADO **VALOR PARA O USUÁRIO** PASSADO COMO PARÂMETRO (CASO O CONTRATO POSSUA TAL VALOR).

EXEMPLO DE USO DO PROJETO

```
VAR USUARIO = 100;
```

```
{ CONTRACT BANCO {
```

```
    PAYABLE DEPOSITAR() {
```

```
        // AQUI PODERIA SER DECLARADA ALGUMA FUNCIONALIDADE AO CONTRATO.
```

```
    } } };
```


EXEMPLO DE USO DO PROJETO

```
{ VAR BANCO = NEW BANCO(USUARIO, 25);  
BANCO.DEPOSITAR(USUÁRIO, 50);  
WRITE(USUARIO);  
WRITE(BANCO.BALANCE); }
```

GRAMÁTICA

$\langle \text{PROGRAMA} \rangle ::= \{ \langle \textbf{DECLARACAO} \rangle ; \langle \text{COMANDO} \rangle \}$

$\langle \text{DECLARACAO} \rangle ::= \langle \text{DECLASSE} \rangle \mid \langle \textbf{DecCONTRATO} \rangle$

.

.

.

GRAMÁTICA

$\langle \text{DECLASSE} \rangle ::= \text{"CLASSE"} \langle \text{ID} \rangle \text{"\{"} \langle \text{DECVARIABEL} \rangle \text{";"} \langle \text{DECPROCEDIMENTO} \rangle \text{"\}" } \mid$
 $\langle \text{DECLASSE} \rangle \text{","} \langle \text{DECLASSE} \rangle$

GRAMÁTICA

$\langle \text{DecContrato} \rangle ::= \text{"CONTRACT"} \langle \text{Id} \rangle \text{"{"} \langle \text{DecVariavel} \rangle \text{";"}$
 $\langle \text{DecProcedimentoGenerico} \rangle \text{"}" | \langle \text{DecContrato} \rangle \text{","} \langle \text{DecContrato} \rangle$

GRAMÁTICA

$\langle \mathbf{DecPROCEDIMENTOGENERICO} \rangle ::= \langle DecPROCEDIMENTO \rangle \mid \langle \mathbf{DecPAYABLE} \rangle \mid$
 $\langle DecPROCEDIMENTOGENERICO \rangle \text{ " , " } \langle DecPROCEDIMENTOGENERICO \rangle$

GRAMÁTICA

$\langle \text{DECPROCEDIMENTO} \rangle ::= \text{"PROC"} \langle \text{Id} \rangle \text{"("} \langle \text{LISTADECLARACAOPARAMETRO} \rangle \text{"}" \text{"{"}$
 $\langle \text{COMANDO} \rangle \text{"}"}$

GRAMÁTICA

$\langle \text{DecPAYABLE} \rangle ::= \text{"PAYABLE"} \langle \text{ID} \rangle "(" \langle \text{LISTADECLARACAOPARAMETRO} \rangle ")" \text{"\{"}$
 $\langle \text{COMANDO} \rangle \text{"\}"}$

DÚVIDAS?

The background is a blue gradient. In the corners, there are decorative white lines resembling circuit traces or a stylized network, with small circles at various points.

OBRIGADO!