Padrão ERC-20

O que é o padrão ERC-20?

- É um padrão específico para o Ethereum

- Padrões similares existem em outras blockchains
  - BEP-20: Binance
  - Solana SPL: Solana
  - Cardano Native Assets: Cardano
  - Polkadot DOT: Polkadot

ERC-20

Ethereum Request for Comment #20

Alguns exemplos de tokens ERC-20

Circle
USDC | Always-on dollars, internet speed | Circle

Seeklogo
Uniswap Logo PNG Vecto...

ERC-20

- Um padrão de contrato inteligente para Ethereum escrito em Solidity
- Já existem mais de 500 mil implementações de ERC-20 disponíveis no mercado

Cubix

Best Practices for Smart Contract Development

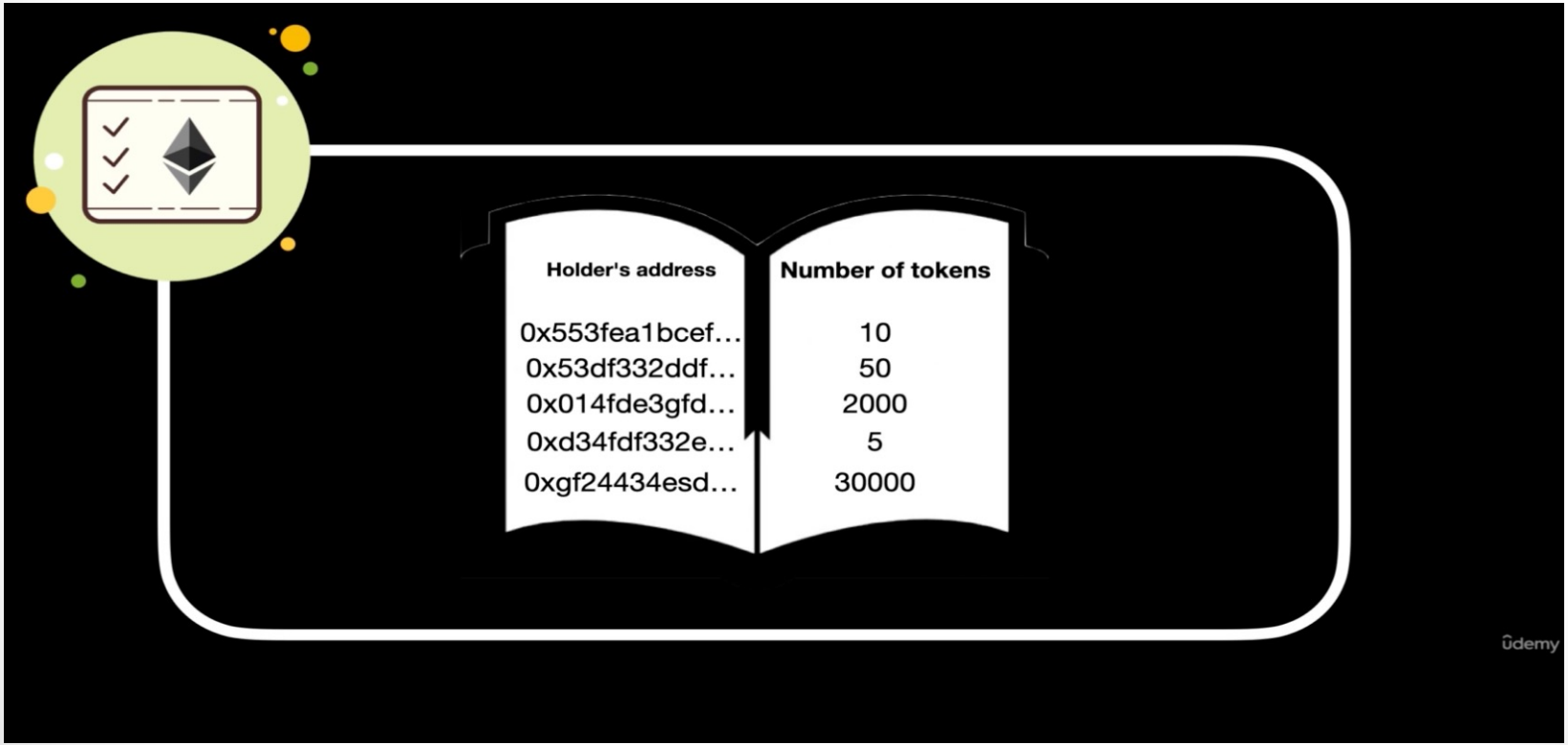
Facilita o trabalho dos desenvolvedores

- **Facilita o Desenvolvimento**: Seguir o padrão ERC-20 simplifica a criação de ativos digitais, economizando tempo e recursos no desenvolvimento de tokens personalizados.
- **Base Pré-Estabelecida**: Desenvolvedores podem utilizar um esboço de desenvolvimento já existente, evitando a necessidade de começar do zero.
- **Compatibilidade Garantida**: Os tokens ERC-20 são compatíveis com uma ampla variedade de softwares e serviços, como carteiras de criptomoedas e corretoras.

Facilita o trabalho dos desenvolvedores

- **Integração Fácil**: A padronização do ERC-20 torna a integração de tokens em aplicativos e serviços mais simples, promovendo sua adoção.
- **Maior Liquidez e Aceitação**: A facilidade de listagem em corretoras e uso em diversos casos de uso impulsiona a liquidez e a aceitação dos tokens ERC-20.
- **Personalização flexível**: Permite que desenvolvedores personalizem características e parâmetros para atender às suas necessidades específicas.

Tokens ERC-20 no livro-contábil



Transferência de tokens

Link para o ERC-20

- https://github.com/ethereum/ercs/blob/master/ERCS/erc-20.md

Constantes

string public constant name “jocoin”;

Nome da criptomoeda

Constantes

string public constant symbol = “JC”;

Símbolo da sua criptomoeda como BTC, ETH, SOL

Constantes

uint8 public constant decimal = 8;

- Números de casas decimais da sua criptomoeda
- O valor 8 significa que a sua criptomoeda pode ser dividido por 100000000
- Valor mínimo de 0,00000001 JC

Variáveis

uint256 totalSupply_;

O total de unidades de criptomoedas
Por exemplo, se totalSupply_ = 1.000.000 então haverá apenas 1 MI JC

Funções

construtor()

Função que será executado assim que a criptomoeda for instanciada

Funções

function totalSupply() public view returns (uint256)

- Função que retorna o total de unidades da criptomoeda
- No exemplo anterior, seria retornaria 1 MI

Funções

function balanceOf(address tokenOwner) public view returns (uint)

- Função que recebe endereço e fornece o saldo de tokens do endereço

Funções

function transfer(address tokenReceiver, uint numTokens) public returns (bool)

- Função que recebe o endereço do recipiente e o # de tokens a ser transferido

Funções

function approve(address delegate, uint numTokens) public returns (bool)

- Função que permite que A delegue ao “delegate” debitar numTokens de A
- Retorna true se sucesso e false do contrário

Funções

function allowance(address _owner, address _spender) public (uint256 remaining)

- Função que permite que receba dois endereços A e B
- Permite informar quantos tokens B pode debitar de A
- Retorna um valor positivo como 200

Funções

function transferFrom(address owner,address buyer, uint numTokens) public returns (bool)

- Função que permite que A compre tokens de owner para buyer
- Pode ser chamada várias vezes
- Retorna true se deu certo e false do contrário

Funções

function transferFrom(address owner,address buyer, uint numTokens) public returns (bool)

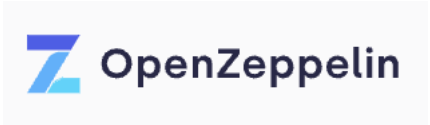
- Função que permite que A compre tokens de owner para buyer
- Pode ser chamada várias vezes
- Retorna true se deu certo e false do contrário

Outros

- Eventos
- Mappings

Vantagens com o ERC-20

- Transferência de tokens de uma conta para outra
- Cálculo do saldo de tokens de uma determinada conta
- Computação do total de tokens disponível na rede (p.ex., jocoin 1e6)
- Formalização que uma conta de terceira parte use um determinado números de tokens de outra conta



ERC-20 com OpenZeppelin

O que é?

- É uma empresa de segurança em criptomoedas que provê um framework de código aberto
- O framework permite construir contratos inteligentes seguros e implementa auditorias de segurança
- Seus clientes incluem a Ethereum Foundation, Coinbase e a carteira Brave

- Com o OpenZeppelin, os desenvolvedores podem se preocupar mais com o desenvolvimento e menos com a segurança
- Um recurso importante para os sistema de DE-FI

Módulos do OpenZeppelin

Monitor (Mitigação)

- Obtém um mapa de riscos do contrato inteligente para detectar possíveis falhas
- Detecte ameaças, receba alertas sobre ameaças e anomalias
- Responde e resolver problemas automaticamente

Tratador de Incidentes (Prevenção)

- Trata ameaças e ataques com ações predefinidas
- Conduz simulações de ataque nos contratos
- Realiza testes de ataques existentes em uma rede separada

Usando o Openzeppelin

- Visualizar o código no link abaixo:

https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC20/ERC20.sol

- Construir um contrato com OpenZeppelin e o ERC-20

https://docs.openzeppelin.com/contracts/5.x/erc20

```
// contracts/GLDToken.sol
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

import {ERC20} from "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract GLDToken is ERC20 {
    constructor(uint256 initialSupply) ERC20("Gold", "GLD") {
        _mint(msg.sender, initialSupply);
    }
}
```

Outro padrão: ERC-721

Fungível e Não-fungível

Mercado Bitcoin
NFTs revolucionando o mercado de colecion...

- "Fungível" significa "intercambiável" e "substituível"
- O Bitcoin (BTC) é fungível, pois qualquer unidade de Bitcoin pode ser substituída por outra
- Por outro lado, cada NFT (Token Não Fungível) é totalmente único
- Um NFT não pode ser substituído por outro devido à sua singularidade

Padrão ERC-721

- O padrão usado para tokens de NFTs no Ethereum
- Também conta com o suporte da OpenZeppelin
- Permite criar tokens únicos para armazenar arte, música e vídeo

- O ERC-20 é voltado para tokens de criptomoedas
- O ERC-721 é para tokens não fungíveis enquanto que o ERC-20 para os fungíveis

Perguntas ??