SOLIDITY

Teoría del Lenguaje - 1C 2021

Carbón Posse, Ana Sofía

Frutos Ramos, Constanza M.

Goijman, Lautaro

Karagoz, Filyan

SOLIDITY

- PROPUESTO EN AGOSTO DEL 2014 POR GAVIN WOOD.
- ES UN LENGUAJE DE ALTO NIVEL ORIENTADO A CONTRATOS.
- SINTAXIS SIMILAR A LA DE JAVASCRIPT.
- ES USADO PARA PROGRAMAR SMART CONTRACTS PARA LA BLOCKCHAIN DE ETHEREUM, QUE SERÁN EJECUTADOS POR LA MÁQUINA VIRTUAL DE ETHEREUM (EVM).

ANTES DE VER CÓDIGO, VEAMOS ALGUNAS DEFINICIONES IMPORTANTES...

BLOCKCHAIN

ES UN SISTEMA PARA GUARDAR INFORMACIÓN DE MANERA QUE SEA DIFÍCIL O IMPOSIBLE DE CAMBIAR, HACKEAR O ENGAÑAR AL SISTEMA.

GUARDA TODAS LAS TRANSACCIONES REALIZADAS EN LA MISMA, DISTRIBUIDOS EN VARIOS NODOS DE UNA RED.

SMART CONTRACTS

- ES UN TIPO ESPECIAL DE INSTRUCCIONES QUE ES ALMACENADA EN LA BLOCKCHAIN.
- TIENE LA CAPACIDAD DE AUTO-EJECUTAR ACCIONES DE ACUERDO A UNA SERIE DE PARÁMETROS YA PROGRAMADOS.
- TODO ESTO DE FORMA INMUTABLE, TRANSPARENTE Y SEGURA.

TOKEN

- ES UN SMART CONTRACT QUE SIGUE UNA SERIE DE REGLAS COMUNES.
- IMPLEMENTA UN CONJUNTO ESTÁNDAR DE FUNCIONES QUE COMPARTEN EL RESTO DE LOS TOKENS.
- HAY DISTINTOS ESTANDARES DE TOKENS.

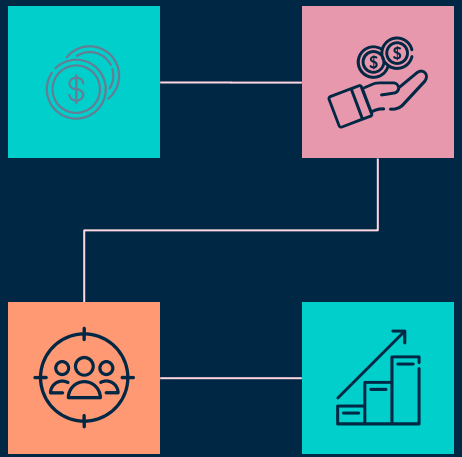
TOKENS Y ESTANDARES

TOKEN

SON BIENES DIGITALES QUE SE CONSTRUYEN SOBRE ETHEREUM.

ESTANDAR

SERIE DE MÉTODOS QUE DEFINEN UNA INTERFAZ QUE PUEDE SER USADA POR CUALQUIERA.



ERC-20

ESTÁNDAR USADO PARA MONEDAS (COMO NUESTROS OZT)

ERC-721

ESTÁNDAR USADO PARA NFTs (COMO NUESTRAS CARTAS)

ESTÁNDAR DE LOS TOKENS USADOS - REQUISITOS

ERC-20

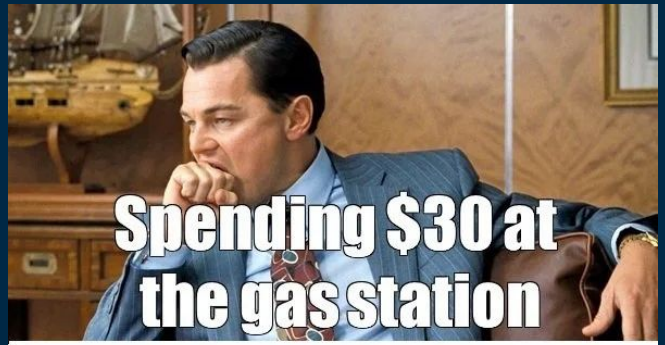
NOMBRE O IDENTIFICADOR
SIMBOLO ASOCIADO
DECIMALES
SUMINISTRO TOTAL
SALDO EN CUENTA
TRANSFERIR
TRANSFERIR DESDE
APROBAR RETIRO DE FONDOS
SUBVENCION
LOS EVENTOS TRANSFER Y APPROVAL

ERC-721

DECIDIR QUIÉN ES EL DUEÑO
COMO CREARLO
TRANSFERENCIA
COMO SE "QUEMAN"

GAS

- COMBUSTIBLE QUE MUEVEN LAS DAPPS DE ETHEREUM.
- LOS USUARIOS DEBEN PAGAR CADA VEZ QUE EJECUTAN UNA FUNCIÓN DE LA DAPP.
- LA CANTIDAD A PAGAR DEPENDE DE LA COMPLEJIDAD DE LA FUNCIÓN.
- EL GAS ES NECESARIO PARA EVITAR QUE UNA DAPP ACAPARE UNA RED.



AHORRO DE GAS

- EMPAQUETAR EN STRUCTS
- USAR MODIFICADORES EN LAS FUNCIONES COMO “VIEW” O “PURE”.

DEPLOY

- SUBIR UN CONTRATO A LA RED.
- UNA VEZ QUE SE ENCUENTRA EN LA MAINNET, ESTA QUEDA EN LA RED PARA SIEMPRE.
- PARA DESARROLLAR UN CONTRATO Y PODER PROBARLO DE MANERA LOCAL HAY HERRAMIENTAS COMO TRUFFLE Y GANACHE.

AHORA SI!
VAMOS AL CÓDIGO !!

LINKS ÚTILES

DOCUMENTACION OFICIAL

Dapp UNIVERSITY

TUTORIALES - CRYPTO ZOMBIES

TODO SOBRE NFT

OPEN ZEPPELIN

TOKENS

ERC-20