03 ERC4626

Vault

- 资产的管理、分红
- 用户充值某项资产，获取某个凭证
- 该凭证作为分红、退出的依据
- Yield Farming/借贷/质押等

投票 最多可选1项

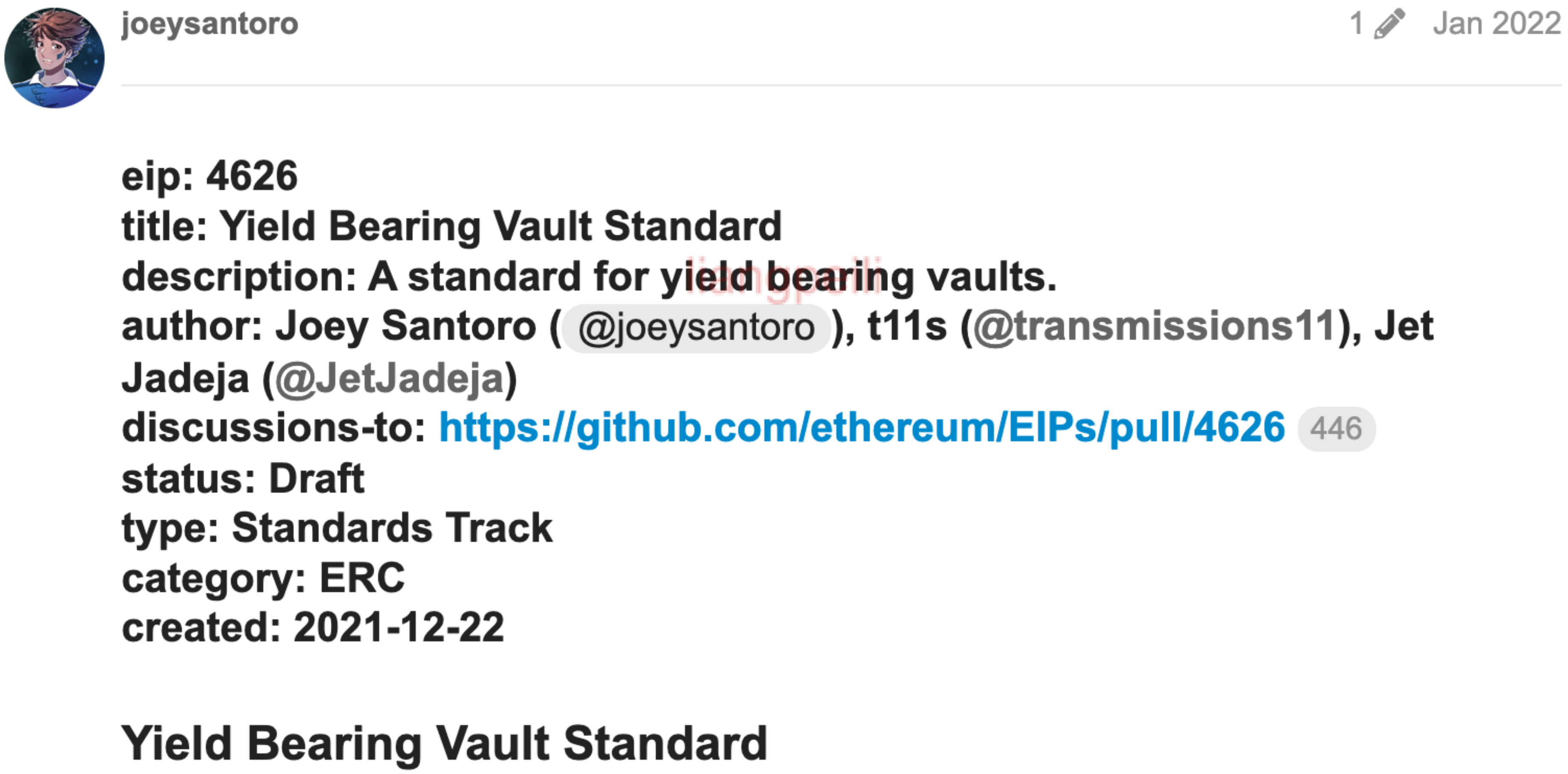
设置

刚刚实现的这个 Vault 合约，自身是否满足ERC20标准？

- A 符合
- B 不符合

提交

ERC4626 的诞生



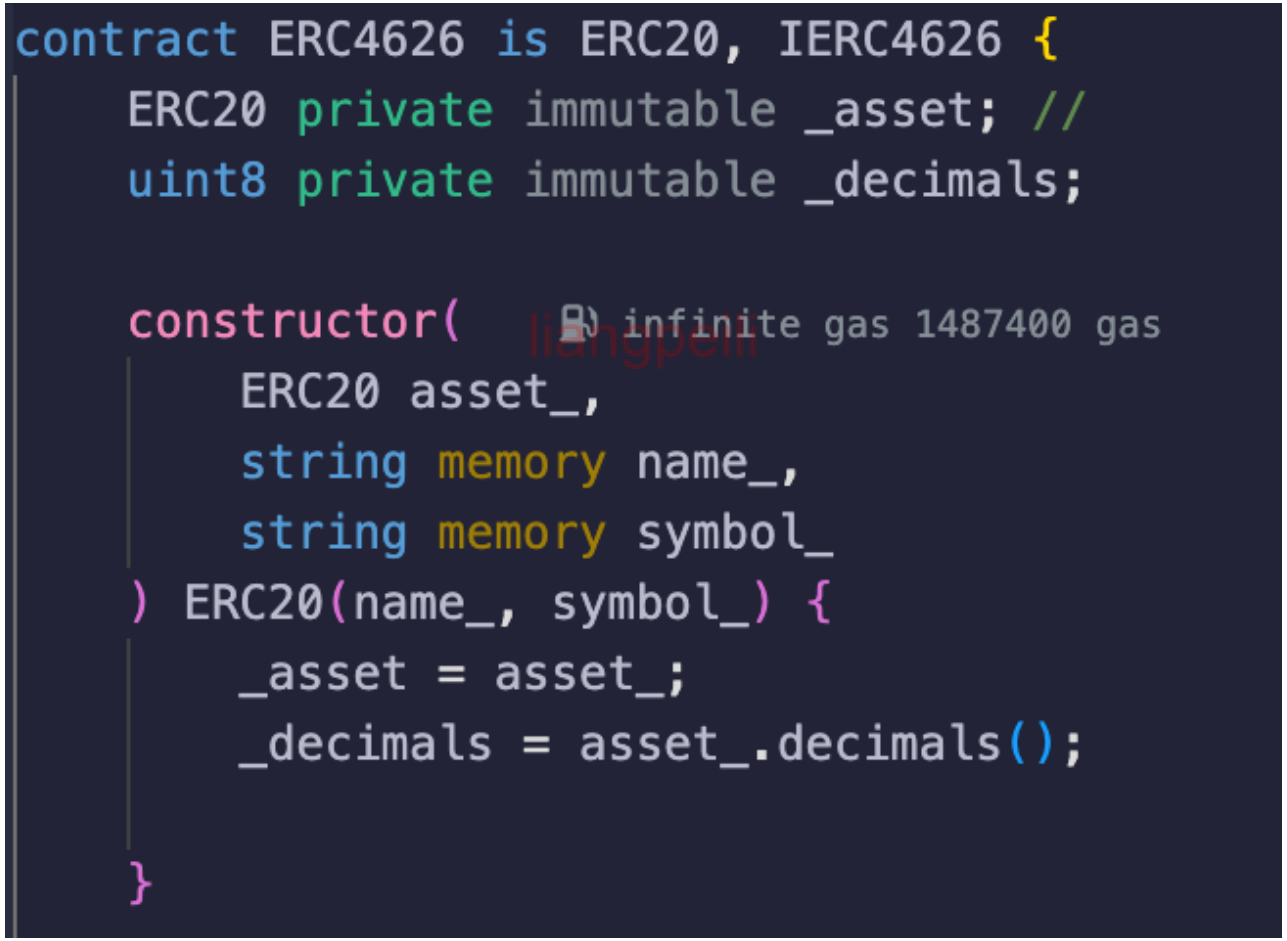
joeysantoro

1 ✎ Jan 2022

eip: 4626
title: Yield Bearing Vault Standard
description: A standard for yield bearing vaults.
author: Joey Santoro (@joeysantoro), t11s (@transmissions11), Jet Jadeja (@JetJadeja)
discussions-to: https://github.com/ethereum/EIPs/pull/4626 446
status: Draft
type: Standards Track
category: ERC
created: 2021-12-22

Yield Bearing Vault Standard

ERC4626 继承 ERC20



```
contract ERC4626 is ERC20, IERC4626 {
    ERC20 private immutable _asset; //
    uint8 private immutable _decimals;

    constructor(    infinite gas 1487400 gas
        ERC20 asset_,
        string memory name_,
        string memory symbol_
    ) ERC20(name_, symbol_) {
        _asset = asset_;
        _decimals = asset_.decimals();

    }
```

ERC4626 assets & shares

返回金库的基础资产代币地址：

- function asset() external view returns (address assetTokenAddress);

返回金库管理的基础代币总额：

- function totalAssets() external view returns (uint256 totalManagedAssets);

数量估计

- function convertToShares(uint256 assets) external view returns (uint256 shares);
- function convertToAssets(uint256 shares) external view returns (uint256 assets);

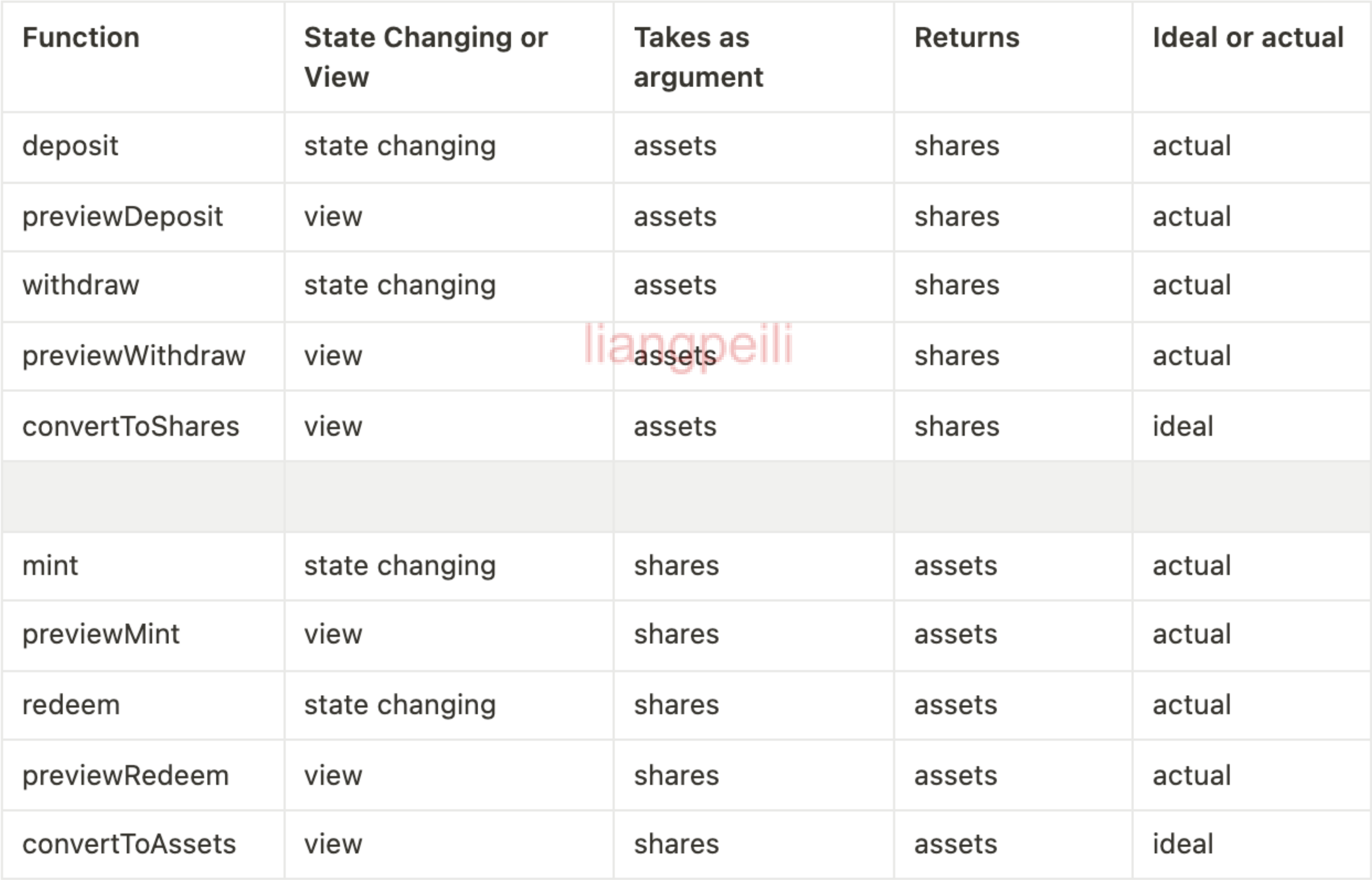
充值资产， 获取 shares

- function maxDeposit(address receiver) external view returns (uint256 maxAssets);
- function previewDeposit(uint256 assets) external view returns (uint256 shares);
- function deposit(uint256 assets, address receiver) external returns (uint256 shares);
- function maxMint(address receiver) external view returns (uint256 maxShares);
- function previewMint(uint256 shares) external view returns (uint256 assets);
- function mint(uint256 shares, address receiver) external returns (uint256 assets);

返还 shares，拿回资产

- function maxWithdraw(address owner) external view returns (uint256 maxAssets);
- function previewWithdraw(uint256 assets) external view returns (uint256 shares);
- function withdraw(uint256 assets, address receiver, address owner) external returns (uint256 shares);
- function maxRedeem(address owner) external view returns (uint256 maxShares);
- function previewRedeem(uint256 shares) external view returns (uint256 assets);
- function redeem(uint256 shares, address receiver, address owner) external returns (uint256 assets);

方法总结



Function	State Changing or View	Takes as argument	Returns	Ideal or actual
deposit	state changing	assets	shares	actual
previewDeposit	view	assets	shares	actual
withdraw	state changing	assets	shares	actual
previewWithdraw	view	assets	shares	actual
convertToShares	view	assets	shares	ideal
mint	state changing	shares	assets	actual
previewMint	view	shares	assets	actual
redeem	state changing	shares	assets	actual
previewRedeem	view	shares	assets	actual
convertToAssets	view	shares	assets	ideal

两个事件

- event Deposit(address indexed sender, address indexed owner, uint256 assets, uint256 shares);
- event Withdraw(

  ```
          address indexed sender,
          address indexed receiver,
          address indexed owner,
          uint256 assets,
          uint256 shares
    );
  ```

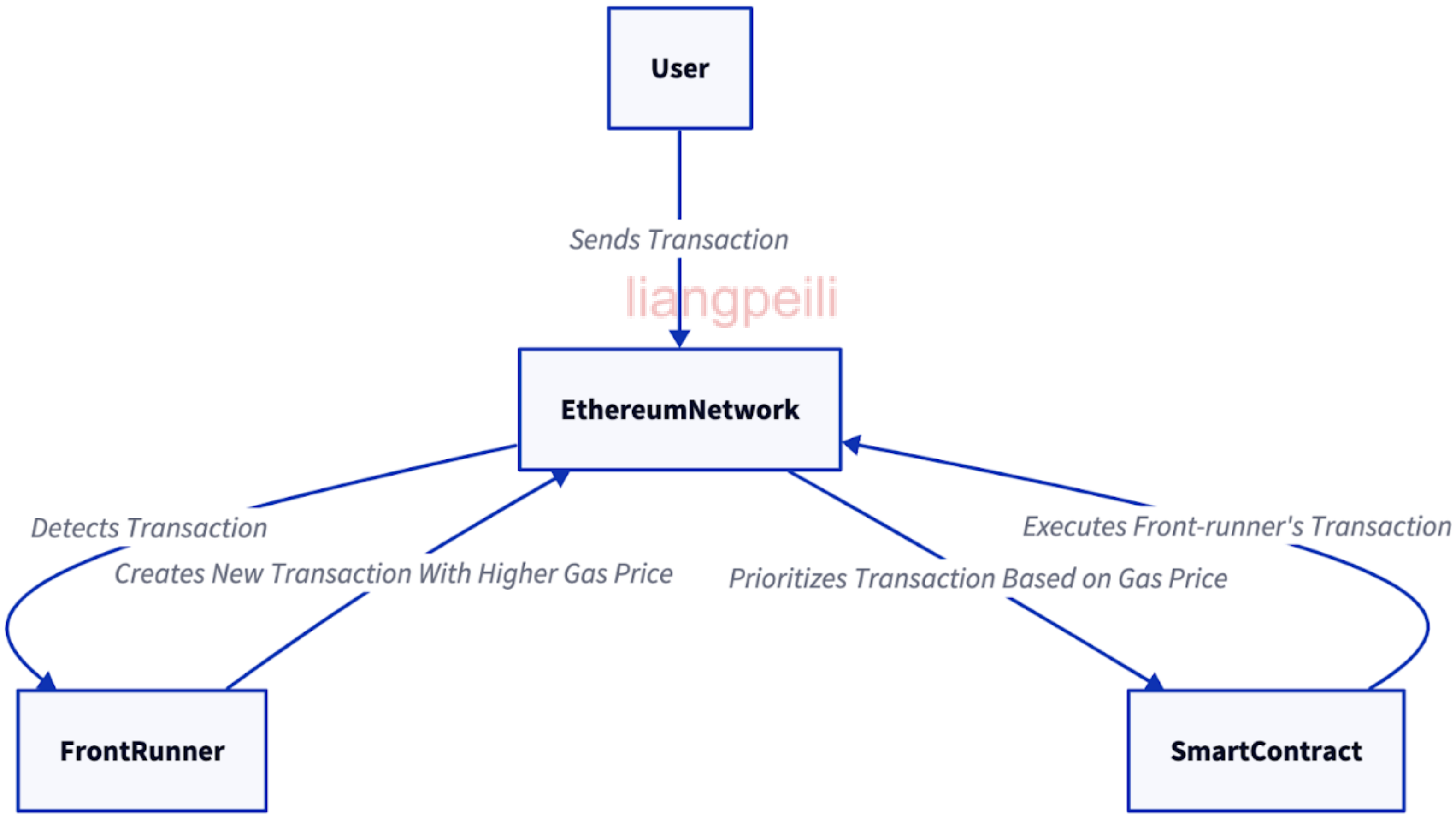
主观题 1分

设置

在 withdraw 操作中，如果 msg.sender != owner，那么 msg.sender 需要先请 owner 调用什么方法，才可以让 msg.sender 来 withdraw 成功？

作答

Front-Running


User
Sends Transaction
EthereumNetwork
Detects Transaction
Creates New Transaction With Higher Gas Price
Prioritizes Transaction Based on Gas Price
Executes Front-runner's Transaction First
FrontRunner
SmartContract

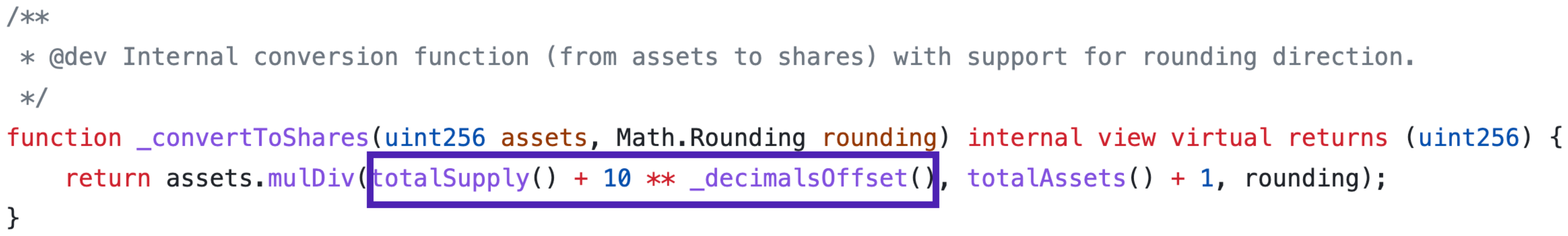
ERC4626 inflation attack

assets_deposited = 1,000

totalSupply() = 1,000

totalAssets() = 1000,000

shares_received = assets_deposited * totalSupply() / totalAssets();



```
/**
 * @dev Internal conversion function (from assets to shares) with support for rounding direction.
 */
function _convertToShares(uint256 assets, Math.Rounding rounding) internal view virtual returns (uint256) {
    return assets.mulDiv(totalSupply() + 10 ** _decimalsOffset(), totalAssets() + 1, rounding);
}
```

参考资料

- EIP-4626: Yield Bearing Vault Standard - EIPs - Fellowship of Ethereum Magicians (ethereum-magicians.org)
- ERC-4626: Tokenized Vaults (ethereum.org)
- ERC-4626 Tokenized Vault Standard | ethereum.org
- openzeppelin-contracts/contracts/interfaces/IERC4626.sol at master · OpenZeppelin/openzeppelin-contracts (github.com)
- ERC4626 Interface Explained (rareskills.io)
- WTF-Solidity/51_ERC4626/readme.md at main · AmazingAng/WTF-Solidity (github.com)
- How to Use ERC-4626 with Your Smart Contract | QuickNode
- ERC4626 Vault Smart Contract tutorial | DeFi Vault tutorial (youtube.com)