L0学习梳理

##学习目标

1.对区块链有简单的认识

2.对智能合约有简单的认识

3.配置好开发环境，熟悉开发过程中用到的概念如钱包，测试网，浏览器，faucet(水龙头)，gas 等

4.熟悉智能合约开发过程中用到常见库和开发工具，remix,hardhat,openzepplin 等

"openzepplin': Unknown word.

##什么是智能合约？

智能合约是一种运行在区块链上的自动化程序，能够在满足特定条件时自动执行预先定义的操作。它的特点包括：

去中心化：运行在区块链上，无需依赖第三方。

不可篡改：一旦部署，代码无法被修改。

透明性：所有操作和规则对参与者可见。

自动化：自动执行，无需人工干预。

智能合约的用途非常广泛，包括去中心化金融（DeFi）、非同质化代币（NFT）、供应链管理、投票系统等。

##什么是区块链

区块链是一种去中心化的分布式账本技术，用于记录和验证交易或数据。能够通过加密手段确保数据的透明性和不可篡改性。

-去中心化 分布式账本

-不可篡改的

-透明性 所有交易记录对网络中的参与者可见，提高了信任度。

-安全性：共识机制（如 PoW、PoS）

智能合约是区块链技术中一种重要的应用形式。

##区块链是如何工作的

-创建交易

-通过共识做一个验证，代表性的：pow、pos，

**Proof of Work (工作量证明)**

是一种区块链网络中使用的共识机制，用于验证交易和生成新的区块。它的核心思想是要求参与者（通常称为“矿工”）完成一定量的计算工作，以证明其投入了资源和努力，从而获得记账权和奖励。最具代表性的就是BTC。

**Proof of Stake（权益证明）**

在区块链和加密货币领域，POS 是一种共识机制，用户通过持有并“抵押”代币来参与网络的验证和记账，从而获得奖励。

以太坊的原生代币是 **ETH**，用于支付交易费用（Gas）和参与网络治理。最初使用 **Proof of Work (PoW)**，但自 2022 年起转向 **Proof of Stake (PoS)**，以降低能源消耗。

-新区块的创建，将验证的交易打包进区块

-链接区块

##应用场景

-加密货币（比特币、以太坊）

-智能合约，部署到链上以后，自动执行，无需信任的协议

-defi，数字资产：nft

-供应链管理

##以太坊和智能合约

-智能合约平台

-ETH（以太币是以太坊中的一种加密货币）

-通过我们设计的EVM和智能合约所带来的可编程性。

以太坊的核心是 EVM（Ethereum Virtual Machine太坊虚拟机

），它是一个全球分布的计算引擎，负责执行智能合约代码。

##demo

-hardhat