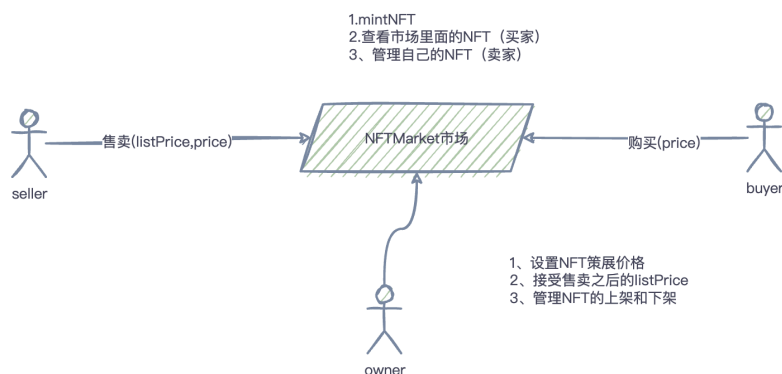


# 下半节

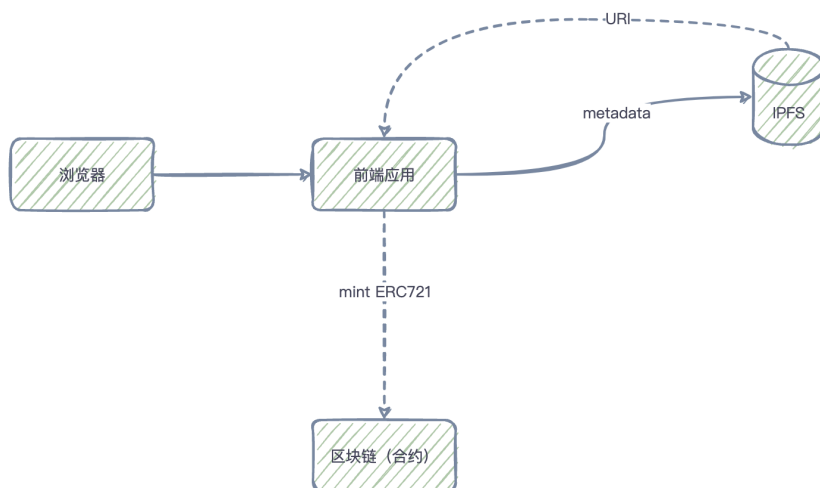
## NFTMARKET市场

### 1、NFTMARKET的主要流程



### 2、NFTMARKET的代码走读

- (1) 重点讲解listPrice，因为这里容易让人误解，卖家需要在创建token的时候支付足够的listPrice给合约，由合约进行保管
- (2) 在售出NFT之后，合约上的listPrice才会支付给策展人



### 3、NFTMARKET的简历包装

#### 项目涉及的主要技术栈：

合约：Solidity, ERC721, OpenZeppelin 前端：React, ethers.js, 服务端：firebase, IPFS (pinata) 其他：Hardhat Alchemy

## 业务内容：

创建和管理NFT市场平台，允许用户创建、交易NFT。

允许用户用加密货币进行交易。

提供基于区块链的NFT鉴定功能，确保NFT的唯一性和所有权

## 负责内容(简历描述参考)：

负责NFT合约的设计、开发和部署，确保合约功能符合市场需求，并通过单元测试确保合约的安全性。使用openzeppelin确保合约实现符合行业开发标准 使用React开发用户界面，确保平台操作简单、直观。集成ethers.js与智能合约的交互，支持用户进行NFT的购买、出售等操作。使用IPFS进行NFT元数据的存储，并提供元数据管理功能。项目使用firebase部署、合约使用alchemy部署

## VOTING

### 1、VOTING的主要流程

注意一个点：

部署合约的用户才是管理员，才能够创建候选人和投票人，只有投票人才能投票。所以需要先切换到66账号创建候选人和投票

### 2、VOTING的代码走读

VOTING的代码比较简单，主要体现了所有存储和业务逻辑都存放在合约上的概念。


### 3、VOTING的展开

目前版本的Voting还比较粗糙，存在Griefing漏洞，因为区块链是完全透明的，所以攻击者可以通过抢跑来干扰项目进行，如何实现盲投？

这是可以用Commit-Reveal模式


#### Commit-Reveal scheme in Solidity

What is it?

 <https://medium.com/coinmonks/commit-reveal-scheme-in-solidity-c06eba4091bb>

#### RareSkills Solidity Interview Question #39 Answered: What is a commit-reveal scheme and when would...

This series will provide answers to the list of Solidity interview questions that were published by RareSkills..

 <https://medium.com/coinmonks/rarekills-solidity-interview-question-39-answered-what-is-a-commit-reveal-scheme-and-when-would-083cfd3cc24d>

