一个简单的基于 Openzeppelin

可升级框架彩票智能合约 DAPP

By 谢跃书 2021/3/29

https://github.com/xieyueshu/Lottery

一、需求分析：

a) 完成大致结构框架 Openzeppelin 可升级智能合约：

i. 根据 Openzeppelin 框架原理，通过 Openzeppelin 插件来发布可升级智能合约即可。需要注意的是，1 可升级智能合约不可以有 constructor，2 智能合约在后续升级只能增加存储变量，并且变量只能放在旧版本变量下面增加。

b) 具体功能

完成一个简单的彩票

4 个兑奖数字

兑奖组合

4 个数字全部顺序符合

3 个数字顺序符合

传统的彩票机制是按照每期来进行，用户在某期时间段内下注，庄家最后开奖，中奖用户分享池内的资金。用户持凭证兑奖。按照此方案开发的话，系统复杂度较高。

而简单的区块链彩票玩法是一次下注实现下注、开奖和兑奖的功能。简单的方案可能存在随机数安全问题。

这里采用简单的彩票玩法。首先，4 位数的组合，假设数字可以重复，例如 0011，1233，2244 都是合法的彩票数字；

每个用户 address 只能下一注，每注金额 1ETH；

合约系统生成随机四位数；

用户如果 4 个数字全部顺序符合，则中一等奖成功匹配，则获得资金池中最多不超过 500ETH；

用户如果 3 个数字顺序符合的，则二等奖成功匹配，则获得资金池中最多不超过 5ETH；

不中奖的资金滚入资金池。

c) Web3.js 的一个简单 React 的兑奖页面

通过 h5 网页方式调用 web3.js 库，使用 React 框架来实现与以太坊区块链节点 rpc 通讯调用智能合约，下注和查看结果。

包括可以查看下注是否成功；查看开奖结果；

为了简化功能，使用时不可以离开当前页面，避免前端数据丢失无法查询下注，及开奖结果。

二、方案及架构

a) 可采用 Hardhat 开发工具协助开发；轻松支持 Web3.js、Ethers.js 插件, OpenZeppelin 可升级智能合约插件等。由于 Ethers.js 是 Web3.js 的一个简化版，本方案采用 Ethers.js 作为 Web3.js 与区块链节点 rpc 交互。

b) 为了加速开发进度，引用网上开源项目。这里引入一个 Hardhat 相关的开源项目《https://github.com/nomiclabs/hardhat-hackathon-boilerplate》作为本 example 的一个项目框架。其中包含 hardhat 工具及相关测试框架和 ethers.js，及一个 Create-React-App 前端代码；在其基础上可以很容易引入 Openzeppelin 插件。

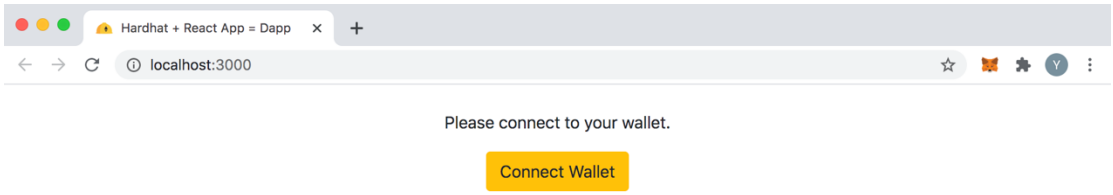
c) 合约中数据存储主要包括：storage 存储资金池数量、parameter 用户输入下注号码、memory 系统自动生成随机号码、event 输出用户开奖结果；

d) 系统自动生成随机码方法设计：
通过区块时间戳哈希，对其求模（10000）得出中奖号码。

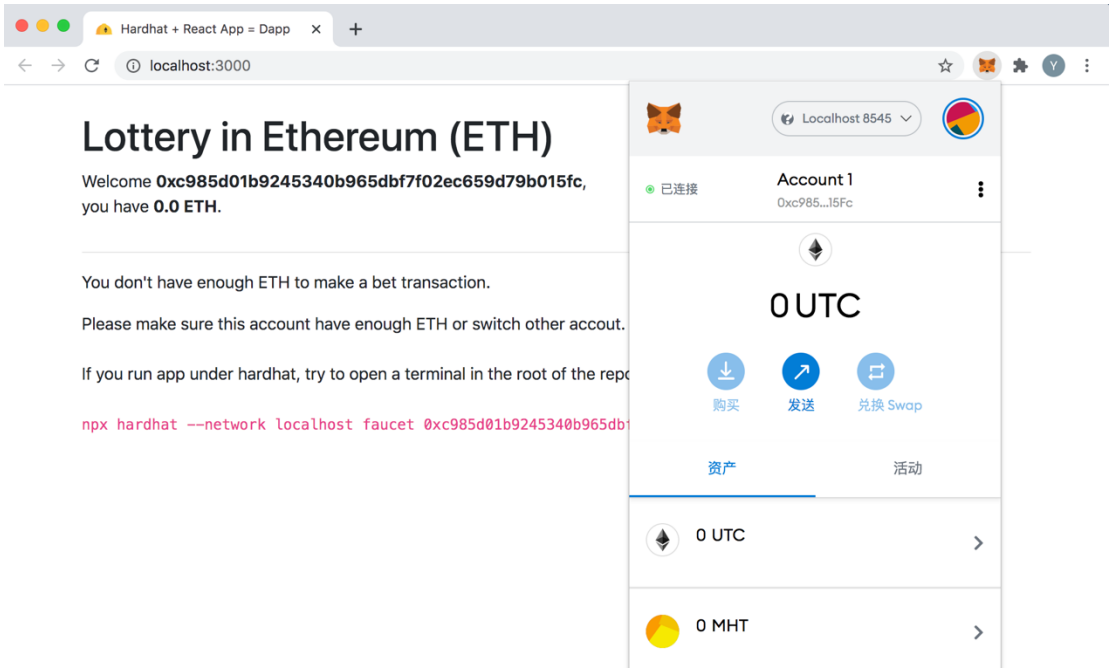
e) 其他，先以功能实现为主，暂时不考虑内存溢出，攻击等安全问题。

三、功能界面

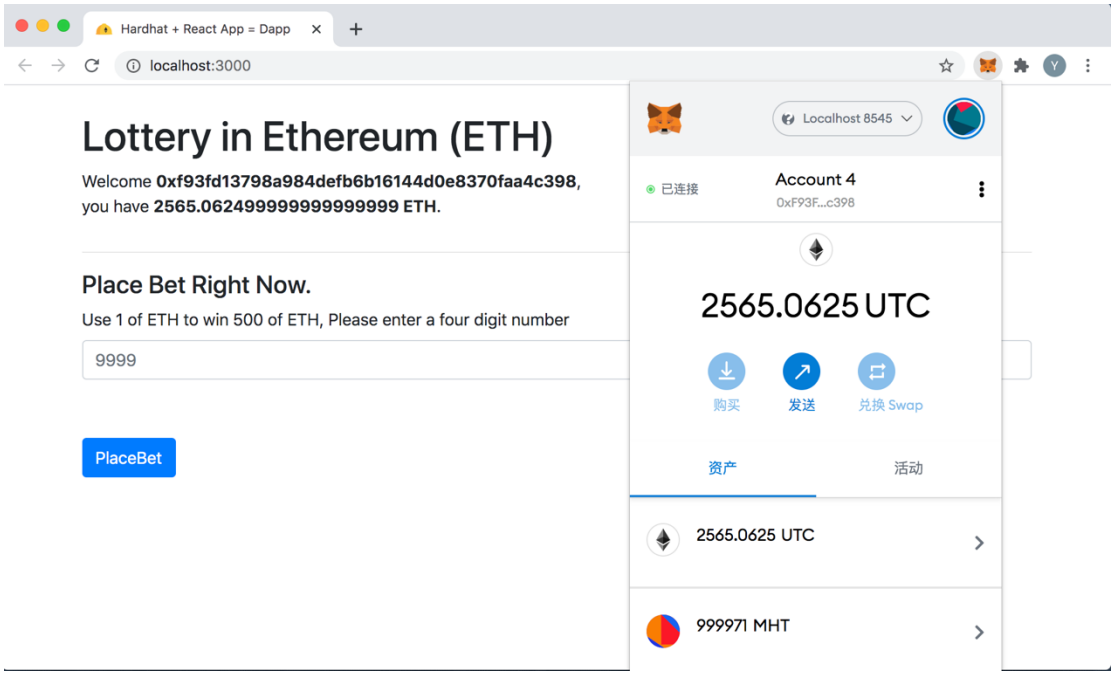
提示用户连接 metaMask 钱包



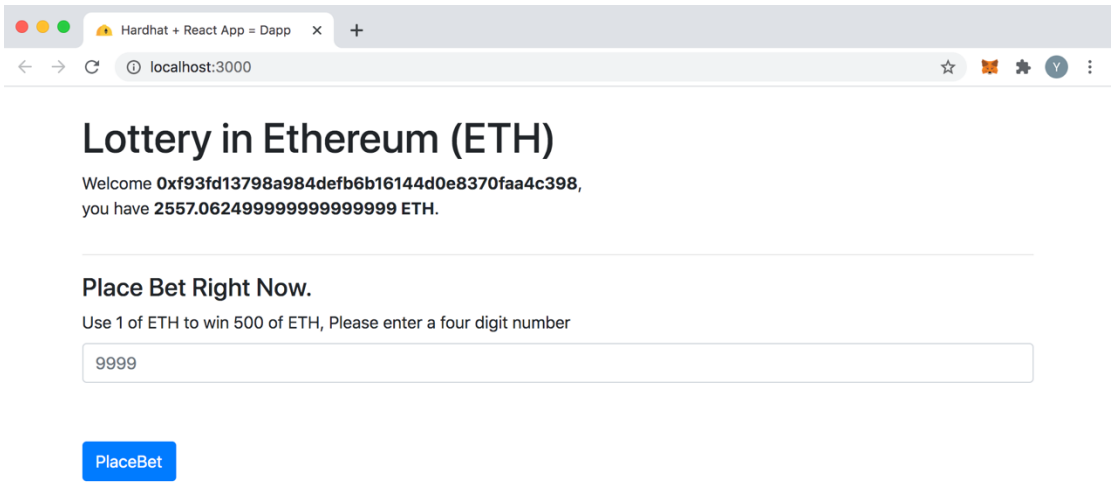
如果钱包余额不足 1ETH 则提示



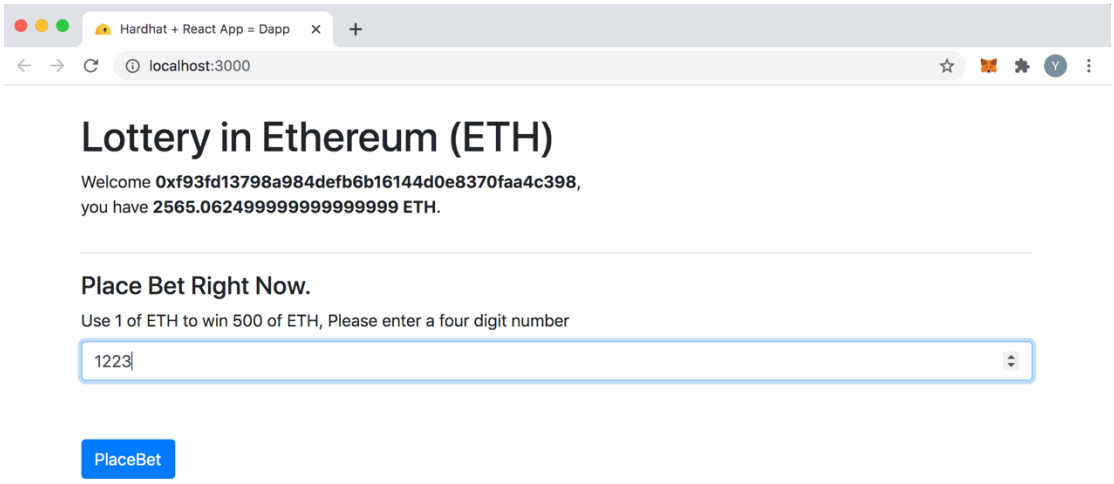
余额充足的界面



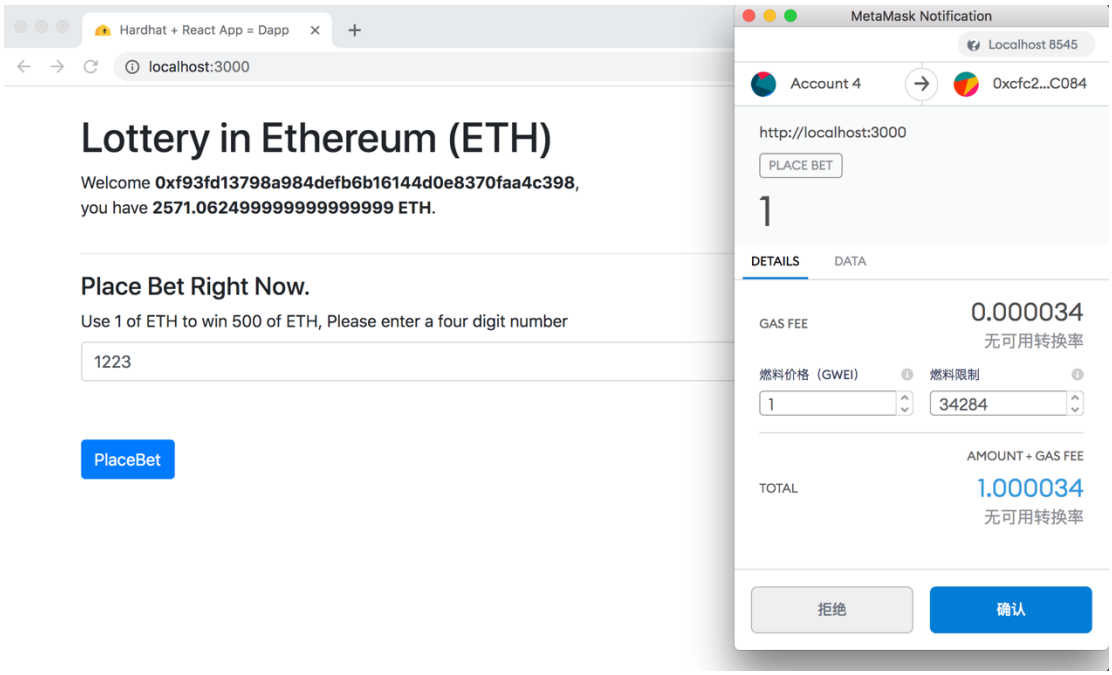
显示下注界面



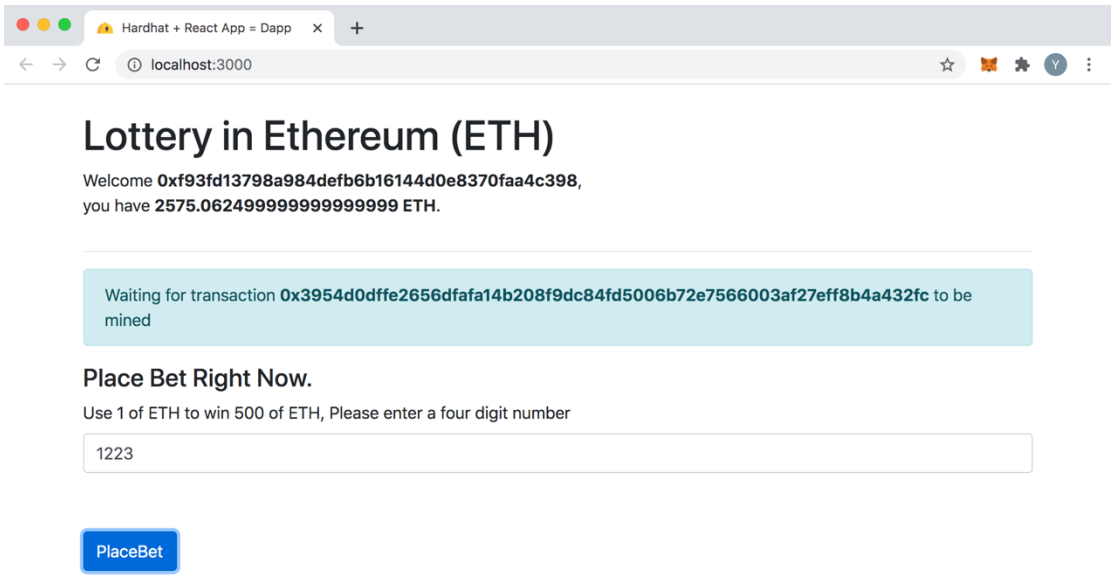
用户输入 4 位数字



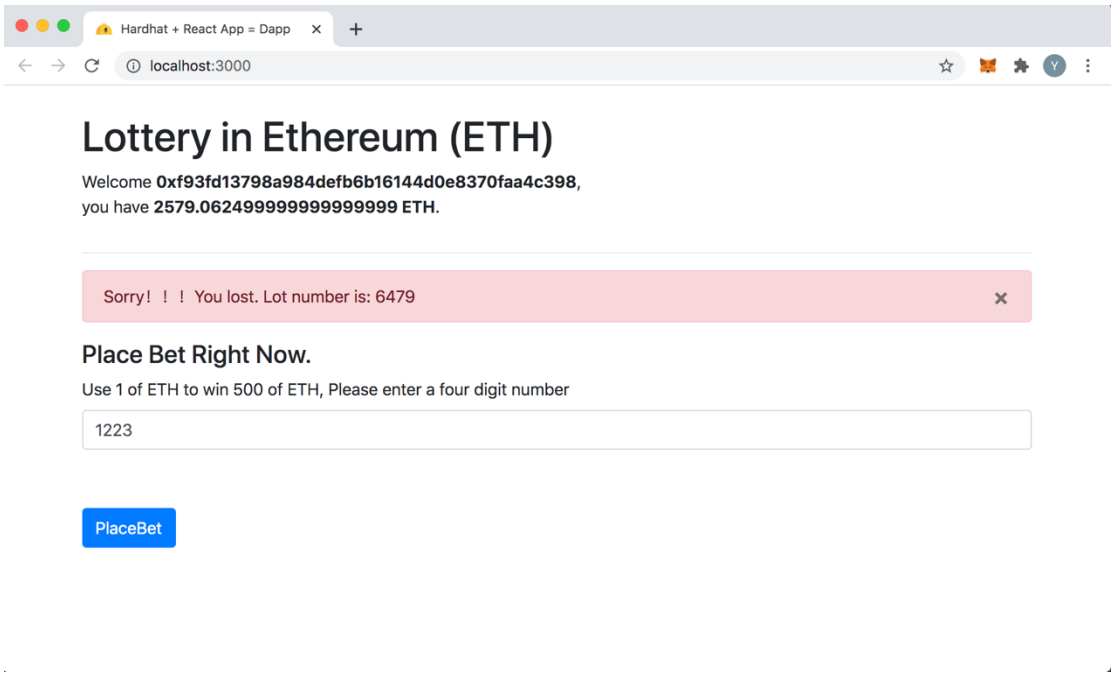
调用 metaMask 钱包



等待交易打包


Hardhat + React App = Dapp
localhost:3000
Lottery in Ethereum (ETH)
Welcome 0xf93fd13798a984defb6b16144d0e8370faa4c398,
you have 2575.062499999999999999 ETH.
Waiting for transaction 0x3954d0dffe2656dfafa14b208f9dc84fd5006b72e7566003af27eff8b4a432fc to be mined
Place Bet Right Now.
Use 1 of ETH to win 500 of ETH, Please enter a four digit number
1223
PlaceBet

显示中奖结果


Hardhat + React App = Dapp
localhost:3000
Lottery in Ethereum (ETH)
Welcome 0xf93fd13798a984defb6b16144d0e8370faa4c398,
you have 2579.062499999999999999 ETH.
Sorry！！！ You lost. Lot number is: 6479
Place Bet Right Now.
Use 1 of ETH to win 500 of ETH, Please enter a four digit number
1223
PlaceBet