

03-第三节 WETH 合约

实验目的

- 掌握 Wrapped ETH 的实现原理；
- 给Wrapped ETH 合约增加简单的功能。

实验环境

- Chrome/Microsoft Edge等浏览器；
- MetaMask 插件钱包；
- Remix IDE: <https://remix.ethereum.org/>;
- CBI 教学测试链 (RPC: <http://210.41.225.34:8502>, Chain ID: 1331, Currency Symbol: CBI) ；
- CBI 教学测试链代币领取平台 (<http://210.41.225.34:9999/>)

备注：CBI 教学测试链仅能在校内访问，校外同学可以使用本地环境。CBI 教学测试链和本地环境二选一配置即可。

实验内容

1. 提前准备好三个账户A、账户B和账户C，都要持有CBI测试币（或者使用本地账户）；
2. 使用账户A部署WETH合约；
3. 使用账户A调用合约的deposit方法，充值1个平台币；
4. 查询账户A的WETH余额；

5. 使用账户A对账户B进行approve操作；
6. 使用账户B调用合约的transferFrom方法，转账0.5个WETH到账户C；
7. 使用账户C调用合约的withdraw方法，提取0.5个WETH到自己账户；
8. 给WETH合约增加 `depositTo(address _toAddress)` 方法，使得充值时可以选择充值地址；增加DepositTo事件，在调用depositTo时可以记录msg.sender, toAddress 和充值金额。比如账户A充值，实际增加的是账户B的余额，同时使用DepositTo记录下该事件；
9. 给WETH合约增加 `withdrawTo(address _toAddress, uint256 wad)` 方法，使得提现到时候可以选择提现地址。增加WithdrawTo事件，在调用withdrawTo时可以记录msg.sender, toAddress 和提现金额。比如账户A操作提现，可以提现到账户B，同时使用WithdrawTo记录该事件；
10. 解释 eth 与 weth 的联系与区别；
11. 解释 payable 的作用；

加分项：

1. 给合约增加一个 `withdrawFrom(address from, address payable to, uint256 value)` 方法，使得一个账户可以提现另一个账户的WETH。比如账户B可以提现账户A的WETH到账户C。

实验报告示例

1. 提前准备好三个账户A、账户B和账户C，都要持有CBI测试币（或者使用本地账户）；

账户A：

0x1aE0EA34a72D944a8C7603FfB3eC30a6669E454C

账户B：

0x0A098Eda01Ce92ff4A4CCb7A4fFFb5A43EBC70DC

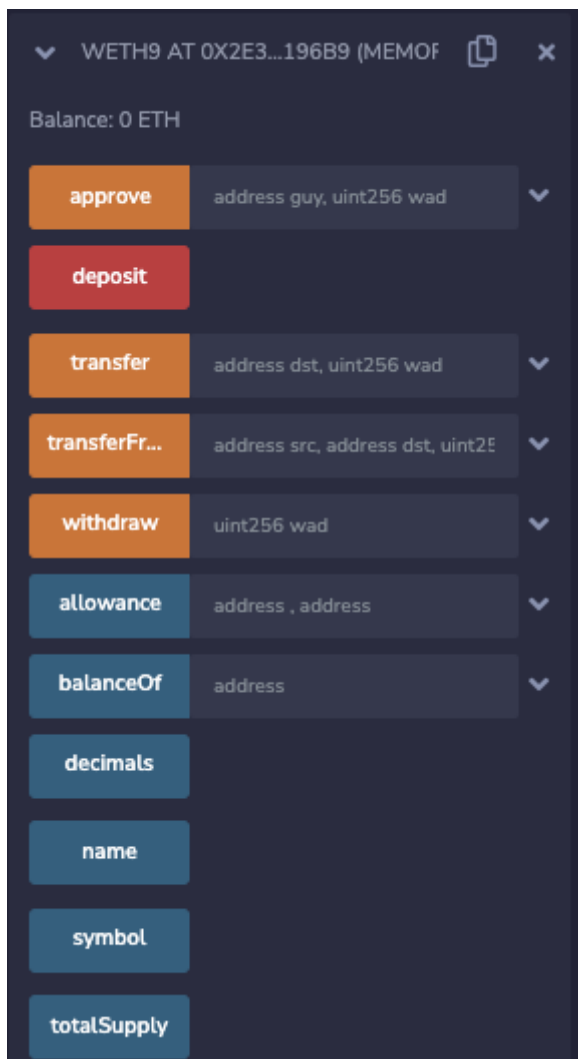
账户C：

0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c

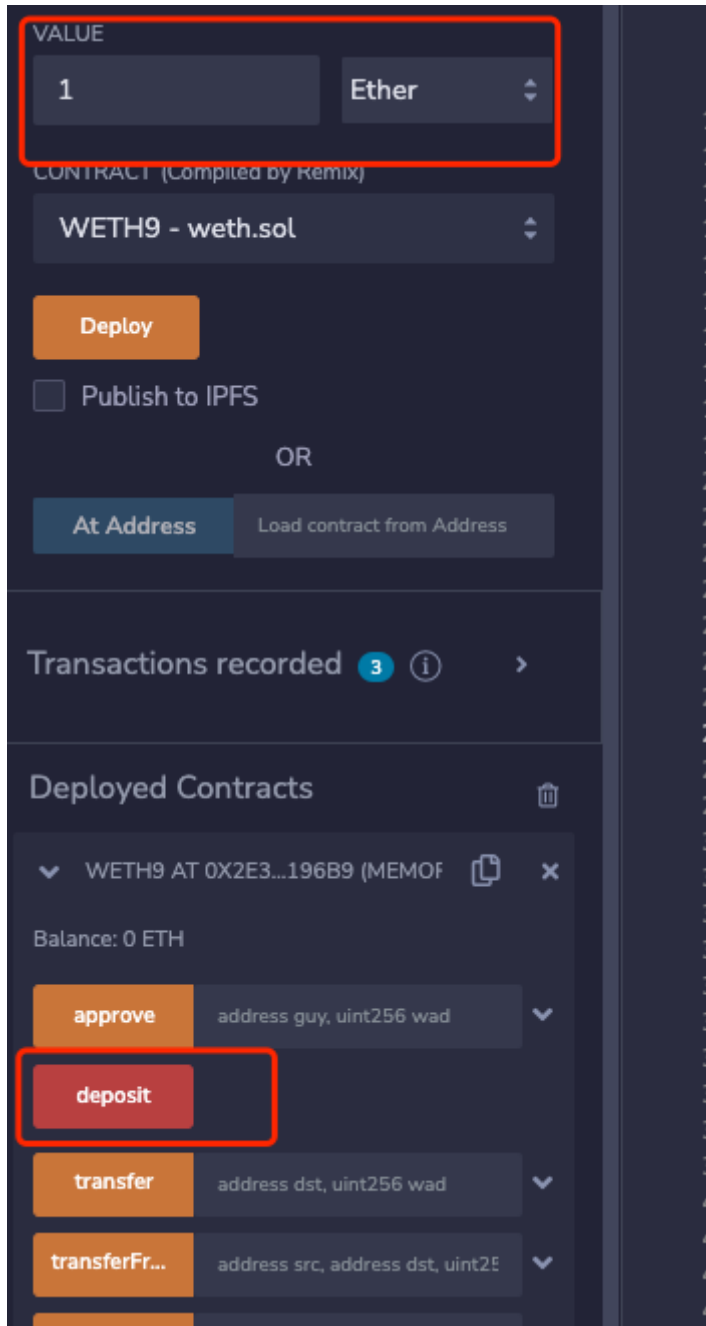
2. 使用账户A部署WETH合约；

合约地址为：

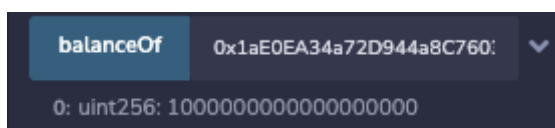
0x2E36EA848fd20fD9b6747789d5a59A8280f196b9



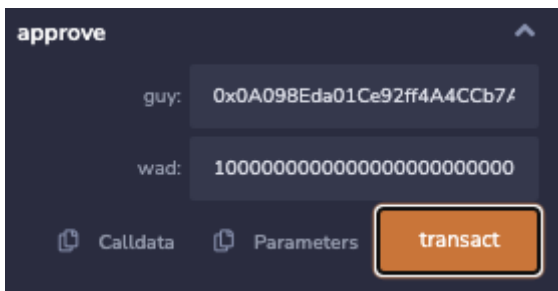
3. 使用账户A调用合约的deposit方法, 充值1个平台币;



4. 查询账户A的WETH余额;



5. 使用账户A对账户B进行approve操作；



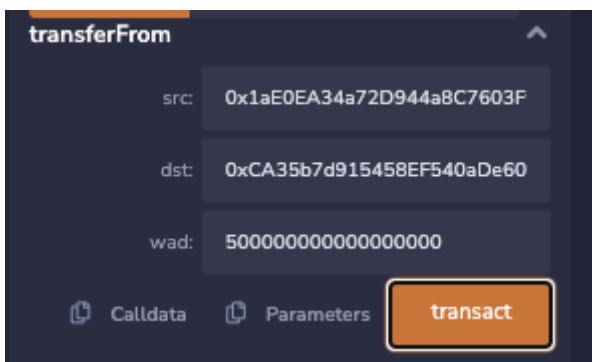
approve

guy: 0x0A098Eda01Ce92ff4A4CCb74

wad: 1000000000000000000000000

Calldata Parameters transact

6. 使用账户B调用合约的transferFrom方法，转账0.5个WETH到账户C；



transferFrom

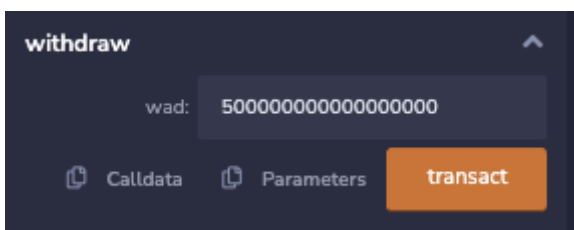
src: 0x1aE0EA34a72D944a8C7603F

dst: 0xCA35b7d915458EF540aDe60

wad: 500000000000000000000000

Calldata Parameters transact

7. 使用账户C调用合约的withdraw方法，提取0.5个WETH到自己账户；此时账户C的余额应增加了0.5个ETH；



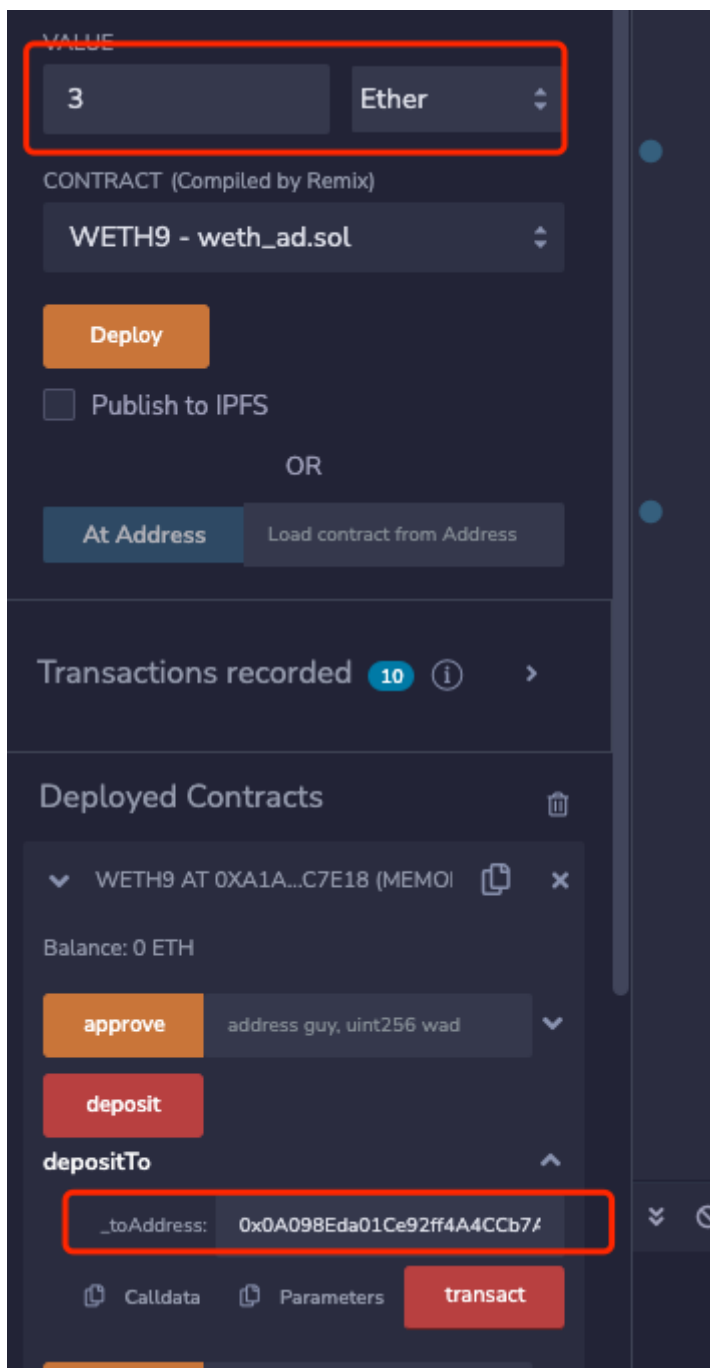
withdraw

wad: 500000000000000000000000

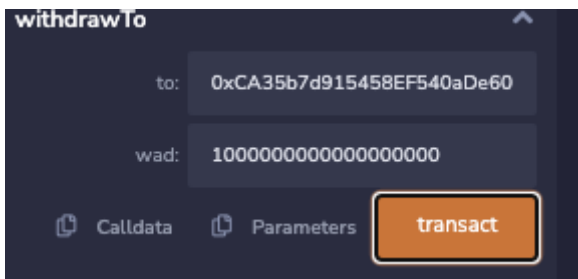
Calldata Parameters transact

8. 给WETH合约增加 `depositTo(address _toAddress)` 方法，使得充值时可以选择充值地址；增加DepositTo事件，在调用depositTo时可以记录msg.sender, toAddress 和充值金额。

比如账户A充值，实际增加的是账户B的余额；



9. 给WETH合约增加 `withdrawTo(address _toAddress, uint256 wad)` 方法，使得提现到时候可以选择提现地址。增加 WithdrawTo事件，在调用withdrawTo时可以记录 `msg.sender`, `toAddress` 和提现金额。比如账户B操作提现，可以提现到账户C；



此时账户C的ETH余额应该增加了1 ETH。

10. 解释 eth 与 weth 的联系与区别；

11. 解释 payable 的作用；

做完以上步骤， 可以找助教提交。

加分项：

1. 给合约增加一个 `withdrawFrom(address from, address payable to, uint256 value)` 方法，使得一个账户可以提现另一个账户的WETH。比如账户B可以提现账户A的WETH。
截图：1. 账户A调用deposit，充值10个ETH到合约；2. 账户A调用合约对账户B进行approve；3. 账户B把账户A的WETH，提现到账户C；

实验报告内容

在实验报告开头中写明：姓名/学号/班级，内容参考上面实验报告示例；

实验报告提交方式

实验报告完成后发送到邮箱 cbireport@163.com, 标题为 学号-班级-姓名-第三次实验报告