# HTLC测试说明

由于Ropsten测试网和Rinkeby测试网络无法及时获取到测试币，所以采用同样支持EVM的FISCO BCOS联盟链进行搭建测试环境。

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

## 准备条件

本人使用的环境是64bit Ubuntu 16.04 以及jdk 1.8版本，FISCO BCOS版本为2.4， 使用控制台（2.8.0）进行合约的部署和调用测试.。具体步骤如下：

将htlc\_test\_chain目录内容拷贝至Linux环境下：

1. 执行node目录中的脚本启动单机4节点区块链网络：

文本

描述已自动生成

文本

描述已自动生成

1. 执行console中get\_account.sh 脚本生成bob和Alice的秘钥；

文本

描述已自动生成

屏幕上有字

描述已自动生成

Alice 公钥地址：0x12dc5c61dbcf0de68569264bb354386edb6e0348

Bob 公钥地址： 0x9508e3525e60015edb0f82556585b6837874059f

1. 执行console中start.sh脚本进入控制台console：

文本

描述已自动生成

图表

描述已自动生成

## 合约部署及初始化

console目录下conract/solidity文件夹中已存放所有合约，不需要重新拷贝，直接调用deploy 合约名即可部署合约，依次部署TokenErc20、TokenErc721、HashedTimeLockERC20、HashedTimeLockERC721合约如下所示：

图形用户界面, 文本

描述已自动生成

其中：

erc20合约地址：0x5980c9ca95378a280f6334b6c1bb53b72146c99e

erc721合约地址： 0x6e3c9cb03aa8fb10c33db0dbceb3cd1a0468329a

erc20哈希时间锁合约：0x53128f8ccdc18168e073e78e55b838e19a0a8c4e

erc721哈希时间锁合约：0x716da32c08eacd82fba96f3407206f3bbb273474

合约部署者给Alice 初始化10000 erc20Token：

手机屏幕截图

描述已自动生成

call TokenErc20 0x5980c9ca95378a280f6334b6c1bb53b72146c99e transfer "0x12dc5c61dbcf0de68569264bb354386edb6e0348" 10000

合约部署者给bob初始化id 为1~5的 erc721 Token：

文本

描述已自动生成

call TokenErc721 0x6e3c9cb03aa8fb10c33db0dbceb3cd1a0468329a addTokenTo "0x9508e3525e60015edb0f82556585b6837874059f" 1

call TokenErc721 0x6e3c9cb03aa8fb10c33db0dbceb3cd1a0468329a addTokenTo "0x9508e3525e60015edb0f82556585b6837874059f" 2

call TokenErc721 0x6e3c9cb03aa8fb10c33db0dbceb3cd1a0468329a addTokenTo "0x9508e3525e60015edb0f82556585b6837874059f" 3

call TokenErc721 0x6e3c9cb03aa8fb10c33db0dbceb3cd1a0468329a addTokenTo "0x9508e3525e60015edb0f82556585b6837874059f" 4

call TokenErc721 0x6e3c9cb03aa8fb10c33db0dbceb3cd1a0468329a addTokenTo "0x9508e3525e60015edb0f82556585b6837874059f" 5

## HTLC测试

用例：Alice 将20个erc20 Token使用HashedTimeLockERC20进行锁定，定义了哈希锁：hash(originalInfo)和时间锁； bob将tokenID=1 的 ert721代币用Alice定义的哈希锁和bob定义的时间锁（需要小于Alice的锁定时间）来创建HashedTimeLockERC721合约进行锁定； Alice通过调用HashedTimeLockERC721合约提取的方法传入了自己在erc20代币哈希锁的原文，在规定的时间内与bob设定的哈希锁进行正确匹配，从而获得bob的ert721代币； bob通过同步区块链数据得到了Alice输入的哈希锁的原文，然后调用Alice的HashedTimeLockERC20的解锁方法，输入原文信息，匹配成功则可以得到Alice锁定的20个 ert20代币。

具体操作如下：

1. 在控制台切换Alice的私钥进行登录，然后对HashedTimeLockERC20合约进行授权2000 个erc20token的操作：

文本

描述已自动生成

bash start.sh 1 -pem ./accounts/0x12dc5c61dbcf0de68569264bb354386edb6e0348.pem

call TokenErc20 0x5980c9ca95378a280f6334b6c1bb53b72146c99e balanceOf "0x12dc5c61dbcf0de68569264bb354386edb6e0348"

call TokenErc20 0x5980c9ca95378a280f6334b6c1bb53b72146c99e approve "0x53128f8ccdc18168e073e78e55b838e19a0a8c4e" 2000

call TokenErc20 0x5980c9ca95378a280f6334b6c1bb53b72146c99e allowancesof "0x12dc5c61dbcf0de68569264bb354386edb6e0348" "0x53128f8ccdc18168e073e78e55b838e19a0a8c4e"

1. 接着调用HashedTimeLockERC20方法进行代币锁定：

文本

中度可信度描述已自动生成

call HashedTimeLockERC20 0x53128f8ccdc18168e073e78e55b838e19a0a8c4e newERC20HTLC "0x9508e3525e60015edb0f82556585b6837874059f" "c888c9ce9e098d5864d3ded6ebcc140a12142263bace3a23a36f9905f12bd64a" 1647788400 "0x5980c9ca95378a280f6334b6c1bb53b72146c99e" 20

其中参数说明：

0x9508e3525e60015edb0f82556585b6837874059f： bob公钥地址

0xc888c9ce9e098d5864d3ded6ebcc140a12142263bace3a23a36f9905f12bd64a：原文为“123456”的哈希值

1647788400 ： 交易过期时间戳

0x5980c9ca95378a280f6334b6c1bb53b72146c99e： erc20 合约的地址

20： 转账erc20代币的金额

返回结果ID： a3e957cb2ab3a55629ca2460a66ddbd0481429786c842f9f42609513aed16f17

1. 这个时候bob看到Alice已经锁定了erc20代币，接着调用HashedTimeLockERC721方法进行erc721代币锁定

首先使用bob私钥登录控制台，并授权HashedTimeLockERC721锁定id=1的erc721代币：

文本

描述已自动生成

bash start.sh 1 -pem ./account/0x9508e3525e60015edb0f82556585b6837874059f.pem

call TokenErc721 0x6e3c9cb03aa8fb10c33db0dbceb3cd1a0468329a balanceOf "0x9508e3525e60015edb0f82556585b6837874059f"

call TokenErc721 0x6e3c9cb03aa8fb10c33db0dbceb3cd1a0468329a approve "0x716da32c08eacd82fba96f3407206f3bbb273474" 1

bob调用HashedTimeLockERC721方法进行代币锁定：

电脑萤幕的截图

描述已自动生成

call HashedTimeLockERC721 0x716da32c08eacd82fba96f3407206f3bbb273474 newERC721HTLC "0x12dc5c61dbcf0de68569264bb354386edb6e0348" "c888c9ce9e098d5864d3ded6ebcc140a12142263bace3a23a36f9905f12bd64a" 1647788400 "0x6e3c9cb03aa8fb10c33db0dbceb3cd1a0468329a" 1

返回lock ID： d706fe12c507b72e2acd316bd276625970a663f8b1dde7d7f103f784d68303d5

1. Alice同步到bob的交易后，在限定时间内调用HashedTimeLockERC721合约的解锁方法输入哈希锁的原文，将erc721代币取回。

文本

描述已自动生成

call HashedTimeLockERC721 0x716da32c08eacd82fba96f3407206f3bbb273474 withdraw "d706fe12c507b72e2acd316bd276625970a663f8b1dde7d7f103f784d68303d5" "123456"

call TokenErc721 0x6e3c9cb03aa8fb10c33db0dbceb3cd1a0468329a balanceOf "0x12dc5c61dbcf0de68569264bb354386edb6e0348"

1. bob同步到alice的解锁交易后，可以获得哈希锁对应的原文信息，在时间锁限定的时间内调用HashedTimeLockERC20合约的解锁方法输入哈希锁的原文，将erc20代币取回。

文本

描述已自动生成

call HashedTimeLockERC20 0x53128f8ccdc18168e073e78e55b838e19a0a8c4e withdraw "a3e957cb2ab3a55629ca2460a66ddbd0481429786c842f9f42609513aed16f17" "123456"

call TokenErc20 0x5980c9ca95378a280f6334b6c1bb53b72146c99e balanceOf "0x9508e3525e60015edb0f82556585b6837874059f"