

Homework of Lecture 5

[Lecture 5 - Homework & Resources](#)

Homework is done by a group.

3.1 Understanding the lecture

1.a) Describe some advantages of conforming to a token standard like ERC-20 or IStandardToken in a few sentences.

*Conforming to a token standard ensures **interoperability** between our token and other tokens in the token standard network. This makes buying and trading our tokens easier for end users as well as investors, increasing the appeal of our token.*

*We can also benefit from **unified efforts at improving the security** of our token standard. The more networks that share the same token standard, the more stakeholders concerned with the token security, the more research is done to improve the token standard security.*

1.b) Describe the purpose of the TimeLockedTransfer contract in a few sentences.

*The TimeLockedTransfer contract allows us to **set a time for the contract execution**. This means that even if all conditions are already fulfilled by a certain time, the contract will not, or cannot, be executed until the prescribed time arrives. It can be used for **scheduled transfers** or **limiting contract accessibility**.*

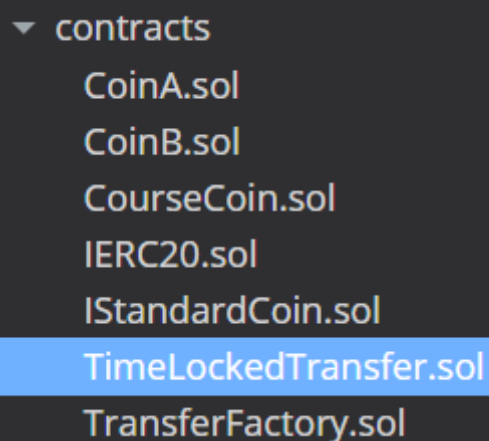
*If one can not withdraw his profit immediately, one might wanna make sure that his customers won't come back asking for a refund, which allows the sender to **cancel the transfer before the specified deadline**.*

3.2 Trying the lecture code

Download the project (github.com/Thegaram/cfx-uma-resources/raw/master/cfx-lecture-5.zip) and import it into Conflux Studio.

In this problem, you will have to deploy three smart contracts on your **local development network**.

First, deploy a **fixed-supply** standard coin with the name "CoinA". Then, deploy a second instance with the name "CoinB".



```
▼ contracts
  CoinA.sol
  CoinB.sol
  CourseCoin.sol
  IERC20.sol
  IStandardCoin.sol
  TimeLockedTransfer.sol
  TransferFactory.sol
```

CoinA: 0x8ad093411fb99e82d35c6adfe494821e3d478a70

Transaction

Basic

Parameters

Tx

Receipt

ABI

Hash

0xda59f8fdb2e0fa73c5bd5dfb18ebc27220eae345e99ad3da4056e2c997d2dad7

Status

CONFIRMED

Contract Name

CoinA

Signer

0x1cd6889bd8df7872506ae8d61bba9448efc9f281

Contract Created

0x8ad093411fb99e82d35c6adfe494821e3d478a70

Cancel

CoinB: 0x824eebd198b057a4638842247b0a788e8888ef49

Transaction

Basic

Parameters

Tx

Receipt

ABI

Hash

0x6cc767aa261e345b5b7f13acb74214613111ca393f4924ea0a7af467b2d0a74b

Status

CONFIRMED

Contract Name

CoinB

Signer

0x1cd6889bd8df7872506ae8d61bba9448efc9f281

Contract Created

0x824eebd198b057a4638842247b0a788e8888ef49

Cancel

Next, deploy an instance of the TimeLockedTransfer contract. Set the unlock time to something greater than 5 minutes.

TimeLockedTransfer: (time = 301 s > 5 min)

Transaction

Basic Parameters Tx Receipt ABI

Hash 0xf40fbe626e24ddb6121ec8c16869072e7c3089fe8d7692decc6c2fbe86cdd627

Status CONFIRMED

Contract Name TimeLockedTransfer

Signer 0x1cd6889bd8df7872506ae8d61bba9448efc9f281

Contract Created 0x878b9be9ccfddec3795a1a7ded53a4fcb2dad8415

Cancel

Basic Parameters Tx Receipt ABI

```

{
  "sender": {
    "type": "address",
    "value": "0x1cd6889bd8df7872506ae8d61bba9448efc9f281"
  },
  "receiver": {
    "type": "address",
    "value": "0x1c4b58c921bdb82104794da09bc14727d35eb966"
  },
  "lockTimeSec": {
    "type": "uint256",
    "value": "301"
  }
}

```

Send 17 CFX, 22 CoinA, and 12 CoinB to the transfer contract.

Send 17 CFX:

New Tab 0x81a1...c6d9

0x878b9be9ccfddec3795a1a7

f depositCFX

Parameters (None)

CFX to Transfer 17

Gas & Storage

Gas Limit Default: 1,000,000

Gas Price Default: 100 drip

Storage Limit

Authorization

Signer 0x1cd6889bd8df7872506ae...

Transaction

Basic Parameters Tx Receipt

Hash 0x0b4207190edc76877e8d64a289d052a91990f053ba35d73026f5e2e4eba66da8

Status CONFIRMED

Contract 0x878b9be9ccfddec3795a1a7ded53a4fcb2dad8415

Function depositCFX

CFX Transferred 17 CFX

Signer 0x1cd6889bd8df7872506ae8d61bba9448efc9f281

Cancel

Send 22 CoinA: (Through contract "CoinA")

send it to the TimeLockedTransfer contract address.

The screenshot shows a transaction confirmation window titled "Transaction" with tabs for "Basic", "Parameters", "Tx", and "Receipt". The "Basic" tab is active, displaying the following details:

- # Hash: 0xe9c2fb256757dd4ebf7080a48715eae4a9fceb71eb5683d61fe42b3b4e5246
- Status: CONFIRMED
- Contract: 0x8ad093411fb99e82d35c6adfe494821e3d478a70
- Function: transfer
- CFX Transferred: 0 CFX
- Signer: 0x1cd6889bd8df7872506ae8d61bba9448efc9f281

The background interface shows a "transfer" button and a "Parameters" section with the following values:

- receiver: 0x878b9be9ccfddec3795a1a7de53a4fcb2dad8415
- amount: 123 22
- Gas Limit: Default: 1,000,000
- Gas Price: Default: 100 drip
- Storage Limit: Default: 1,000,000

The screenshot shows the "Parameters" tab of the transaction confirmation window. It displays a JSON object representing the transaction parameters:

```
{
  "receiver": {
    "type": "address",
    "value": "0x878b9be9ccfddec3795a1a7ded53a4fcb2dad8415"
  },
  "amount": {
    "type": "uint256",
    "value": "22"
  }
}
```

Send 12 CoinB: (Through contract "CoinB")

The screenshot shows a transaction confirmation window titled "Transaction" with tabs for "Basic", "Parameters", "Tx", and "Receipt". The "Basic" tab is active, displaying the following details:

- # Hash: 0xdf1370ee694e8b6e568f861d81321a81088e58e90a27fa90480e2ac61a129997
- Status: CONFIRMED
- Contract: 0x824eebd198b057a4638842247b0a788e888ef49
- Function: transfer
- CFX Transferred: 0 CFX
- Signer: 0x1cd6889bd8df7872506ae8d61bba9448efc9f281

The background interface shows a "transfer" button and a "Parameters" section with the following values:

- receiver: 0x878b9be9ccfddec3795a1a7de53a4fcb2dad8415
- amount: 123 12
- Gas Limit: Default: 1,000,000
- Gas Price: Default: 100 drip
- Storage Limit: Default: 1,000,000

```
Basic Parameters Tx Receipt

{
  "receiver": {
    "type": "address",
    "value": "0x878b9be9ccfddec3795a1a7ded53a4fcb2dad8415"
  },
  "amount": {
    "type": "uint256",
    "value": "12"
  }
}
```

After the deadline, withdraw all these tokens from the transfer contract.

withdraw CFX:

cfx-lecture-5

New Tab 0x878b...8415 x

0x878b9be9ccfddec3795a1a7

f() withdrawCFX ▶

Parameters

(None)

Gas & Storage

Gas Limit

Default: 1,000,000

Gas Price

Default: 100 drip

Storage Limit

Authorization

Signer

0x1c4b58c921bdb821047... [Calculate](#)

Transaction

Basic Parameters Tx Receipt

Hash

0xf9bd88bc6783e771e285475235bb420f4a7ade158142c1c76693c513fec87d9a

Status

CONFIRMED

Contract

0x878b9be9ccfddec3795a1a7ded53a4fcb2dad8415

f() Function

withdrawCFX

CFX Transferred

0 CFX

Signer

0x1c4b58c921bdb82104794da09bc14727d35eb966

Cancel

after:

f() balance ▶

f() CFXWithdraw ▶

Parameters

Result

Success

"0"

Event Logs

EPOCH

70457

AMOUNT

uint256

17000000000000000000

withdraw CoinA:

Transaction

Basic

Parameters

Tx

Receipt

Hash

0xb51f40325a23c6ec02b5e4c8ea701d2e420cc72ae8fbb9782e1e6fb4b5d6c03c

Status

CONFIRMED

Contract

0x878b9be9ccfddec3795a1a7ded53a4fcb2dad8415

f(⌘) Function

withdrawCoin

CFX Transferred

0 CFX

Signer

0x1c4b58c921bdb82104794da09bc14727d35eb966

Cancel

Basic

Parameters

Tx

Receipt

```
{
  "coinContract": {
    "type": "address",
    "value": "0x8ad093411fb99e82d35c6adfe494821e3d478a70"
  }
}
```

withdraw CoinB:

Transaction

Basic

Parameters

Tx

Receipt

Hash

0x81a6f86e5177b196861e68cb149a9df7b92c0ebffbd8ded8a10cc1460bc3bc3

Status

CONFIRMED

Contract

0x878b9be9ccfddec3795a1a7ded53a4fcb2dad8415

f(⌘) Function

withdrawCoin

CFX Transferred

0 CFX

Signer

0x1c4b58c921bdb82104794da09bc14727d35eb966

Cancel

BasicParametersTxReceipt

```
{
  "coinContract": {
    "type": "address",
    "value": "0x824eebd198b057a4638842247b0a788e888ef49"
  }
}
```

after:

f(x) CoinWithdraw ▾	
Event Logs	
EPOCH	AMOUNT uint256
71248	12
71192	22

Document the process using screenshots and a short description of each step.

+1. Transfer Factory [OPTIONAL]

Look at the file TransferFactory.sol. Try to understand what it does and explain it using your own words.

Show us how to deploy and use this contract.

It creates and maintains a list of "TimeLockedTransfer" contracts.

Each time the function "create" is called, a new "TimeLockedTransfer" contract is deployed.

Deploy: 0x833791606cc08d5e4f5fd9a2d6953faff6c0c494

Transaction

BasicParametersTxReceiptABI

Hash0x2a8d6847e60489c2d35453da9d3a7c43bdfa298a53c1c661450f769e176a18d8

☐ StatusCONFIRMED

Contract NameTransferFactory

Signer0x1cd6889bd8df7872506ae8d61bba9448efc9f281

Contract Created0x833791606cc08d5e4f5fd9a2d6953faff6c0c494

Cancel

Create: (3 times)

New Tab0x8337...c494

0x833791606cc08d5e4f5fd9

f create

Parameters

sender0x1cd6889bd8df7872506ae8d61bba9448efc9f281

recipient0x18239eed8e95eb6b98f85fdc9fbb18e8b44dc988

lock_time_s12315

Gas & Storage

Gas LimitDefault: 1,000,000

Gas Price

Transaction

BasicParametersTxReceipt

Hash0x32dac0a034250ff03e6603d9ecda82c53ab6705e911eca0aa7e9daa3eec99423

StatusCONFIRMED

Contract0x833791606cc08d5e4f5fd9a2d6953faff6c0c494

f Functioncreate

CFX Transferred0 CFX

Signer0x1cd6889bd8df7872506ae8d61bba9448efc9f281

Cancel

BasicParametersTxReceipt

```
{
  "sender": {
    "type": "address",
    "value": "0x1cd6889bd8df7872506ae8d61bba9448efc9f281"
  },
  "recipient": {
    "type": "address",
    "value": "0x18239eed8e95eb6b98f85fdc9fbb18e8b44dc988"
  },
  "lock_time_s": {
    "type": "uint256",
    "value": "15"
  }
}
```

New Tab0x8337...c494

0x833791606cc08d5e4f5fd9

f create

Parameters

sender0x1cd6889bd8df7872506ae8d61bba9448efc9f281

recipient0x1c4b58c921bdb82104794c4a

lock_time_s1237

Gas & Storage

Gas LimitDefault: 1,000,000

Gas Price

Transaction

BasicParametersTxReceipt

Hash0x87acd4015a85ad203537c23badb6ef6a8b4fd57ab176c4ef5cbb6f8386985b17

StatusCONFIRMED

Contract0x833791606cc08d5e4f5fd9a2d6953faff6c0c494

f Functioncreate

CFX Transferred0 CFX

Signer0x1cd6889bd8df7872506ae8d61bba9448efc9f281

Cancel


```
Basic Parameters Tx Receipt

{
  "sender": {
    "type": "address",
    "value": "0x1cd6889bd8df7872506ae8d61bba9448efc9f281"
  },
  "recipient": {
    "type": "address",
    "value": "0x1c4b58c921bdb82104794da09bc14727d35eb966"
  },
  "lock_time_s": {
    "type": "uint256",
    "value": "7"
  }
}
```

Transaction

Basic Parameters Tx Receipt

Hash0x22dd730ed4218f2cf650c9aa7a8cf83b0bc0e069c41f25b960ded8397f749ed5

StatusCONFIRMED

Contract0x833791606cc08d5e4f5fd9a2d6953fa9ff6c0c494

Functioncreate

CFX Transferred0 CFX

Signer0x1cd6889bd8df7872506ae8d61bba9448efc9f281

Cancel

Parameters

sender0x1cd6889bd8df7872506ae8d61bba9448efc9f281

recipient0x13c1f4778f694c4093134b651ffbcfa5428603ef

lock_time_s123 5

Gas & Storage

Gas LimitDefault: 1,000,000

Gas Price

```
Basic Parameters Tx Receipt

{
  "sender": {
    "type": "address",
    "value": "0x1cd6889bd8df7872506ae8d61bba9448efc9f281"
  },
  "recipient": {
    "type": "address",
    "value": "0x13c1f4778f694c4093134b651ffbcfa5428603ef"
  },
  "lock_time_s": {
    "type": "uint256",
    "value": "5"
  }
}
```

And we can see those 3 contract infos: (saved in the list called "transfers")

f(*) transfers ▾ ▶	f(*) NewTransfer ▾ ▶								
Parameters (param0) 123 2 Result Success "0x81467498a94c490c3de0841cc9639041e25fca99"	Event Logs <table> <thead> <tr> <th>EPOCH</th><th>ID uint256</th></tr> </thead> <tbody> <tr> <td>76649</td><td>2</td></tr> <tr> <td>76551</td><td>1</td></tr> <tr> <td>75860</td><td>0</td></tr> </tbody> </table>	EPOCH	ID uint256	76649	2	76551	1	75860	0
EPOCH	ID uint256								
76649	2								
76551	1								
75860	0								

BUT these tranfers doesn't work like I expected, and all the contract addresses are invalid.

+1. Cancel transfer [OPTIONAL]

Modify TimeLockedTransfer.sol in a way that allows the sender to cancel the transfer before the specified deadline.

Provide a way for the sender to re-acquire all their tokens from the transfer contract after cancelling it.

Cancel test:

Transaction

Basic
Parameters
Tx
Receipt

Hash
0xde2ae30f0c9102b41df64e329ebde1f48d587ef88b6ed65e6bbd7724c25720dd

Status
CONFIRMED

Contract
0x8f5abdd832b16dae879a33b1befd04b76b0d8f1f

f(*) Function
cancel

CFX Transferred
0 CFX

Signer
0x1cd6889bd8df7872506ae8d61bba9448efc9f281

The main source code is as follows: (including several changes in other files not showing here)

```

1  // SPDX-License-Identifier: GPL-3.0-or-later
2
3  pragma solidity ^0.7.1;
4
5  import "./IStandardCoin.sol";
6
7  contract TimeLockedTransfer {
8      address _sender;
9      address _receiver;
10     address [] public contracts;
11     uint256 _unlockAfter; // point in time
12
13     event CFXDeposit(uint256 amount);
14     event CFXWithdraw(uint256 amount);

```

```

15     event CoinDeposit(uint256 amount);
16     event CoinWithdraw(uint256 amount);
17     event Cancel(uint256 number);
18
19     constructor(address sender, address receiver, uint256 lockTimeSec) {
20         _sender = sender;
21         _receiver = receiver;
22
23         // current time: `block.timestamp` (`now` in older versions)
24         _unlockAfter = block.timestamp + lockTimeSec;
25     }
26
27     function balance() external view returns (uint256) {
28         return address(this).balance;
29     }
30
31     function depositCFX() external payable {
32         require(msg.sender == _sender, "TLT: Unauthorized");
33         uint256 amount = msg.value;
34         emit CFXDeposit(amount);
35     }
36
37     function withdrawCFX() external {
38         require(msg.sender == _receiver, "TLT: Unauthorized");
39         require(block.timestamp >= _unlockAfter, "TLT: Timelock still
active");
40         uint256 amount = address(this).balance;
41         msg.sender.transfer(amount);
42         emit CFXWithdraw(amount);
43     }
44
45     function depositCoin(address coinContract) external payable {
46         require(msg.sender == _sender, "TLT: Unauthorized");
47
48         contracts.push(coinContract);
49
50         IStandardCoin coin = IStandardCoin(coinContract);
51         uint256 amount = (uint256)(msg.value / 1000000000000000000);
52         coin.transfer2(msg.sender, address(this), amount);
53         emit CoinDeposit(amount);
54     }
55
56     function withdrawCoin(address coinContract) external {
57         // Alice will deposit coins to this contract through the contract
58         // Bob can withdraw after the deadline by passing the coin contract
address
59         require(msg.sender == _receiver, "TLT: Unauthorized");
60         require(block.timestamp >= _unlockAfter, "TLT: Timelock still
active");
61
62         IStandardCoin coin = IStandardCoin(coinContract);
63         uint256 amount = coin.balanceOf(address(this));
64         coin.transfer(msg.sender, amount);
65         emit CoinWithdraw(amount);
66     }
67
68     function cancel() external{
69         require(msg.sender == _sender, "TLT: Unauthorized");

```

```

70     require(block.timestamp < _unlockAfter, "TLT: Timelock is no longer
    active");
71
72     // cancel CFX
73     uint256 amount = address(this).balance;
74     msg.sender.transfer(amount);
75
76     // cancel other coins
77     for(uint i = 0; i < contracts.length; i = i + 1){
78         address coinContract = contracts[i];
79         IStandardCoin coin = IStandardCoin(coinContract);
80         amount = coin.balanceOf(address(this));
81         coin.transfer(msg.sender, amount);
82     }
83
84     emit Cancel(amount);
85 }
86 }

```

A more step by step demo:

(1) Deploy it with 10 mins delay:

Deploy Contract **TimeLockedTransfer**

Constructor Parameters

sender

0x1cd6889bd8df7872506ae8d61bba9448efc9f281
Vel

receiver

0x174babda7b72b606d2f3486616358d4b72b2cad8
Jessica

lockTimeSec

123 600

Signer

0x1cd6889bd8df7872506ae8d61bba9448efc9f281
Vel

Gas Limit

Default: 1,000,000

Gas Price

\$ Default: 100 drip

Storage Limit

Cancel Deploy

BasicParametersTxReceiptABI

Hash0x3e04e36a9ccfc89c2f126d1a440e9f5ebc4076c8422f2ebfe721164d0dd01ec2

Status

CONFIRMED

Contract Name

TimeLockedTransfer

Signer

0x1cd6889bd8df7872506ae8d61bba9448efc9f281

Contract Created

0x82b741514d11ef4946329a104e8fa015d1e9af78

BasicParametersTxReceiptABI

```
{
  "sender": {
    "type": "address",
    "value": "0x1cd6889bd8df7872506ae8d61bba9448efc9f281"
  },
  "receiver": {
    "type": "address",
    "value": "0x174babda7b72b606d2f3486616358d4b72b2cad8"
  },
  "lockTimeSec": {
    "type": "uint256",
    "value": "600"
  }
}
```

(2) check the CoinA(2317) and CoinB(1234):

0x877c...65210x8a50...61410x82b7...af78+

0x877c46debd509453574eaa6bd59c1ee34dab6521

f(*) transfer ▶

f(*) balanceOf ▶

f(*) Transfer ▶

Parameters

Parameters

Event Logs

receiver

address

amount

123uint256

Gas & Storage

addr

0x1cd6889bd8df7872506ae8dVel

Result

Success

2317

EPOCH	FROM address
100632	0x8f5abdd83
100462	0x1cd6889bc
94806	0x1cd6889bc
92277	0x1cd6889bc

0x877c...65210x8a50...61410x82b7...af78+

0x8a505f9ef5c34e6c94c75504296778bea42a6141

f(*) transfer ▶

f(*) balanceOf ▶

f(*) Transfer ▶

Parameters

Parameters

Event Logs

receiver

address

amount

123uint256

Gas & Storage

addr

0x1cd6889bd8df7872506ae8dVel

Result

Success

1234

EPOCH	FROM address
100632	0x8f5abdd832b1
100507	0x1cd6889bd8df


(3) send CFX(11), CoinA(12), CoinB(13):

f(x) depositCFX ▶

Parameters

(None)


CFX to Transfer

 11


f(x) depositCoin ▶

Parameters

coinContract

 0x877c46debd509453574eaa6bd5f


CFX to Transfer

 12


f(x) depositCoin ▶

Parameters

coinContract

 0x8a505f9ef5c34e6c94c7550429f

CFX to Transfer

 13

(4) Check CFX(11), the CoinA(2317 - 12 = 2305) and CoinB(1234 - 13 = 1221):

f(x) CFXDeposit ▶

Event Logs

EPOCH	AMOUNT uint256
102604	1100000000000000000000

f(x) balanceOf

▶

Parameters

addr

📍

0x1cd6889bd8df7872506ae8d

Vel

Result

Success

"2305"

f(x) balanceOf

▶

Parameters

addr

📍

0x1cd6889bd8df7872506ae8d

Vel

Result

Success

"1221"

(5) **cancel**:

⌛ PENDING

⌛ cancel

EXECUTED

⌚ 11/07 01:59:02

0x82b741514d11ef4946329a104e8fa015d1e9af78

🔍 RECENT TRANSACTIONS

✓

depositCoin

⌚ 11/07 01:55:20

0x82b741514d11ef4946329a104e8fa015d1e9af78

✓

depositCoin

⌚ 11/07 01:55:14

0x82b741514d11ef4946329a104e8fa015d1e9af78

✓

depositCFX

⌚ 11/07 01:54:37

0x82b741514d11ef4946329a104e8fa015d1e9af78

✓

Deploy

⌚ 11/07 01:51:28

TimeLockedTransfer

CFX(0), CoinA(2317) and CoinB(1234) again:

f(×) balance ▾▶

▼ Parameters

(None)

▼ Result Success

"0"

f(×) balance0f ▾▶

▼ Parameters

addr

📍

0x1cd6889bd8df7872506ae8d

Vel

▼ Result Success

"2317"

f(×) balance0f ▾▶

▼ Parameters

addr

📍

0x1cd6889bd8df7872506ae8d

Vel

▼ Result Success

"1234"