



# **ETHEREUM SECURITY DESIGN PATTERNS**

Date: 12/03/2018

Brent Anthony Tudas

Sandra Alleine Blanca

Jaymar Dingcong

Robert Aries Dela Paz

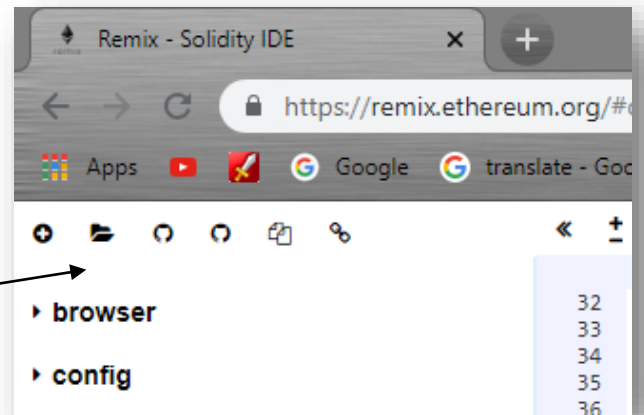
Kimberly Mae Reyes

Patrick Oliver Palmero

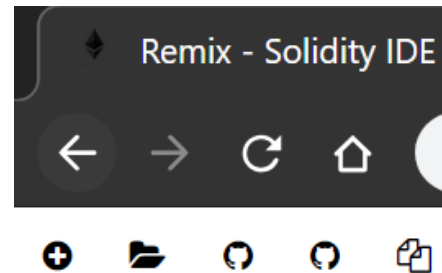
# INSTRUCTIONS

Go to <https://remix.ethereum.org/>

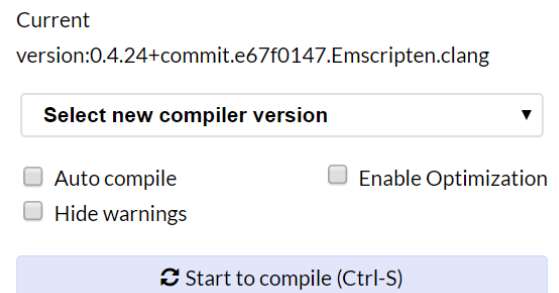
1. Click the icon and go to the folder Directory of this document and select Transfer.sol



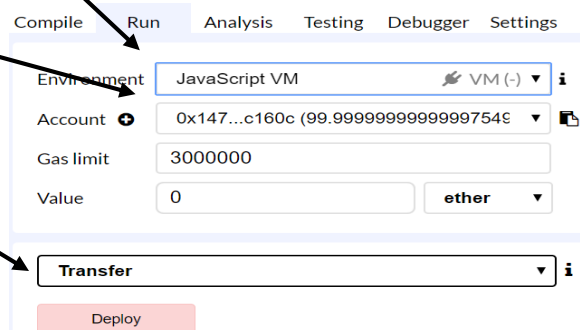
2. Click "browser" and it will collapse find "Transfer.sol" and select it.



3. Select new compiler version. Set it to 0.4.24+commit version.  
Then, select Run tab.



4. Select **Environment** change it to JavaScript VM.
5. Select **Account** from the drop down button. Remember you chosen account.
6. Click deploy.



## Making a new account

Find the value field and put 5 there. Make sure that the other field is in ether if not then kindly select ether.

Value  ether ▼

Enter your name inside the double quotation. Then click addAccount button to submit.

Ex. "Brent"

addAccount ▼

## Checking the account balance

Find the getValue field and click it. You will get the following

getValue

0: uint256: 50000000000000000000

---

## Depositing

Find the value field and put 2 there. Make sure the other field is in ether.

Value  ether ▼

Find the deposit button and click it.

deposit


Notice that when your balance again it will now return this.

getValue

0: uint256: 70000000000000000000

## Withdrawing



Check your account balance first and remember the value like so

Account  0xca3...a733c (92.99999999999847335 ▼ 

Find the withdraw button and enter 3 in the field. And click it.

withdraw  ▼

Notice that now the account balance is added by 3.

Account  0xca3...a733c (95.99999999999842625 ▼ 

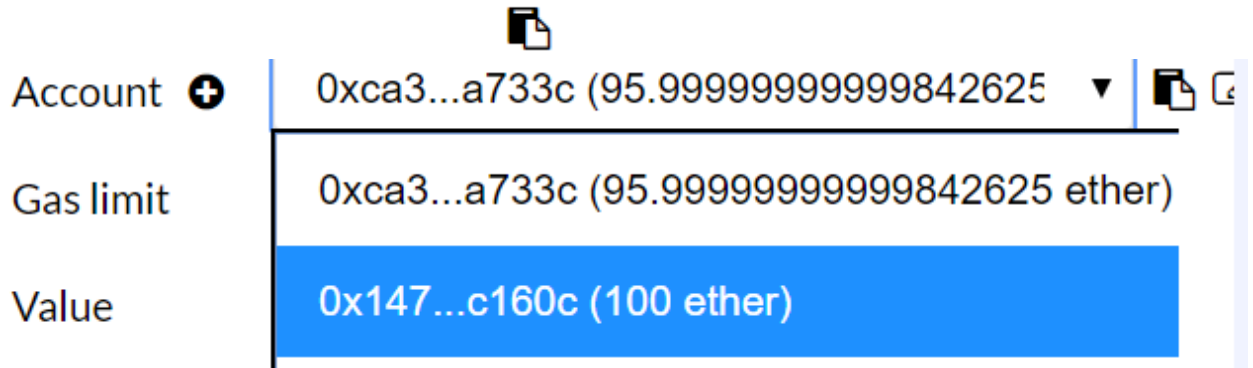
## Sending Money

Check the account balance first. You should have this value.

getValue

0: uint256: 40000000000000000000

Now go to the account and click it and select the second value like sxo.



A screenshot of a transaction form. The form has three rows: 'Account', 'Gas limit', and 'Value'. The 'Account' row shows '0xca3...a733c (95.99999999999842625 ether)' with a dropdown arrow and a copy icon. The 'Gas limit' row shows '0xca3...a733c (95.99999999999842625 ether)'. The 'Value' row shows '0x147...c160c (100 ether)' and is highlighted with a blue background. A copy icon is also visible in the top right corner of the form.

Account	0xca3...a733c (95.99999999999842625 ether)
Gas limit	0xca3...a733c (95.99999999999842625 ether)
Value	0x147...c160c (100 ether)

After selecting it click the copy icon.

Reminder:

(MAKE SURE TO CREATE AN ACCOUNT IN THIS ADDRESS FIRST BEFORE PROCEEDING)

(PROCESS OF CREATING A NEW ACCOUNT IS DISCUSSED ABOVE. KINDLY DO IT AGAIN FOR THIS AGAIN)

If you're done creating the account. Then go back to the first account like so.

Account	0x147...c160c (100 ether)
Gas limit	0xca3...a733c (95.99999999999842625 ether)
Value	0x147...c160c (100 ether)

Now paste the copied text inside the field by hitting (ctrl + v) in the keyboard like so.

sendMoney	0x14723a09acff6d2a60dcdf7aa4aff308fddc160c
-----------	--

Now put a comma and put 2 like so. And click sendMoney. And now your done.

sendMoney	0x14723a09acff6d2a60dcdf7aa4aff308fddc160c, 2
-----------	---

## Checking if the account received the sent money

Make sure to select this account.

Account	0x147...c160c (99.99999999999997549 ether)
Gas limit	0xca3...a733c (91.999999999996821588 ether)
Value	0x147...c160c (99.99999999999975494 ether)

Click getValue and you should have this amount as result.

getValue
----------

0: uint256: 20000000000000000000

## **Patterns Used:**

**Access Restriction** – provide authorization to certain sensitive parts of the contracts

**Guard Check** – ensures the inputs of functions called in the contract are valid

**Check Effects Interactions** – reduces the risks of re-entrancy of external function calls

**Pull Over Push** – ensures the transferring of ethers to accounts are validated.

**Secure Ether Transfer** – ensures transfers of ether from an account to another is secure.

**Emergency Stop** – shuts down the contract if suspicious transactions occur.

