Introduction to blockchain and Ethereum smart contracts

Using Ethereum Wallet and deploying your first smart contract

Written by Peter, Ho Man Fai

Microsoft

The Hong Kong Polytechnic University
香港理工大學

Department of Computing
電子計算學系

Learning outcomes

After you complete this lab, you will be able to:

1. Install a Ethereum Wallet in your computer.
2. Use the graphical user interface provided by Ethereum Wallet.
3. Deploy a Solidity smart contract using Ethereum Wallet.
4. Call and send transactions to a smart contract using Ethereum Wallet.

Reminder

You should have two Ethereum nodes running on your network, and make sure both of your machines are running the Ethereum Geth program.

As a reminder, you may use this command to start your blockchain node (change the yellow-highlighted content to a path that points to your Ethereum folder, and change the green-highlighted content to a random integer).

```
geth --datadir "C:\Users\Admin\Desktop\ethereum-private-net" --
networkid 1234567890
```

Run "**geth attach**" to start the Ethereum CLI in your **first computer** → execute the following JavaScript command in the CLI to **start the mining process**.

```
miner.start(1);
```

Install Ethereum Wallet

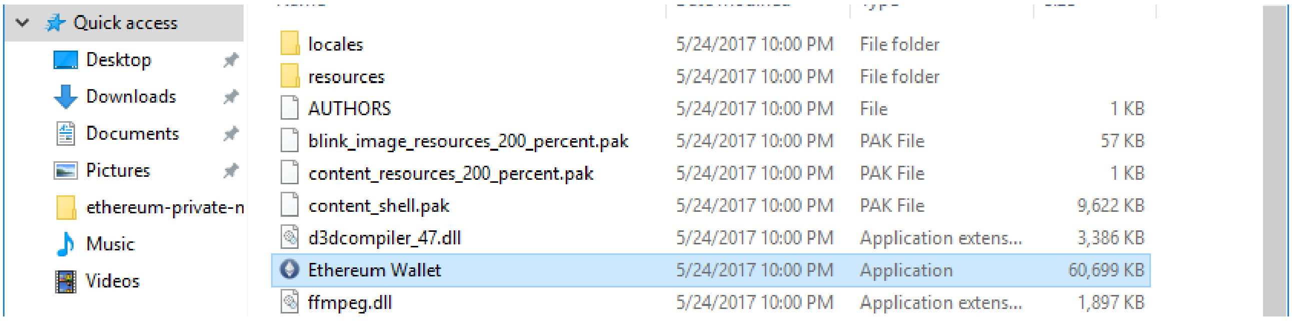
In the previous tutorial, we have used the Ethereum CLI to give commends to our blockchain. Today, we are going to use the graphical user interface (GUI) to interact with Ethereum. The GUI tool is called Ethereum Wallet.

1. In your first computer, visit https://github.com/ethereum/mist/releases/tag/v0.9.2 → Scroll down and look for the "Downloads" section → Click "**Ethereum-Wallet-installer-0-9-2.exe**".

Important note:

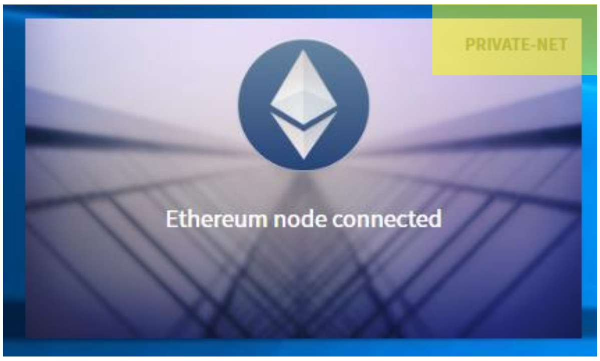
The version of Ethereum Wallet keeps updating. By the time you are reading this, you should be able to download a version that is beyond 0.9.2. However, **DO NOT use other versions except 0.9.2 for this series of tutorial.** It is because this tutorial is written for version 0.9.2. We do not guarantee the materials here will work other than that version.

2. Install it → Open the “Ethereum Wallet.exe” executable.



locales	5/24/2017 10:00 PM	File folder	
resources	5/24/2017 10:00 PM	File folder	
AUTHORS	5/24/2017 10:00 PM	File	1 KB
blink_image_resources_200_percent.pak	5/24/2017 10:00 PM	PAK File	57 KB
content_resources_200_percent.pak	5/24/2017 10:00 PM	PAK File	1 KB
content_shell.pak	5/24/2017 10:00 PM	PAK File	9,622 KB
d3dcompiler_47.dll	5/24/2017 10:00 PM	Application extens...	3,386 KB
Ethereum Wallet	5/24/2017 10:00 PM	Application	60,699 KB
ffmpeg.dll	5/24/2017 10:00 PM	Application extens...	1,897 KB

3. **Skip any dialog** when you are asked to upgrade your Geth → When you launch the application, a splash screen (see below) will be displayed, and it should display “**PRIVATE-NET**” **on the top-right corner**.

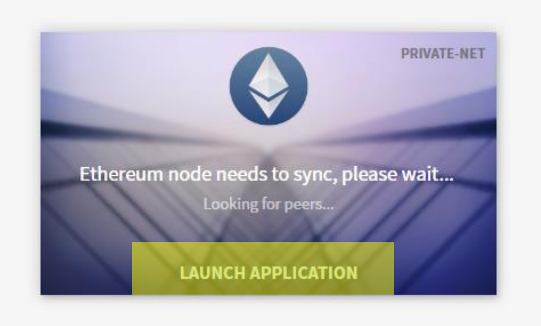


Ethereum node connected

> **Important note:**
>
> If you cannot see the “PRIVATE-NET” word in your splash screen, it means you DID NOT start your Geth private net. Instead, your Ethereum Wallet connects you to the Ethereum global public network and thus it shows nothing. So, remember to start your Ethereum private chain before you proceed!

4. **Repeat all the steps in your second computer.**

> **Important note:**
>
> If you are stuck at the following screen, click the “Launch application” text.

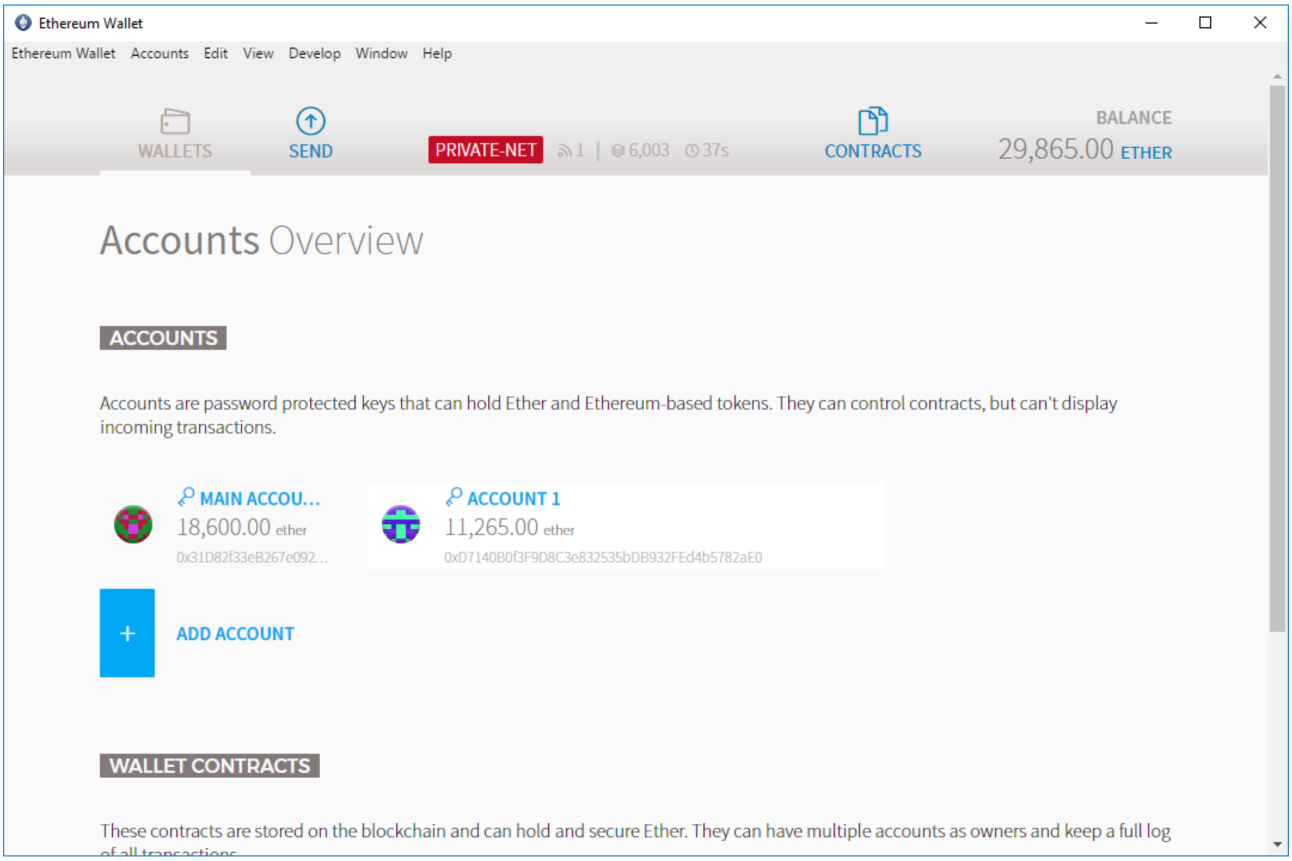


Ethereum node needs to sync, please wait...

Looking for peers...

Using the Ethereum Wallet

5. **You should see something similar to this**. Note that there is a "**PRIVATE-NET**" in red on top.



Accounts Overview

ACCOUNTS

Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.

MAIN ACCOU...
18,600.00 ether
0x31D82f33eB267e092...

ACCOUNT 1
11,265.00 ether
0xD7140B0f3F9D8C3e832535bDB932FEd4b5782aE0

WALLET CONTRACTS

These contracts are stored on the blockchain and can hold and secure Ether. They can have multiple accounts as owners and keep a full log of all transactions

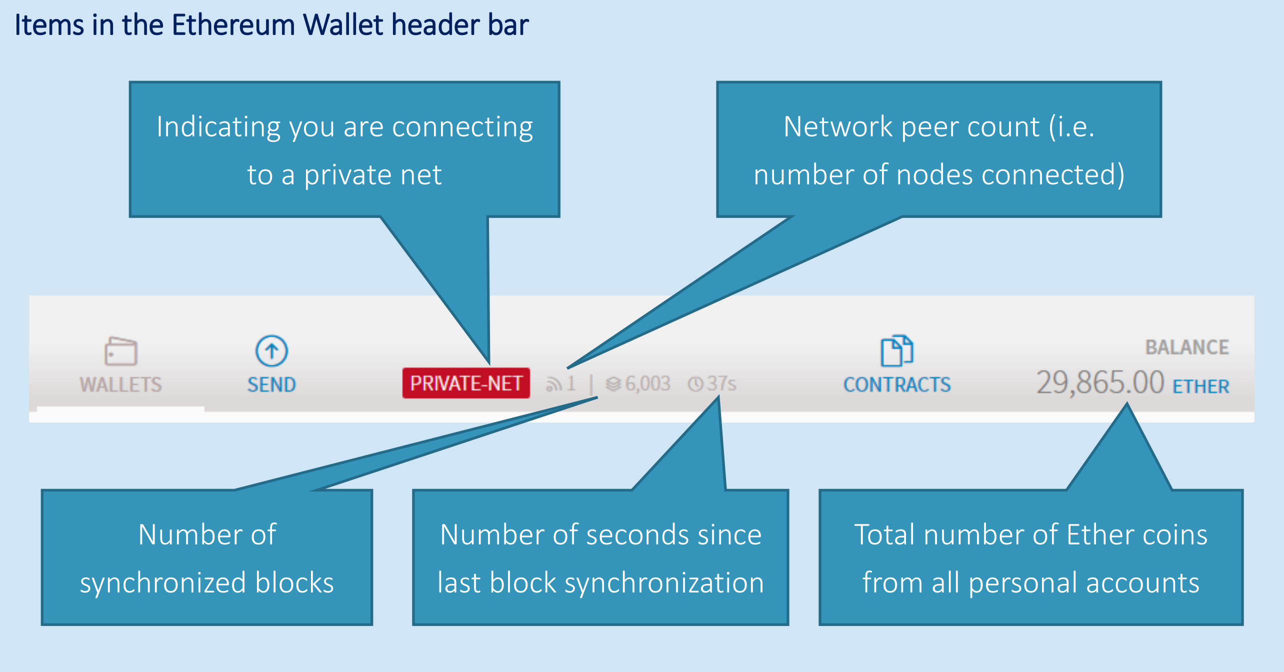
Ethereum CLI vs Ethereum Wallet

Most of the common Ethereum CLI operations can be done in Ethereum Wallet. For example, you can create new personal accounts, check Ether balances, view accounts' transactions, send Ethers from one account to another, check number of connected peers, etc.

However, some of the commands to the Ethereum node can only be done using the Ethereum CLI. For example, start or stop the mining process, view other accounts' transaction, check the Ethereum node's or connected node's information, etc.

In summary, the Ethereum Wallet helps to you manage your accounts easily. On the other hand, the Ethereum CLI provides a full accessibility for you to query information and make function calls.

It is common to use both of them at the same time.



Items in the Ethereum Wallet header bar

Indicating you are connecting to a private net

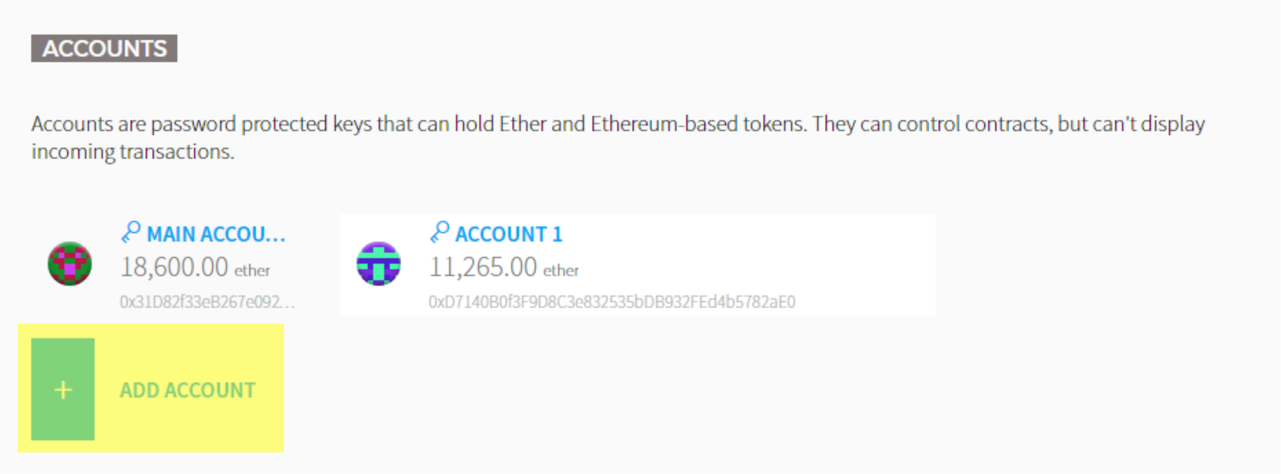
Network peer count (i.e. number of nodes connected)

Number of synchronized blocks

Number of seconds since last block synchronization

Total number of Ether coins from all personal accounts

6. Let’s practice by trying to create a new personal account using the Ethereum Wallet. **In your first computer**, click the “**Add Account**” button under the Accounts section.



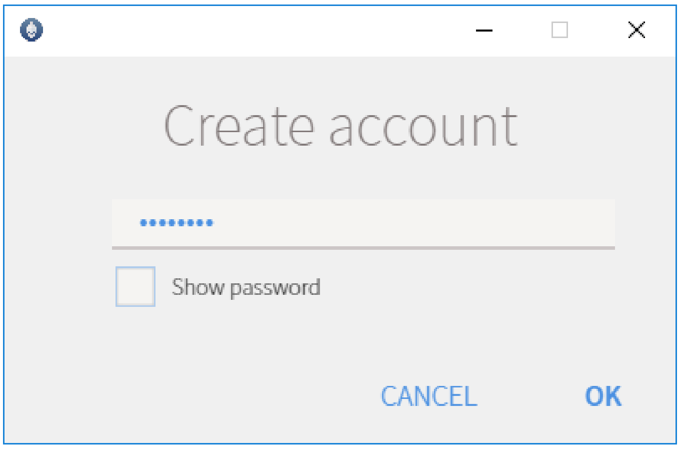
ACCOUNTS

Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.

MAIN ACCOU...
18,600.00 ether
0x31D82f33eB267e092...

ACCOUNT 1
11,265.00 ether
0xD7140B0f3F9D8C3e832535bDB932FEd4b5782aE0

7. **Enter your password for locking the new personal account** → Enter once more to confirm your password **(do not forget your password! There is no forgot password feature in Ethereum!)**

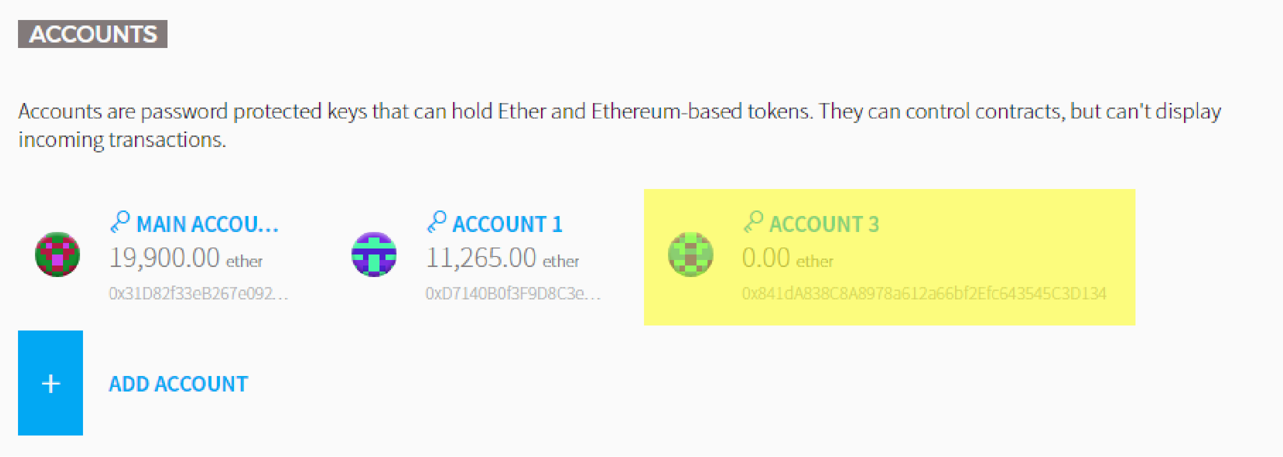


Create account

••••••••

□ Show password

8. Now, a personal account has been created. Let's transfer some Ethers from an account to this new account. **Click your new account item**.



ACCOUNTS

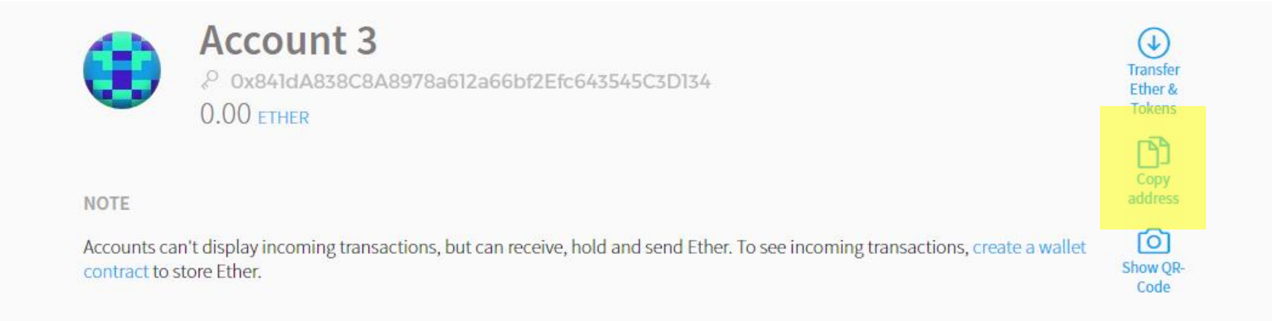
Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.

MAIN ACCOU...
19,900.00 ether
0x31D82f33eB267e092...

ACCOUNT 1
11,265.00 ether
0xD7140B0f3F9D8C3e...

ACCOUNT 3
0.00 ether
0x841dA838C8A8978a612a66bf2Efc643545C3D134

9. Click "**Copy address**" from the right-hand-side → When a dialog is prompted, click "**Copy anyway**".

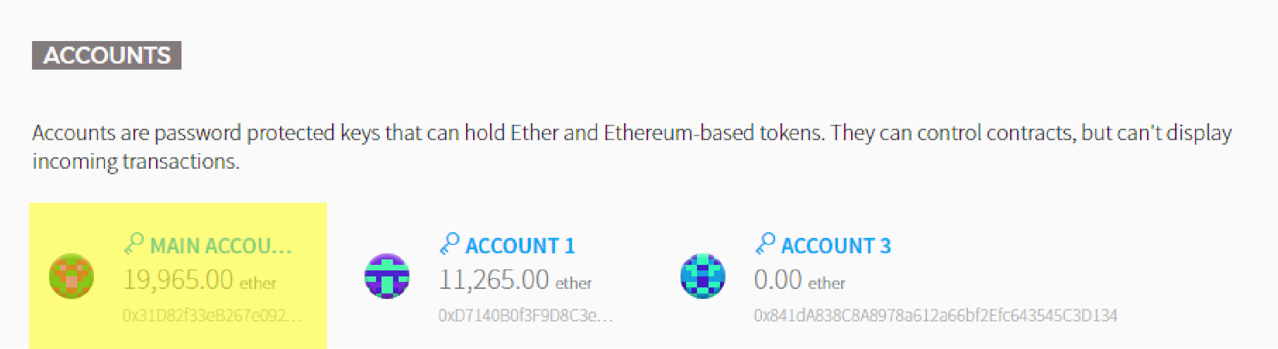


Account 3
0x841dA838C8A8978a612a66bf2Efc643545C3D134
0.00 ETHER

NOTE

Accounts can't display incoming transactions, but can receive, hold and send Ether. To see incoming transactions, create a wallet contract to store Ether.

10. Click "Wallets" for going back to the homepage → select **one of your accounts that contains Ether.**



ACCOUNTS

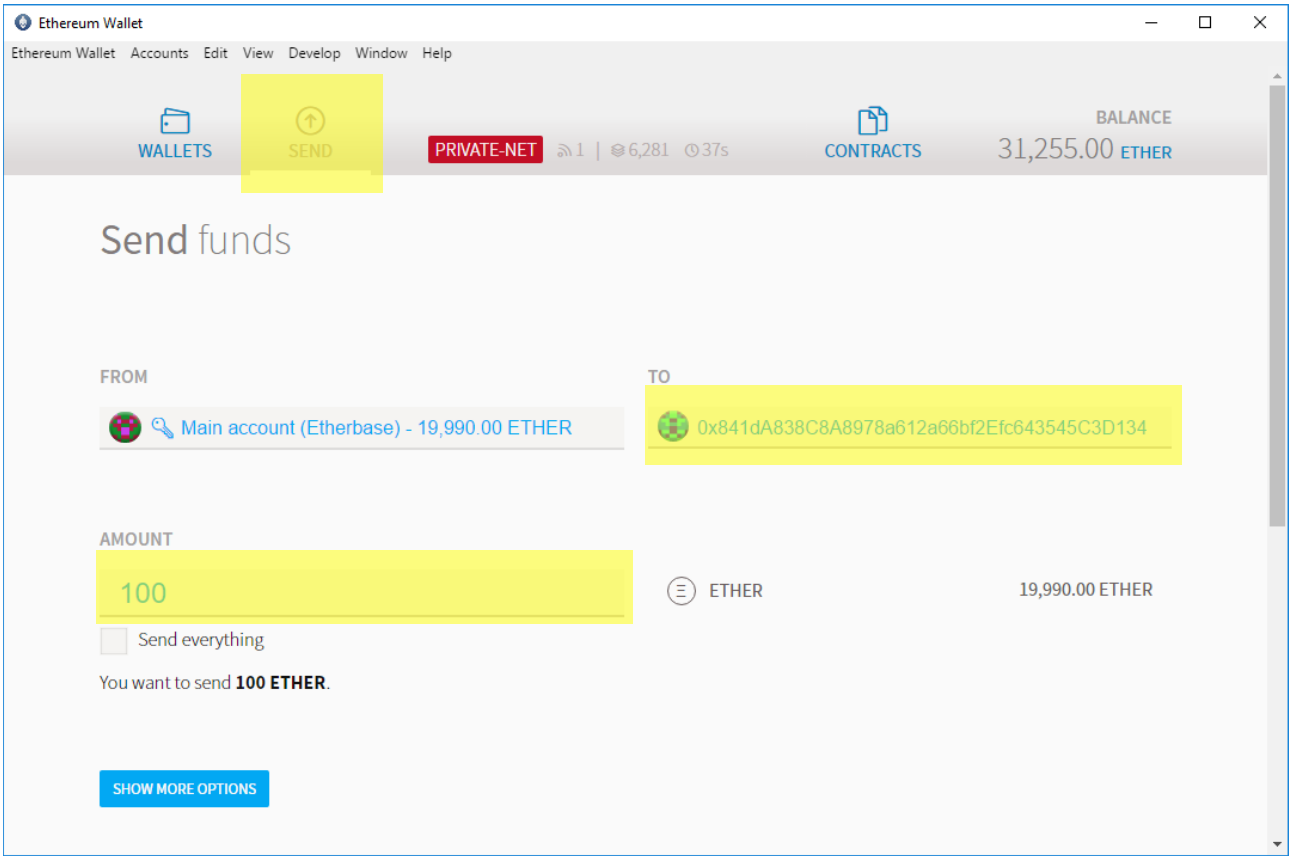
Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.

MAIN ACCOU...
19,965.00 ether
0x31D82f33eB267e092...

ACCOUNT 1
11,265.00 ether
0xD7140B0f3F9D8C3e...

ACCOUNT 3
0.00 ether
0x841dA838C8A8978a612a66bf2Efc643545C3D134

11. Click "**Send**" on top → **Paste the copied address into the "To" textbox → Enter the amount** of Ether coins you want to send.


Ethereum Wallet
Ethereum Wallet Accounts Edit View Develop Window Help
WALLETS
SEND
PRIVATE-NET 1 | 6,281 37s
CONTRACTS
BALANCE
31,255.00 ETHER
SHOW MORE OPTIONS

Send funds

FROM

Main account (Etherbase) - 19,990.00 ETHER

TO

0x841dA838C8A8978a612a66bf2Efc643545C3D134

AMOUNT

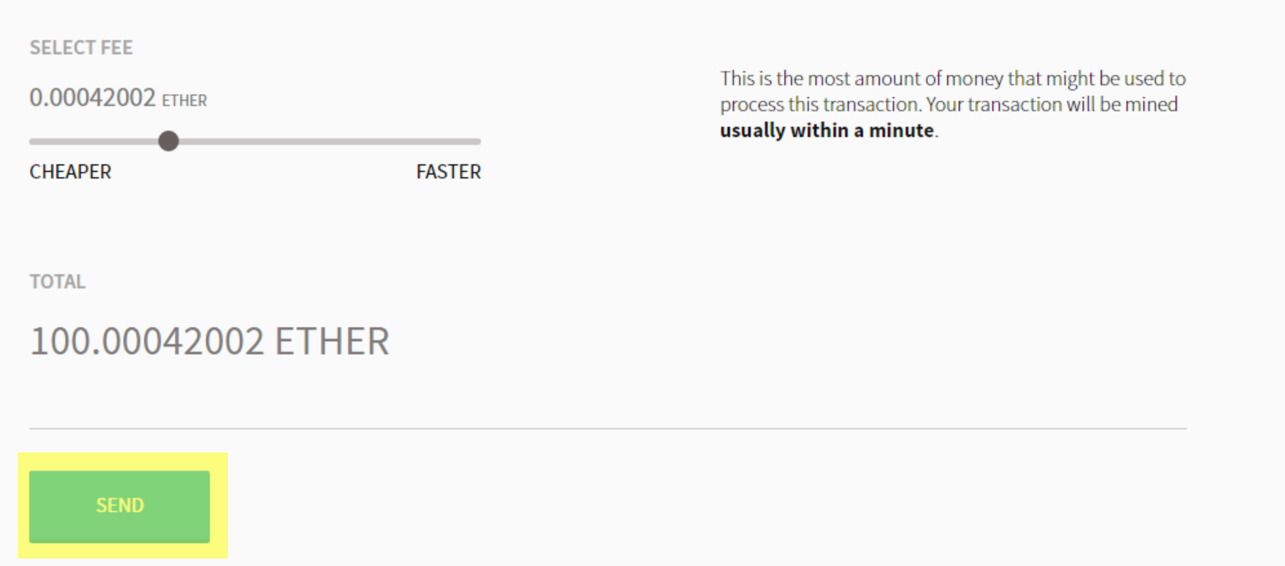
100

ETHER 19,990.00 ETHER

□ Send everything

You want to send **100 ETHER**.

12. Scroll down → **Click the "Send" button (leave the value of "select fee" unchanged)**.



SELECT FEE

0.00042002 ETHER

This is the most amount of money that might be used to process this transaction. Your transaction will be mined **usually within a minute**.

TOTAL

100.00042002 ETHER

What is a select fee?

The select fee is also known as the transaction fee. It acts like a tip for block miners to incentivize them to include your transaction into a new block. It might seem useless in any private net like we are working right now. However, it is meaningful in a very large blockchain network like the Ethereum global net.

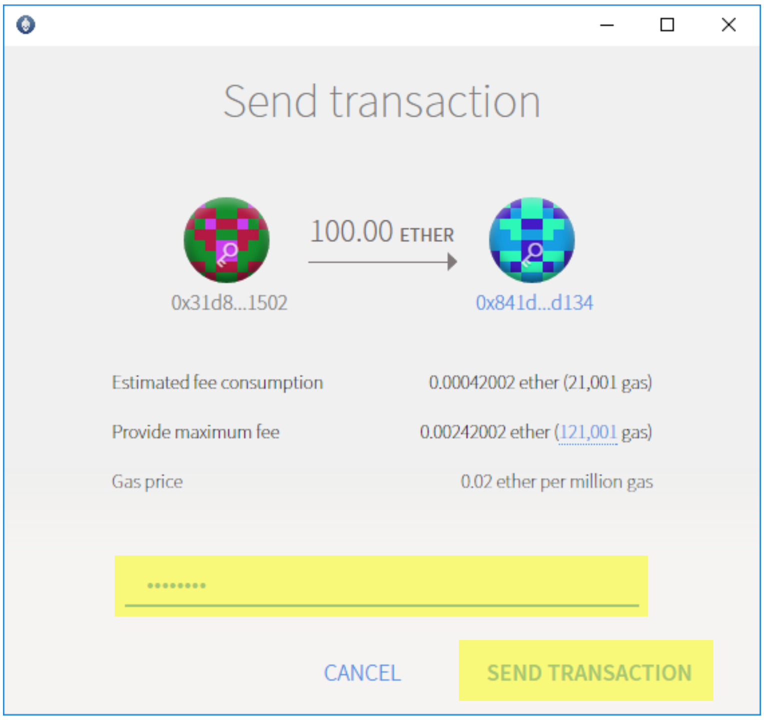
To understand this, you have to know one thing: the size of a block is always limited. That is, it is not possible to save hundreds of megabytes, or even a gigabyte, inside a single block (otherwise, every node will just store endless amount of data). Every block has their storage capacity (in fact, a block in Ethereum is around few kilobytes to few megabytes, depending on the amount and the nature of transactions)

But the number of transactions can be huge in a network like Ethereum global net! So, the problem comes: **as miners, we may not always be able to include all pending transactions to a single block**. For example, there are 10,000 pending transactions out there and we can only include 3,000 of them at once. Which transactions should we pick?

I hope you already see the use of the select fee: Transactions are selected base on the amount of select fee. **The higher the select fee embedded in a transaction, the more eagerness a miner will have for including your transaction into the newly mined block, and thus the faster your transaction is being propagated to all network nodes.**

In private net, we only have a few participants with a few transactions, so you may just ignore the select fee and leave it to the default value.

13. **Enter your personal account's password** to unlock your account → Click "**Send transaction**".



Send transaction

100.00 ETHER

0x31d8...1502 → 0x841d...d134

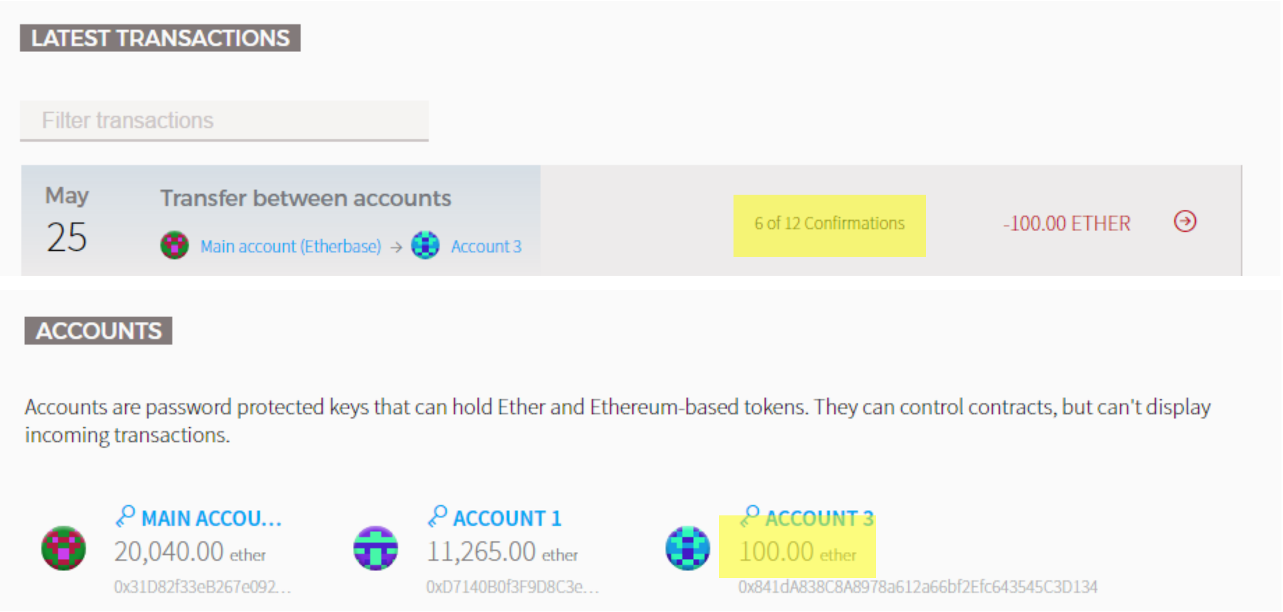
Estimated fee consumption 0.00042002 ether (21,001 gas)

Provide maximum fee 0.00242002 ether (121,001 gas)

Gas price 0.02 ether per million gas

••••••••

14. You will be redirected to the Wallets page → scroll down to the "**Latest transactions**" section, you should see your transaction is greyed out → **Wait a few seconds for the next block being mined → Once there is a confirmation, scroll up and check the new account's balance**.



LATEST TRANSACTIONS

Filter transactions

May 25 Transfer between accounts Main account (Etherbase) → Account 3 6 of 12 Confirmations -100.00 ETHER

ACCOUNTS

Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.

MAIN ACCOU... 20,040.00 ether 0x31D82f33eB267e092...

ACCOUNT 1 11,265.00 ether 0xD7140B0f3F9D8C3e...

ACCOUNT 3 100.00 ether 0x841dA838C8A8978a612a66bf2Efc643545C3D134

What are the confirmations?

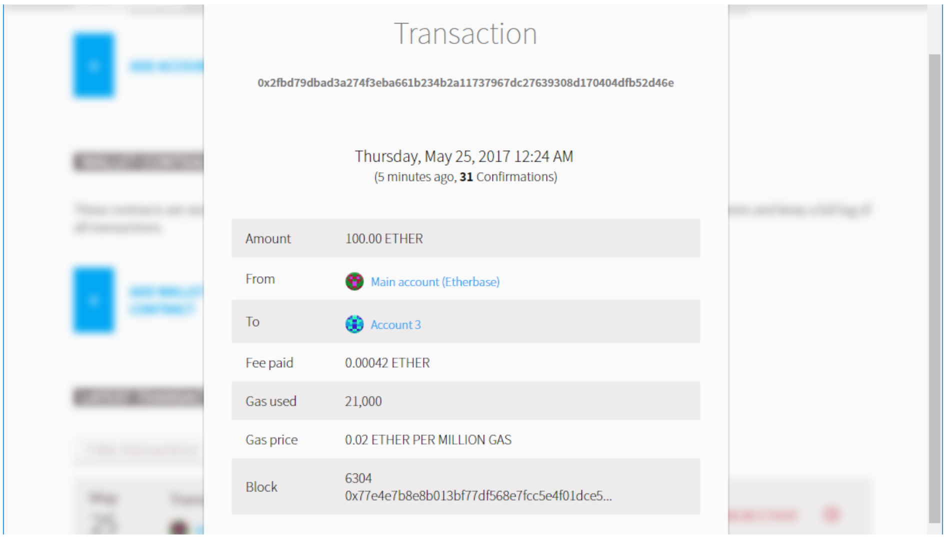
Please look at the "X of 12 confirmations" in your transaction record. What are these confirmations?

If you still remember what we have discussed before, we have mentioned how can a hacker modify a blockchain: he/she must create a longer (but fake) chain than the genuine one and propagates his/her chain to the rest of the network. That is extremely difficult if he/she wants to modify a block, let's say, block #N, in the middle of the chain since he/she needs to recalculate all the hashes and nonce values of all blocks ahead of #N. **That tells us one thing: the older the block, the more difficult for a hacker to hack, and thus more secure.** However, what if a hacker wants to modify a block that is closer to the latest block (for example, block #998 in 1000-length chain)? That is relatively easy compare to a modification of a very old block!

And that is the reason why Ethereum Wallet shows you the number of confirmations. The more confirmations, means the transaction is being buried deeper in the blockchain, and more difficult for a hacker to modify (and thus more secure, too).

If a transaction is being included in block, the Ethereum officials recommends waiting for 12 more blocks to bury that transaction before you take actions base on that (say, you are a retail merchant and someone called Mary pays you Ether to buy some equipment, when you see a transaction that claims "Mary pays you 50 Ether", wait for 12 more blocks before you send her the equipment goods).

15. Scroll down and back to the "**Latest transactions**" section → Click your transaction to review the transaction details and take a look.



Transaction

0x2fbd79dbad3a274f3eba661b234b2a11737967dc27639308d170404dfb52d46e

Thursday, May 25, 2017 12:24 AM
(5 minutes ago, **31** Confirmations)

Amount	100.00 ETHER
From	Main account (Etherbase)
To	Account 3
Fee paid	0.00042 ETHER
Gas used	21,000
Gas price	0.02 ETHER PER MILLION GAS
Block	6304 0x77e4e7b8e8b013bf77df568e7fcc5e4f01dce5...

Deploy your first smart contract

What is a smart contract?

Until now, we have played around with personal accounts: sending Ethers from one account to another. However, we still haven't witness the true power of Ethereum: smart contract.

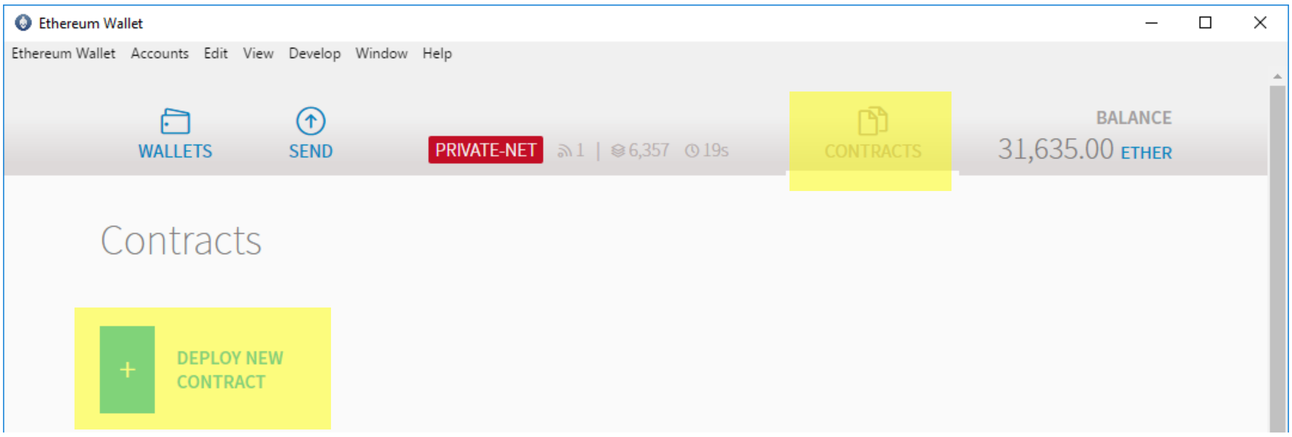
Smart contract is a small piece of program that runs on a Ethereum network. One of the smart contract programming language is called **Solidity**, which is "Turing-complete". That is, the language provides variable constructions and logic flow statements like if-else and for-loop to let you program almost anything (In theory only, to be honest. There are some limitations in smart contract programming).

Unlike traditional applications, where applications are stored and executed by a single server or entity, **a smart contract is run by all Ethereum network nodes**. This feature allows users and developers to create custom behavior and logic inside the blockchain network, or act as a virtual middleman.

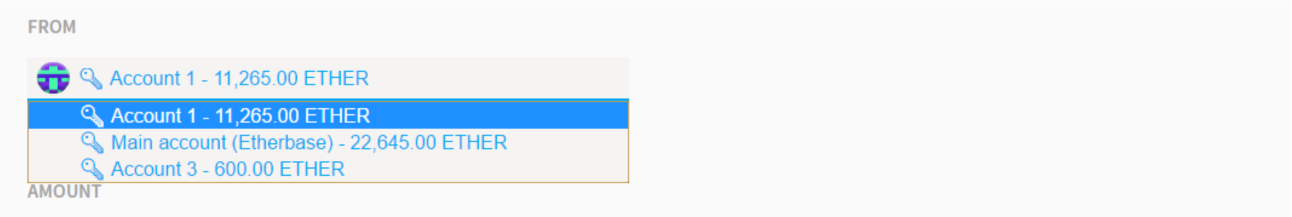
Same as transactions, **any smart contract code being published onto the blockchain are publicly-accessible and immutable**. Note that the immutability only applies to the code itself, but not the states (i.e. variables) of the smart contract. That is, **everyone is not allowed to modify the code, but able to change state values** by calling smart contract functions (which is being done by sending transactions to the contract). Since all transactions are being recorded onto the blockchain and they are immutable, therefore, **even though someone changes a variable of a smart contract, all users will be able to trace all versions of the variable values by looking into the blockchain.**

16. In your first computer, click "**Contracts**" on top of the Ethereum Wallet → click "**Deploy new**

contract".



17. Select an account that contains some Ether.



FROM

Account 1 - 11,265.00 ETHER

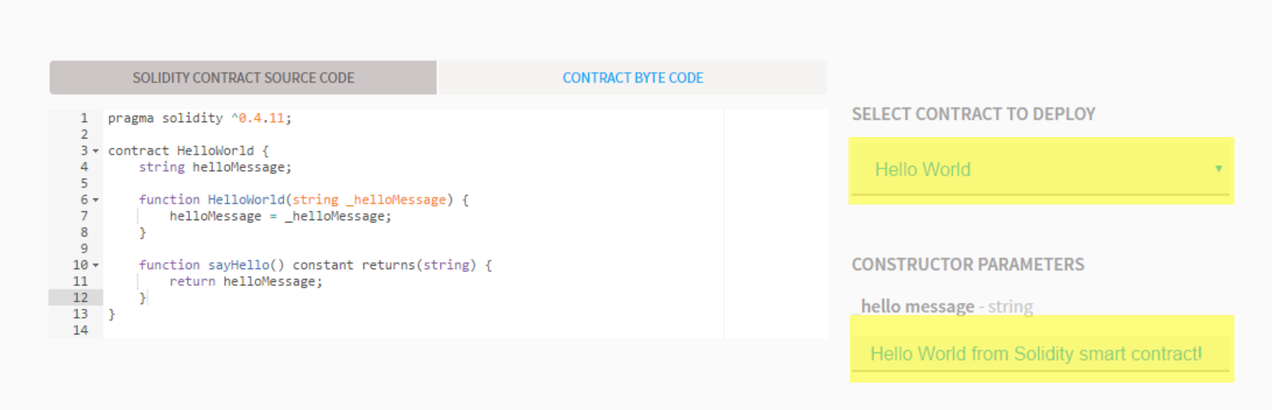
Account 1 - 11,265.00 ETHER
Main account (Etherbase) - 22,645.00 ETHER
Account 3 - 600.00 ETHER

AMOUNT

18. Scroll down to the "**Solidity contract source code**" section → **Enter the following program into the textbox**.

```
pragma solidity ^0.4.11;

contract HelloWorld {
    string helloMessage;

    function HelloWorld(string _helloMessage) {
        helloMessage = _helloMessage;
    }

    function sayHello() constant returns(string) {
        return helloMessage;
    }

    function changeHello(string _newHelloMessage) {
        helloMessage = _newHelloMessage;
    }
}
```

19. On the right-hand-side, select "**Hello World**" in the "Select contract to deploy" menu → After the selection, a textbox should appear below → In the "Constructor parameters", enter "**Hello World from Solidity smart contract!**" into the textbox.



```
pragma solidity ^0.4.11;

contract HelloWorld {
    string helloMessage;

    function HelloWorld(string _helloMessage) {
        helloMessage = _helloMessage;
    }

    function sayHello() constant returns(string) {
        return helloMessage;
    }
}
```

SELECT CONTRACT TO DEPLOY

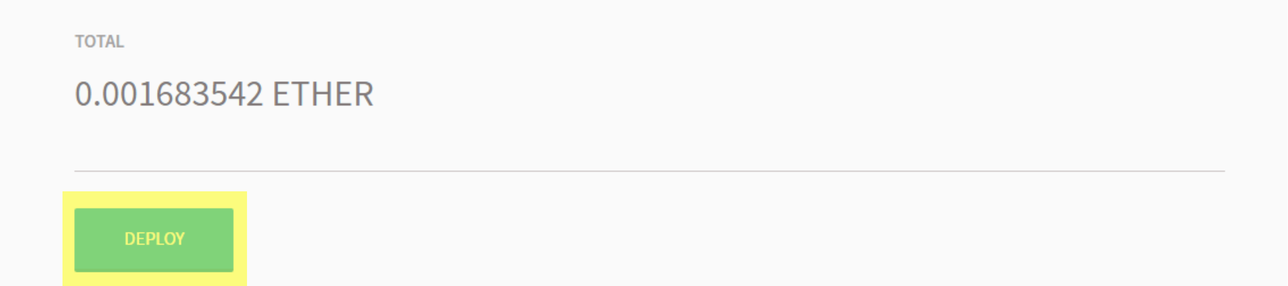
Hello World

CONSTRUCTOR PARAMETERS

hello message - string

Hello World from Solidity smart contract!

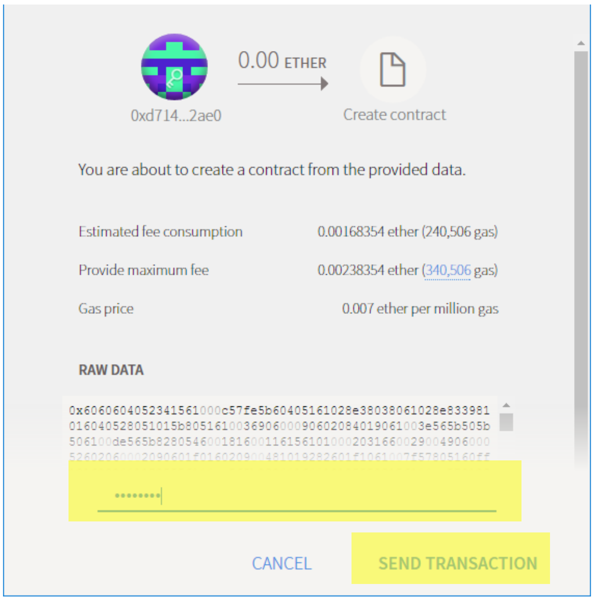
20. **Scroll down and click "Deploy"** (ignore the select fee)



TOTAL

0.001683542 ETHER

21. A confirmation dialog should appear → **Enter your account's password** → Click "**Send transaction**".



0xd714...2ae0

0.00 ETHER

Create contract

You are about to create a contract from the provided data.

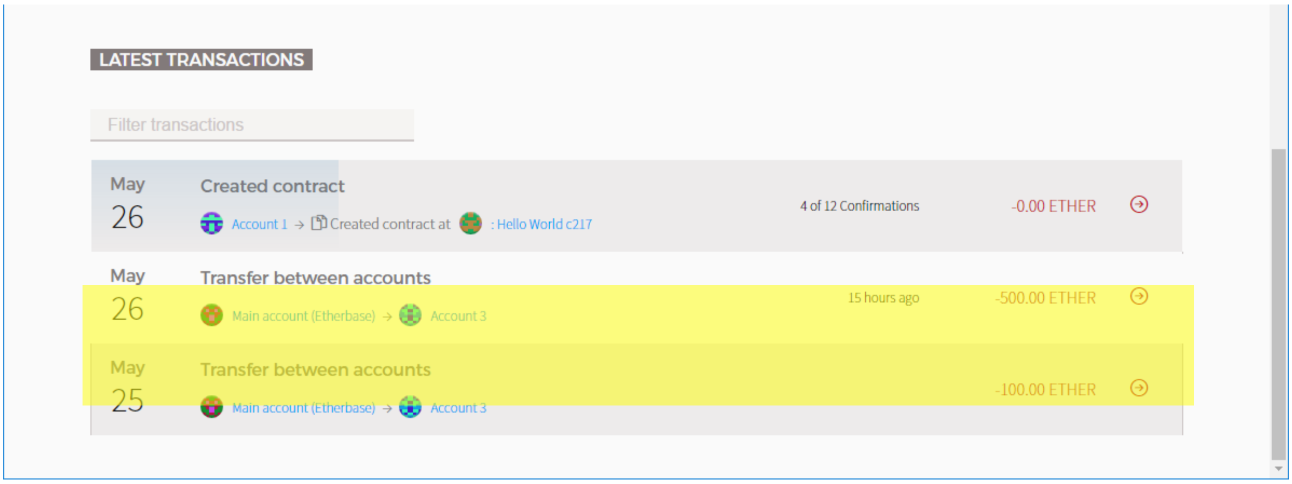
Estimated fee consumption	0.00168354 ether (240,506 gas)
Provide maximum fee	0.00238354 ether (340,506 gas)
Gas price	0.007 ether per million gas

RAW DATA

```
0x6060604052341561000c57fe5b60405161028e38038061028e833981
01604052805101 5b805161003690600090602084019061003e565b505b
506100de565b828054600181600116156101000203166002900490600
5260206000209060 1f016020900481019282601f10610 07f57805160ff
```

••••••••

22. When the transaction is sent, you will be redirected back to the Wallets homepage → Scroll down and check your **contract creation transaction** in the “Latest transactions” section.



LATEST TRANSACTIONS

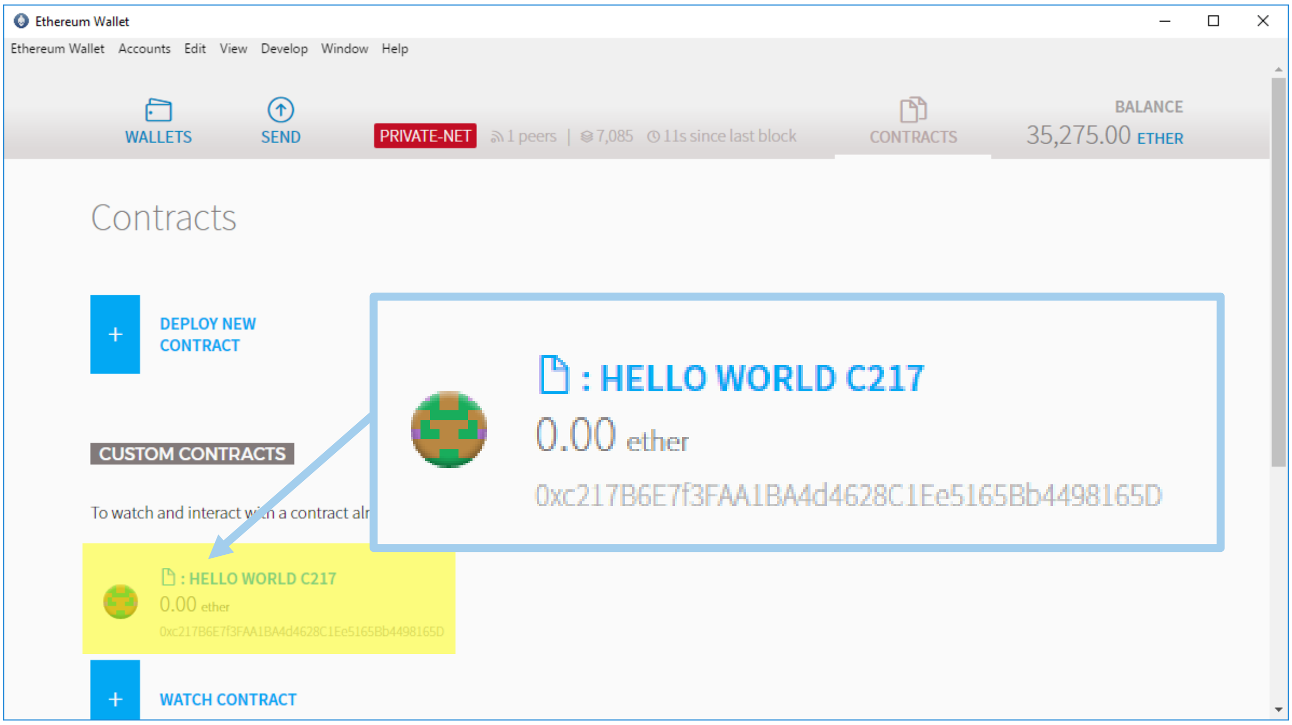
Filter transactions

May 26 Created contract — Account 1 → Created contract at : Hello World c217 — 4 of 12 Confirmations — -0.00 ETHER

May 26 Transfer between accounts — Main account (Etherbase) → Account 3 — 15 hours ago — -500.00 ETHER

May 25 Transfer between accounts — Main account (Etherbase) → Account 3 — -100.00 ETHER

23. Once there are some confirmations, back to the “Contracts” page → **You should see your contract is being deployed in the “Custom contracts” section** (you may have a different contract name then mine, the Ethereum auto-generates a contract name for you).



Ethereum Wallet
Ethereum Wallet Accounts Edit View Develop Window Help
WALLETS
SEND
PRIVATE-NET
1 peers | 7,085 11s since last block
CONTRACTS
BALANCE
35,275.00 ETHER
Contracts
DEPLOY NEW CONTRACT
CUSTOM CONTRACTS
To watch and interact with a contract alr
WATCH CONTRACT

: HELLO WORLD C217
0.00 ether
0xc217B6E7f3FAA1BA4d4628C1Ee5165Bb4498165D

Contract account vs personal account

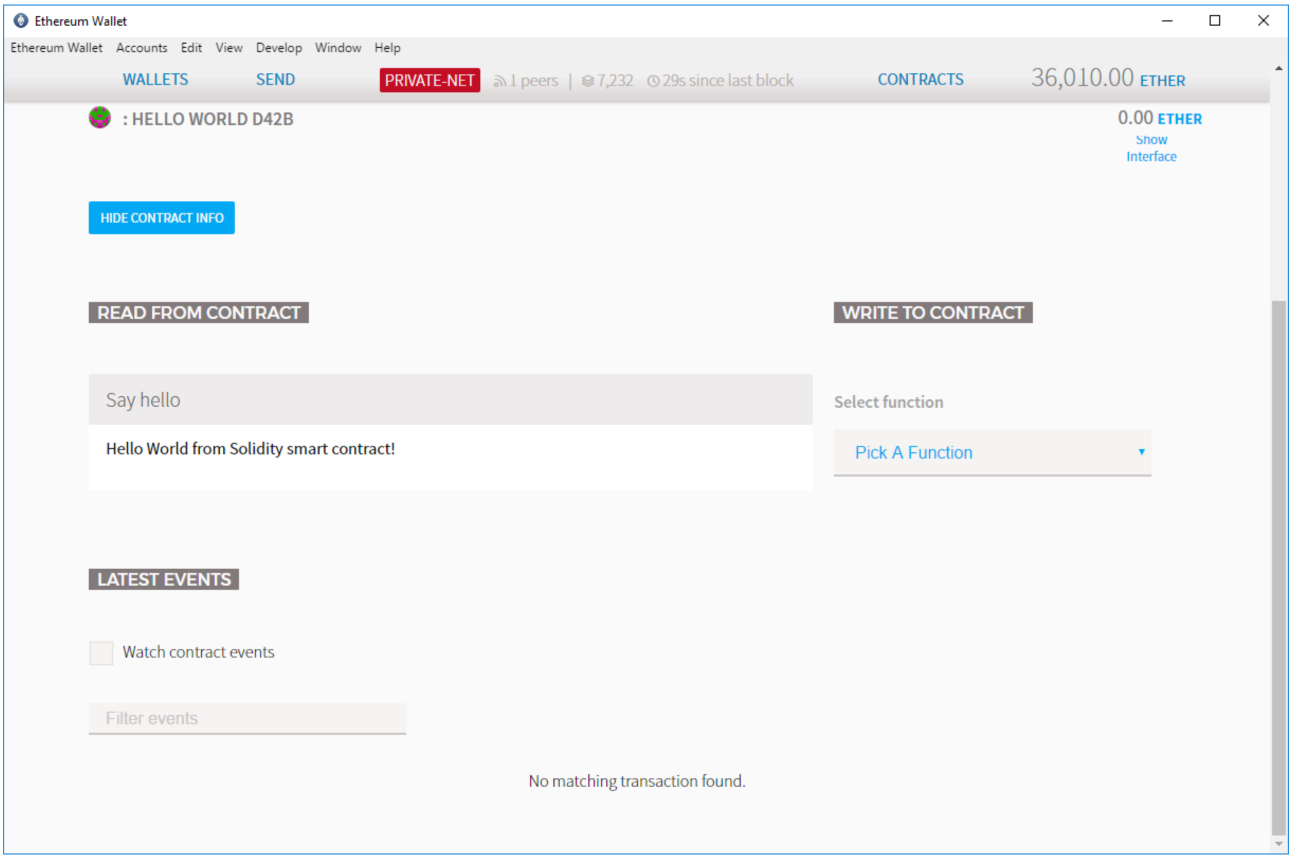
Please note that smart contract is also an account too, which is known as the “contract account”.

There are some similarities and differences between contract accounts and personal accounts.

- **Similarities**: Both of them uses public keys as addresses; They all can own Ethers.
- **Differences**: Contract account can store code while personal account cannot; No users own a contract account’s private key.

Run your smart contract

24. **Click your smart contract in the "Contracts" page →** Check the "Read from contract" and "Write to contract" sections.



Hello World from Solidity smart contract!

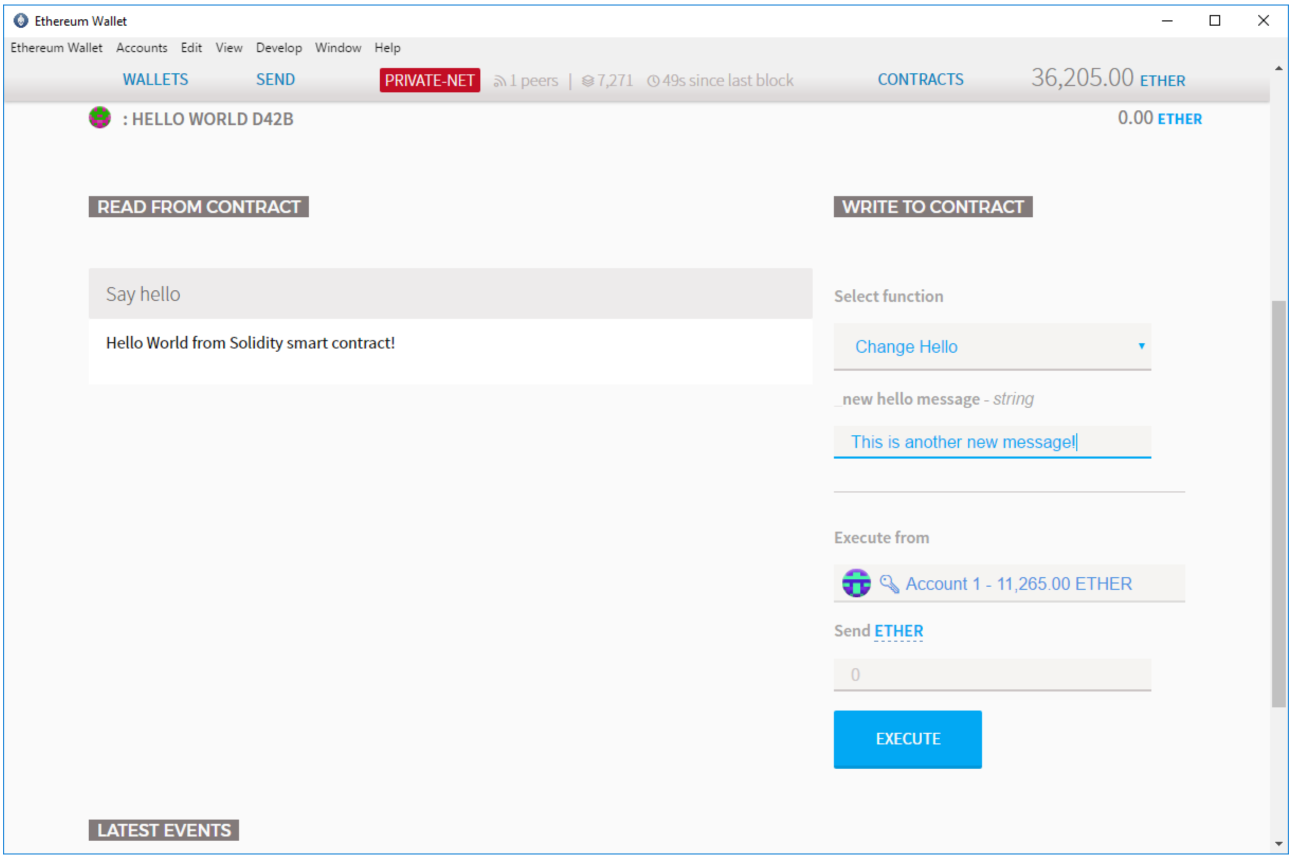
No matching transaction found.

Explanations:

The "Read from contract" section on the left shows all contract constant functions' return values in the blockchain. For example, in our smart contract, we have a function called "sayHello" and it returns the value of the variable "helloMessage". Since we have set the value of that variable when we deploy the contract. Therefore, it shows "Hello World from Solidity smart contract!".

On the right-hand-side, we can pick a smart contract function to call. In our smart contract, we have a function called "changeHello". If you pick that function and provide a string parameter, the value of the variable "helloMessage" will change.

25. In the “Select function” menu, pick the “**Change Hello**” function → **In the “_new hello message” textbox, input whatever text you want to change** → Select an account with some Ethers → click “**Execute**” → Input your account’s password.



: HELLO WORLD D42B 0.00 ETHER

Say hello

Hello World from Solidity smart contract!

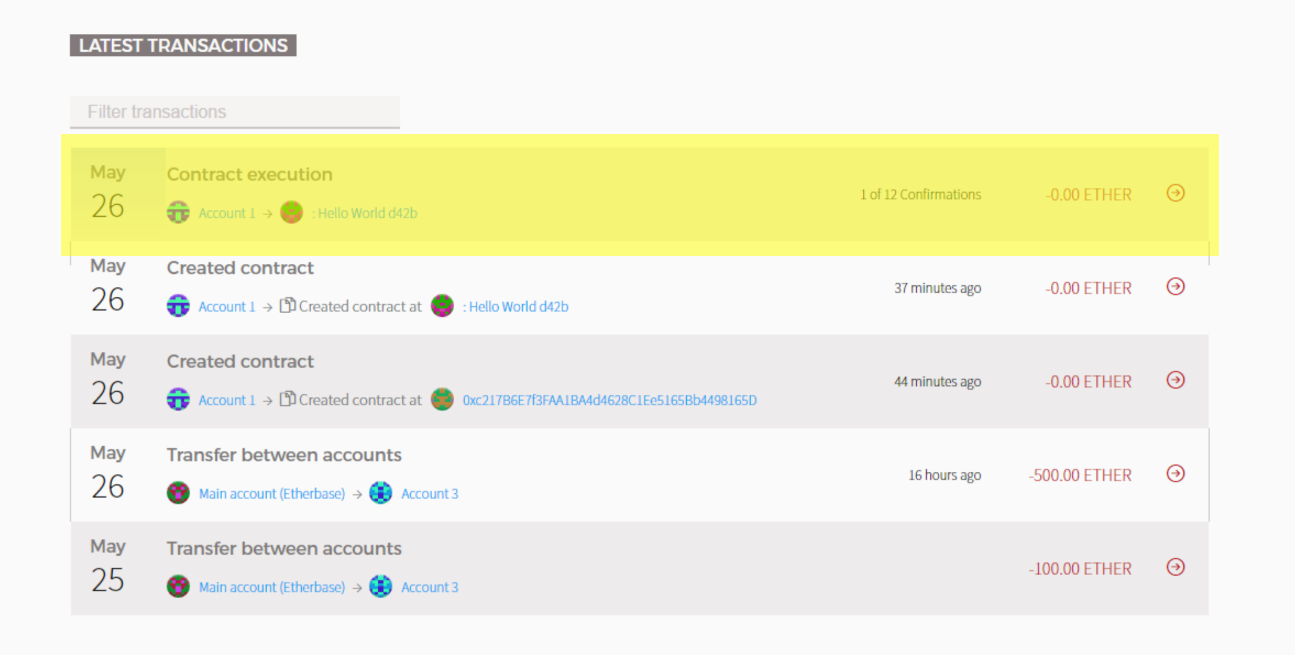
Select function: Change Hello

_new hello message - *string*: This is another new message!

Execute from: Account 1 - 11,265.00 ETHER

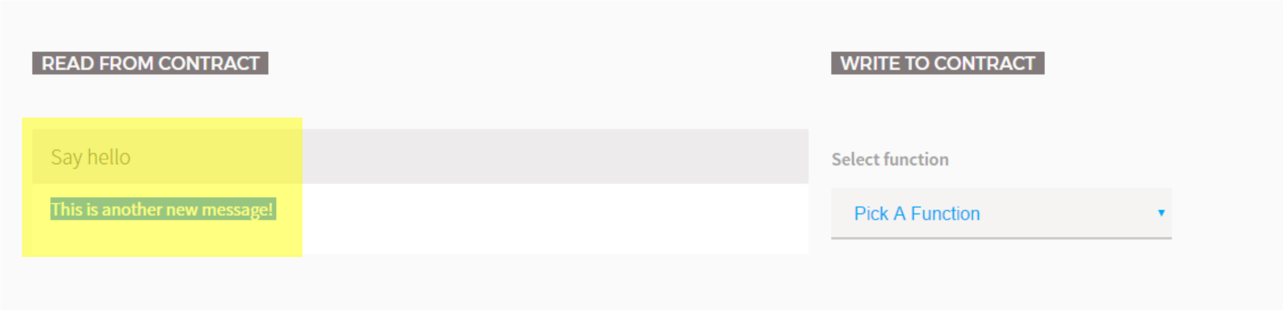
Send ETHER: 0

26. You should see a green-colored “Transaction sent” dialog box pops up → **Back to the Wallets homepage → Check your new transaction → wait for a confirmation.**



May 26	Contract execution Account 1 → : Hello World d42b	1 of 12 Confirmations	-0.00 ETHER
May 26	Created contract Account 1 → Created contract at : Hello World d42b	37 minutes ago	-0.00 ETHER
May 26	Created contract Account 1 → Created contract at 0xc217B6E7f3FAA1BA4d4628C1Ee5165Bb4498165D	44 minutes ago	-0.00 ETHER
May 26	Transfer between accounts Main account (Etherbase) → Account 3	16 hours ago	-500.00 ETHER
May 25	Transfer between accounts Main account (Etherbase) → Account 3		-100.00 ETHER

27. Back to the **Contracts** page → Click your contract → Check to see if your new hello message is there. **You should have your new message in the "Say hello" function like below**.

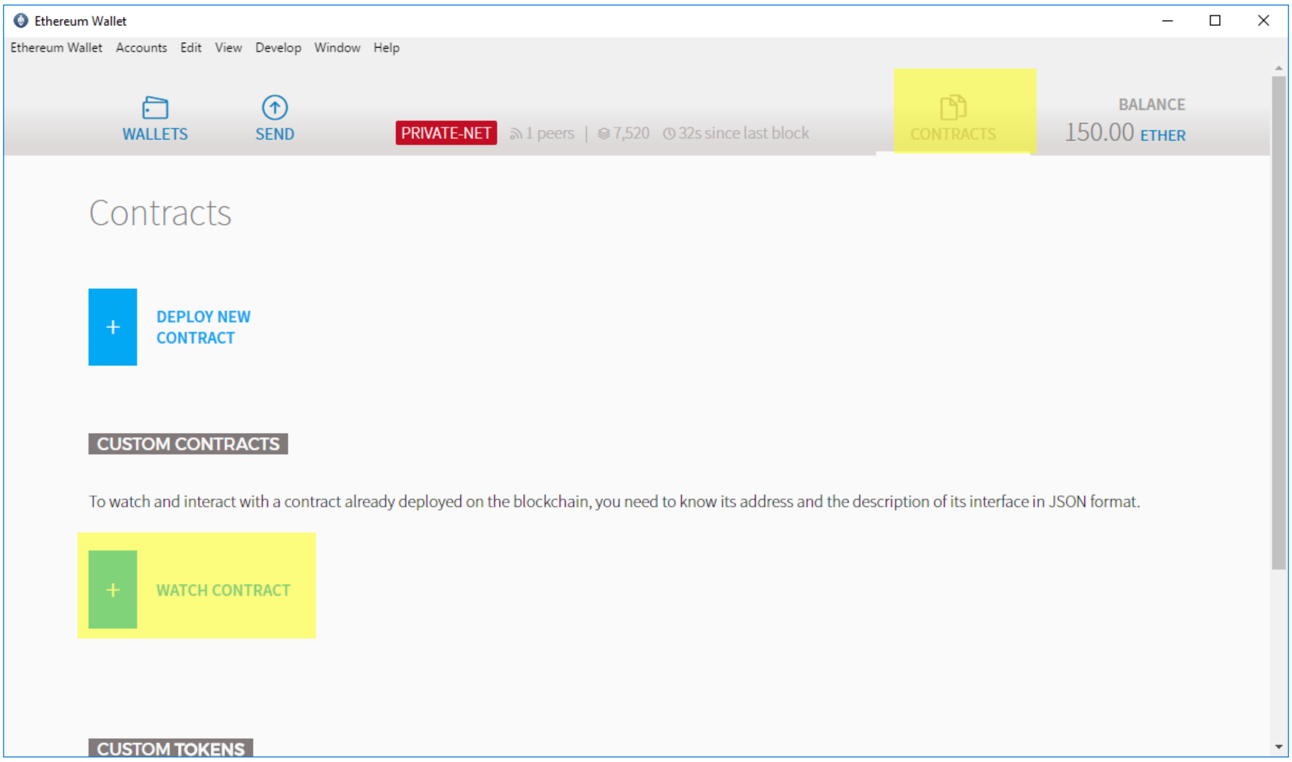


Explanations:
Now, you have changed the value inside your smart contract! Such change is also already propagated across your Ethereum private network. **All network nodes should see the same value same this by now**!

Run the smart contract in other network nodes

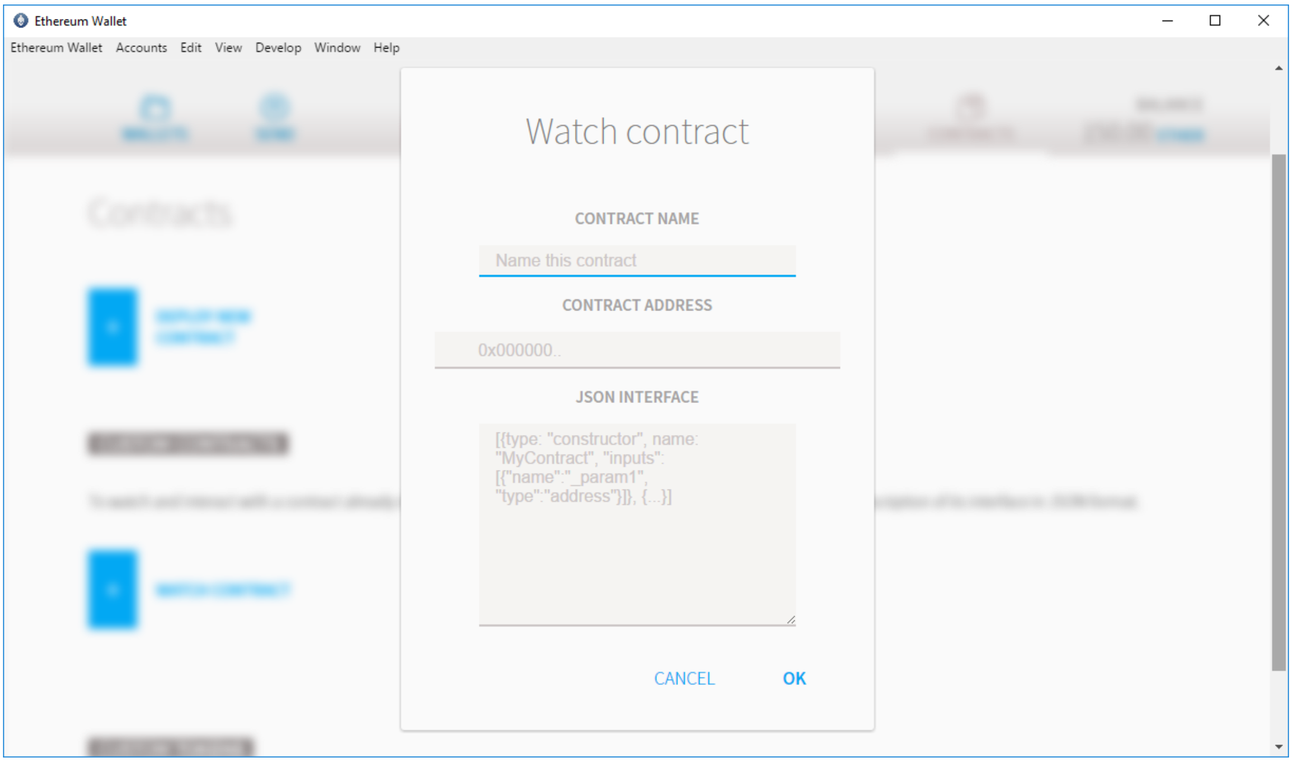
You have already deployed a smart contract onto your Ethereum private network. That means, **your smart contract is now public and everyone on the network can view, use or call your smart contract**. Now, let's try to view and call your smart contract in your second computer.

28. **Switch to your second computer** → Click Contracts → Click "Watch contract" button.

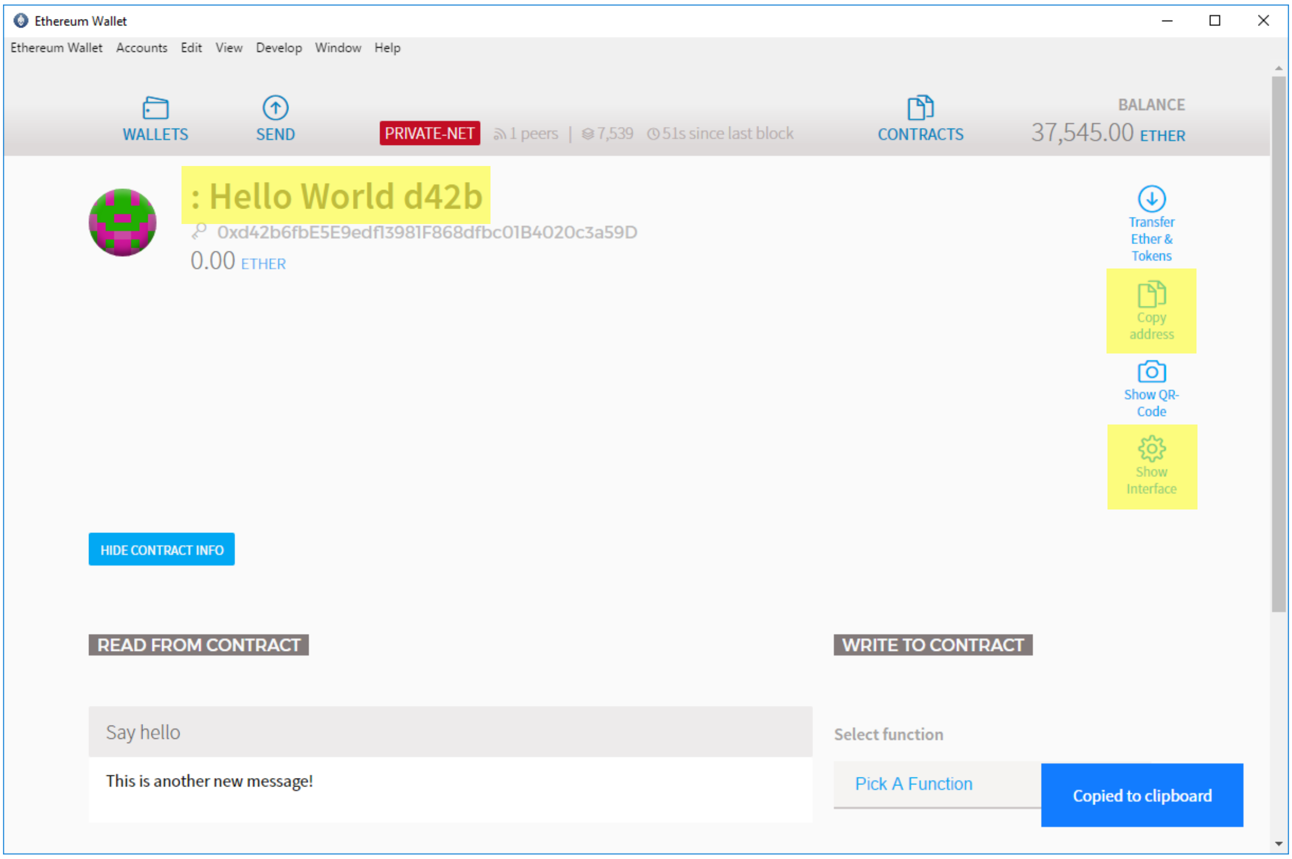


To watch and interact with a contract already deployed on the blockchain, you need to know its address and the description of its interface in JSON format.

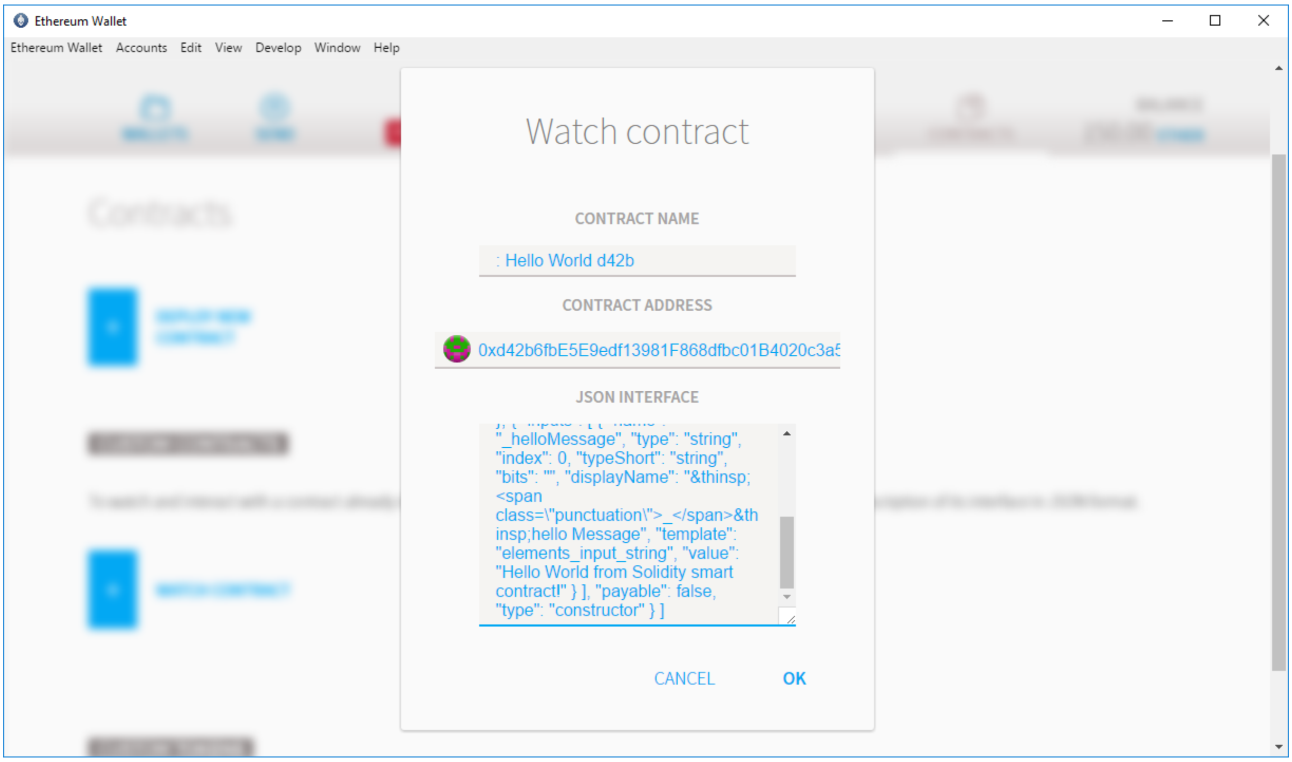
29. You are asked to provide a name of the contract, the contract account address and the contract JSON interface.


Ethereum Wallet
Ethereum Wallet Accounts Edit View Develop Window Help
Watch contract
CONTRACT NAME
Name this contract
CONTRACT ADDRESS
0x000000..
JSON INTERFACE
[{type: "constructor", name: "MyContract", "inputs": [{"name":"_param1", "type":"address"}]}, {...}]
CANCEL
OK

30. **Switch back to your first computer → Copy the name, contract account address and JSON interface** by clicking the buttons highlighted below → **paste the copied string back** to the dialog (see the previous image) in your second computer.



31. Click OK.



Watch contract

CONTRACT NAME

: Hello World d42b

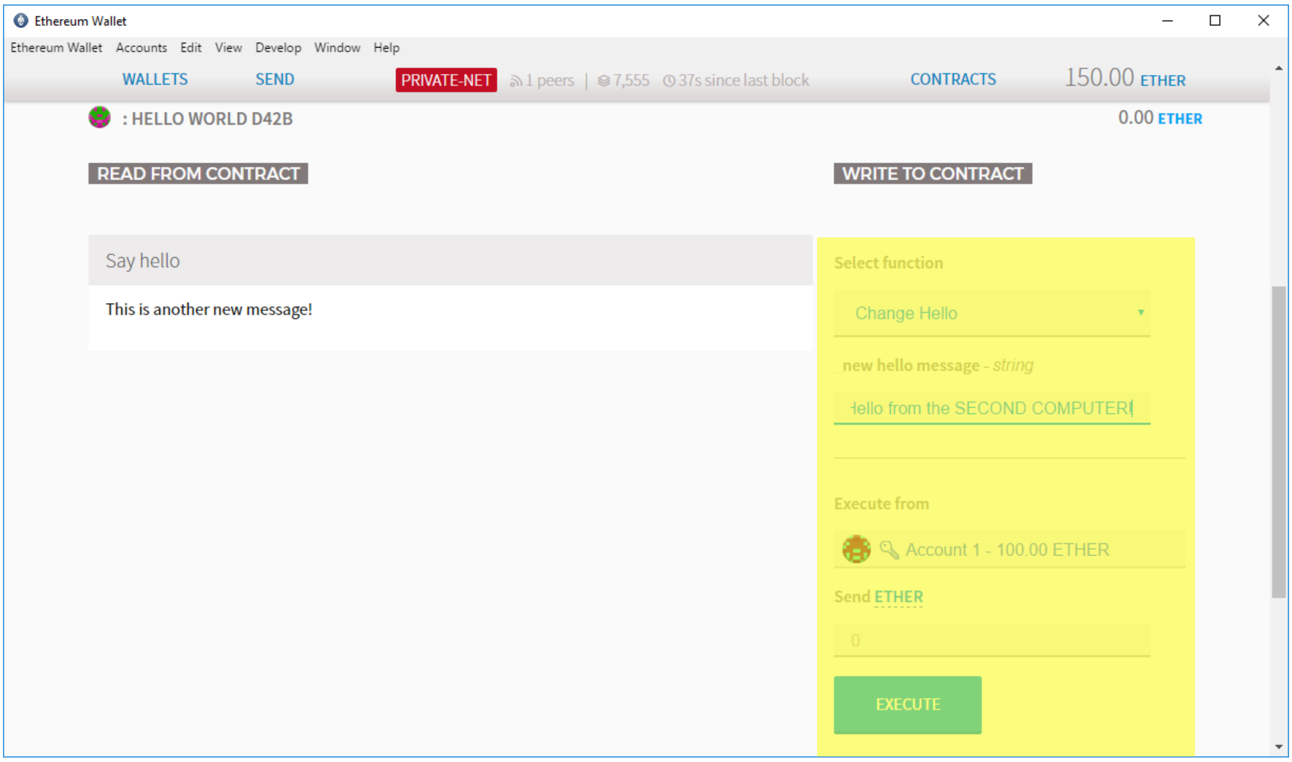
CONTRACT ADDRESS

0xd42b6fbE5E9edf13981F868dfbc01B4020c3a5

JSON INTERFACE

```
"_helloMessage", "type": "string",
"index": 0, "typeShort": "string",
"bits": "", "displayName": "&thinsp;
<span
class=\"punctuation\">_</span>&th
insp;hello Message", "template":
"elements_input_string", "value":
"Hello World from Solidity smart
contract!" } ], "payable": false,
"type": "constructor" } ]
```

32. **Now, your second computer is able to interact with your smart contract.** → Click the smart contract → Select an account with Ethers and change the message like what you have just did.


Ethereum Wallet
Ethereum Wallet Accounts Edit View Develop Window Help
WALLETS
SEND
PRIVATE-NET
1 peers | 7,555 37s since last block
CONTRACTS
150.00 ETHER
EXECUTE

: HELLO WORLD D42B

0.00 ETHER

READ FROM CONTRACT

Say hello

This is another new message!

WRITE TO CONTRACT

Select function

Change Hello

new hello message - *string*

Hello from the SECOND COMPUTER!

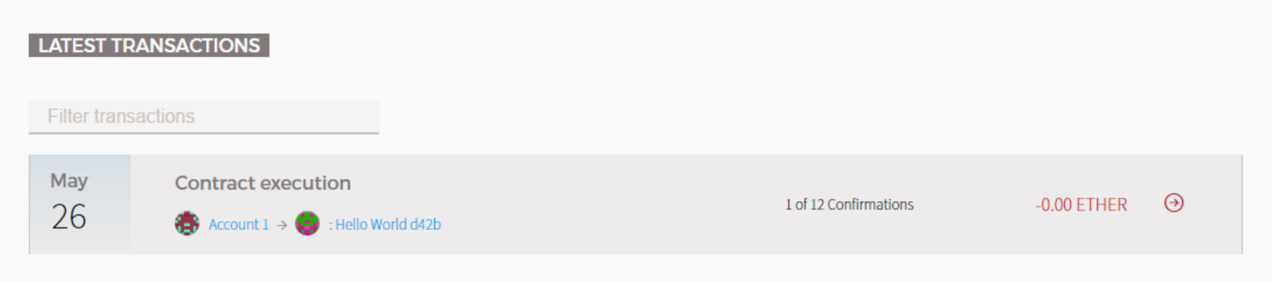
Execute from

Account 1 - 100.00 ETHER

Send ETHER

0

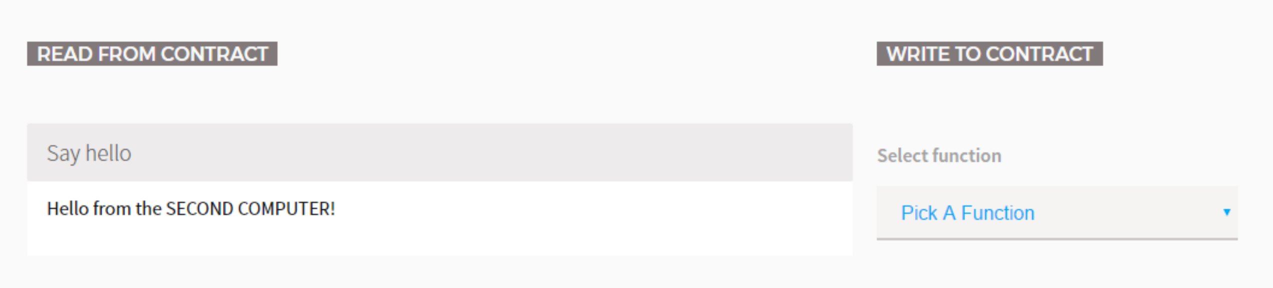
33. Execute the transaction → Back to the Wallets homepage and wait for the next block being mined → When mined, back to the contract page and check if the text has been modified.



LATEST TRANSACTIONS

Filter transactions

May 26 Contract execution Account 1 → : Hello World d42b 1 of 12 Confirmations -0.00 ETHER



READ FROM CONTRACT

Say hello

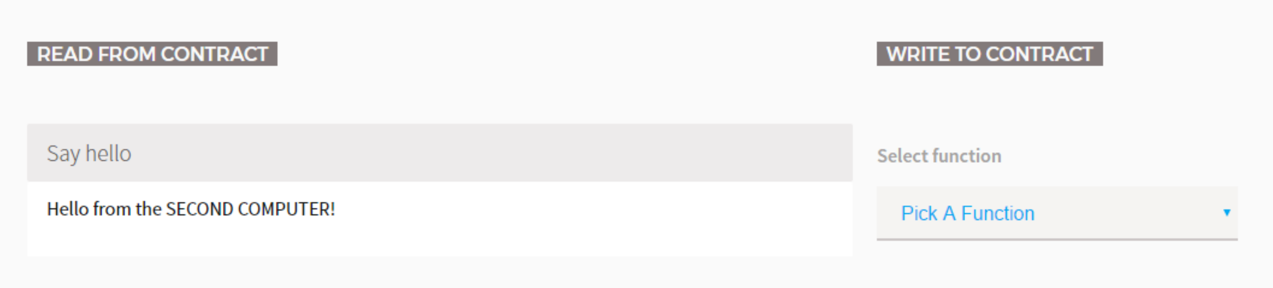
Hello from the SECOND COMPUTER!

WRITE TO CONTRACT

Select function

Pick A Function

34. Back to your first computer → enter your contract's page and check if the text has been modified.



READ FROM CONTRACT

Say hello

Hello from the SECOND COMPUTER!

WRITE TO CONTRACT

Select function

Pick A Function

Explanations:

The results are the same! As you can see, both computers share the same data! You have just created a contract in your first computer, modified the variable string, and then modified it again on your second computer!

Note that your smart contract is now public. Everyone on your Ethereum private network can view, use or call it.

References

1. Ethereum Official Website
   https://www.ethereum.org/

2. Ethereum Wallet and Mist GitHub:
   https://github.com/ethereum/mist/releases

3. Solidity Official Documentation Website
   https://solidity.readthedocs.io/en/develop/