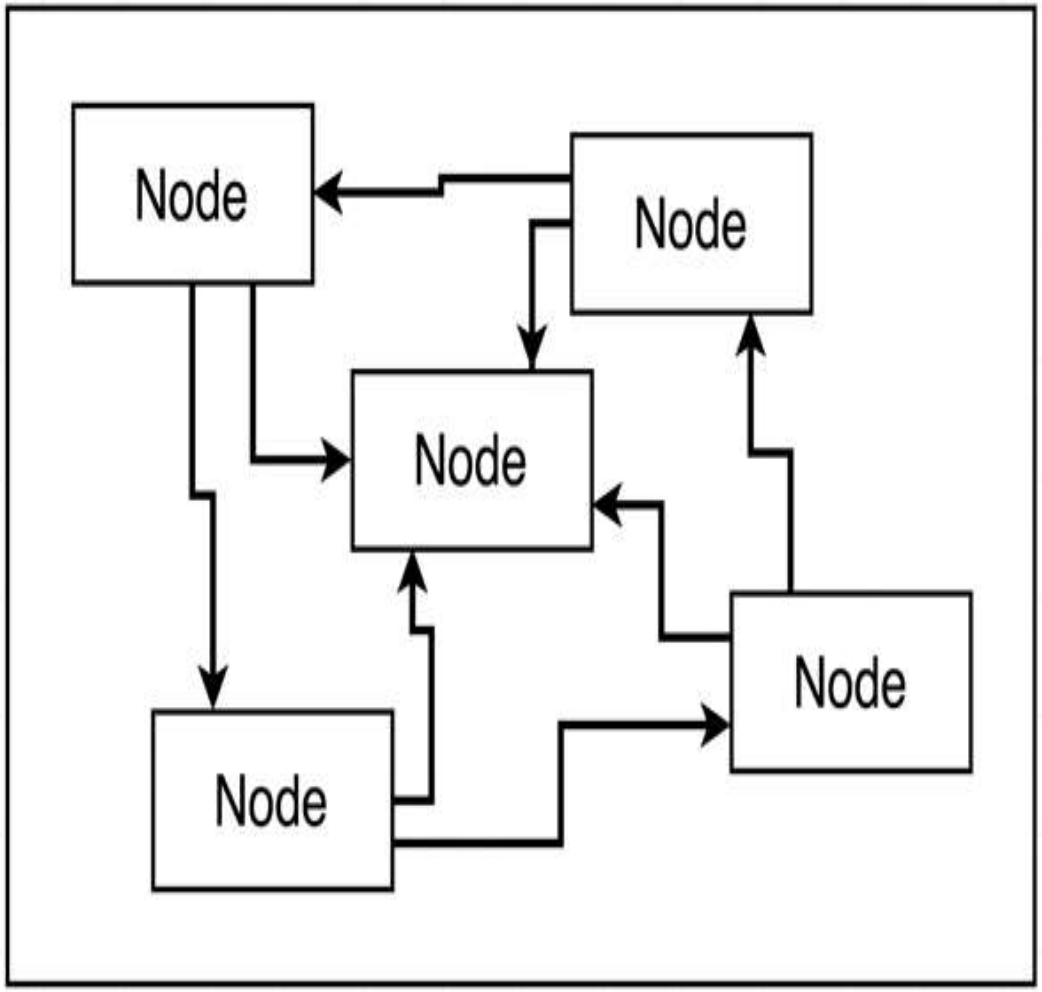
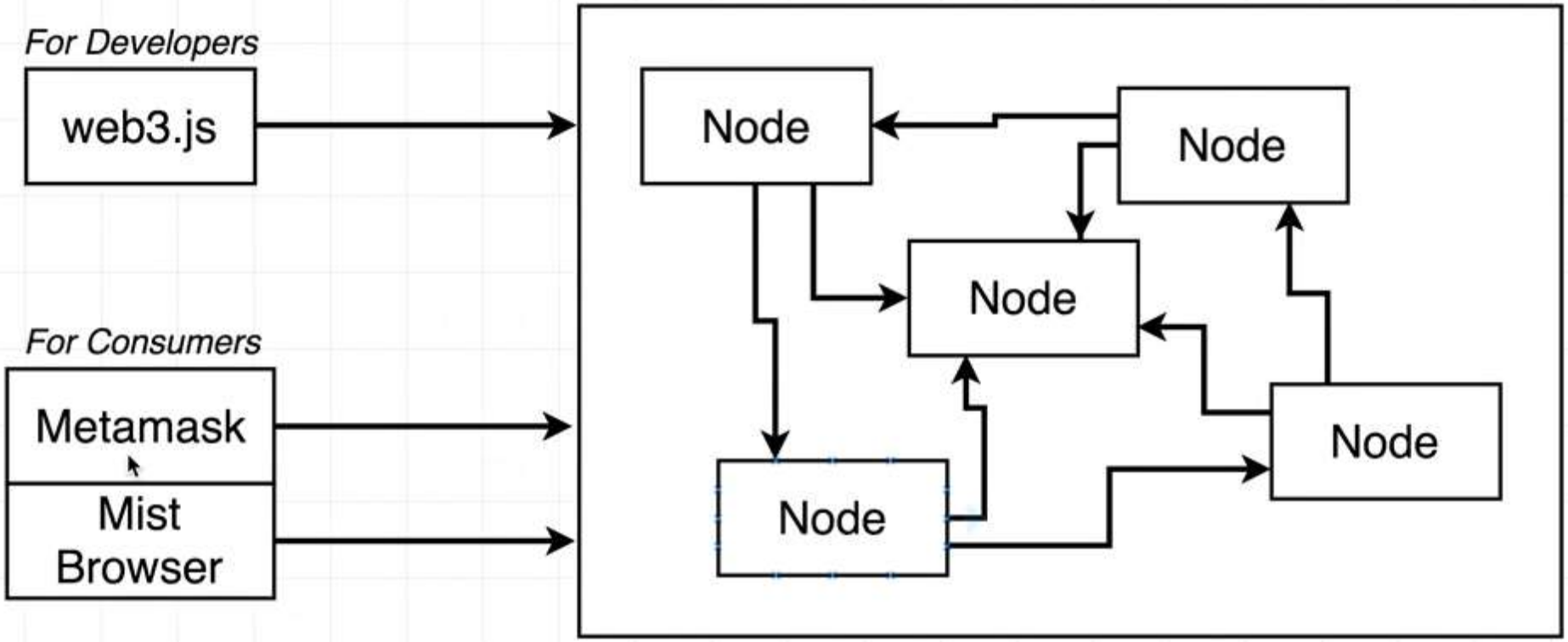
ethereum

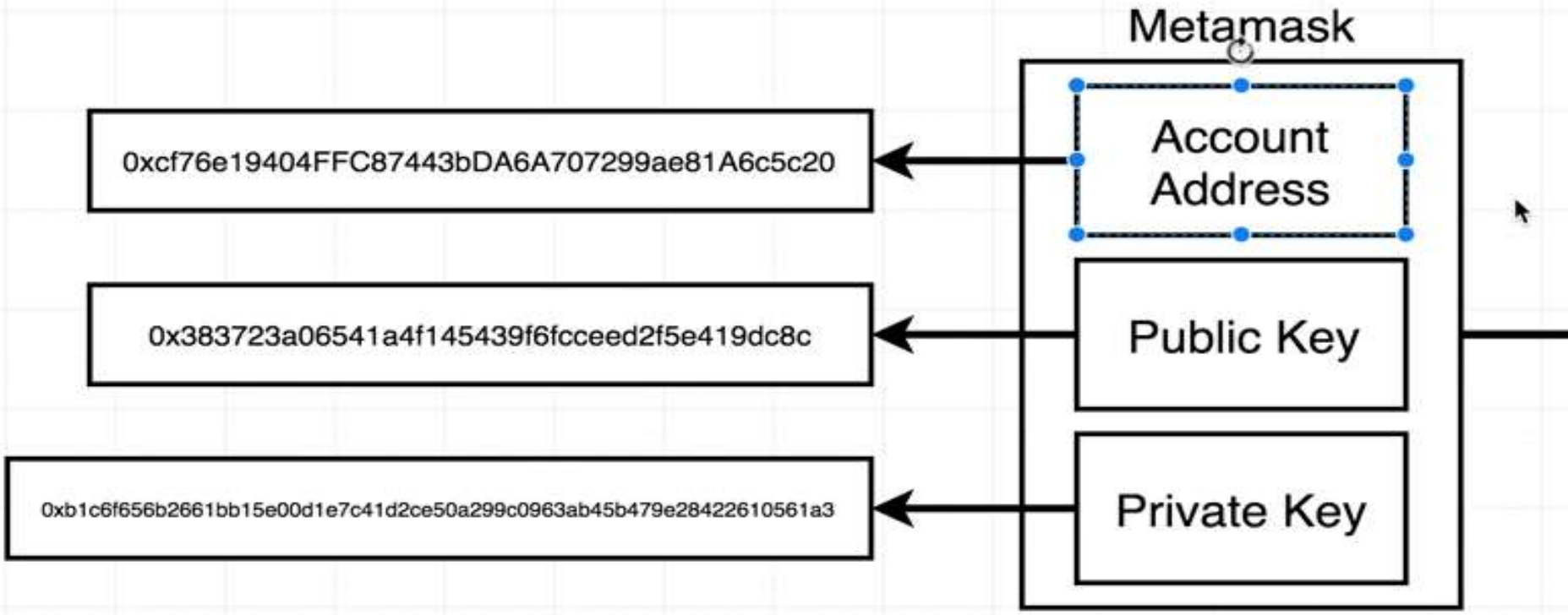
An Ethereum Network

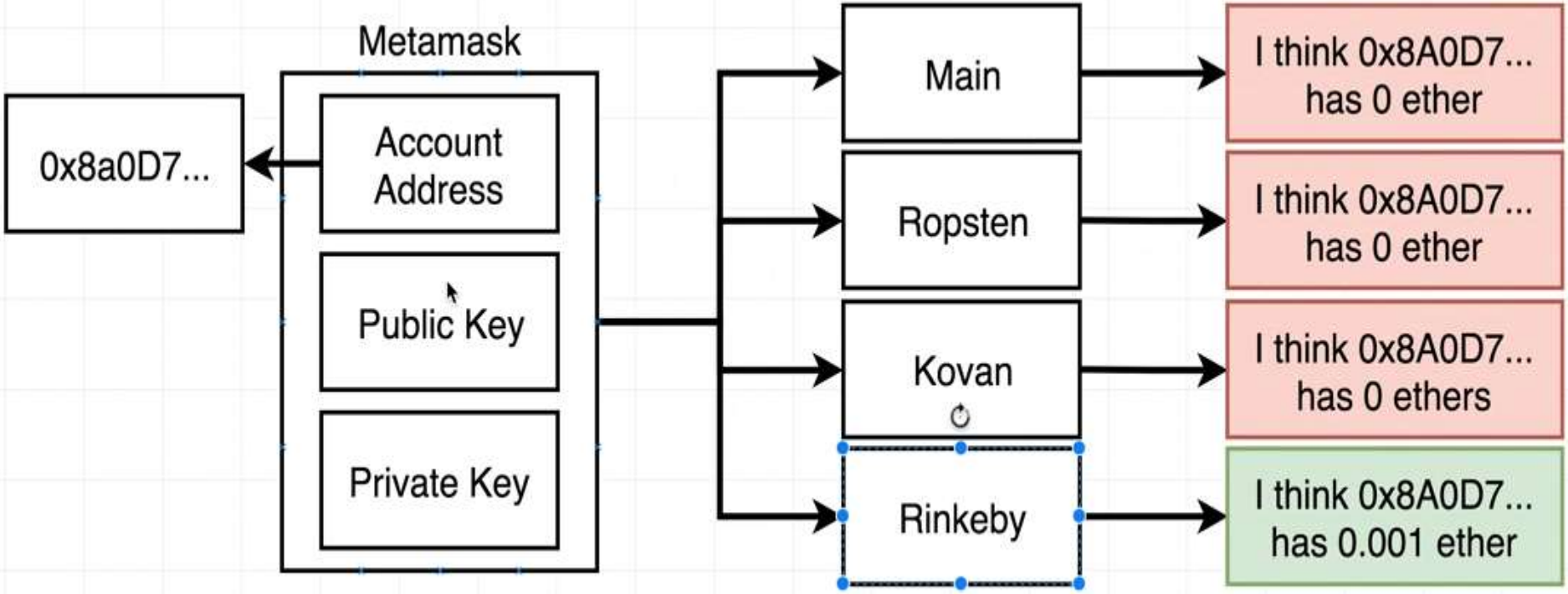


Ethereum networks are used to transfer money and store data
There are many different Ethereum networks.
Networks are formed by one or more nodes.
Each node is a machine running an ethereum client.
Anyone can run a node.
Each node can contain a full copy of the blockchain
The 'blockchain' is a database that stores a record of every transaction that has ever taken place

Ropsten Network, Kovan Network, Rinkeby Test Network, Localhost


For Developers
web3.js
For Consumers
Metamask
Mist
Browser
Node
Node
Node
Node
Node


Metamask
Account Address
Public Key
Private Key
0xcf76e19404FFC87443bDA6A707299ae81A6c5c20
0x383723a06541a4f145439f6fcceed2f5e419dc8c
0xb1c6f656b2661bb15e00d1e7c41d2ce50a299c0963ab45b479e28422610561a3


Metamask
0x8a0D7...
Account Address
Public Key
Private Key
Main
Ropsten
Kovan
Rinkeby
I think 0x8A0D7... has 0 ether
I think 0x8A0D7... has 0 ether
I think 0x8A0D7... has 0 ethers
I think 0x8A0D7... has 0.001 ether

Rinkeby Ether Faucet!

Not secure | rinkeby-faucet.com

Apps Empire Jira :: EmployWise :: Segment - The ulti... Salary Slip B

Rinkeby Ether Faucet

Give me your address and I'll give you .001 ether!

My Address: Submit

https://rinkeby-faucet.com/

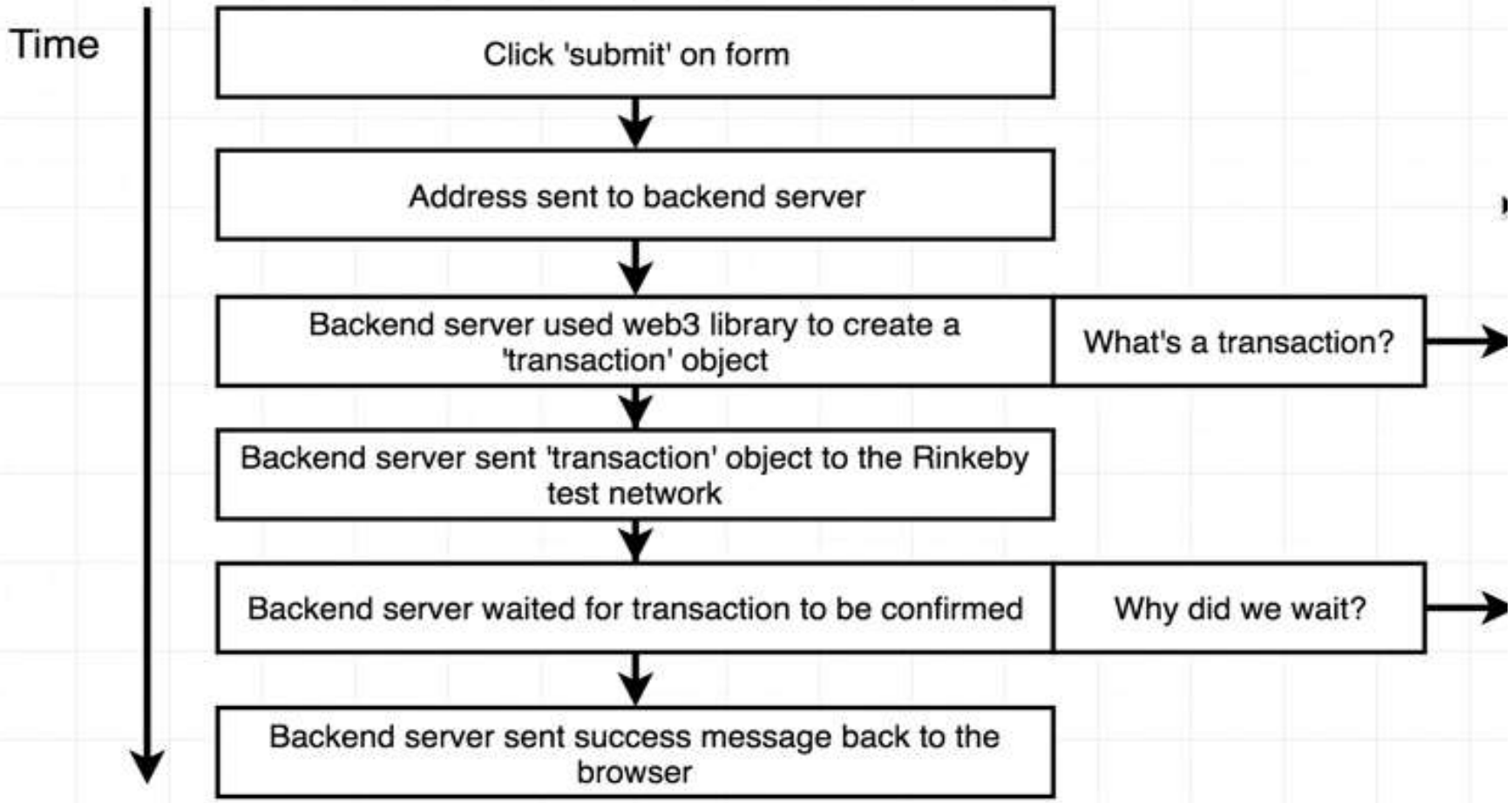
Rinkeby Ether Faucet

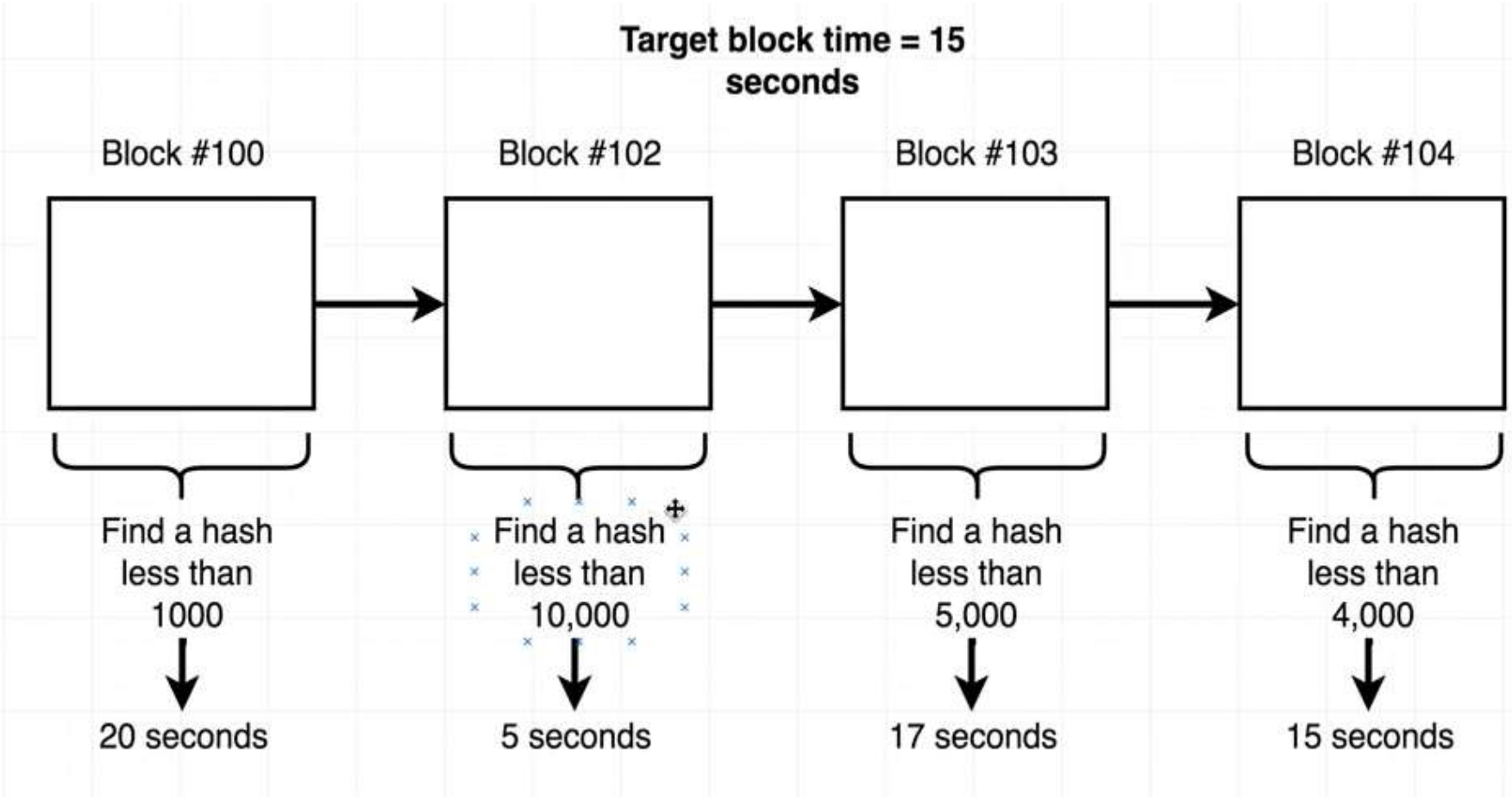
Give me your address and I'll give you .001 ether!

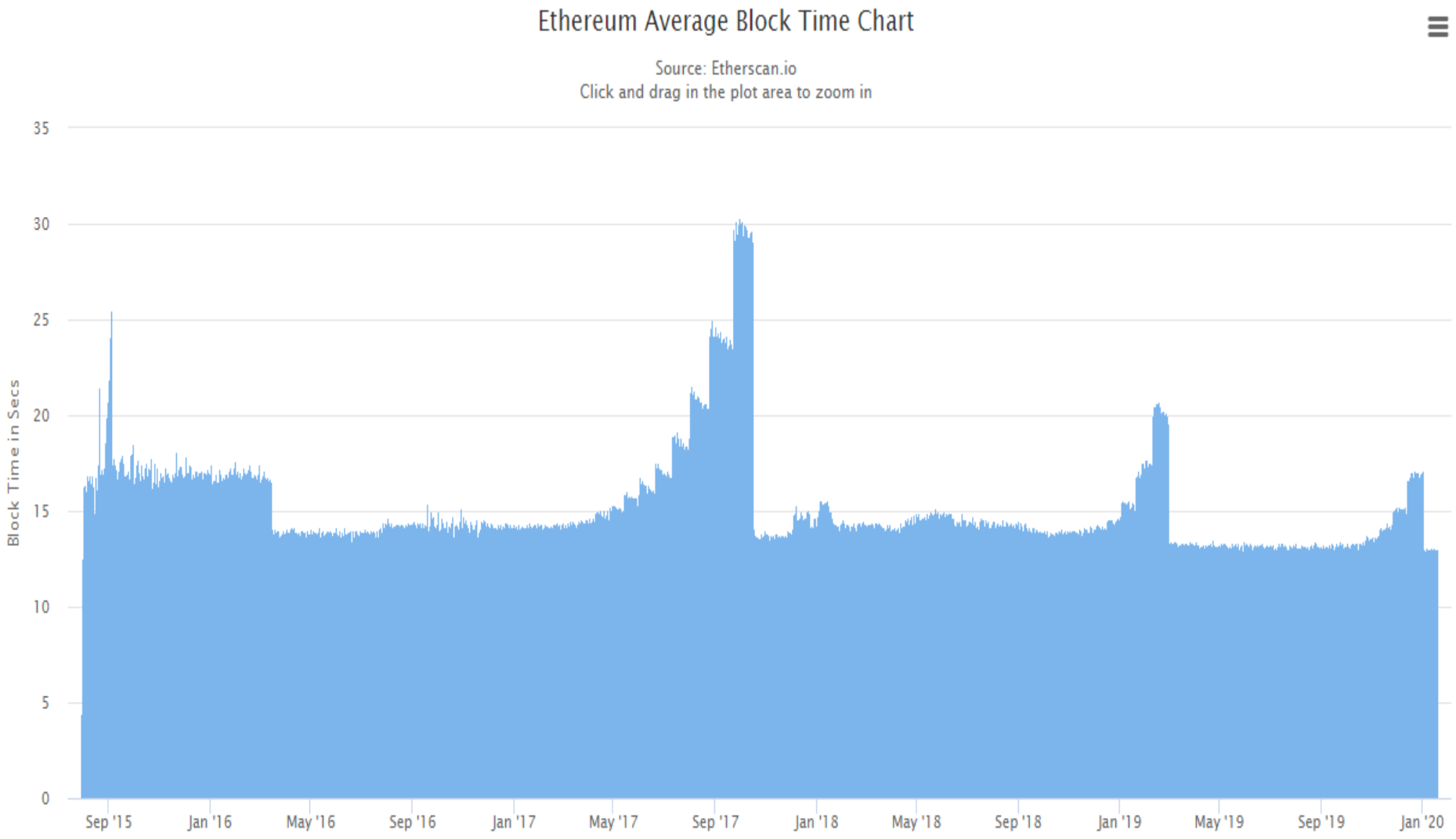
My Address: Submit

Great, coins are on the way!

If you're curious, here is your transaction id: 0xc36ba4807b8f5e2f593fdc2213dfe5cc7b0f864d1b69ddae0389e62b1b10087e


Time
Click 'submit' on form
Address sent to backend server
Backend server used web3 library to create a 'transaction' object
What's a transaction?
Backend server sent 'transaction' object to the Rinkeby test network
Backend server waited for transaction to be confirmed
Why did we wait?
Backend server sent success message back to the browser


Target block time = 15 seconds
Block #100
Block #102
Block #103
Block #104
Find a hash less than 1000
Find a hash less than 10,000
Find a hash less than 5,000
Find a hash less than 4,000
20 seconds
5 seconds
17 seconds
15 seconds


Ethereum Average Block Time Chart
Source: Etherscan.io
Click and drag in the plot area to zoom in
Block Time in Secs
35
30
25
20
15
10
5
0
Sep '15
Jan '16
May '16
Sep '16
Jan '17
May '17
Sep '17
Jan '18
May '18
Sep '18
Jan '19
May '19
Sep '19
Jan '20

METAMASK

Secret Backup Phrase

Your secret backup phrase makes it easy to back up and restore your account.

WARNING: Never disclose your backup phrase. Anyone with this phrase can take your Ether forever.

seven awake weekend skin garden insane camera achieve orient grain section allow

Remind me later

Next

Tips:

Store this phrase in a password manager like 1Password.

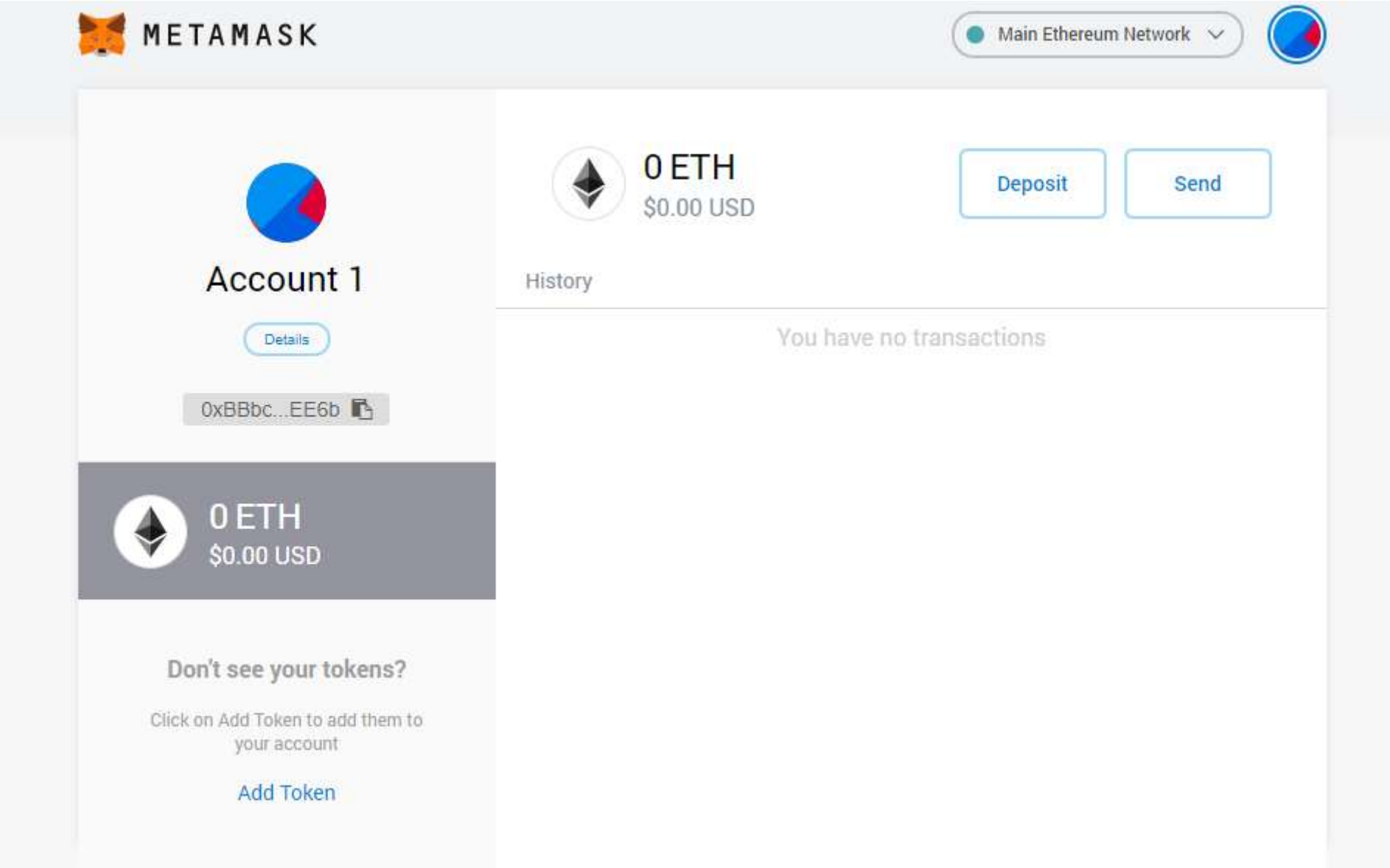
Write this phrase on a piece of paper and store in a secure location. If you want even more security, write it down on multiple pieces of paper and store each in 2 - 3 different locations.

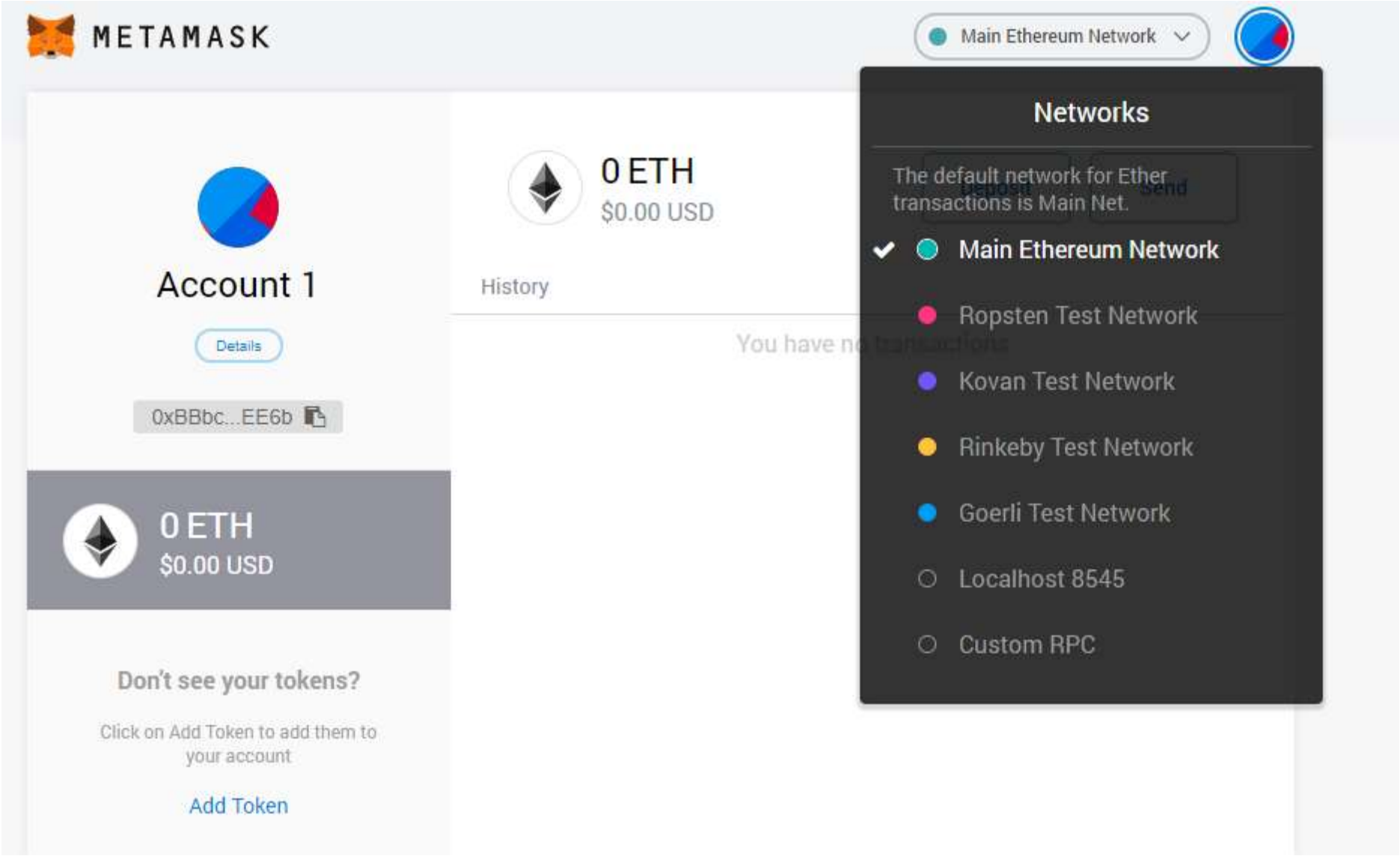
Memorize this phrase.

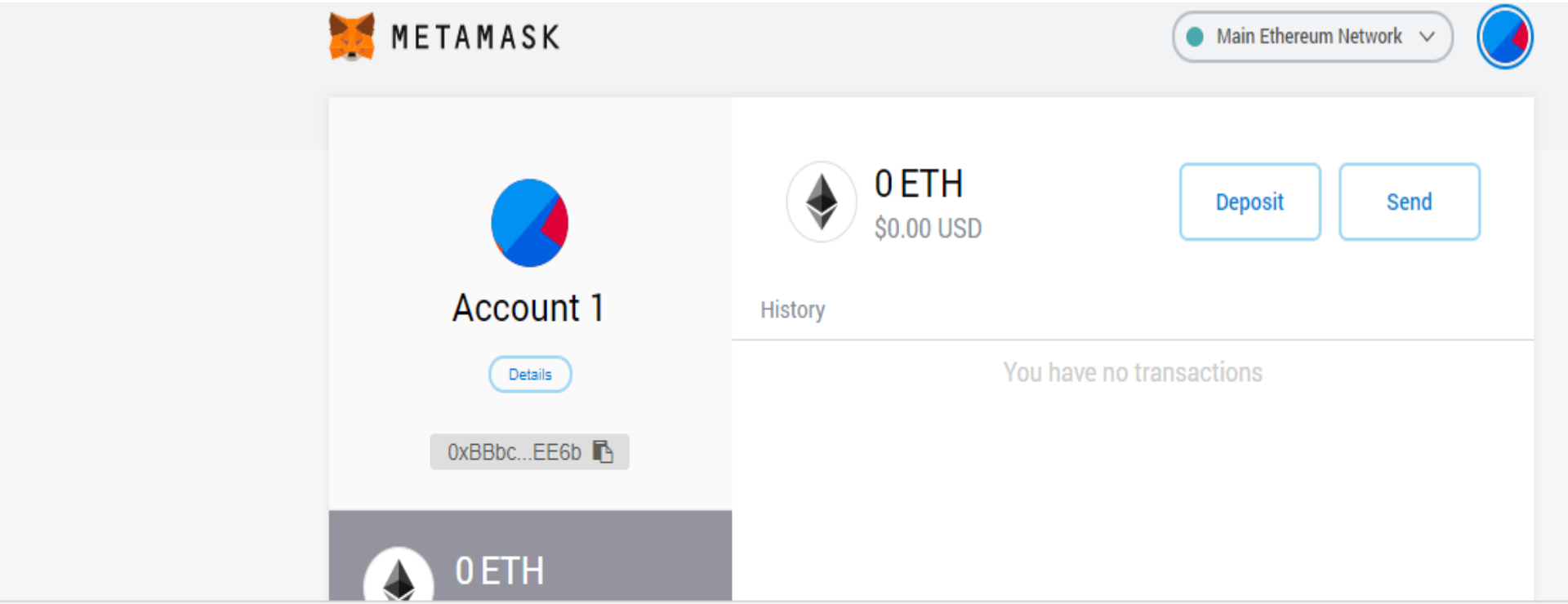
Download this Secret Backup Phrase and keep it stored safely on an external encrypted hard drive or storage medium.

https://www.trufflesuite.com/ganache

https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn/rela


METAMASK
Main Ethereum Network
Account 1
Details
0xBBbc...EE6b
0 ETH
$0.00 USD
Don't see your tokens?
Click on Add Token to add them to your account
Add Token
0 ETH
$0.00 USD
Deposit
Send
History
You have no transactions


METAMASK
Main Ethereum Network
Account 1
Details
0xBBbc...EE6b
0 ETH
$0.00 USD
Don't see your tokens?
Click on Add Token to add them to your account
Add Token
0 ETH
$0.00 USD
History
Networks
The default network for Ether transactions is Main Net.
Main Ethereum Network
Ropsten Test Network
Kovan Test Network
Rinkeby Test Network
Goerli Test Network
Localhost 8545
Custom RPC



Elements Console Sources Network Performance Memory Application Security Audits

top Filter Default levels

```
Setting up Sentry Remote Error Reporting: SENTRY_DSN_PROD
> 0xBBbcd68918B19d58B887ebC428b1120A70d1EE6b
< 1.0717925029220792e+48
```

Rinkeby Ether Faucet!

Not secure | rinkeby-faucet.com

Apps Empire Jira :: EmployWise :: Segment - The ulti... Salary Slip B

Rinkeby Ether Faucet

Give me your address and I'll give you .001 ether!

My Address: Submit

https://rinkeby-faucet.com/

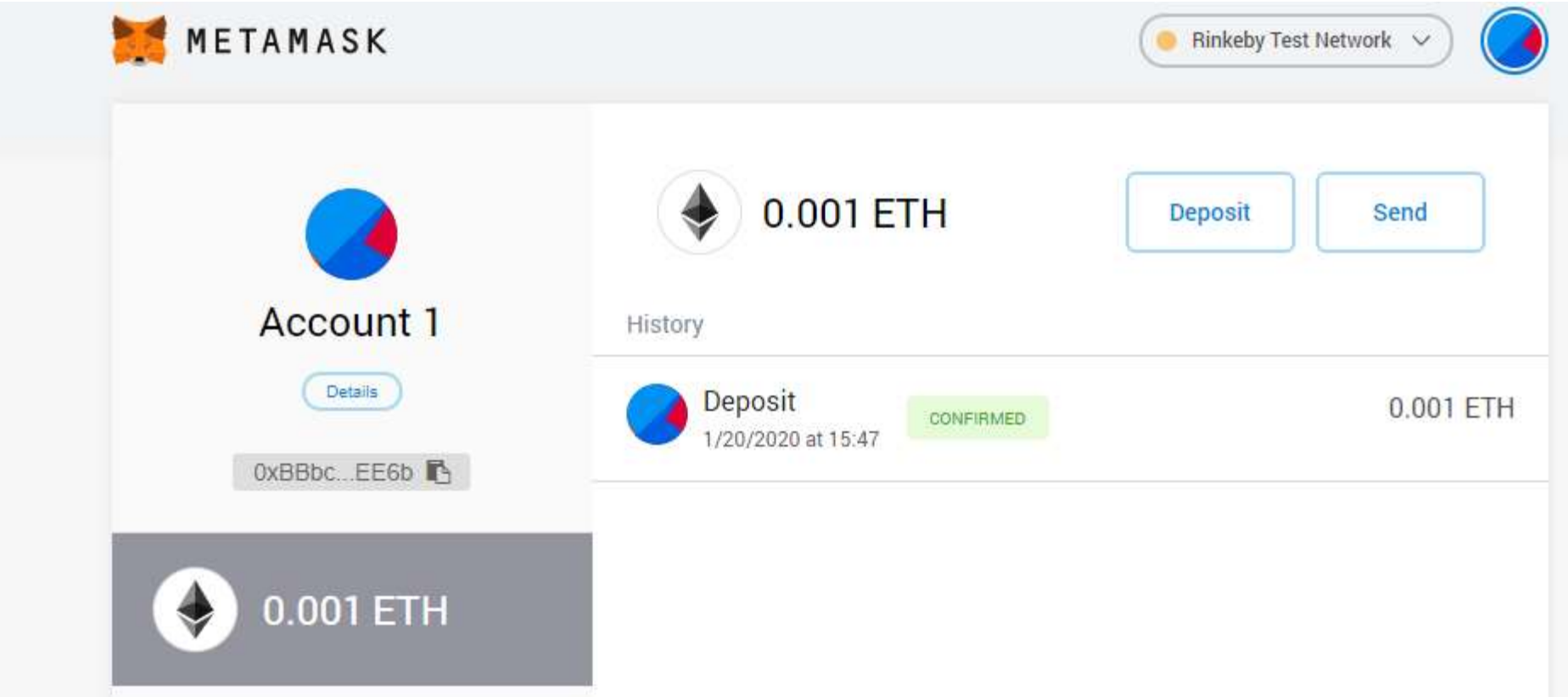
Rinkeby Ether Faucet

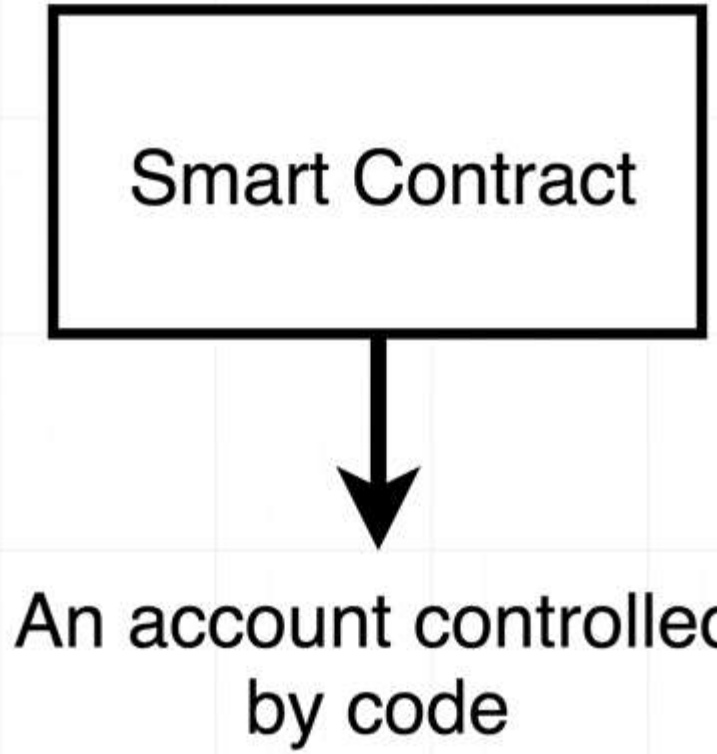
Give me your address and I'll give you .001 ether!

My Address: Submit

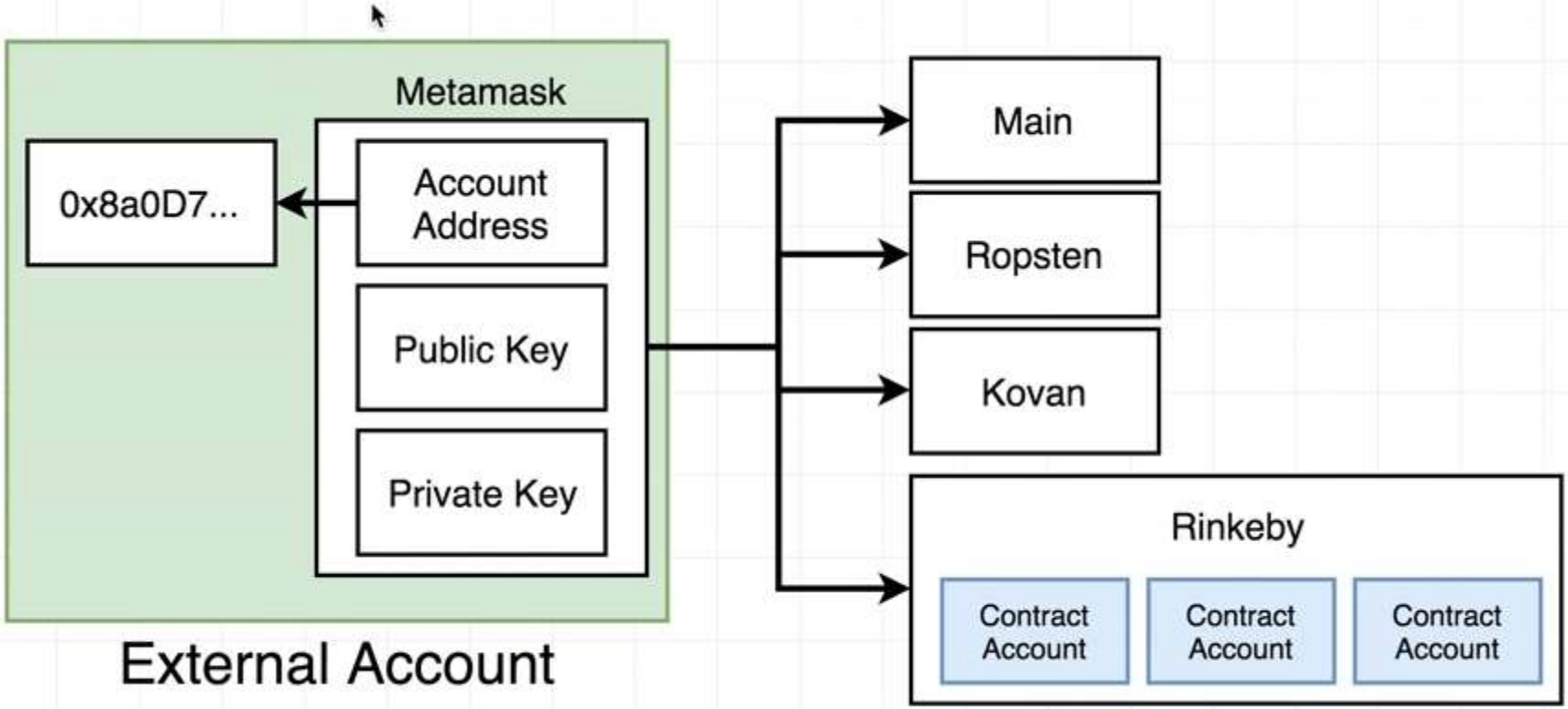
Great, coins are on the way!

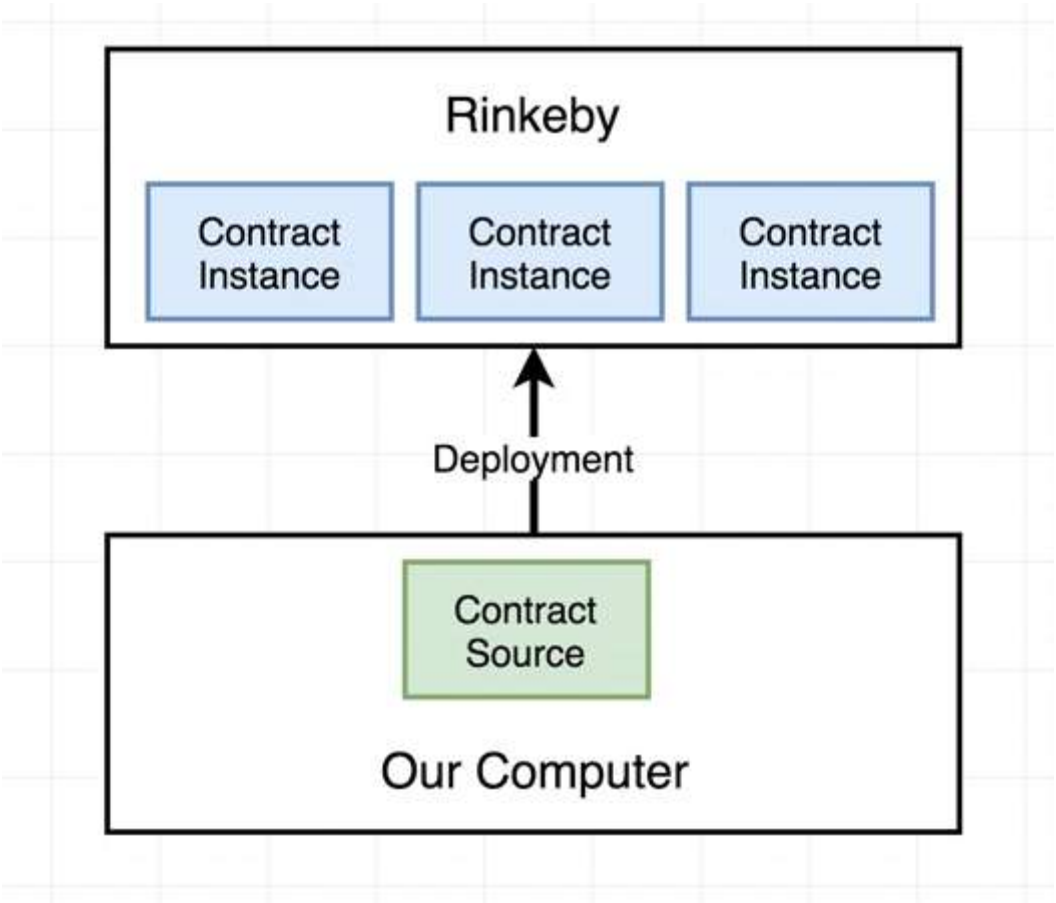
If you're curious, here is your transaction id: 0xc36ba4807b8f5e2f593fdc2213dfe5cc7b0f864d1b69ddae0389e62b1b10087e


METAMASK
Rinkeby Test Network
Account 1
Details
0xBBbc...EE6b
0.001 ETH
0.001 ETH
Deposit
Send
History
Deposit
1/20/2020 at 15:47
CONFIRMED
0.001 ETH


Smart Contract
An account controlled by code

Contract Account	
Field	Description
balance	Amount of ether this account owns
storage	Data storage for this contract
code	Raw machine code for this contract


Metamask
0x8a0D7...
Account Address
Public Key
Private Key
External Account
Main
Ropsten
Kovan
Rinkeby
Contract Account
Contract Account
Contract Account


Rinkeby
Contract Instance
Contract Instance
Contract Instance
Deployment
Contract Source
Our Computer

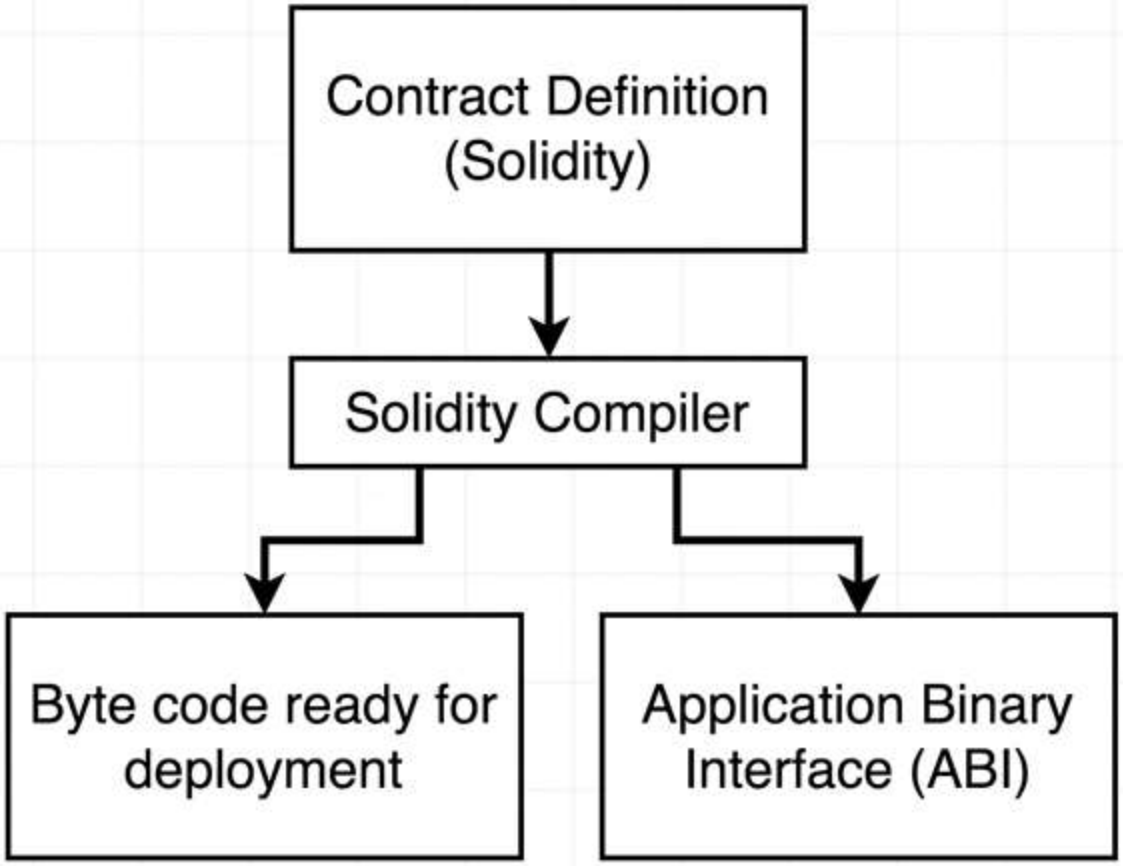
Solidity Programming Language

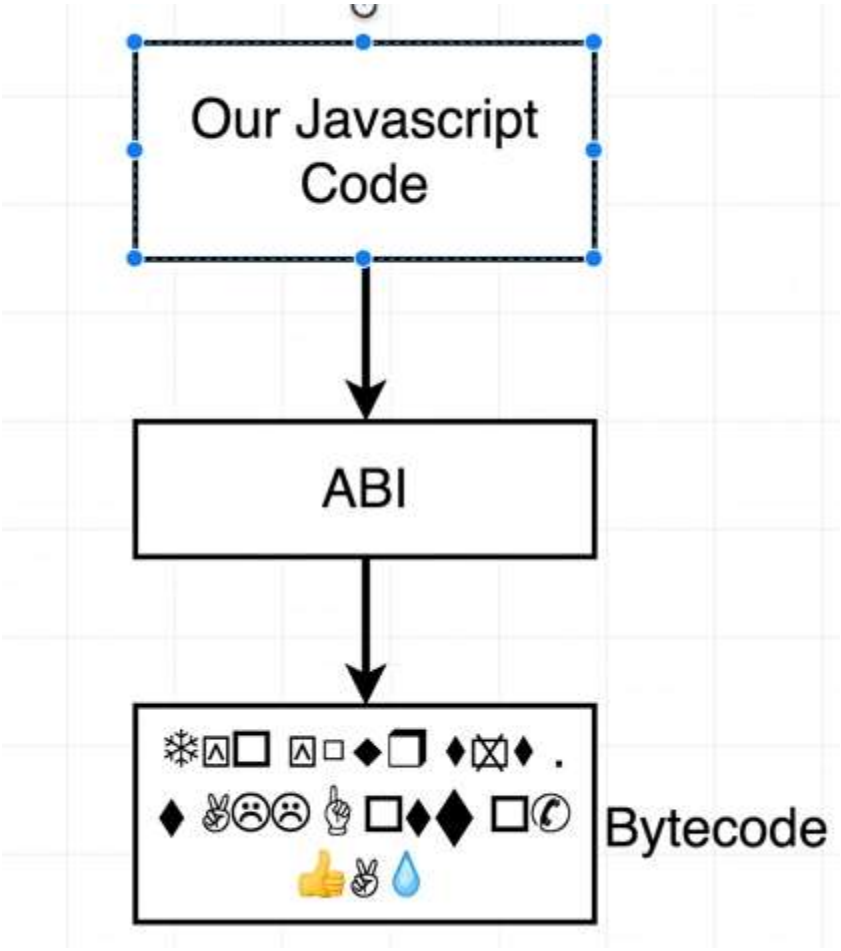
Written in .sol files

Strongly typed

Similar to Javascript

Has several huge, gigantic 'gotchas'


Contract Definition (Solidity)
Solidity Compiler
Byte code ready for deployment
Application Binary Interface (ABI)


Our Javascript Code
ABI
Bytecode

REMIX.ETHEREUM.ORG

browser/ballot_test.sol

Compile Run Analysis Testing Debugger Settings

browser
- ballot_test.sol
- ballot.sol

config

```
import "remix_tests.sol"; // this import is automatically injected by Remix.
import "./ballot.sol";

contract test3 {

    Ballot ballotToTest;
    function beforeAll () public {
        ballotToTest = new Ballot(2);
    }

    function checkWinningProposal () public {
        ballotToTest.vote(1);
        Assert.equal(ballotToTest.winningProposal(), uint(1), "1 should be the winning proposal");
    }

    function checkWinninProposalWithReturnValue () public view returns (bool) {
        return ballotToTest.winningProposal() == 1;
    }
}
```

Switch to the new interface!

Current version:0.5.12+commit.7709ece9.Emscripten.clang

Select new compiler version

Auto compile
Enable Optimization
Hide warnings

Start to compile (Ctrl-S)

Ballot
Swarm

Details ABI Bytecode

Static Analysis raised 28 warning(s) that requires your attention.
Click here to show the warning(s).

remix_tests.sol:2:1: Warning: Source file does not
library Assert {
^ (Relevant source part starts here and spans acros

browser/ballot_test.sol:2:1: Warning: Source file d
import "remix_tests.sol"; // this import is automat
^ (Relevant source part starts here and spans acros

[2] only remix transactions, script

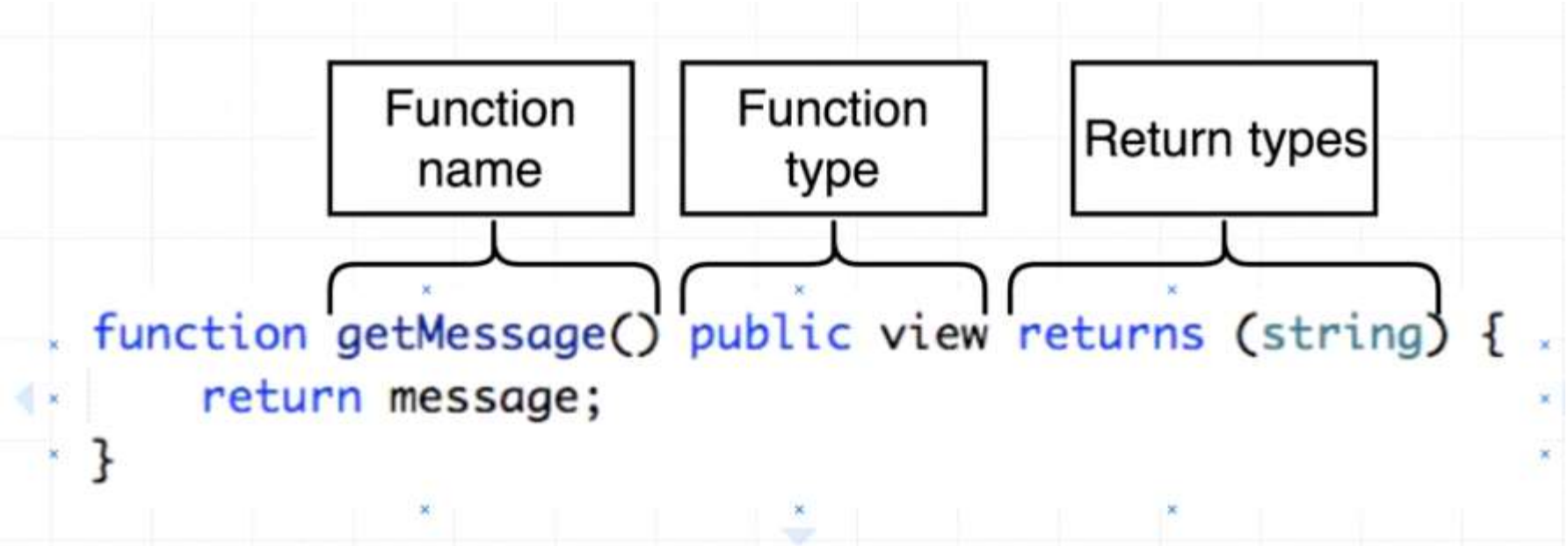
Search transactions

You can use this terminal for:

- Checking transactions details and start debugging.
- Running JavaScript scripts. The following libraries are accessible:
  - web3 version 1.0.0
  - ethers.js
  - swarmgw
  - compilers - contains currently loaded compiler
- Executing common command to interact with the Remix interface (see list of commands above). Note that these commands can also be included and run from a JavaScript script.
- Use exports/.register(key, obj)/.remove(key)/.clear() to register and reuse object across script executions.

First contract

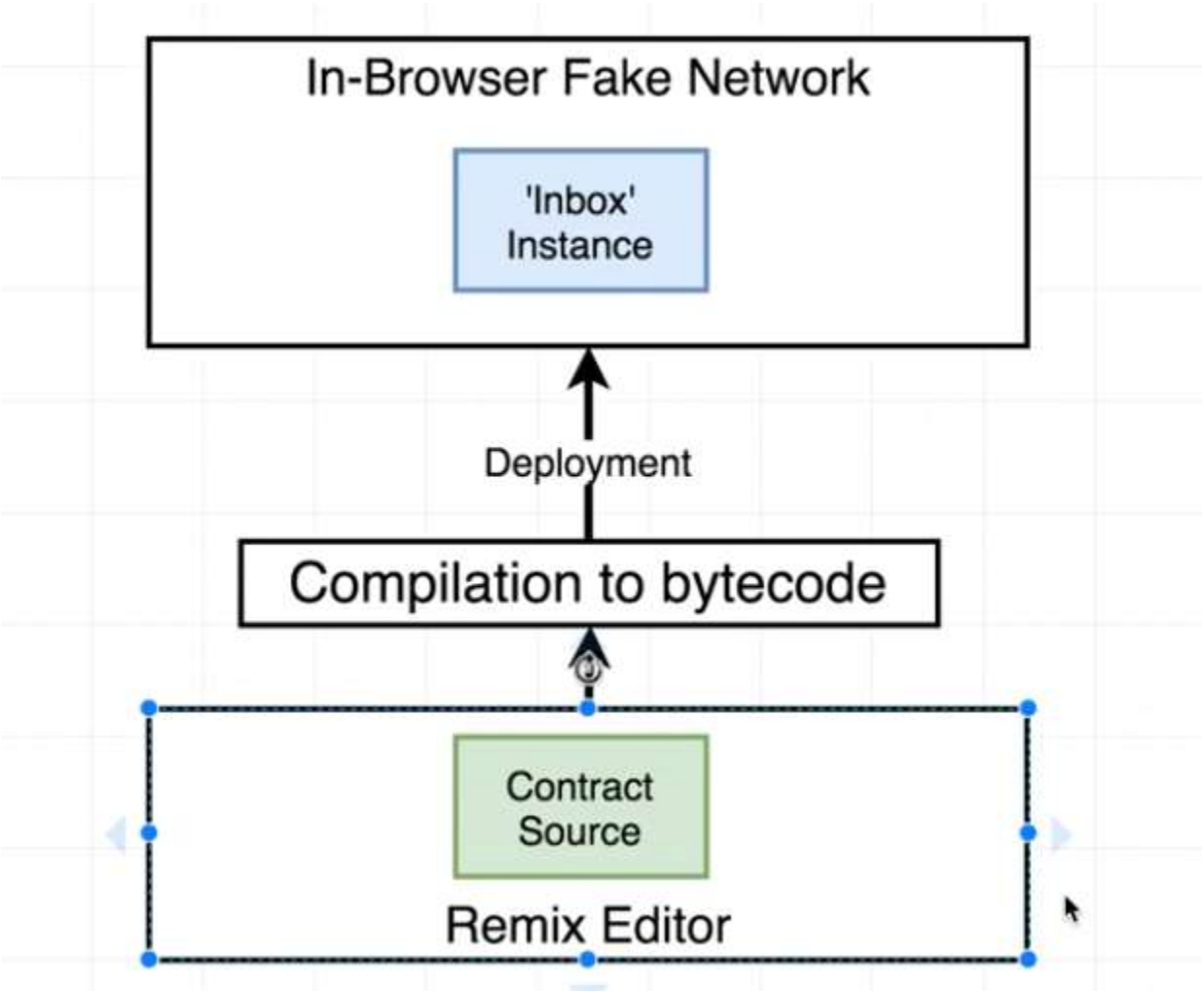
```
pragma solidity ^0.4.17;

contract Inbox {
    string public message;

    function Inbox(string initialMessage) public {
        message = initialMessage;
    }

    function setMessage(string newMessage) public {
        message = newMessage;
    }

    function getMessage() public view returns (string) {
        return message;
    }
}
```


Function name
Function type
Return types
function getMessage() public view returns (string) {
return message;
}

Function Types

	Common Function Types	
Can only use one per function	public	Anyone can call this function
	private	Only this contract can call this function.
They mean the same thing	view	This function returns data and does *not* modify the contract's data
	constant	This function returns data and does *not* modify the contract's data
	pure	Function will not modify or even *read* the contract's data
	payable	When someone call this function they might send ether along

What will remix do



Compiling contract

ContractDefinition Inbox 0 reference(s)

```
pragma solidity ^0.4.17;

contract Inbox {
    string public message;

    function Inbox(string initialMessage) public {
        message = initialMessage;
    }

    function setMessage(string newMessage) public {
        message = newMessage;
    }

    function getMessage() public view returns (string
        return message;
    }
}
```

Compile Run Settings Debugger Analysis

Start to compile Auto compile

Inbox Details Publish on Swarm

Static Analysis raised 3 warning(s)

Inbox

- **JavaScript VM :** This lets you run your contract directly in the browser using a JavaScript implementation of the Ethereum virtual machine (EVM). It is good for simple testing but each time when you reload the page it will start a new blockchain.

- **Injected Web3 :** Web3 is the interface for interacting with an Ethereum node. When you install Metamask, it injects web3 implementation into every web page. Using this option, you can use that injected implementation to deploy your contract to test networks or main Ethereum network.

- **Web3 Provider :** Using this option you can directly connect to an Ethereum node via HTTP. You can use this option to connect to Ganache or Geth.

Settings.....

browser/ballot.sol

```
pragma solidity ^0.4.17;

contract Inbox {
    string public message;

    function Inbox(string initialMessage) public {
        message = initialMessage;
    }

    function setMessage(string newMessage) public {
        message = newMessage;
```

[2] only remix transactions, script

Search transactions

remix

Compile | Run | Settings | Debugger | Analysis | Support

Environment	Injected Web3 — Rinkeby (4)
Account	0x8a0...c3f23 (0.001 ether)
Gas limit	3000000
Value	0 wei

Inbox

string initialMessage — Create

Load contract from Address — At Address

0 pending transactions

0 contract Instances

More settings...

Compile Run Settings Debugger Analysis Support

Environment JavaScript VM VM (-)

Account 0xca3...a733c (99.9999999999996323

Gas limit 3000000

Value 0 wei

Inbox

"Hi there!" Create

Load contract from Address At Address

0 pending transactions

Inbox at 0x692...77b3a (memory)

Compile Run Settings Debugger Analysis Support

Environment JavaScript VM VM (-)

Account

✓ 0xca3...a733c (100 ether)
0x147...c160c (100 ether)
0x4b0...4d2db (100 ether)
0x583...40225 (100 ether)
0xdd8...92148 (100 ether)

Gas limit

Value

Inbox

string initialMessage Create

Load contract from Address At Address

0 pending transactions

0 contract Instances

Inbox at 0x692...77b3a (memory)

message

getMessage 0: string: Hi there!

setMessage string newMessage

Inbox

"Hi there!" Create

Load contract from Address At Address

0 pending transactions

Inbox at 0x692...77b3a (memory)

message

getMessage 0: string: Bye there!

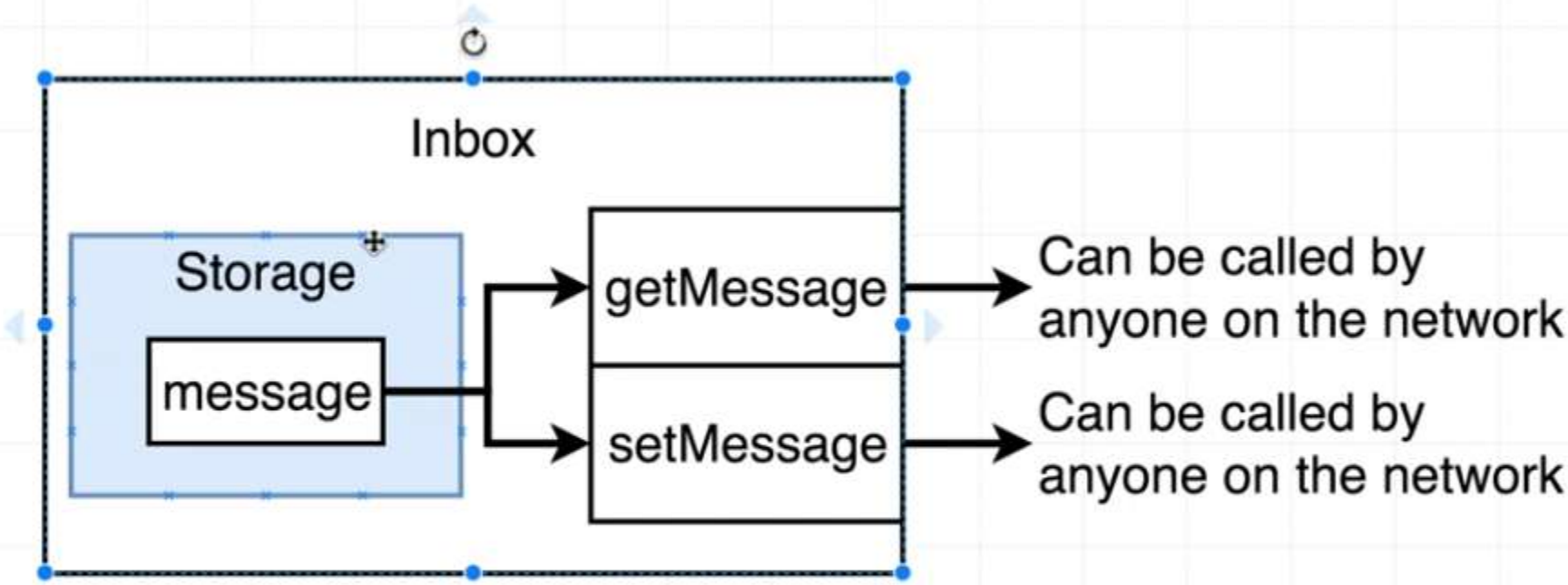
setMessage "Bye there!"

Inbox at 0x692...77b3a (memory)

message

getMessage

setMessage string newMessage



Remark 1:

- Whenever we mark a variable **as public in the contract,**
- solidity will automatically **create a function** with the **name same as the name of variable**
- The function will **return the value of the variable.**

Deleting get message

browser/ballot.sol

```
pragma solidity ^0.4.17;

contract Inbox {
    string public message;

    function Inbox(string initialMessage) public {
        message = initialMessage;
    }

    function setMessage(string newMessage) public {
        message = newMessage;
    }
}
```

[2] only remix transactions, script

Search transactions

```
4e8fa733c, to:Inbox.(fallback), data:ce
...d41de, return:

ation of Inbox pending...

] from:0xca3...a733c, to:Inbox.(constru
r), value:0 wei, data:0x606...00000, 0
gs, hash:0x208...5d32b
```

Details Debug

Compile Run Settings Debugger Analysis Support

Gas limit 3000000

Value 0 wei

Inbox

"Apple!" Create

Load contract from Address At Address

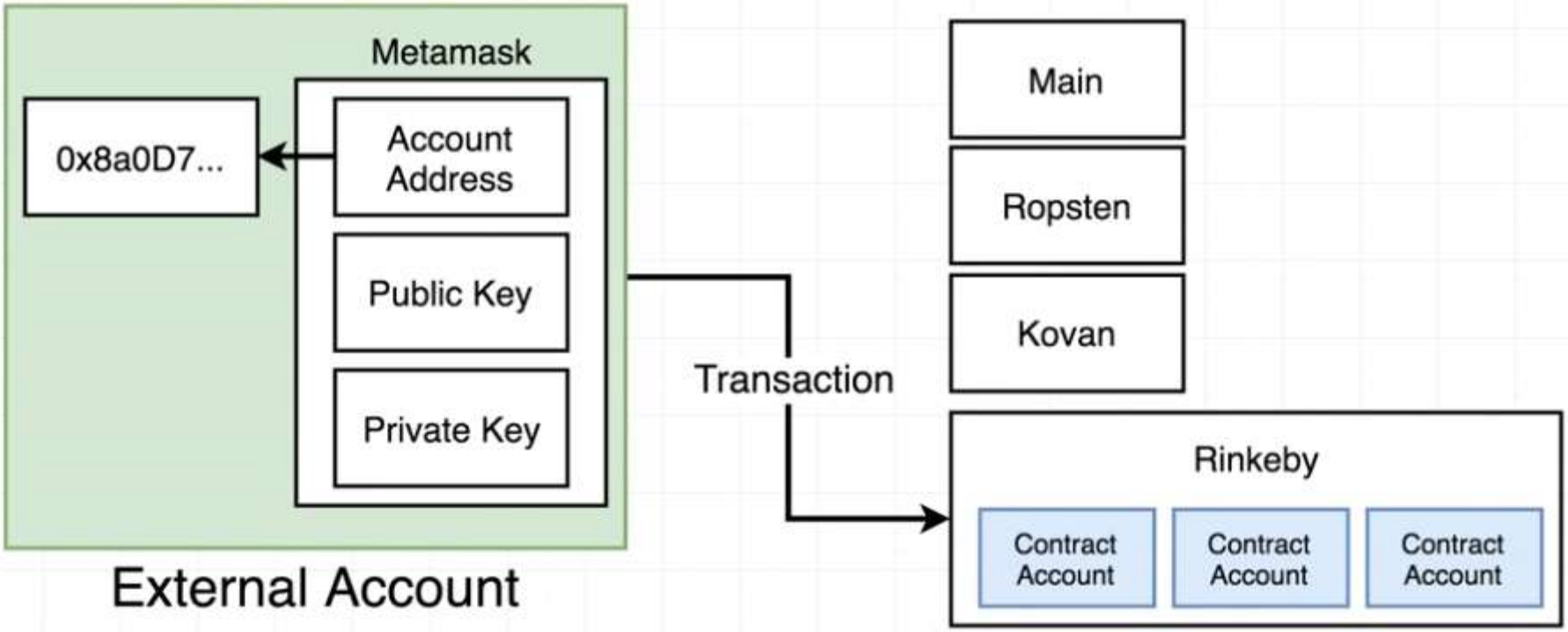
0 pending transactions

Inbox at 0x0dc...97caf (memory)

message

setMessage string newMessage

Creating a Contract (Behind the scene)



Normal Transaction

Transaction

nonce	How many times the sender has sent a transaction
to	Address of account this money is going to
value	Amount of ether to send to the target address
gasPrice	Amount of ether the sender is willing to pay per unit gas to get this transaction processed
startGas/gasLimit	Units of gas that this transaction can consume
v	Cryptographic pieces of data that can be used to generate the senders account address. Generated from the *sender's* private key.
r	
s	

Difference b/w Normal Transaction and External Account to Create Contract Transaction

Transaction

nonce	How many times the sender has sent a transaction
to	Address of account this money is going to
value	Amount of ether to send to the target address
gasPrice	Amount of ether the sender is willing to pay per unit gas to get this transaction processed
startGas/gasLimit	Units of gas that this transaction can consume
v	Cryptographic pieces of data that can be used to generate the senders account address. Generated from the *sender's* private key.
r	
s	

External Account to Create Contract

nonce	How many times the sender has sent a transaction
to	-
data	Compiled bytecode of the contract
value	Amount of 'Wei' to send to the target address
gasPrice	Amount of Wei the sender is willing to pay per unit gas to get this transaction processed
startGas/gasLimit	Units of gas that this transaction can consume
v	Cryptographic pieces of data that can be used to generate the senders account address. Generated from the *sender's* private key.
r	
s	

What is gas

- Want to execute code on AWS -> Pay some money

- Want to deploy our code on the Ethereum network
- & want the network to run our code
- → there is some cost associated with it

gasPrice	Amount of Wei the sender is willing to pay per unit gas to get this transaction processed
startGas/gasLimit	Units of gas that this transaction can consume

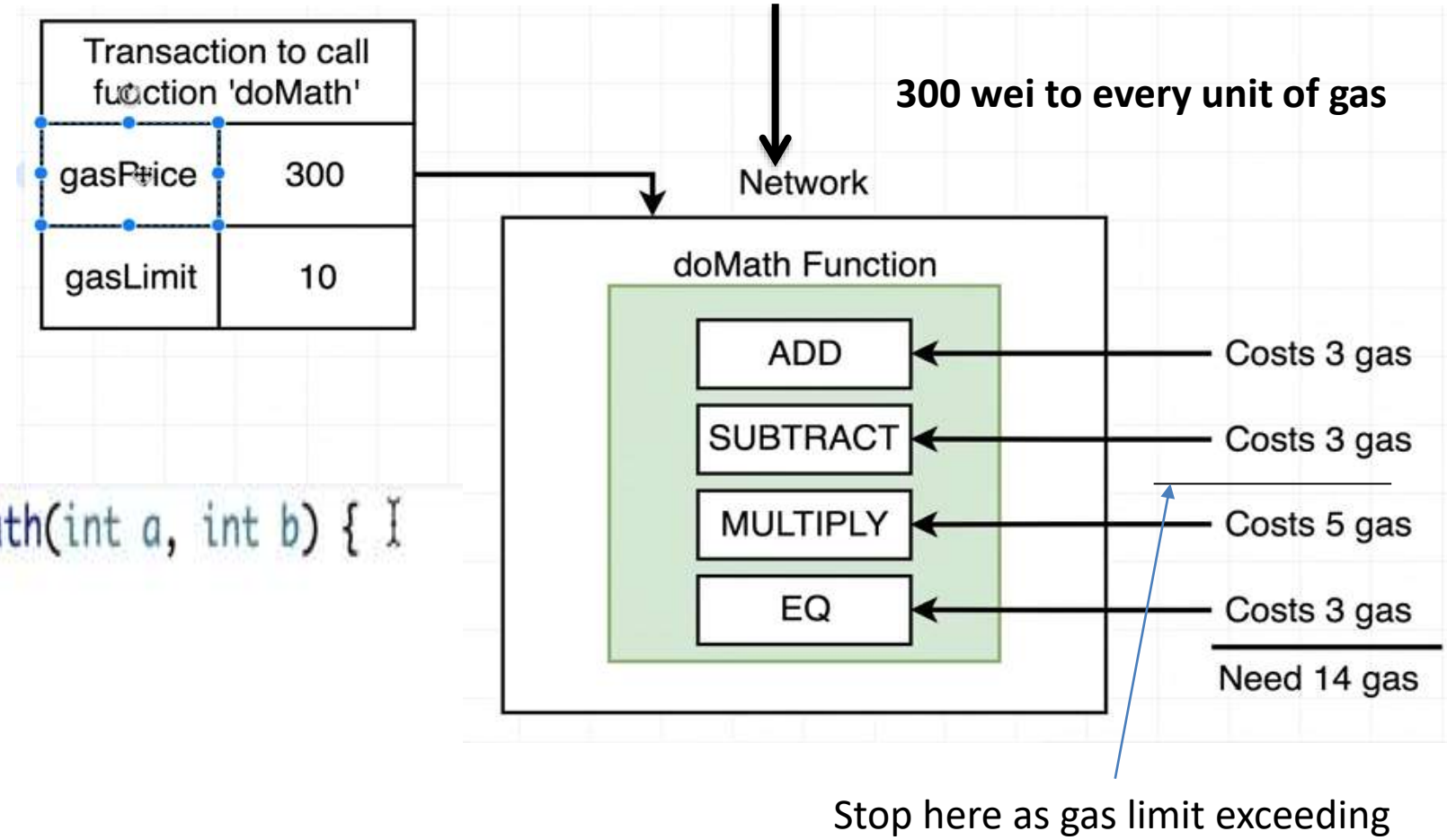
Mnemonic	Gas Used	Subset	Removed from stack	Added to stack	Notes
STOP	0	zero	0	0	Halts execution.
ADD	3	verylow	2	1	Addition operation
MUL	5	low	2	1	Multiplication operation.
SUB	3	verylow	2	1	Subtraction operation.
DIV	5	low	2	1	Integer division operation.
SDIV	5	low	2	1	Signed integer division operation
MOD	5	low	2	1	Modulo remainder operation
SMOD	5	low	2	1	Signed modulo remainder operat
ADDMOD	8	mid	3	1	Modulo addition operation.
MULMOD	8	mid	3	1	Modulo multiplication operation.
EXP	FORMULA		2	1	Exponential operation.
SIGNEXTEND	5	low	2	1	Extend length of two's compleme
LT	3	verylow	2	1	Less-than comparison.
GT	3	verylow	2	1	Greater-than comparison.

All operations that store or modify the data → Charges the gas

https://docs.google.com/spreadsheets/d/1m89CVujrQe5LAFJ8-YAUCcNK950dUzMQPMJBxRtGCqs

Gas calculations

Suppose the code having




```
function doMath(int a, int b) {
    a + b;
    b - a;
    a * b;
    a == 0;
}
```

Gas used

```
function doMath(int a, int b) {
    a + b;
    b - a;
    a * b;
    a == 0;
}
```

If gas limit exceed to <u>20</u>

gasPrice	300

Used 14 gas

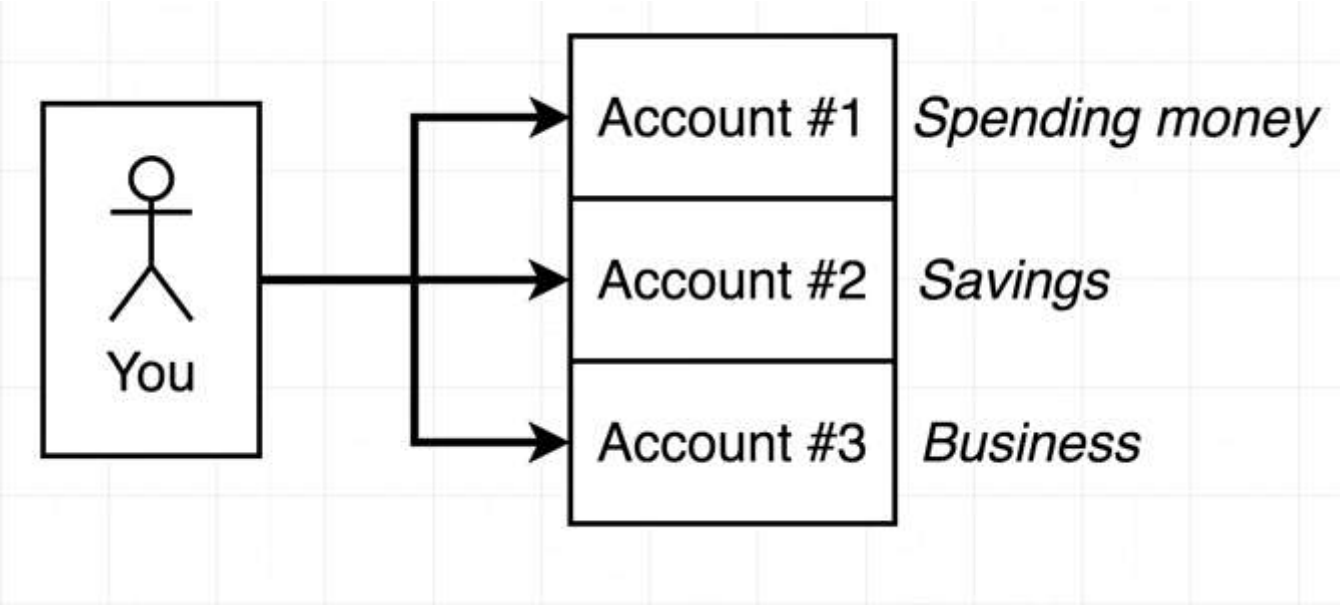
$$\text{Total cost} = 300\ \frac{\text{wei}}{\text{gas}} \times 14\ \text{gas} = 4{,}200\ \text{wei}$$

<u>Challenges:</u>

- **We cannot compute gas amount easily in complex codes e.g. loops, conditions**
- **Social media/email services do not charge a money: need a modified payment system**

Key Management

Single user multiple accounts



Key Management

Information to be kept secret

Account #1

Address	0xcF01971DB0CAB2CBeE4A8C21BB7638aC1FA1c38c
Public	0xCA7442E17Dfe52542E50D6310b9aB64ca448DD13
Private	0xcF01971DB0CAB2CBeE4A8C21BB7638aC1FA1c38c

Account #2

Address	0xf3Dd04C449669a89a7cF492c6fA8EF9aF388Ebd8
Public	0xd2A1faC633568cde440789D061Ef08D4f8a7054a
Private	0xf3Dd04C449669a89a7cF492c6fA8EF9aF388Ebd8

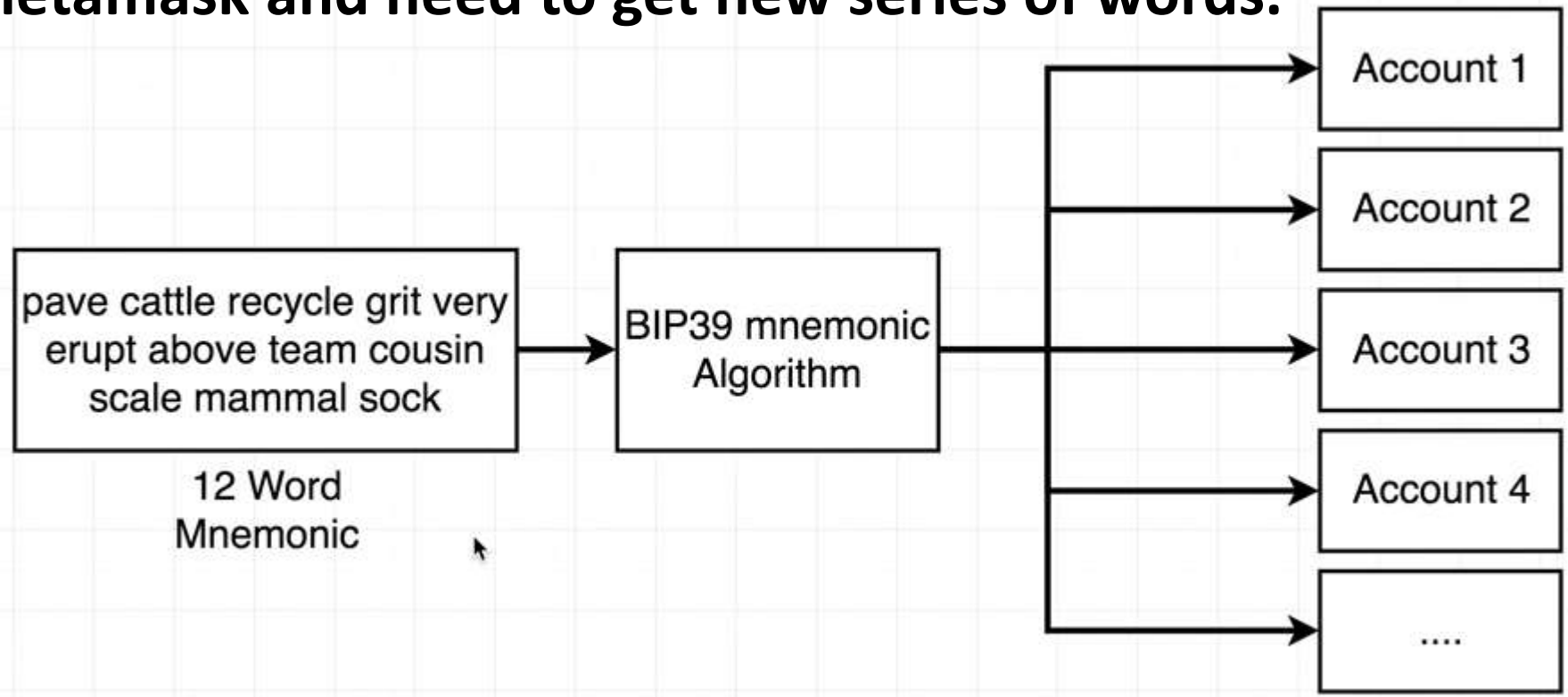
Account #3

Address	0xcF01971DB0CAB2CBeE4A8C21BB7638aC1FA1c38c
Public	0xC1b6c46e1fc19B8b990AdF4601db9B0842e22C9F
Private	0xcF01971DB0CAB2CBeE4A8C21BB7638aC1FA1c38c

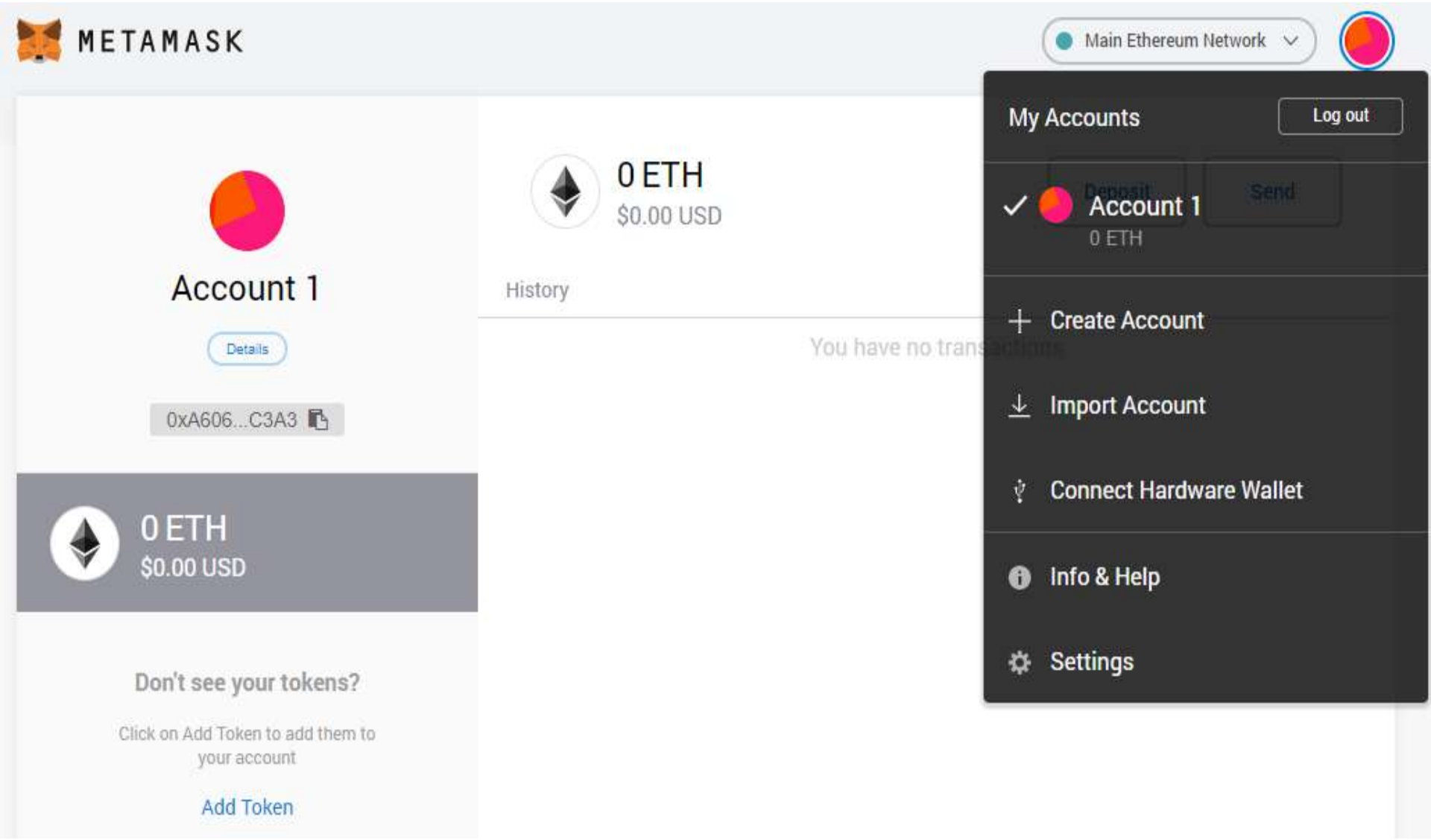
Key Management

1 Mnemonic and n accounts

- **A new mnemonic cannot be created for account.**
- **If we want a completely new series, we need to reinstall metamask and need to get new series of words.**



Create n new accounts



https://iancoleman.io/bip39/

- Check the link for more details.

- Metamask Phrase

Getting more ethers on rinkeby

www.faucet.rinkeby.io

https://rinkebyfaucet.com/

Rinkeby Authenticated Faucet

Social network URL containing your Ethereum address... | Give me Ether

7 peers 5871033 blocks 9.046256971665328e+56 Ethers 337608 funded

How does this work?

This Ether faucet is running on the Rinkeby network. To prevent malicious actors from exhausting all available funds or accumulating enough Ether to mount long running spam attacks, requests are tied to common 3rd party social network accounts. Anyone having a Twitter or Facebook account may request funds within the permitted limits.

To request funds via Twitter, make a tweet with your Ethereum address pasted into the contents (surrounding text doesn't matter).
Copy-paste the tweets URL into the above input box and fire away!

To request funds via Facebook, publish a new **public** post with your Ethereum address embedded into the content (surrounding text doesn't matter).
Copy-paste the posts URL into the above input box and fire away!

You can track the current pending requests below the input field to see how much you have to wait until your turn comes.

The faucet is running invisible reCaptcha protection against bots.

FB identification

Funding request accepted for
vikas.hassija@facebook into
0xA6061ea63fa8645588e00a8f4980Ec7195fFC

Rinkeby Authenticated Faucet

https://www.facebook.com/vikas.hassija/posts/281437995200987 7 | Give me Ether

0xa6061ea63fa8645588e00a8f4980ec7195ffc3a3 | in 5 minutes

6 peers 5871067 blocks 9.046256971665328e+56 Ethers 337608 funded

Rinkeby Test Network

Account 1
0xA606...C3A3

18.75 ETH

Deposit | Send

History

You have no transactions

Linking between Ganache & Metamask

Live Demo

Contract deployment on Network

To be continued…