FTEC 4004

E-payment Systems and Cryptocurrency Technologies

Tutorial 12

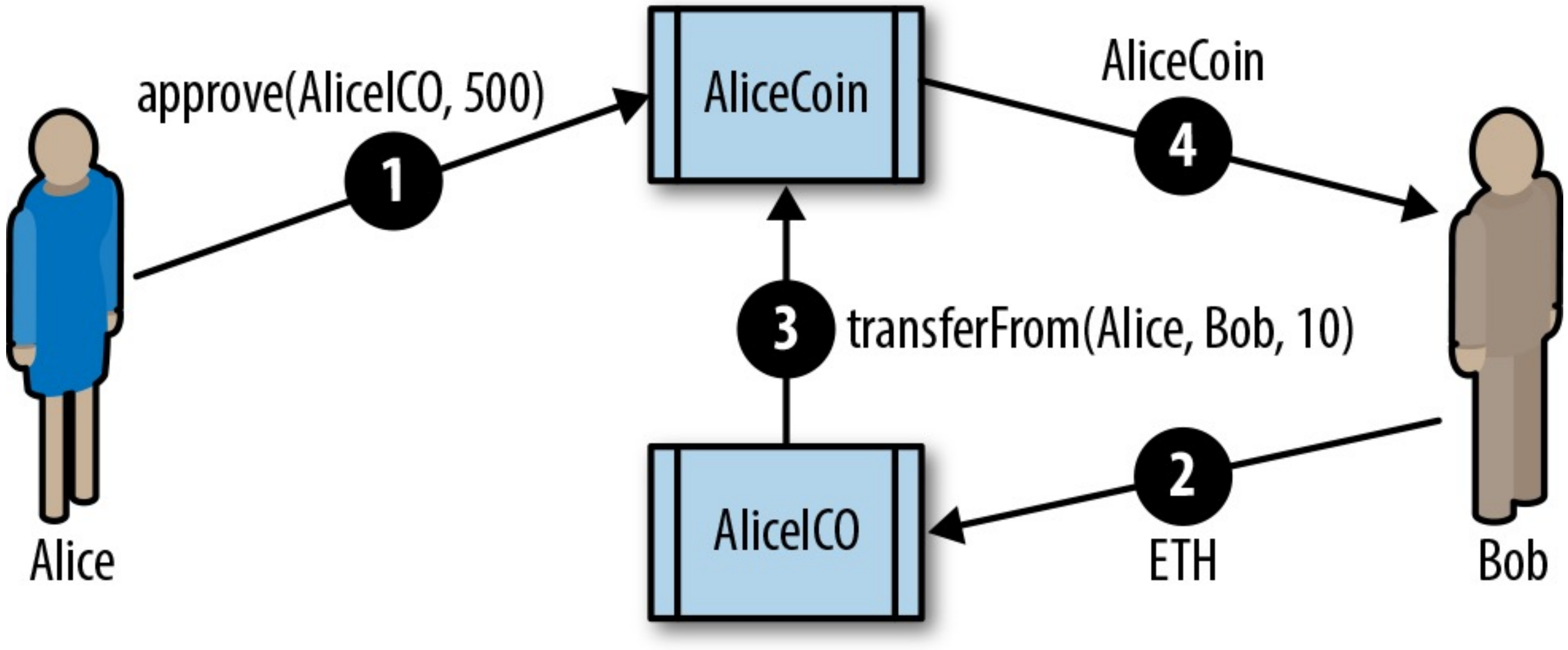
Smart Contract Deployement and Security Concerns

WANG Xianbo

xianbo@ie.cuhk.edu.hk

More about Homework 5

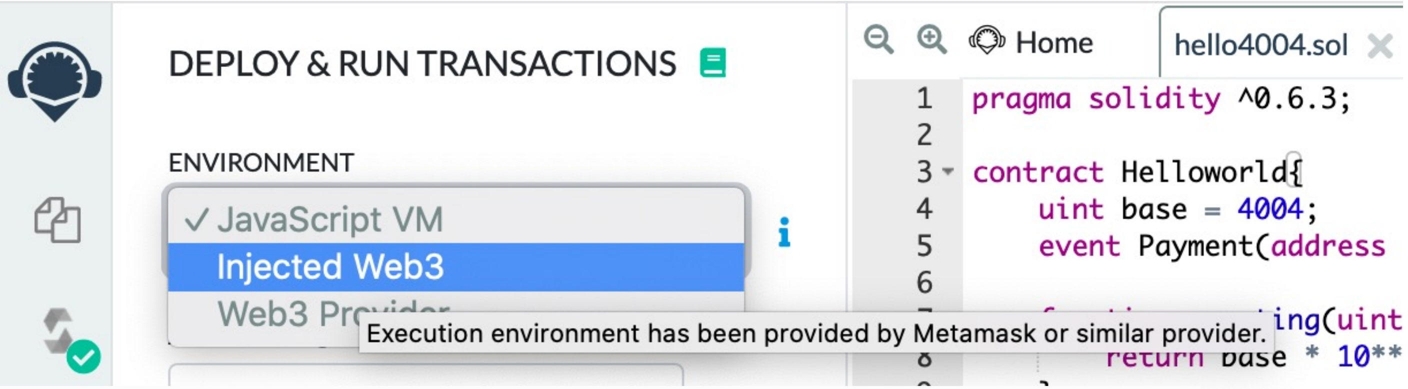
- The content of last lecture is important
  - How Ethereum Smart Contract works
  - The concept of ICO (Token and Crowdsale)



Overview of today’s topic

- How to deploy a smart contract
- How to interact with and monitor contracts after deployment
- Security Issues of smart contract

JsVM to EVM



DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

✓ JavaScript VM
Injected Web3
Web3 Pr

Execution environment has been provided by Metamask or similar provider.

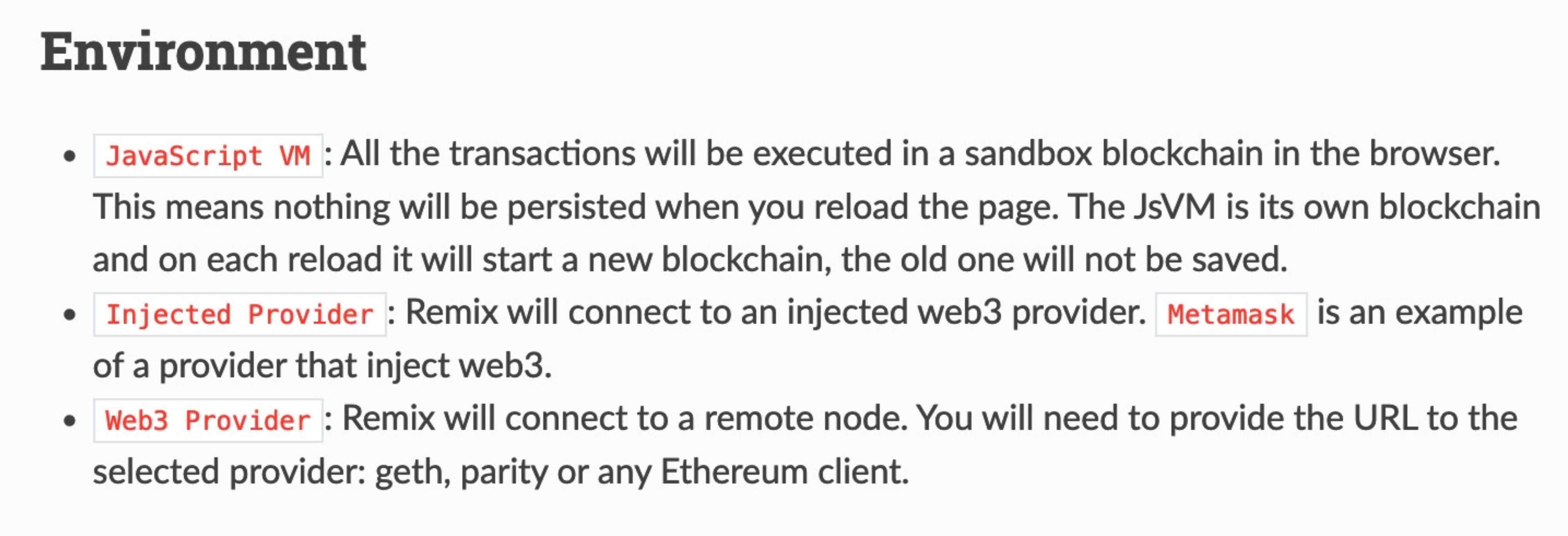
```
pragma solidity ^0.6.3;

contract Helloworld{
    uint base = 4004;
    event Payment(address

                    ing(uint
        return base * 10**

 ayme() publi
 ayment(msg.s

 alance() pub
 urn amount o
 address(thi
```

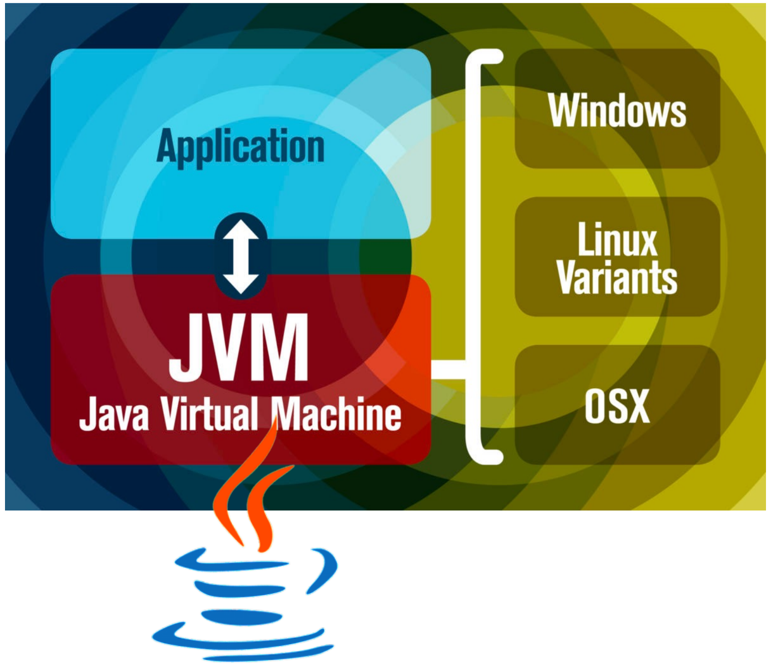


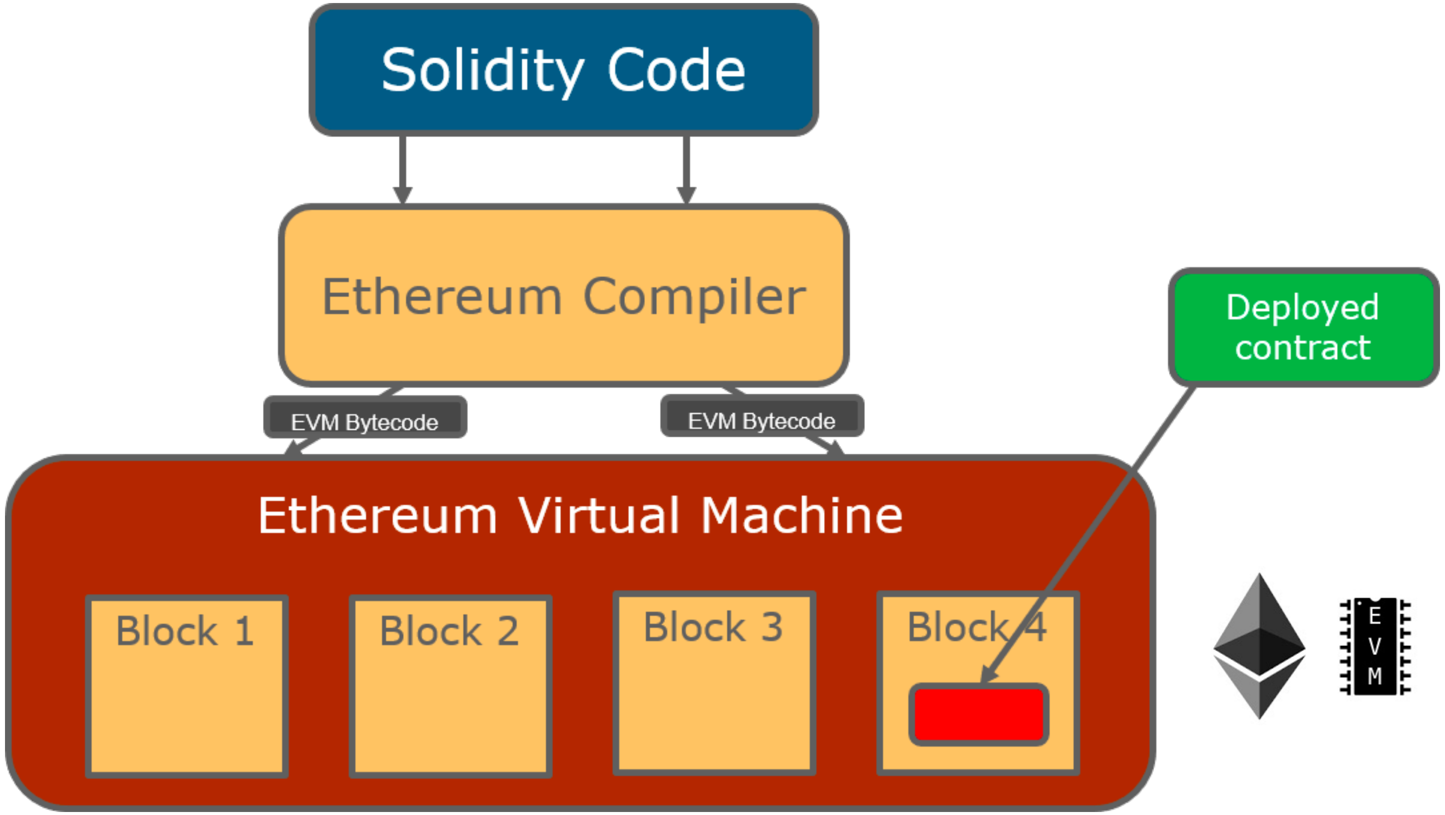
Environment

- `JavaScript VM`: All the transactions will be executed in a sandbox blockchain in the browser. This means nothing will be persisted when you reload the page. The JsVM is its own blockchain and on each reload it will start a new blockchain, the old one will not be saved.
- `Injected Provider`: Remix will connect to an injected web3 provider. `Metamask` is an example of a provider that inject web3.
- `Web3 Provider`: Remix will connect to a remote node. You will need to provide the URL to the selected provider: geth, parity or any Ethereum client.

EVM

Stack based virtual machine



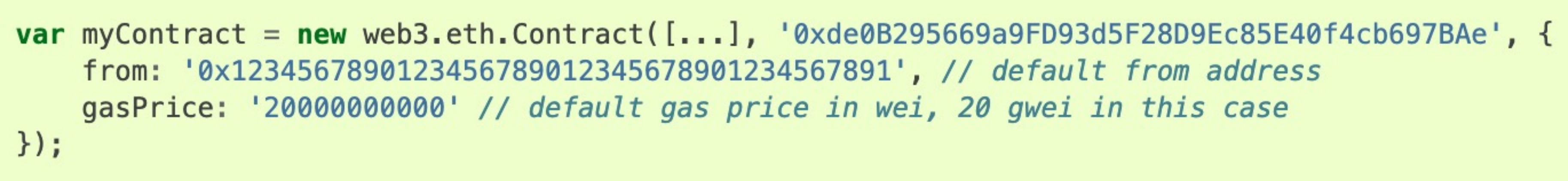


JsVM

- The Ethereum VM implemented in Javascript
  - https://github.com/ethereumjs/ethereumjs-vm
- Local (in-browser) simulation of Ethereum Blockchain Network
  - Fast, instant block confirmation
  - Can create accounts with arbitrary amount of ether
  - Suitable for debugging

Web3.js

- Ethereum JavaScript API
  - https://github.com/ethereum/web3.js/
  - Enable web application to interact with Ethereum Blockchain Network

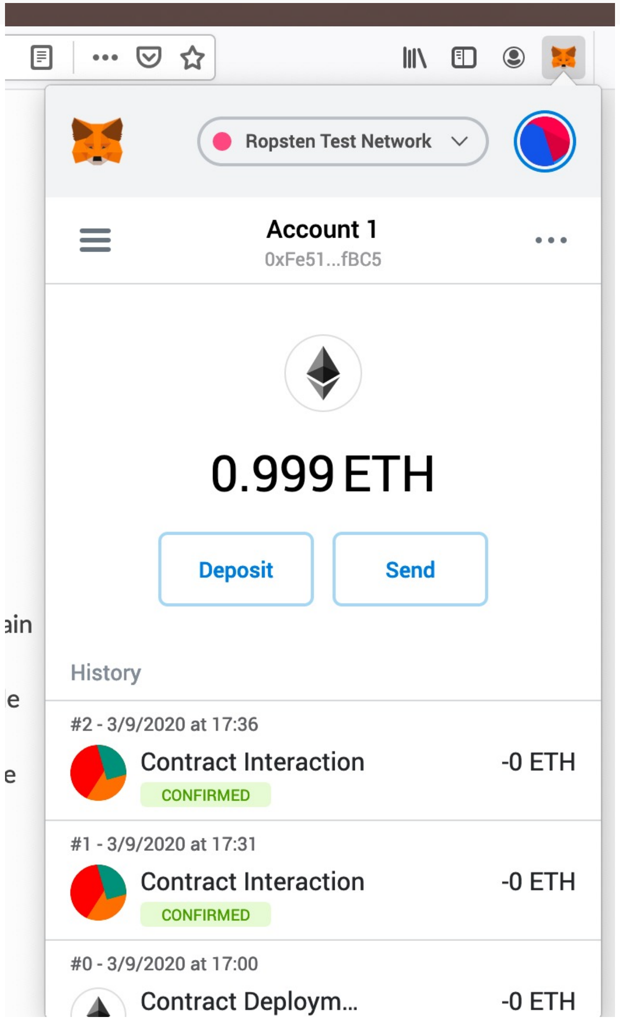


```
var myContract = new web3.eth.Contract([...], '0xde0B295669a9FD93d5F28D9Ec85E40f4cb697BAe', {
    from: '0x1234567890123456789012345678901234567891', // default from address
    gasPrice: '20000000000' // default gas price in wei, 20 gwei in this case
});
```

MetaMask

Interact with Deployed Contract

- A crypto wallet & gateway to blockchain apps
  - https://metamask.io/
  - Can be run as a Chrome extensionl
  - It inject Web3.js into web pages, enable their interaction with blockchain.
  - Can be used as a light wallet



Account 1
0xFe51...fBC5

0.999 ETH

History

#2 - 3/9/2020 at 17:36
Contract Interaction -0 ETH
CONFIRMED

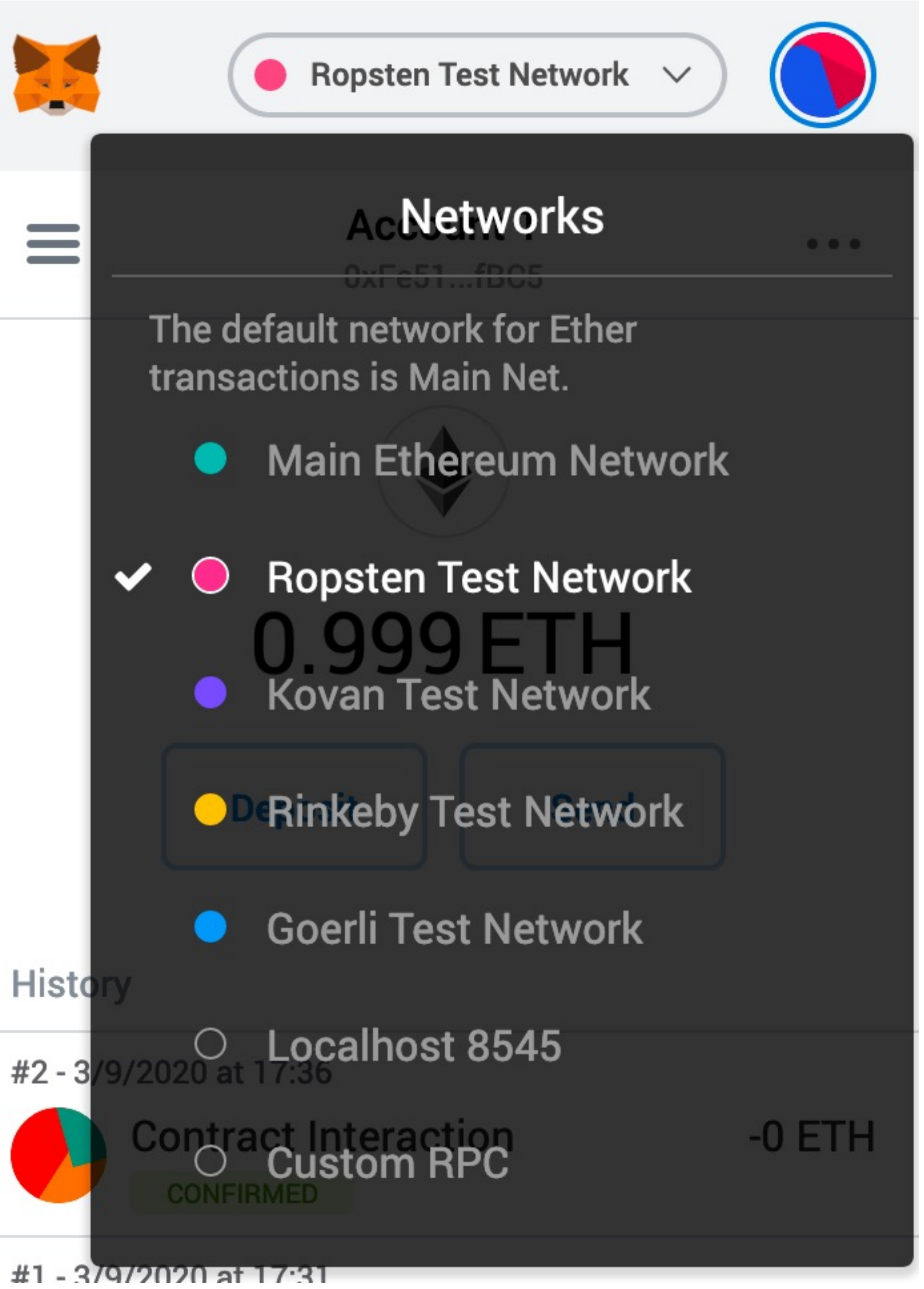
#1 - 3/9/2020 at 17:31
Contract Interaction -0 ETH
CONFIRMED

#0 - 3/9/2020 at 17:00
Contract Deploym... -0 ETH

TestNets

Apart from the Main Ethereum Network (MainNet), there are also several Test Networks (TestNets)

- TestNets are run by developers
- TestNets are copies of certain Ethereum version
- Ethers in TestNets have no real value
- It is easy to get free Ethers in TestNet with “faucet”.



Ropsten Test Network

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

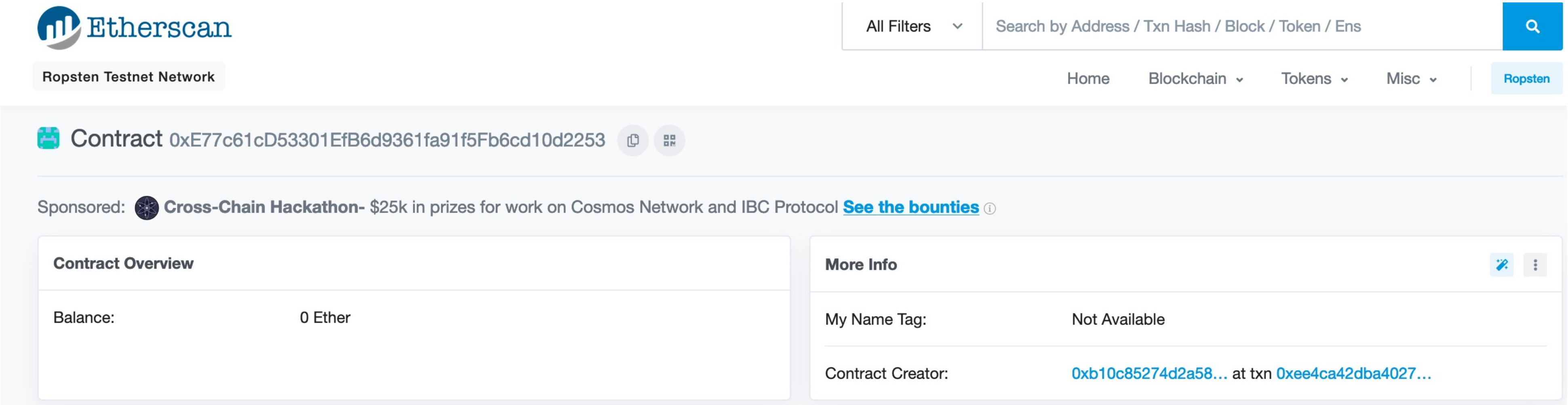
Different TestNets

- Ropsten
  - PoW (Proof-of-Work).
  - Best reproduces the current production environment.
  - Ethers can be mined, noticable confirmation delay (< 30 seconds).
  - Started in Nov 2016, was attacked several time, unstable.
- Koven
  - PoA (Proof-of-Authority), blocks are validated by certain small group of accounts.
  - Ethers cannot be mined, fast transactions (4 seconds)
  - Immune to spam attacks.
  - Started in Mar 2017.
- Rinkeby, Goerli, …
  - PoA
  - …

Reference: https://ethereum.stackexchange.com/questions/27048/comparison-of-the-different-testnets

Etherscan
Ethereum Blockchain Explorer

- Like the Bitcoin Explorer we used for Homework 4, Etherscan is the most popular blockchin explorer for Ethereum.
- It also supports different TestNets, e.g., https://ropsten.etherscan.io
- It has richer functions related to tokens and smart contracts.



Contract 0xE77c61cD53301EfB6d9361fa91f5Fb6cd10d2253

Sponsored: Cross-Chain Hackathon- $25k in prizes for work on Cosmos Network and IBC Protocol See the bounties

Contract Overview

Balance: 0 Ether

More Info

My Name Tag: Not Available

Contract Creator: 0xb10c85274d2a58... at txn 0xee4ca42dba4027...

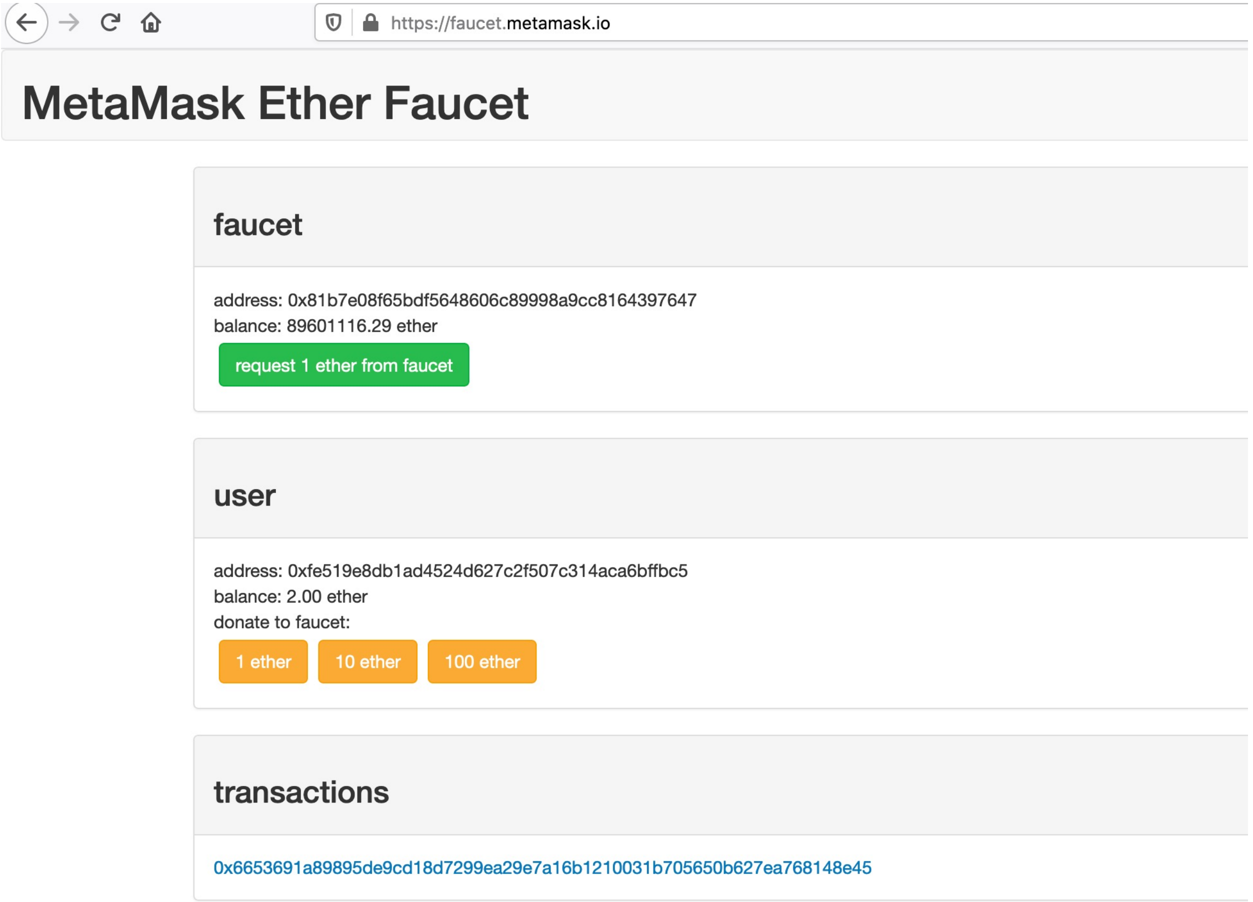
Faucet

Website for requesting free test ethers

There are plenty of faucet available, you just need to Google “<TestNet Name> faucet”, e.g., “Ropsten faucet”.

- https://faucet.metamask.io/
- https://faucet.ropsten.be/

- There are limits, e.g., 3 ethers per (IP, account) per day



MetaMask Ether Faucet

faucet

address: 0x81b7e08f65bdf5648606c89998a9cc8164397647
balance: 89601116.29 ether

user

address: 0xfe519e8db1ad4524d627c2f507c314aca6bffbc5
balance: 2.00 ether
donate to faucet:

transactions

0x6653691a89895de9cd18d7299ea29e7a16b1210031b705650b627ea768148e45

Demo: Deploy and Testing a Contract in TestNet

Note:

- You need some ether in your account for deploying a contract (Why?)
- You need to wait some time before some actions are done now, unlike when you tested in JavaScript VM.

Security Concerns

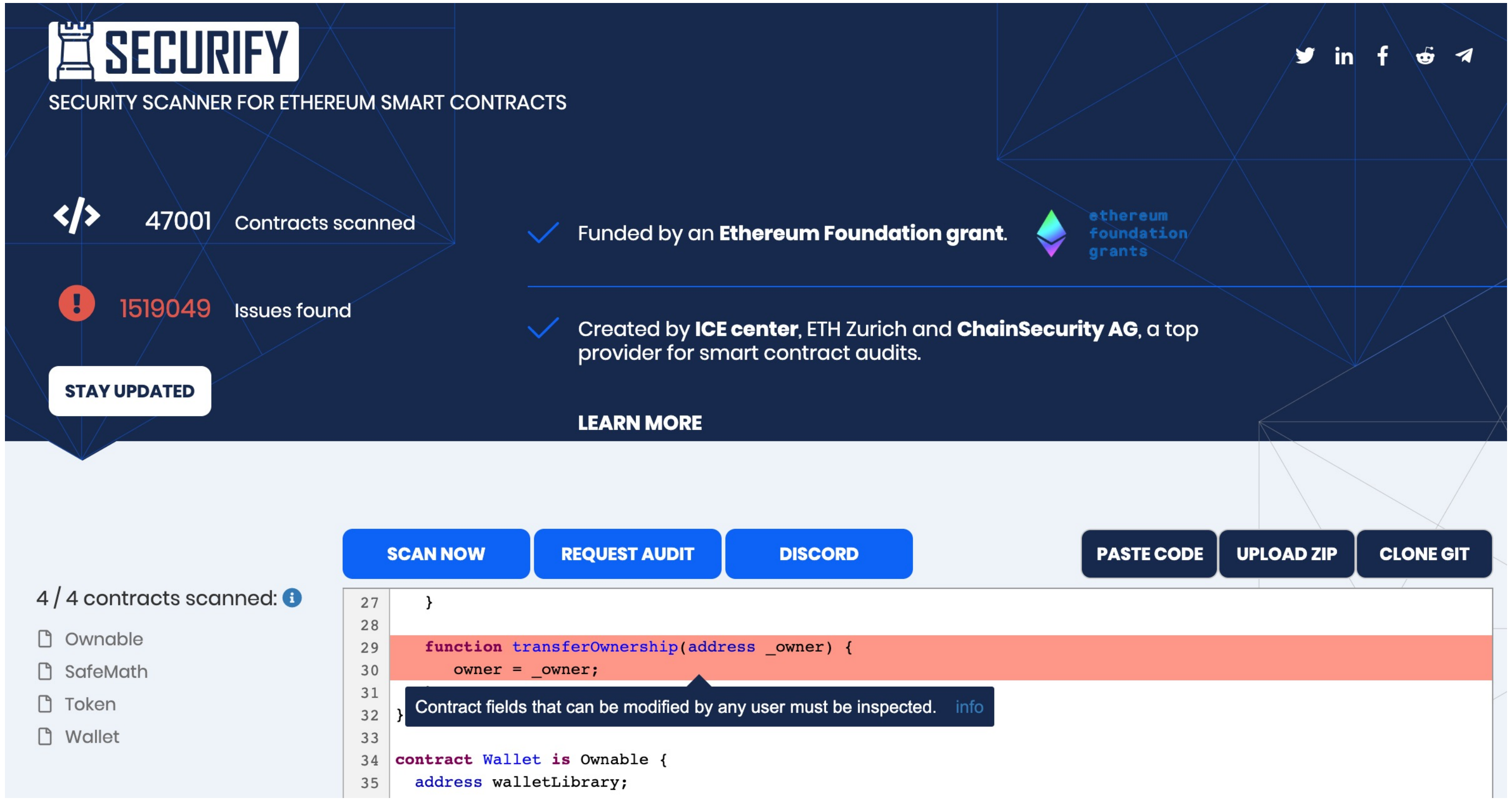
- Every bit of data in Ethereum Blockchain, namely, every variables in your smart contract and every transactions you made is publically available.
    - Think about the Rock Paper Scissors game with Smart Contract.

- It is not trivial to write a smart contract without any security flaws.
    - https://dasp.co/, Top 10 Common Smart Contract Vulnerabilities.
    - Some classic vulnerabilities were discussed in detail in the lecture.

Smart Contract Security Analyzer

There are tools/services that can help to check common vulnerabilities in your smart contart code

- https://securify.chainsecurity.com/
- https://mythx.io/
- https://tool.smartdec.net/
- https://oyente.melonport.com/



47001 Contracts scanned

1519049 Issues found

✓ Funded by an **Ethereum Foundation grant**.

✓ Created by **ICE center**, ETH Zurich and **ChainSecurity AG**, a top provider for smart contract audits.

4 / 4 contracts scanned:

```
  }

  function transferOwnership(address _owner) {
    owner = _owner;

}

contract Wallet is Ownable {
  address walletLibrary;
```

Contract fields that can be modified by any user must be inspected. info

Security Training

- Train yourself to get familiar with common vulnerability patterns in smart contract (know your enemy).
- **The Ethernaut:** https://ethernaut.openzeppelin.com/
  - Wargame style, 22 levels currently.
  - Learn how to break/hack smart contracts
  - Can be completed in browser with MetaMask

Ethernauts

Complete levels by hacking smart contracts

Q&A

References

- Solidity Document, https://solidity.readthedocs.io/, where some sample codes in my slides are from.
- Ethereum Developer Resources, https://ethereum.org/developers/, recources listed on Ethereum official website.
- Learn to Code Blockchain DApps By Building Simple Games, https://cryptozombies.io/, strongly recommended as a start point to learn Solidity coding.
- The Ethernaut - Smart Contract Wargame, https://ethernaut.openzeppelin.com/, strongly recommended if you want to learn more about smart contract security.