Ethereum Basics

박경민

여기서 배울 수 있는 것은?

1. Wallet을 만들고
2. Ether를 전송? 송금하고
3. 간단한 Smart contract를 작성해서
4. 실행해본다.

Ether Currency Units

Ether?

Table 1. Ether denominations and unit names

Value (in wei)	Exponent	Common name	SI name
1	1	wei	Wei
1,000	10^3	Babbage	Kilowei or femtoether
1,000,000	10^6	Lovelace	Megawei or picoether
1,000,000,000	10^9	Shannon	Gigawei or nanoether
1,000,000,000,000	10^{12}	Szabo	Microether or micro
1,000,000,000,000,000	10^{15}	Finney	Milliether or milli
1,000,000,000,000,000,000	*10^{18}*	*Ether*	*Ether*
1,000,000,000,000,000,000,000	10^{21}	Grand	Kiloether
1,000,000,000,000,000,000,000,000	10^{24}		Megaether

Wallet

- 지갑?
- Ethereum wallet
  - MetaMask
  - Jaxx
  - MyEtherWallet(MEW)
  - Emerald Wallet

Control and Responsibility

- 개인키에 대한 기본적인 준수 사항들
- Air-gapped device???
- 개인키에 대한 백업은 종이로.... 오프라인 추천?
  - 이렇게 해야 하나?
- 큰 전송 전에 작은 전송으로 먼저 테스트
  - 돌다리도 두들겨 보고
- Block explorer에서도 노출은 조심

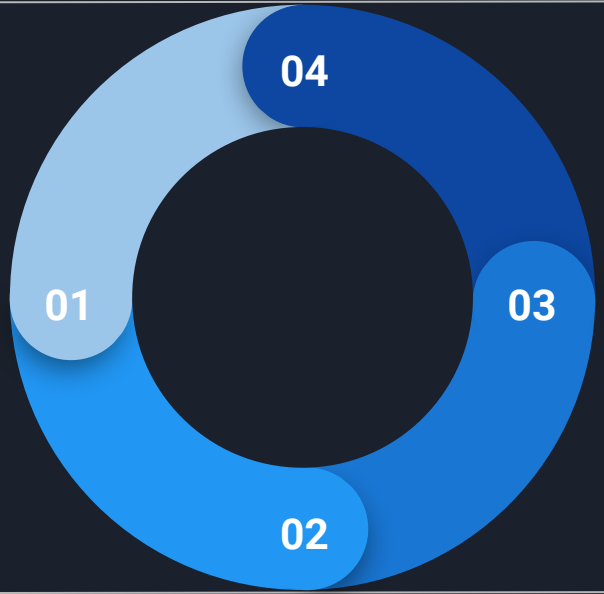
MetaMask 사용해보기

MetaMask 생성

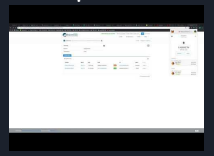
Chrome extension

Testnet 접속

Robsten으로 연습

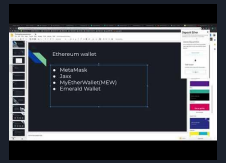


Eth 송금해보기



Account 개념

Eth 충전

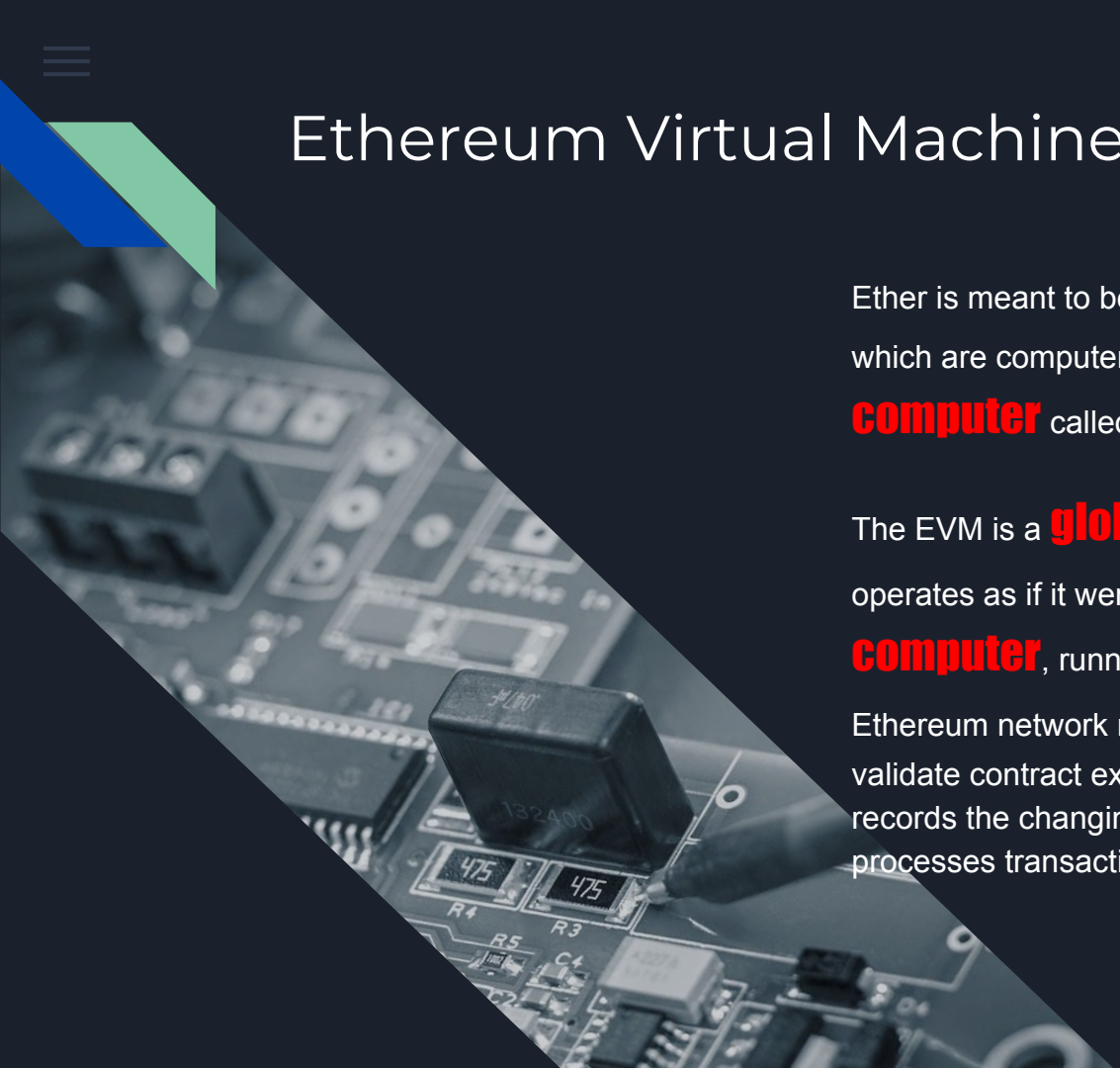


Faucet에서 테스트용 얻기

EOAs and Contract

- Externally Owned Accounts
  - Have private key
  - Have address
- Contract
  - Have address too
  - Doesn’t hava private key
  - Code

Ethereum Virtual Machine



Ether is meant to be used to pay for running smart contracts, which are computer programs that run on an **emulated computer** called the Ethereum Virtual Machine (EVM).

The EVM is a **global singleton**, meaning that it operates as if it were a global, **single-instance computer**, running everywhere. Each node on the Ethereum network runs a **local copy** of the EVM to validate contract execution, while the Ethereum blockchain records the changing state of this world computer as it processes transactions and smart contracts.

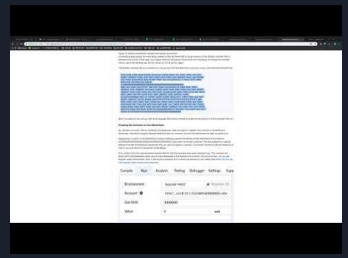
Smart contract by Solidity

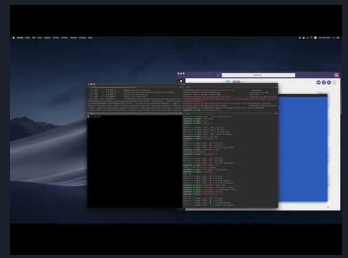
```
PUSH1 0x60 PUSH1 0x40 MSTORE CALLVALUE ISZERO PUSH2 0xF JUMPI PUSH1 0x0 DUP1
REVERT JUMPDEST PUSH1 0xE5 DUP1 PUSH2 0x1D PUSH1 0x0 CODECOPY PUSH1 0x0 RETURN
STOP PUSH1 0x60 PUSH1 0x40 MSTORE PUSH1 0x4 CALLDATASIZE LT PUSH1 0x3F JUMPI
PUSH1 0x0 CALLDATALOAD PUSH29
0x100000000000000000000000000000000000000000000000000000
SWAP1 DIV PUSH4 0xFFFFFFFF AND DUP1 PUSH4 0x2E1A7D4D EQ PUSH1 0x41 JUMPI
JUMPDEST STOP JUMPDEST CALLVALUE ISZERO PUSH1 0x4B JUMPI PUSH1 0x0 DUP1 REVERT
JUMPDEST PUSH1 0x5F PUSH1 0x4 DUP1 DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD SWAP1
SWAP2 SWAP1 POP POP PUSH1 0x61 JUMP JUMPDEST STOP JUMPDEST PUSH8
0x16345785D8A0000 DUP2 GT ISZERO ISZERO ISZERO PUSH1 0x77 JUMPI PUSH1 0x0 DUP1
REVERT JUMPDEST CALLER PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND
PUSH2 0x8FC DUP3 SWAP1 DUP2 ISZERO MUL SWAP1 PUSH1 0x40 MLOAD PUSH1 0x0 PUSH1
0x40 MLOAD DUP1 DUP4 SUB DUP2 DUP6 DUP9 DUP9 CALL SWAP4 POP POP POP POP ISZERO
ISZERO PUSH1 0xB6 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST POP JUMP STOP LOG1 PUSH6
0x627A7A723058 KECCAK256 PUSH9 0x13D1EA839A4438EF75 GASLIMIT CALLVALUE LOG4 0x5f
PUSH24 0x7541F409787592C988A079407FB28B4AD000290000000000
```

첫번째 Smart contract by Solidity

https://remix.ethereum.org

```
// Our first contract is a faucet!
contract Faucet {

    // Give out ether to anyone who asks
    function withdraw(uint withdraw_amount) public {

        // Limit withdrawal amount
        require(withdraw_amount <= 100000000000000000);

        // Send the amount to the address that requested it
        msg.sender.transfer(withdraw_amount);
    }

    // Accept any incoming amount
    function () public payable {}

}
```





Control and Respons

- Externally Owned Accounts
  - Have private key
  - Have address

- Contract
  - Have address too
  - Doesn’t hava private key
  - Code

Thank you!