A short introduction to Ethereum

...

2019

github.com/jgege/FTalk2019feb

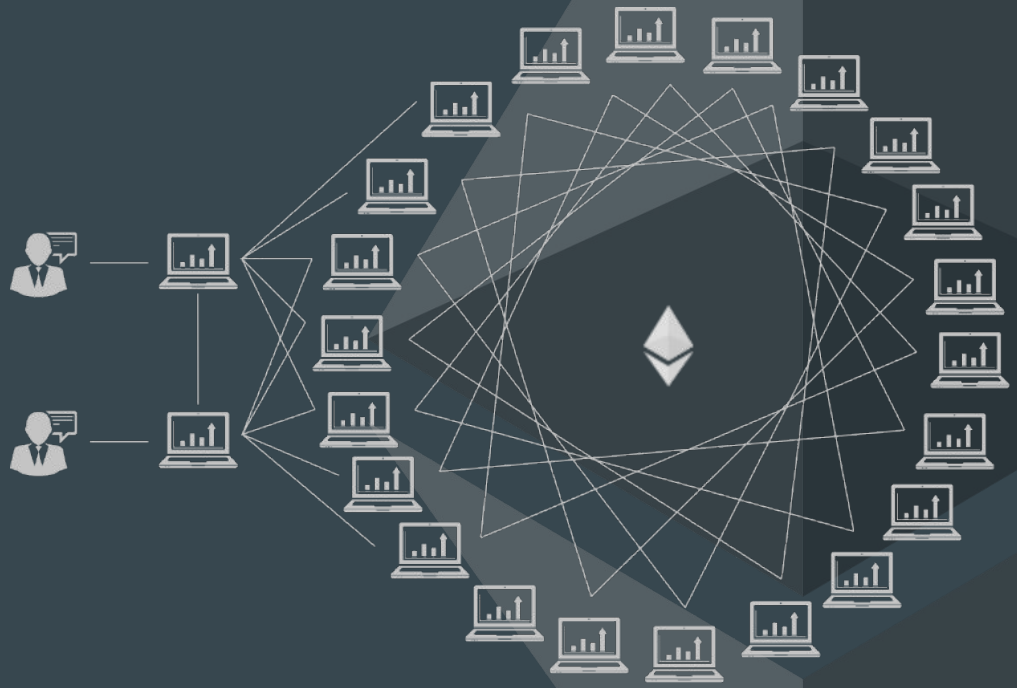
in/gergelyjuhasz92

Ethereum Basics

- Created by Vitalik Buterin, inspired by Bitcoin
- Public, open-source, decentralised platform that runs smart contracts
- Cryptocurrency
  - Ether
  - Units: (1) Ether, (1000000) Szabo, (1000000000000000000) Wei
- Consensus mechanism
  - Proof-Of-Work (it will change soon to Proof-Of-Stake)
- Uses “gas” for pricing transactions (important because of smart contracts)
  - Contract creation: 53000 gas
  - Transaction: 21000 gas
- Account types (address has the same format)
  - Externally Owned Account (EOA)
    - Public and private key
  - Contract

The Ethereum network

- Create transaction
  - Sign it using the private key
- Pass it to the neighbours
  - Each neighbour do some basic validation
- Eventually a miner node will receive it
  - They will choose the ones that worth more (higher gas price)
  - Execute the transaction
  - Include it in the block
- Every transaction and all of its data is visible to everyone in the network



Transactions

Field	Description	Example value
Nonce	A sequence number, issued by the originating EOA, used to prevent message replay	42
Gas price	The price of gas (in wei) the originator is willing to pay	2000000000
Gas limit	The maximum amount of gas the originator is willing to buy for this transaction	3000000
Recipient	The destination Ethereum address	0xbED0D3c46123e6dB10f4eb19ea9041AC8e8f7db5
Value	The amount of ether to send to the destination	5000000000000000
Data	The variable-length binary data payload	0x7f74657374320...0600057
v,r,s	The three components of an ECDSA digital signature of the originating EOA	

Smart Contracts

- The Ethereum Virtual Machine
  - Byte code
  - Opcode
  - https://medium.com/@blockchain101/solidity-bytecode-and-opcode-basics-672e9b1a88c2
  - deterministic
- Solidity
  - https://solidity.readthedocs.io/en/v0.5.3/index.html
  - Compiled to EVM bytecode
- Many other languages
  - Vyper
  - LLL
  - Serpent

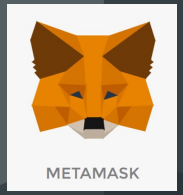
6080604052348015610010576000080fd5b5060405160208061
08b28339810180604052608[…]

PUSH1 0x80 PUSH1 0x40 MSTORE PUSH1 0x40 DUP1 MLOAD SWAP1 DUP2 ADD PUSH1 0x40 MSTORE DUP1[…]

```
pragma solidity ^0.5.0;

/**
 * A simple contract that let's users increase a number by one wi
 * It can only be increased by
 */
contract SimpleCounter {

    uint public counter = 0;

    address lastUser; // address used last time to increment the

    /**
     * Runs only once, at the creation of the contract
     */
    constructor()
    public
    {
        lastUser = msg.sender; // set the initial value to the co
    }
```

Smart Contract Development

- MetaMask - http://metamask.io
  - Easy way to connect to the network (even without downloading it)
- Remix IDE - https://remix.ethereum.org
  - Online code editor with great features
- Truffle Suite - https://trufflframework.com
  - Truffle framework - helps with compiling and deploying smart contracts
  - Ganache - simulated Ethereum blockchain with nice settings (GUI & CLI)
  - Drizzle - Frontend framework to help you create GUI for your application



People worth following

Andreas Antonopoulos

@aantonop

Vitalik Buterin

@VitalikButerin

Kris Bennett

in/kbennett2000

Resources

- Ethereum project's website - https://www.ethereum.org/
- Mastering Ethereum - https://ethereumbook.info - by Andreas M. Antonopoulos, Gavin Wood
- Dapp University (Youtube channel)
- Ethereum Blockchain Developer: Build Projects Using Solidity - https://www.udemy.com/blockchain-developer
- OpenZeppelin - https://openzeppelin.org/
- Smart Contract security: https://medium.com/coinmonks/common-attacks-in-solidity-and-how-to-defend-against-them-9bc3994c7c18
- Enterprise Ethereum Alliance - https://entethalliance.org/
- Blockchain Training Alliance - https://blockchaintrainingalliance.com/

Public SM source codes

- Tug of War - https://medium.com/@etherplay/our-first-unstoppable-game-tug-of-war-bb69c63a8734
- CryptoKitties - https://medium.com/loom-network/how-to-code-your-own-cryptokitties-style-game-on-ethereum-7c8ac86a4eb3
- CryptoZombies - https://cryptozombies.io/

Any questions before the demo?