A quick introduction to Ethereum

...

2019

github.com/jgege/FTalk2019feb

in/gergelyjuhasz92

What is Ethereum?

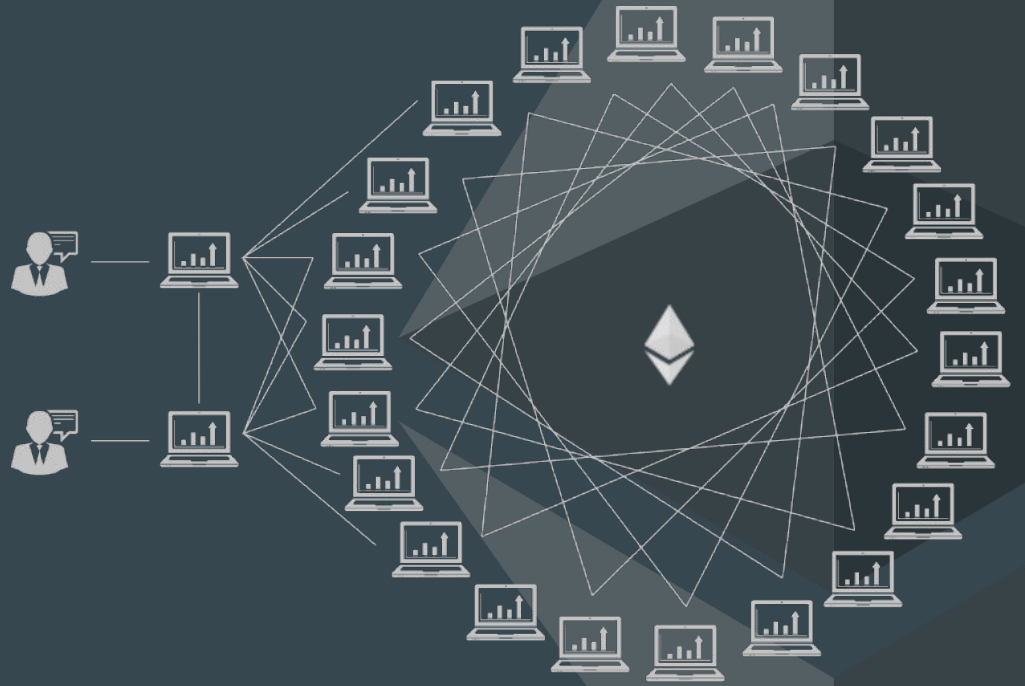
- decentralised platform that runs smart contracts
- public, open-source
- powerful shared global infrastructure that can move value around and represent the ownership of property
- inspired by Bitcoin

Ethereum Basics

- Cryptocurrency
  - Ether
- Consensus mechanism
  - Proof-Of-Work (it will change soon to Proof-Of-Stake)
- Uses “gas” for pricing transactions (important because of smart contracts)
- 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



Transactions

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

Smart Contracts

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

```
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/
- Enterprise Ethereum Alliance - https://entethalliance.org/
- Blockchain Training Alliance - https://blockchaintrainingalliance.com/

Any questions before the demo?