Ethereum concepts:

- Core Concepts

Discount Coupon Link to UDEMY course:

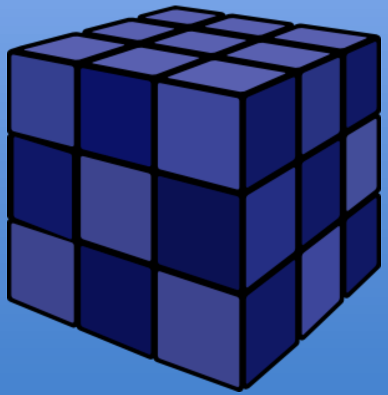
https://www.udemy.com/ethereum-dapp/?couponCode=ETHDAPP101

This deck is part of a online course on “Ethereum: Design and Development of Decentralized Apps.

raj@acloudfan.com

@acloudfan

http://ACloudFan.com

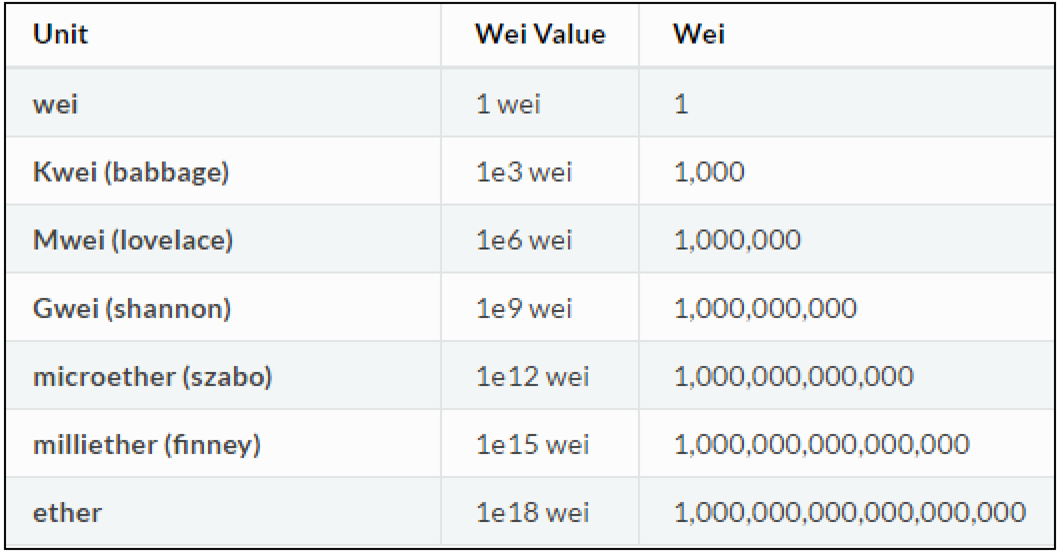


Ethereum?

- **Open source** public Blockchain network
  - Value token = **Ether**
  - De-centralized Turing-complete Virtual Machine
  - Smart contracts platform
  - Execution requires payment - gas

Ethers (ETH)

- Ethereum : Value token
- Denominations:



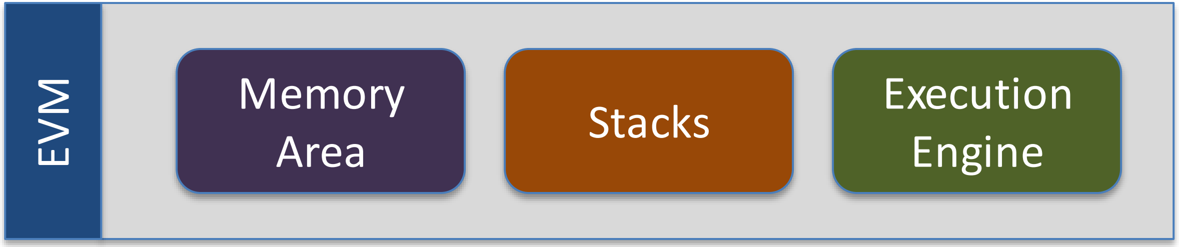
Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

Ethers Supply

- Ether creation
  - Presale (2014): 60 Million
  - 12 Million created to fund the development
  - 5 Ethers created as reward for every block; roughly ~14 seconds
  - Sometimes 2-3 Ethers for non-winning miners (*uncle rewards*)
- Contract invocation – Users pay by *Ethers*
- Incentive for the miners

EVM

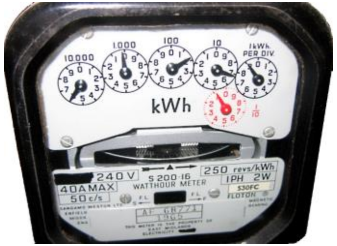
- An software that can execute Ethereum Bytecode
  - Follows the EVM specifications *(Ethereum protocol)*
  - Runs as a process on a computer/sever



  - EVM implemented in multiple languages

Gas

- User invoking the transaction pays for the execution

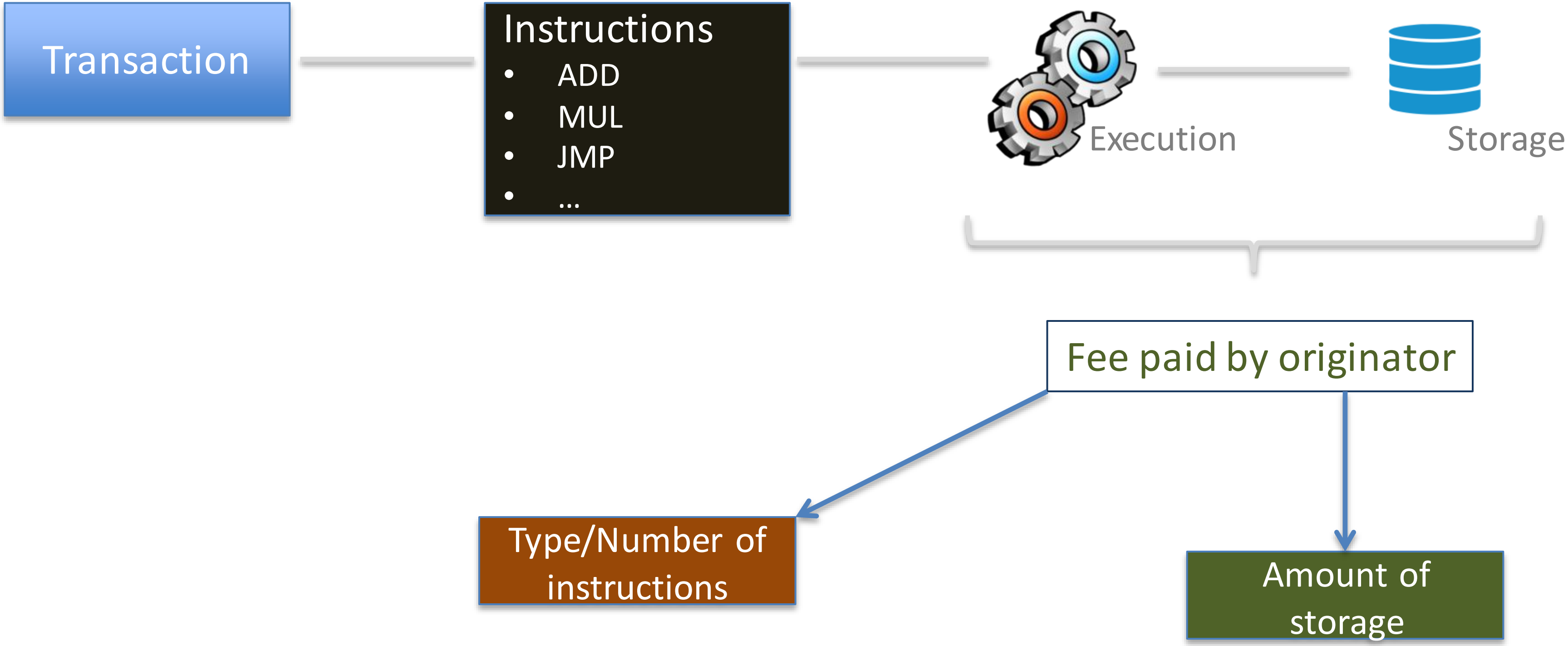


Measures: kWH used

Measures: Gallons of water used

- Gas is the unit in which EVM resource usage is measured

Gas Calculations



Transaction

Instructions

- ADD
- MUL
- JMP
- …

Execution

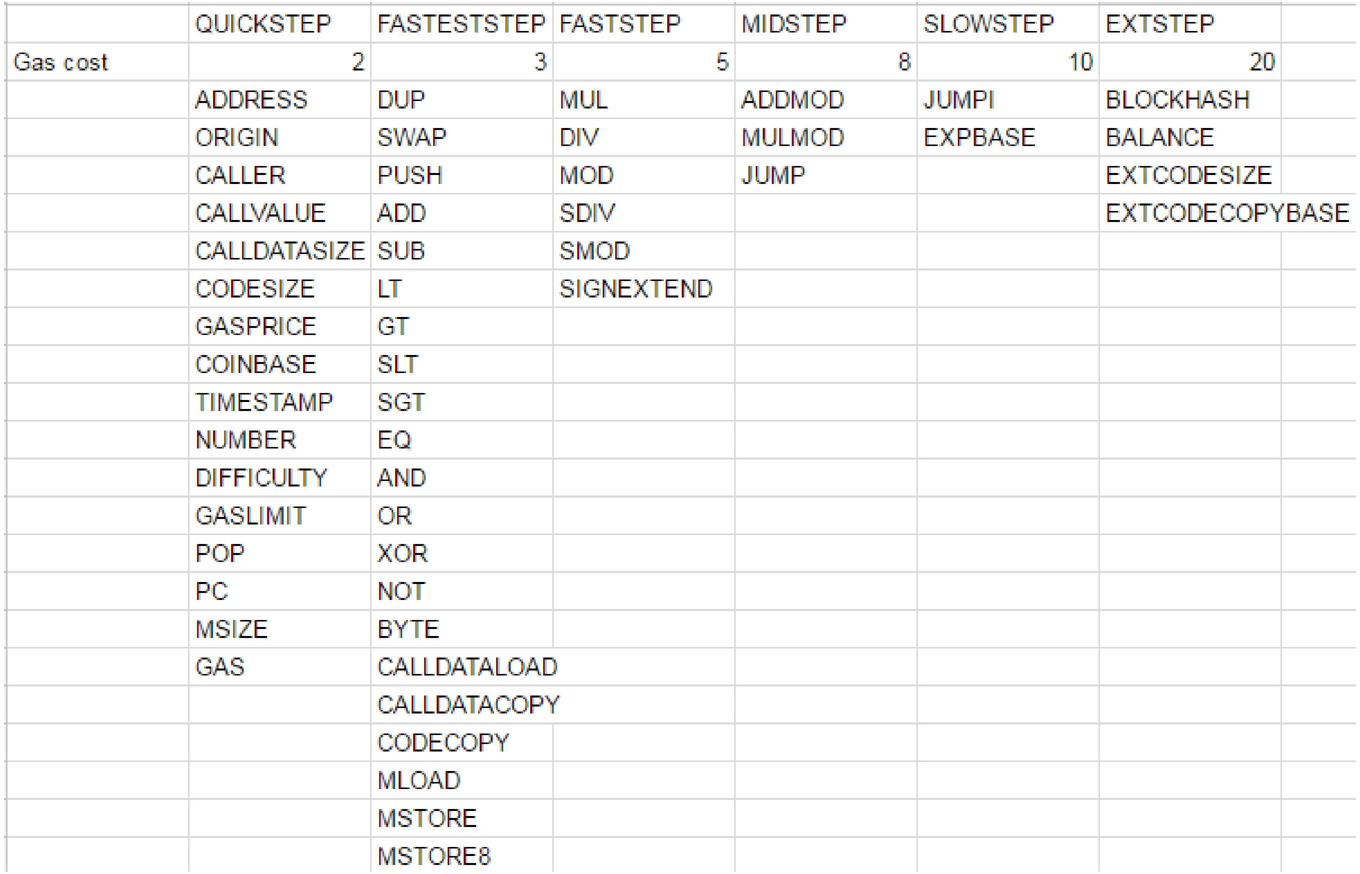
Storage

Fee paid by originator

Type/Number of instructions

Amount of storage

Opcodes & Gas



	QUICKSTEP	FASTESTSTEP	FASTSTEP	MIDSTEP	SLOWSTEP	EXTSTEP
Gas cost	2	3	5	8	10	20
	ADDRESS	DUP	MUL	ADDMOD	JUMPI	BLOCKHASH
	ORIGIN	SWAP	DIV	MULMOD	EXPBASE	BALANCE
	CALLER	PUSH	MOD	JUMP		EXTCODESIZE
	CALLVALUE	ADD	SDIV			EXTCODECOPYBASE
	CALLDATASIZE	SUB	SMOD			
	CODESIZE	LT	SIGNEXTEND			
	GASPRICE	GT				
	COINBASE	SLT				
	TIMESTAMP	SGT				
	NUMBER	EQ				
	DIFFICULTY	AND				
	GASLIMIT	OR				
	POP	XOR				
	PC	NOT				
	MSIZE	BYTE				
	GAS	CALLDATALOAD				
		CALLDATACOPY				
		CODECOPY				
		MLOAD				
		MSTORE				
		MSTORE8				

Fee Calculation

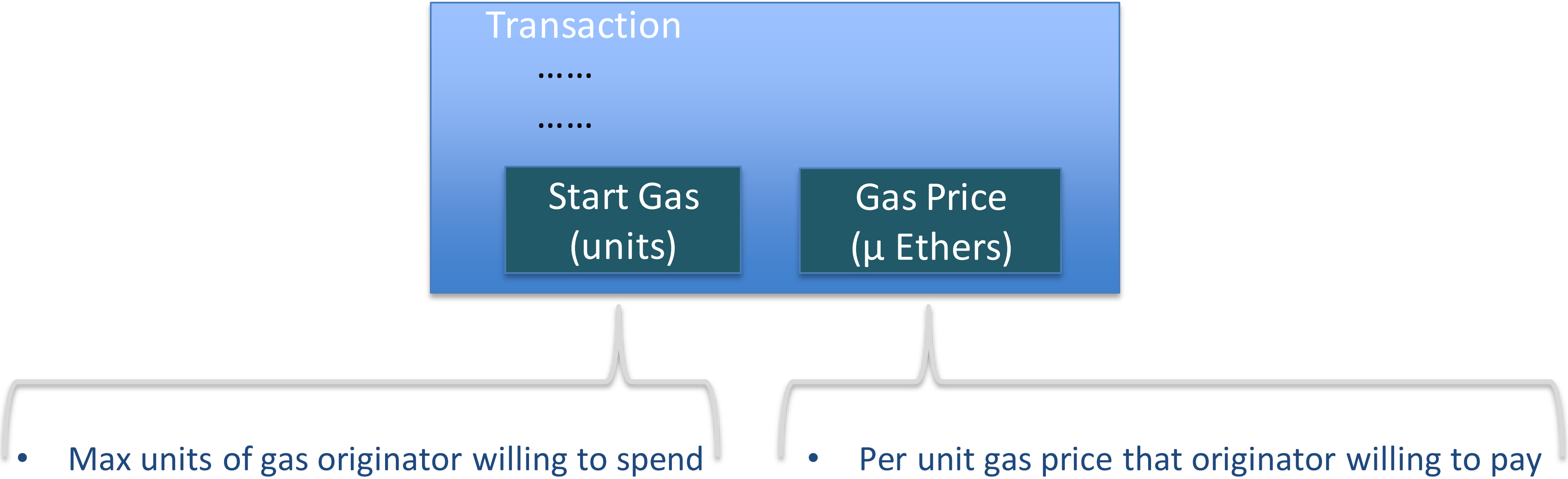
gasUsed = Instructions executed (summed up gas)

gasPrice = User specified in the transaction

Miners decides the minimal acceptable price

Transaction Fee = gasUsed * gasPrice

Transaction Fee : Parameters



Transaction

……

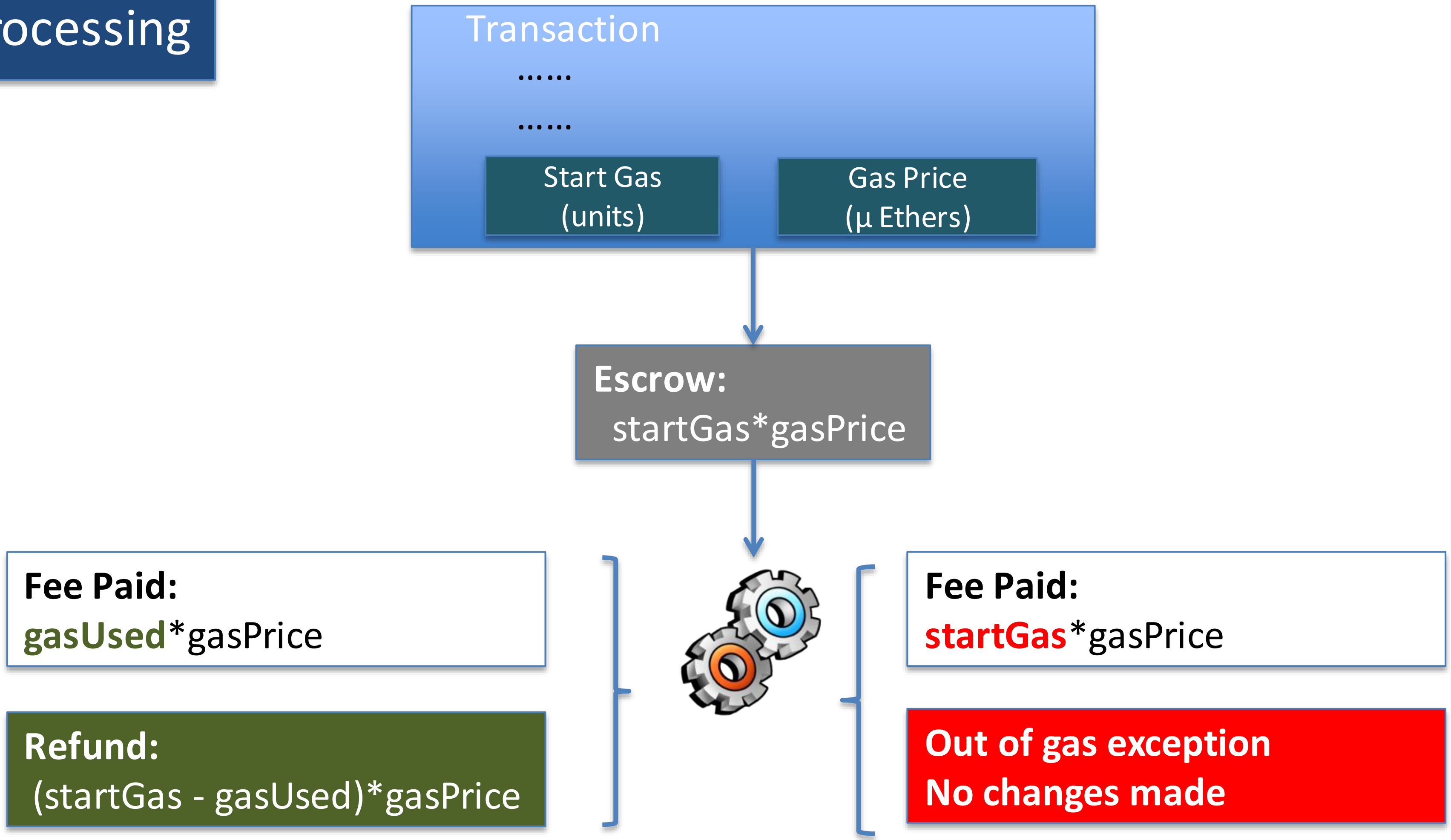
……

Start Gas (units)

Gas Price (µ Ethers)

- Max units of gas originator willing to spend
- Per unit gas price that originator willing to pay

Processing



Transaction

……

……

Start Gas (units)

Gas Price (µ Ethers)

Escrow: startGas*gasPrice

Fee Paid: gasUsed*gasPrice

Refund: (startGas - gasUsed)*gasPrice

Fee Paid: startGas*gasPrice

Out of gas exception

No changes made

Consensus

- Process by which blocks get created
  - Validate transactions
  - Secures the network

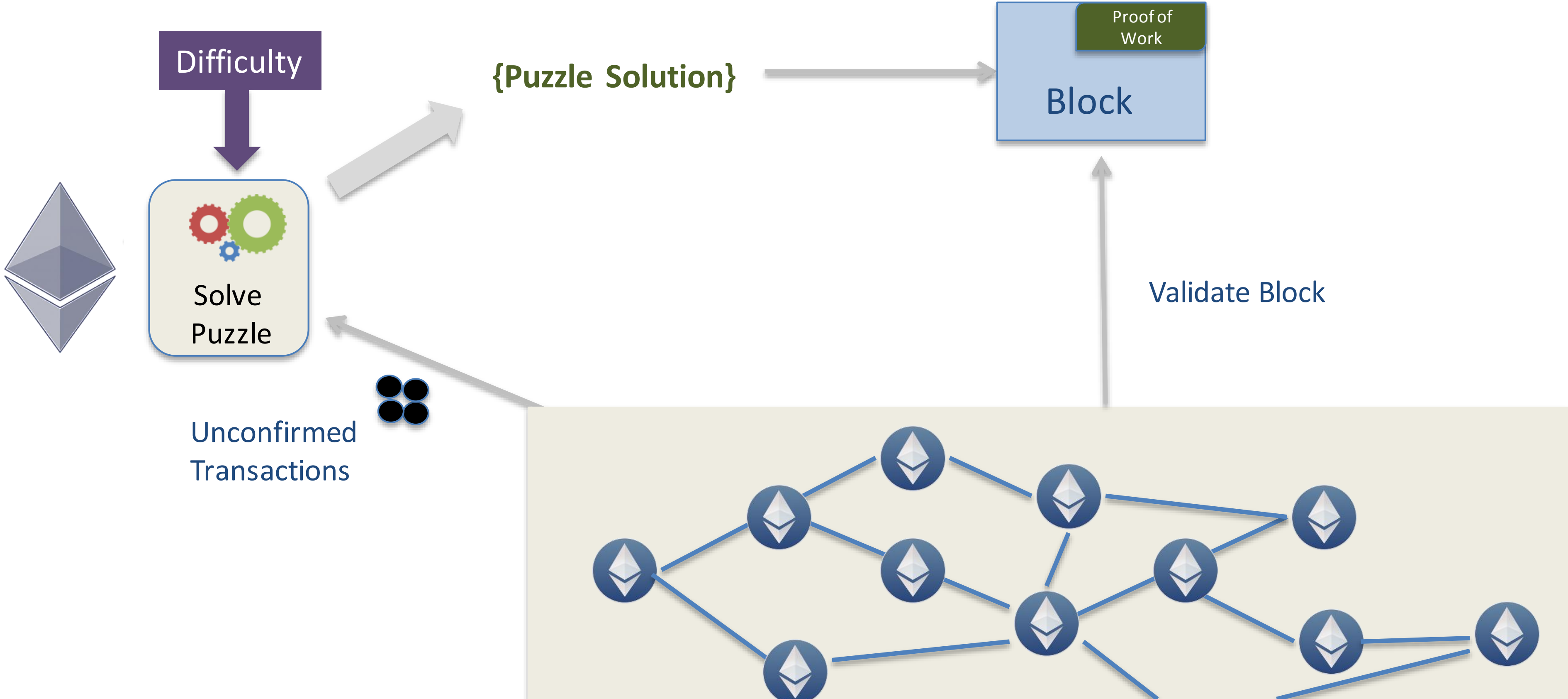
Proof of Work

Proof of Stake

- Incentive driven model
  - Fixed reward in tokens
  - Transaction fee

Proof of Work

- Computationally (CPU | Memory | Bandwidth) intensive



Difficulty

Solve Puzzle

{Puzzle Solution}

Proof of Work

Block

Validate Block

Unconfirmed Transactions

Ethereum: Proof of Work

- Protocol: GHOST
- Algorithm: ETHash
- Difficulty: Network adjusted; block created ~12 seconds
- Incentive: 5 Ether

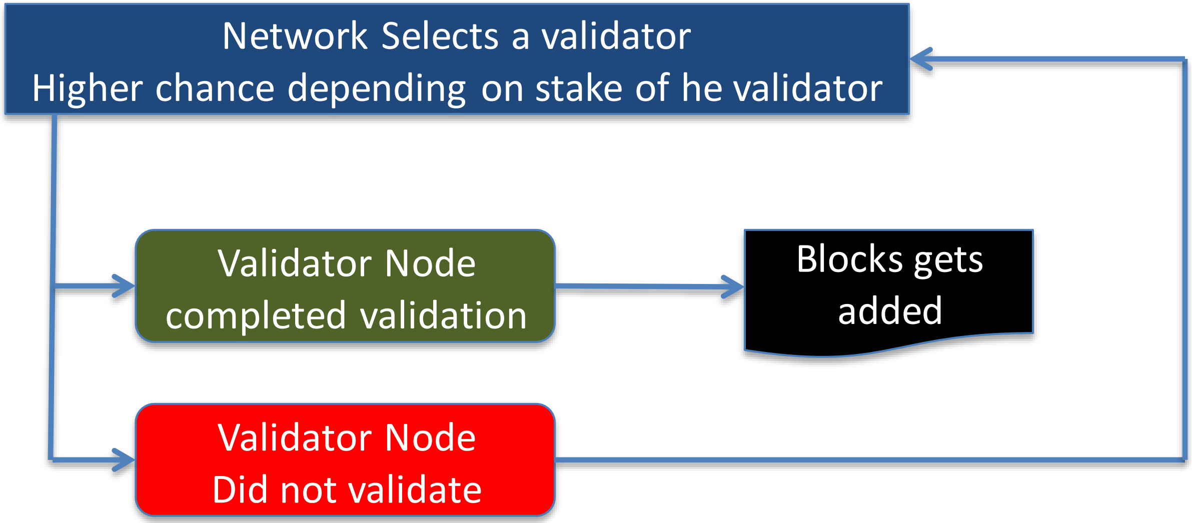
  Gas fee for transactions

  Uncles reward 4.375 ETH Max: 2

Proof of work is environmentally Un-Friendly

Proof of Stake

- Node to validate selected by the network | No competition
  - **Stake** – refers to the wealth that users holds on the network
  - Node that validates referred to as *Validator* not a miner



Ethereum: Proof of Stake

- Ethereum future version will switch to ***Proof of Stake***
  - Protocol: CASPER

- Why switch to Proof Of Stake?
  - Reduced energy consumption
  - A lower incentive needed for motivation
  - Stake in the network will promote good behavior
  - Punishment as part of the protocol will act as deterrent

Ethereum Network

Live Network

- Network ID = 1

Test-Net

- Network ID = 2 Morden *retired*
- **Network ID = 3 Ropsten** *current*

KOVAN *RINKEBY (ID=4)* *current*

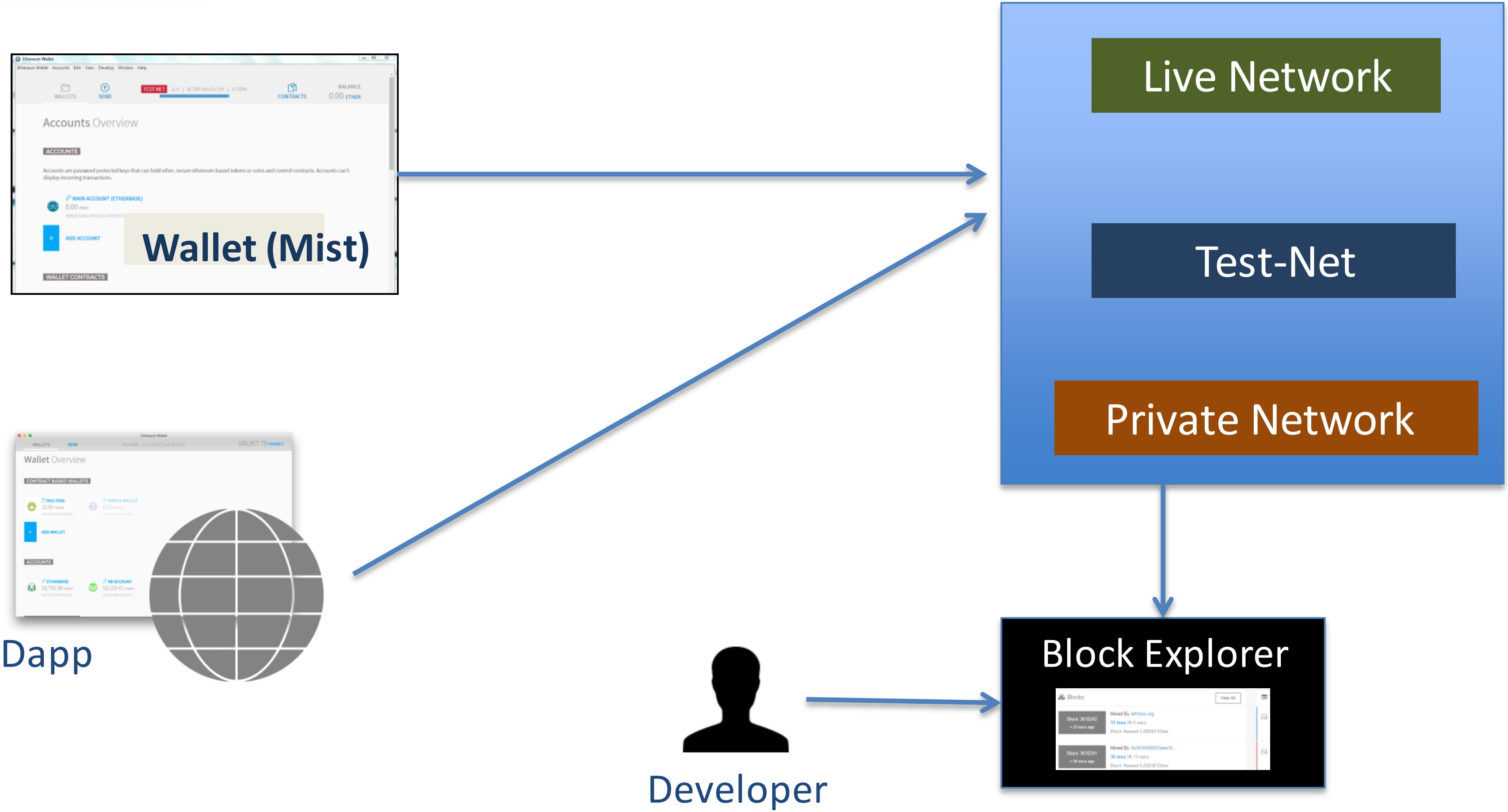
Private Network

- Network ID = Assigned

Private Network

- Data privacy
- As a distributed database
- Consortium
  - Industry verticals
  - Permissioned
  - Internal transactions & contracts

Interaction



Wallet (Mist)

Dapp

Live Network

Test-Net

Private Network

Block Explorer

Developer

Ethereum concepts:

- Wallet
- Explorer
- Account types

Discount Coupon Link to UDEMY course:

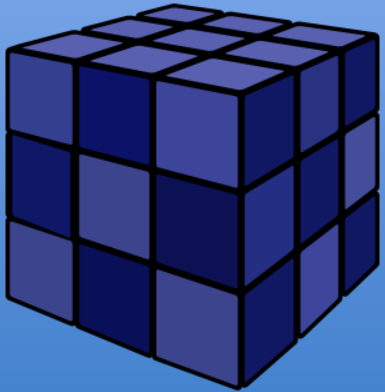
https://www.udemy.com/ethereum-dapp/?couponCode=ETHDAPP101

This deck is part of a online course on "Ethereum: Design and Development of Decentralized Apps.

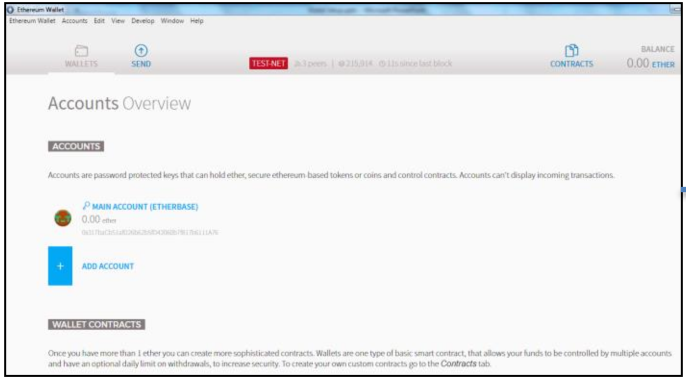
raj@acloudfan.com

@acloudfan

http://ACloudFan.com



Wallet Architecture


Ethereum Wallet
Ethereum Wallet Accounts Edit View Develop Window Help
WALLETS
SEND
TEST-NET
3 peers | 215,014 11s since last block
CONTRACTS
BALANCE
0.00 ETHER

Accounts Overview

ACCOUNTS

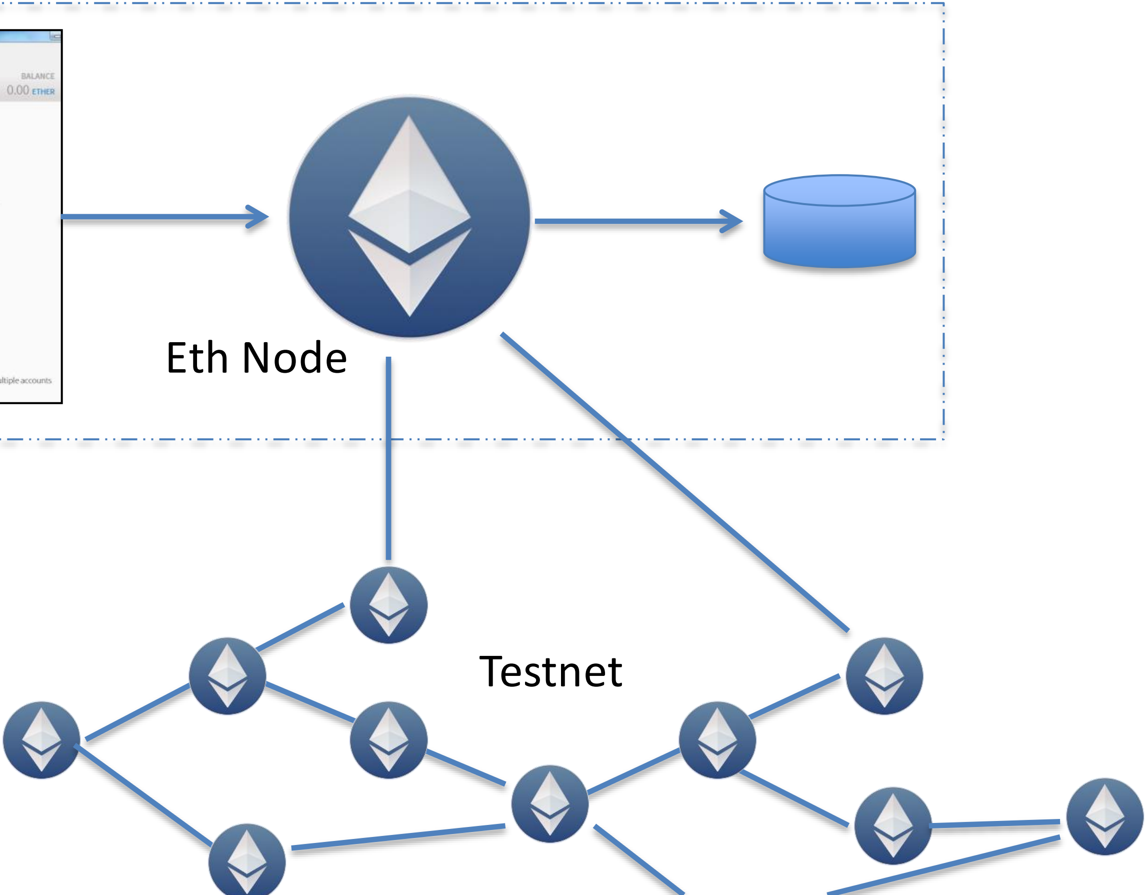
Accounts are password protected keys that can hold ether, secure ethereum-based tokens or coins and control contracts. Accounts can't display incoming transactions.

MAIN ACCOUNT (ETHERBASE)
0.00 ether
[illegible]

+ ADD ACCOUNT

WALLET CONTRACTS

Once you have more than 1 ether you can create more sophisticated contracts. Wallets are one type of basic smart contract, that allows your funds to be controlled by multiple accounts and have an optional daily limit on withdrawals, to increase security. To create your own custom contracts go to the *Contracts* tab.



Blockchain explorer

- Websites (or webapps) that show information on
  - Transactions
  - Blocks
  - Accounts

Etherscan
The Ethereum Block Explorer

ether.camp

Etherchain.org

https://etherscan.io/

https://live.ether.camp/

https://etherchain.org/

https://testnet.etherscan.io/

Type of Accounts

Externally Owned Account

- Has an address
- Private key protected by password

Contract Account

- Has an address but NO private key
- Holds/Run code
  - Associated with Account(s)
  - NOT free to use

Contract Account

Single Owner

- One *Account* creates & owns

MultiSig

- One *Account* creates
- Multiple owners
  - M-of-N type wallets

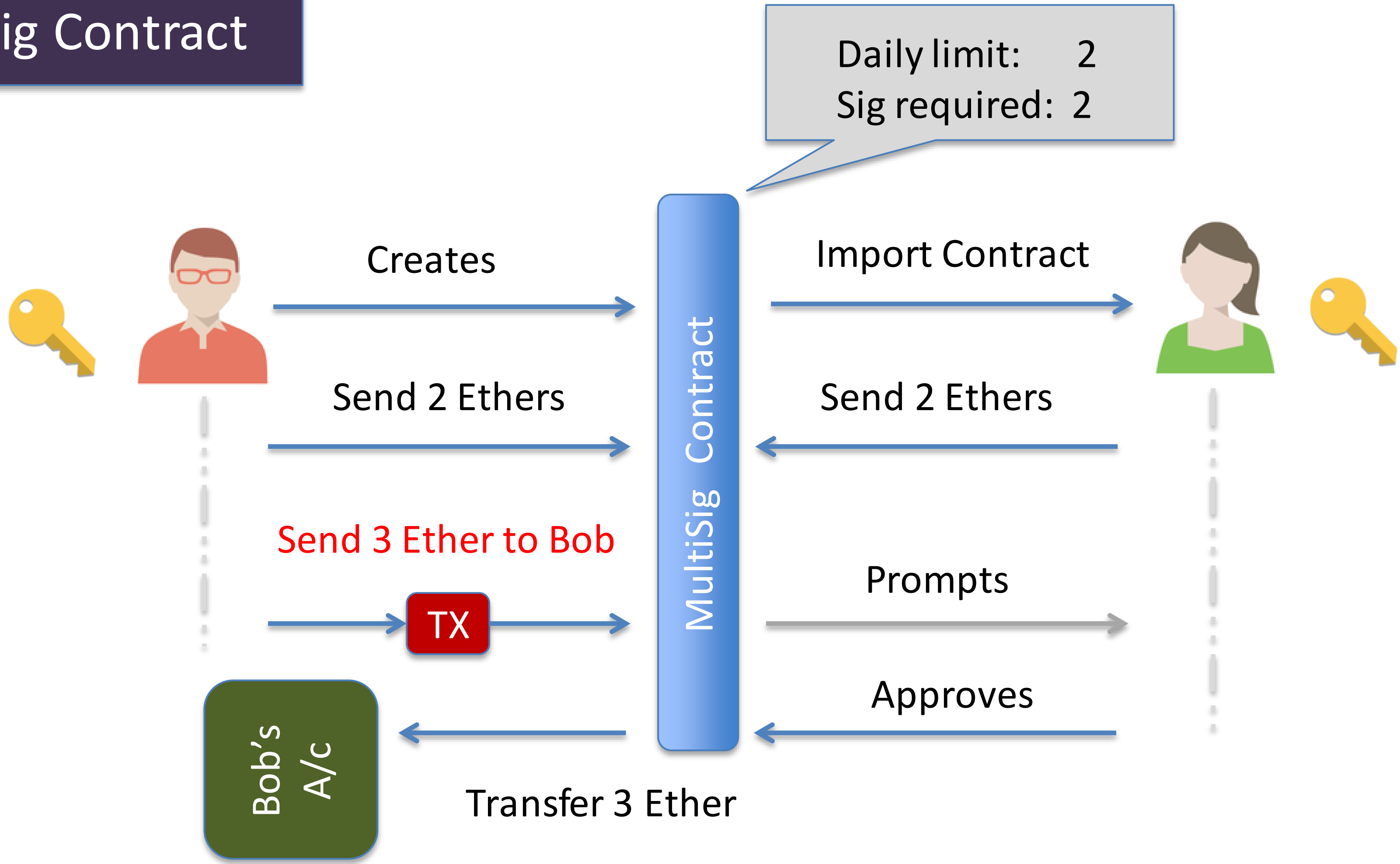
    N = Number of owners

    M = Required to confirm transaction

Single Owner

- Accounts can't display incoming transactions
- Create simple contract to see incoming transactions

MultiSig Contract



Decentralized Apps

- Working
- Architecture

Discount Coupon Link to UDEMY course:

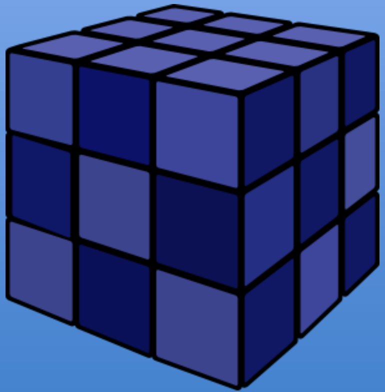
https://www.udemy.com/ethereum-dapp/?couponCode=ETHDAPP101

This deck is part of a online course on
“Ethereum: Design and Development of Decentralized Apps.

raj@acloudfan.com

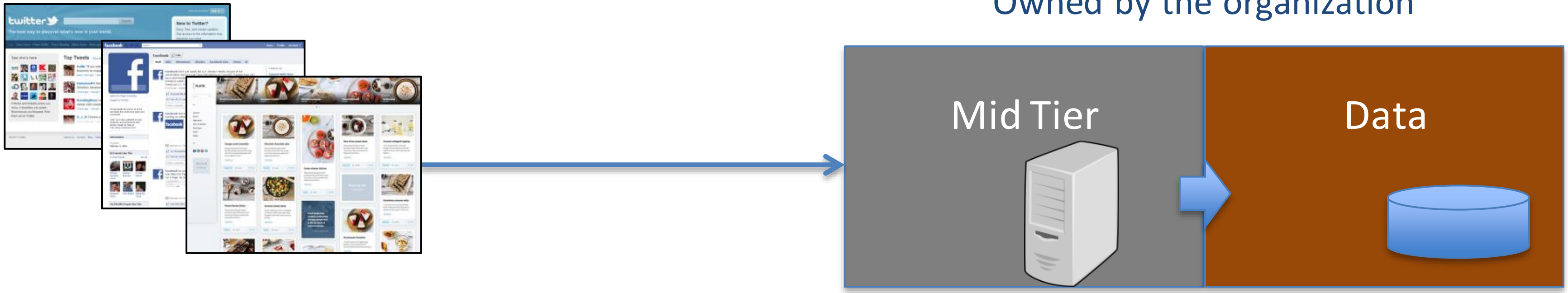
@acloudfan

http://ACloudFan.com



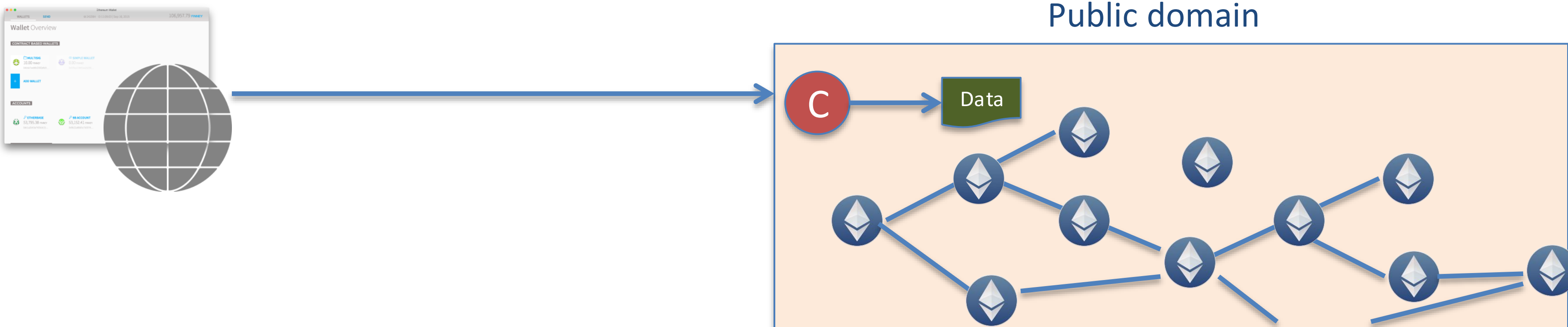
Web App → DAPP

Centralized Resources
Owned by the organization



Front end apps

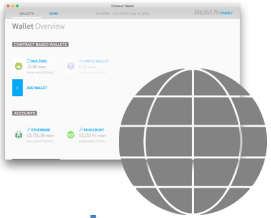
Decentralized Resources
Public domain



Working of Dapp

Invoke Contract

- App user pays *gas/fee*



Ethereum Wallet

WALLETS SEND 106,957.79 FINNEY

Wallet Overview

CONTRACT BASED WALLETS

MULTISIG 10.00 FINNEY

SIMPLE WALLET 0.00 FINNEY

+ ADD WALLET

ACCOUNTS

ETHERBASE 53,795.38 FINNEY

9B ACCOUNT 53,152.41 FINNEY

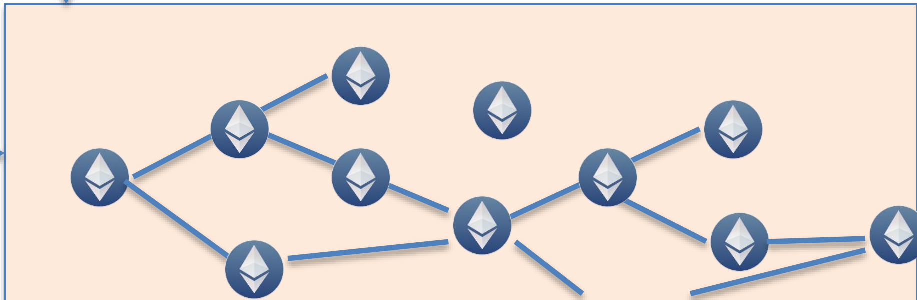
Ethereum Wallet

Version 0.5.2
License GPL-3.0
GitHub github.com/ethereum/mist

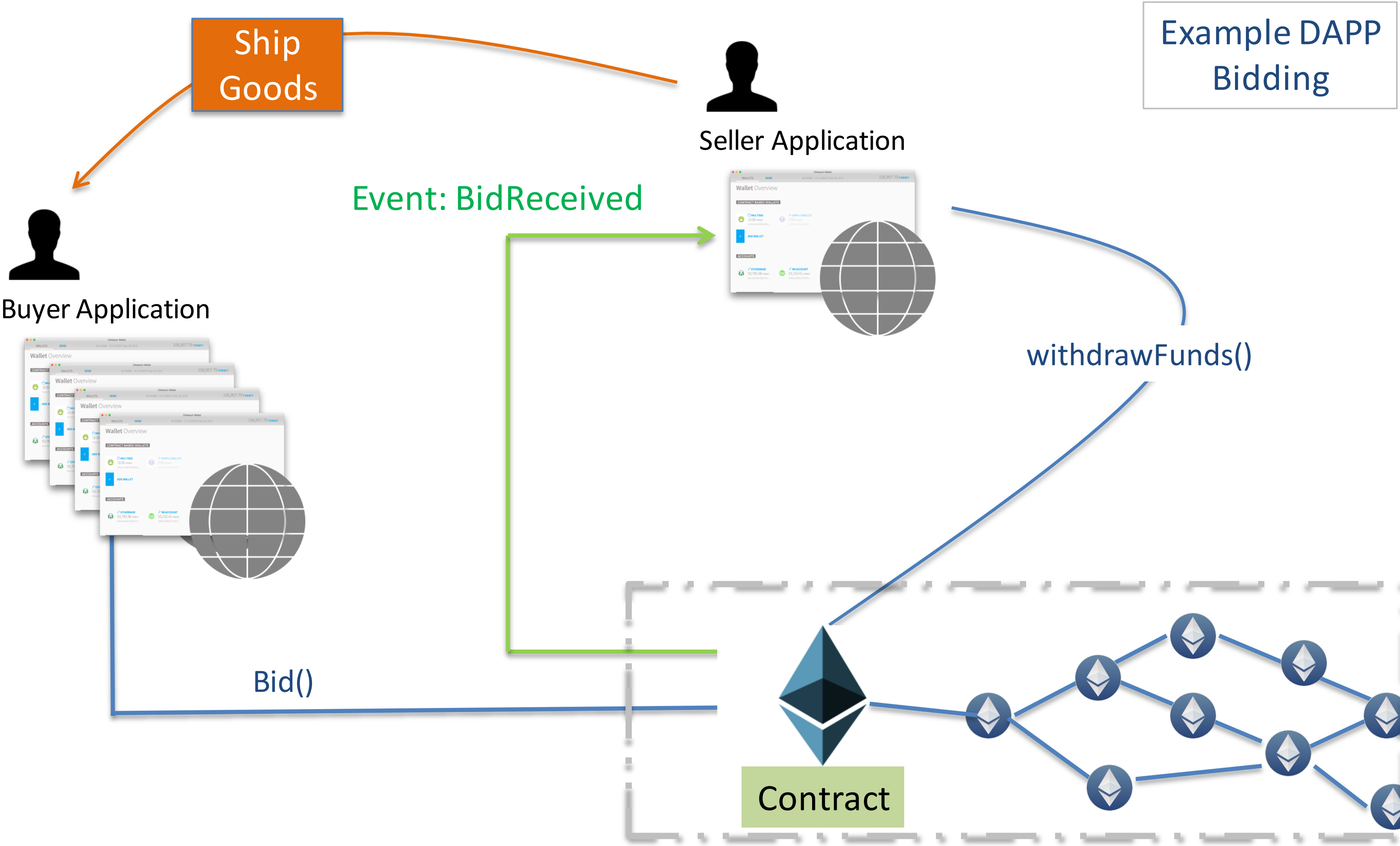
Copyright 2016 Ethereum Foundation

- Manage funds
- Invoke Contracts

- Miner collects
- Transaction validated/mined
- Recorded in ledger



Example DAPP Bidding



DAPP Technology Stack

HTML CSS JS

Java

python

Microsoft® .NET

C++

web3

OLIDITY

Serpent

Lisp Like Language

Decentralized Apps

- MetaMask

Discount Coupon Link to UDEMY course:

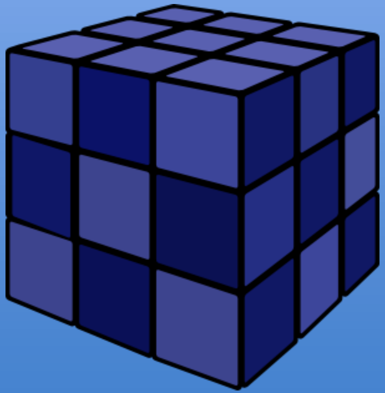
https://www.udemy.com/ethereum-dapp/?couponCode=ETHDAPP101

This deck is part of a online course on “Ethereum: Design and Development of Decentralized Apps.

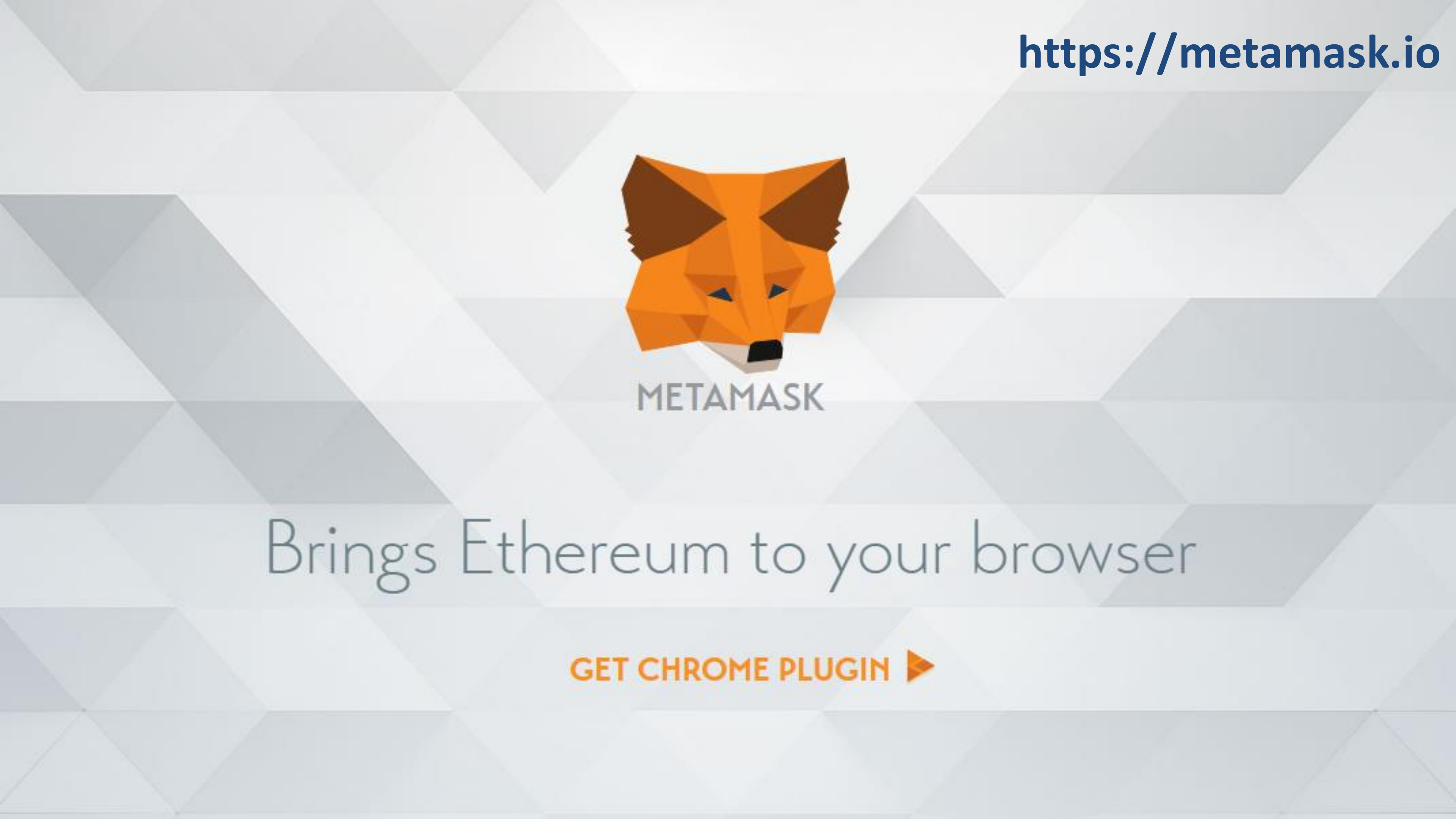
raj@acloudfan.com

@acloudfan

http://ACloudFan.com



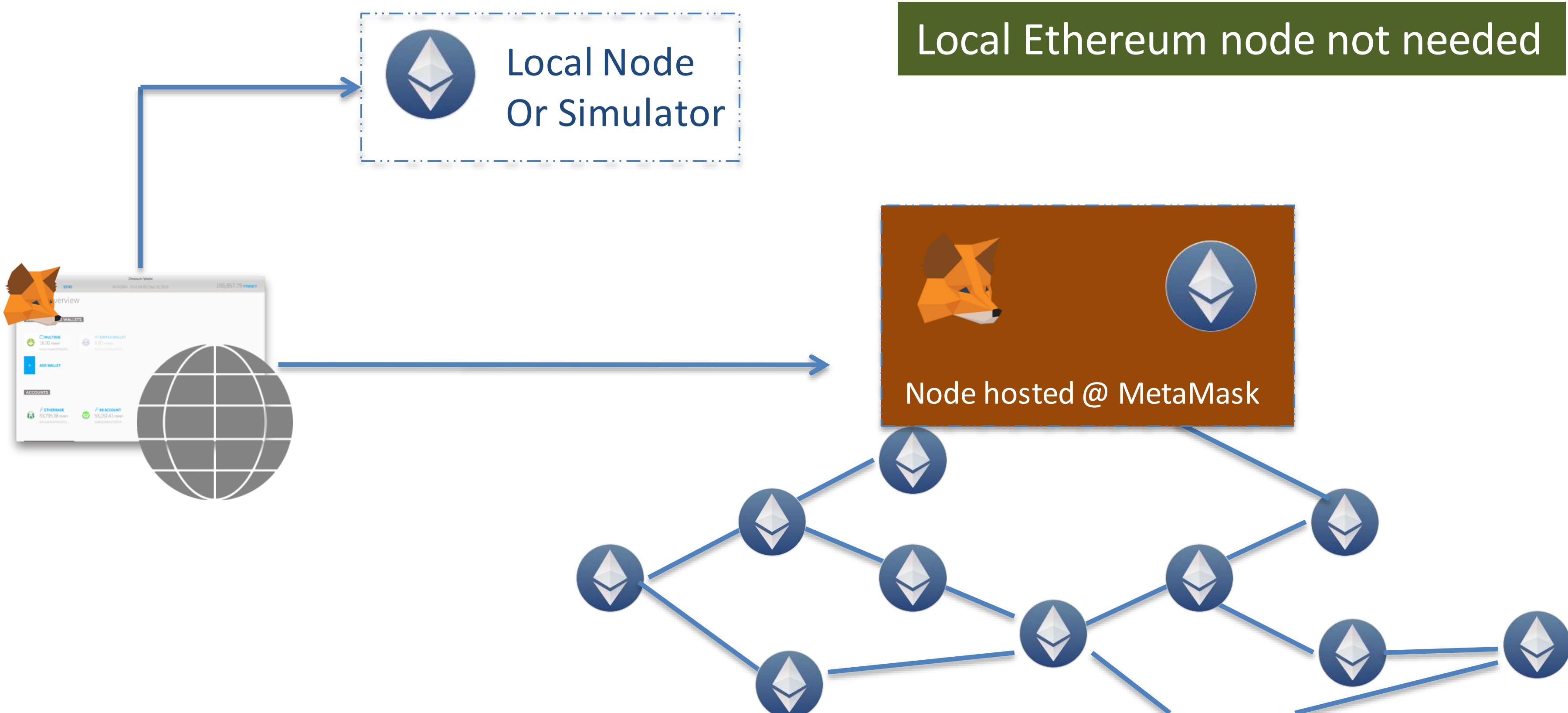
https://metamask.io



Brings Ethereum to your browser

Meta Mask

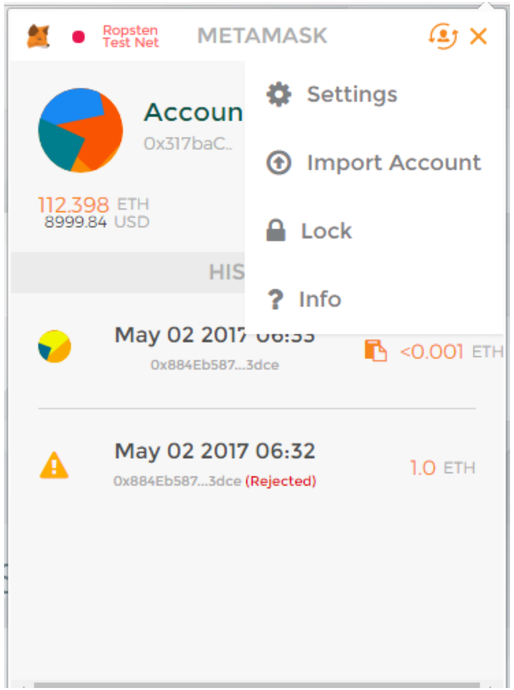
Chrome plugin turns browser into DAPP container



Local Node
Or Simulator

Local Ethereum node not needed

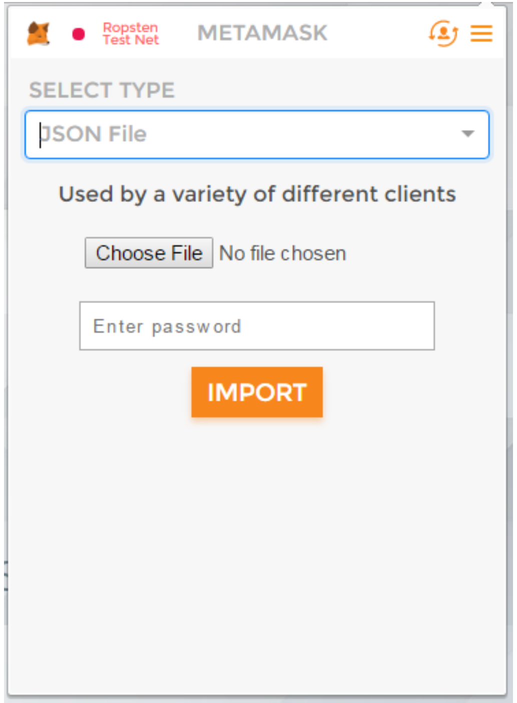
Node hosted @ MetaMask



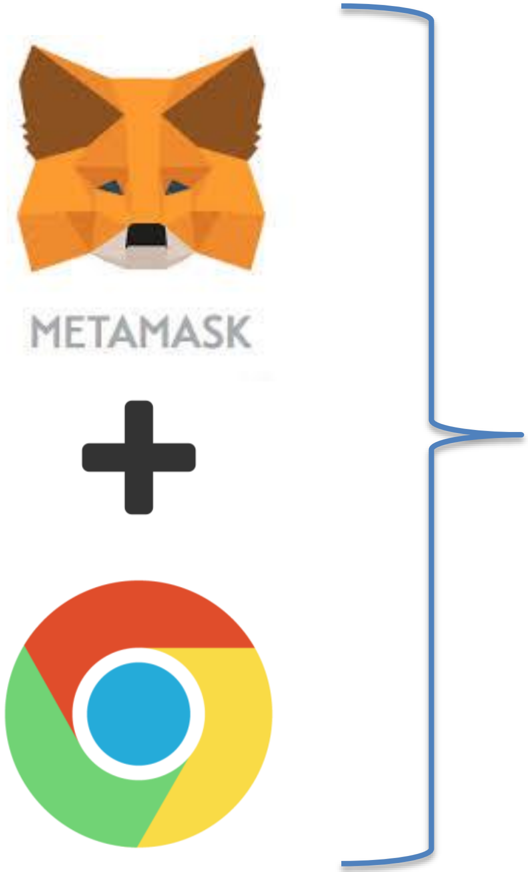
Accoun
0x317baC..
112.398 ETH
8999.84 USD

May 02 2017 06:33
0x884Eb587...3dce
<0.001 ETH

May 02 2017 06:32
0x884Eb587...3dce (Rejected)
1.0 ETH



SELECT TYPE
JSON File
Used by a variety of different clients
No file chosen
Enter password



- Manage accounts in a browser vault
  - Export/Import accounts
  - Send Funds
- Exposes web3 object to browser app
  - Single Page Applications
- Supports multiple endpoints
- Does not support contract deployment
- Does not support mining

Decentralized Apps

- Remix – Broswer solidity

Discount Coupon Link to UDEMY course:

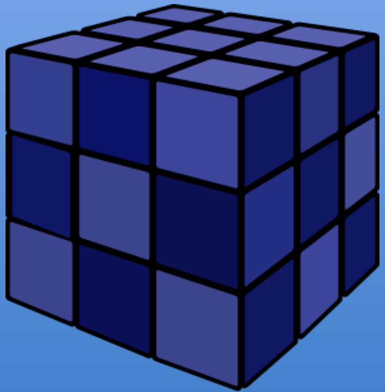
https://www.udemy.com/ethereum-dapp/?couponCode=ETHDAPP101

This deck is part of a online course on “Ethereum: Design and Development of Decentralized Apps.

raj@acloudfan.com

@acloudfan

http://ACloudFan.com



Remix

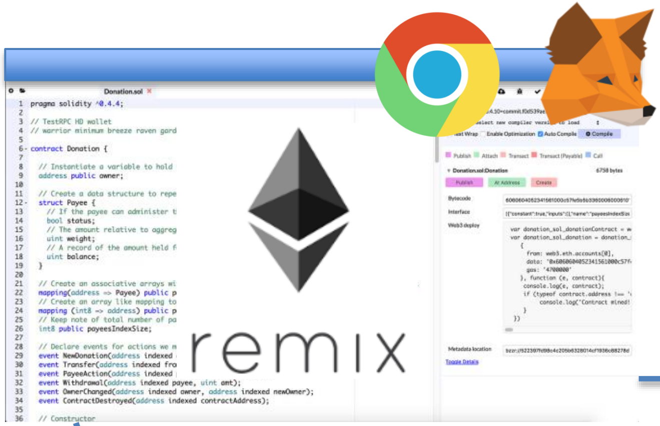
https://ethereum.github.io/browser-solidity

- Code smart contracts in a browser
- Test the contracts in simulator
- Deploy the contracts to live network

- Does not have account management

Browser Solidity

https://ethereum.github.io/browser-solidity



```
pragma solidity ^0.4.4;

// TestRPC HD wallet
// warrior minimum breeze raven gard

contract Donation {

  // Instantiate a variable to hold
  address public owner;

  // Create a data structure to repe
  struct Payee {
    // If the payee can administer t
    bool status;
    // The amount relative to aggreg
    uint weight;
    // A record of the amount held f
    uint balance;
  }

  // Create an associative arrays wi
  mapping(address => Payee) public p
  // Create an array like mapping to
  mapping (int8 => address) public p
  // Keep note of total number of pa
  int8 public payeesIndexSize;

  // Declare events for actions we m
  event NewDonation(address indexed
  event Transfer(address indexed fro
  event PayeeAction(address indexed
  event Withdrawal(address indexed payee, uint amt);
  event OwnerChanged(address indexed owner, address indexed newOwner);
  event ContractDestroyed(address indexed contractAddress);

  // Constructor
```

.4.10+commit.f0d539ae

elect new compiler versi to load

ext Wrap □ Enable Optimization ☑ Auto Compile

Donation.sol:Donation 6758 bytes

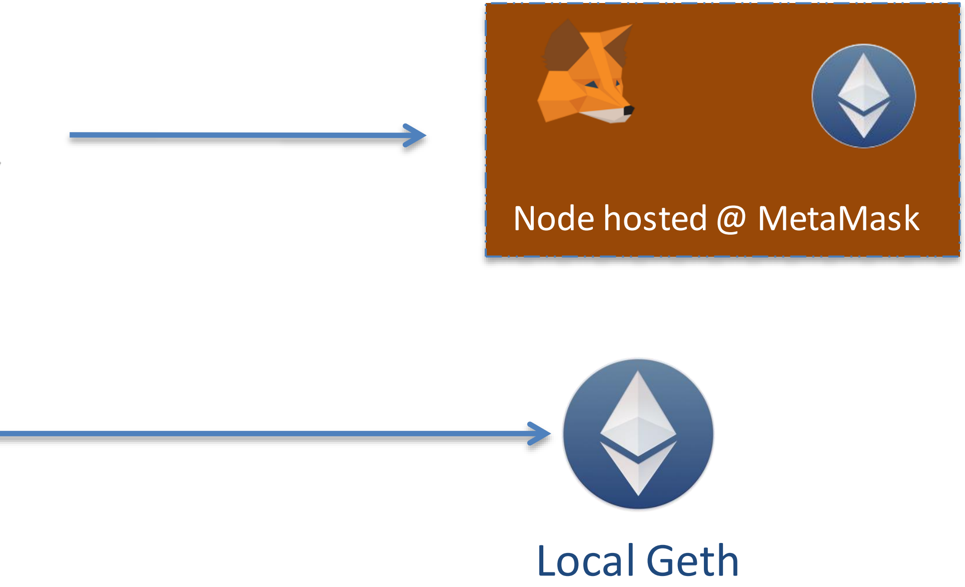
Bytecode 6060604052341561000c57fe5b5b3360008060810

Interface [{"constant":true,"inputs":[],"name":"payeesIndexSiz

Web3 deploy

```
var donation_sol_donationContract = w
var donation_sol_donation = donation_
   {
     from: web3.eth.accounts[0],
     data: '0x6060604052341561000c57f
     gas: '4700000'
   }, function (e, contract){
    console.log(e, contract);
    if (typeof contract.address !== '
         console.log('Contract mined!
    }
 })
```

Metadata location bzzr://5223097fd98e4c206b6328014cf1936c88278d



Javascript VM

Memory

Decentralized Apps

- Online Wallet

Discount Coupon Link to UDEMY course:

https://www.udemy.com/ethereum-dapp/?couponCode=ETHDAPP101

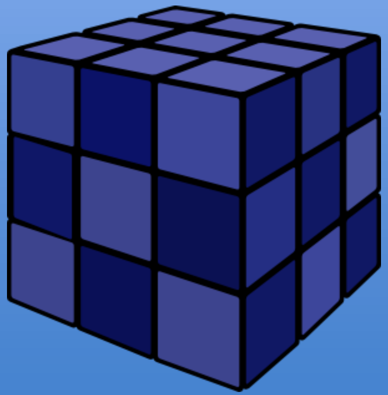
This deck is part of a online course on

“Ethereum: Design and Development of Decentralized Apps.

raj@acloudfan.com

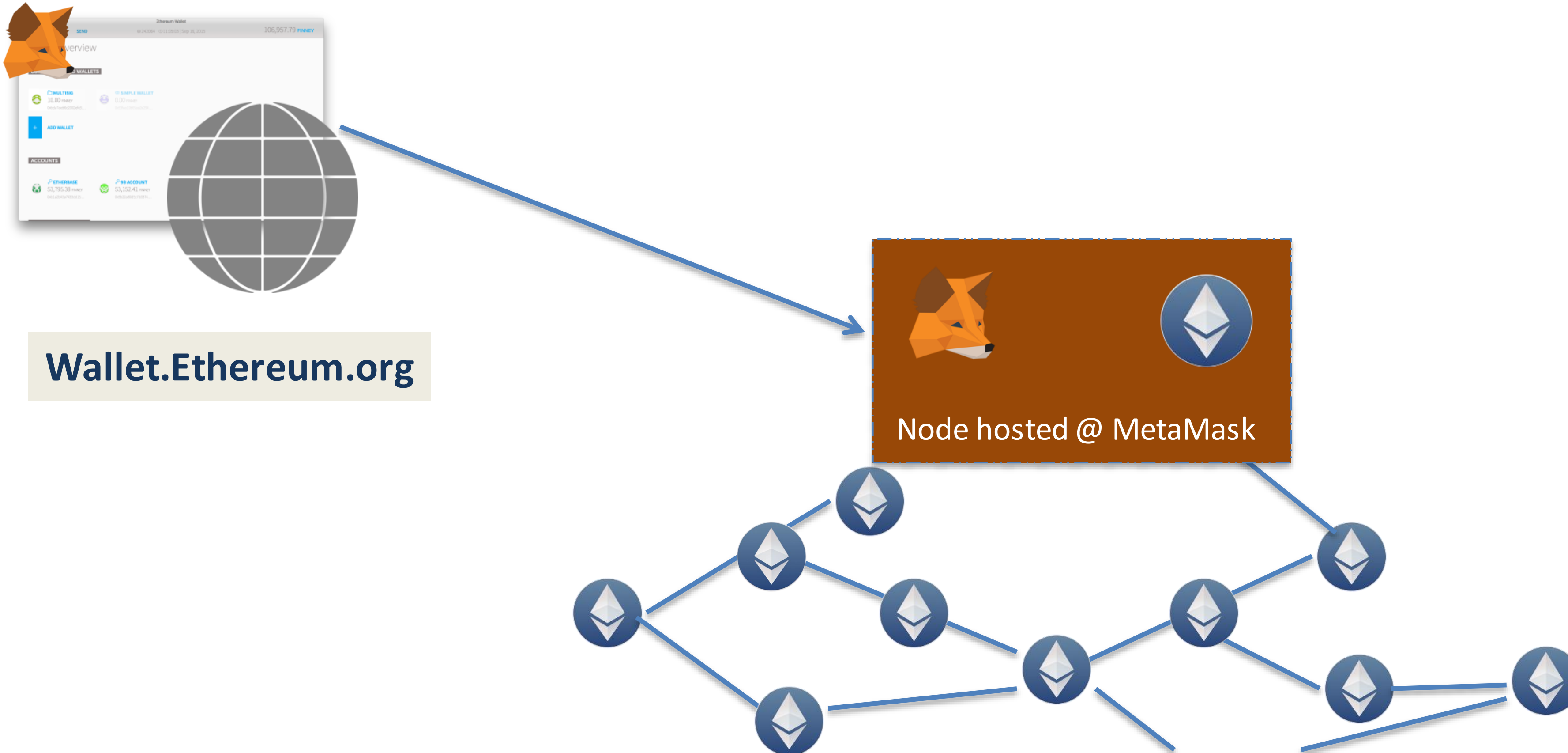
@acloudfan

http://ACloudFan.com



Online Wallet

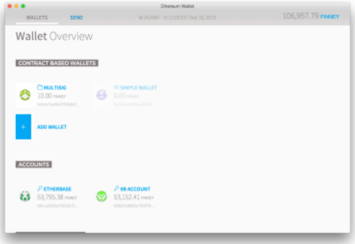
- Available at http://wallet.ethereum.org
    - Accounts managed in *MetaMask*



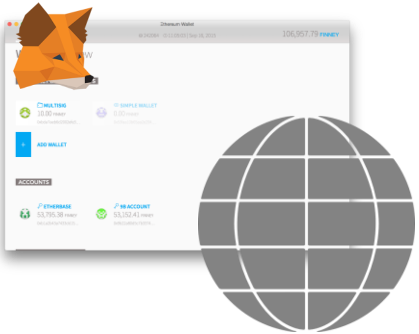
Wallet.Ethereum.org

Node hosted @ MetaMask

Local versus Online Wallet



- Use local node (e.g., geth)
- Unavailable till fully synched
- Keystore managed by app
- Number of n/w limited



No mining option

- Use external hosted node
- Available right away
- Keystore managed by *MetaMask*
- Supports many n/w including private