Ethereum concepts:

- Core Concepts

Discount Coupon Links to UDEMY courses:

https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

https://www.udemy.com/rest-api/?couponCode=DKRST1099

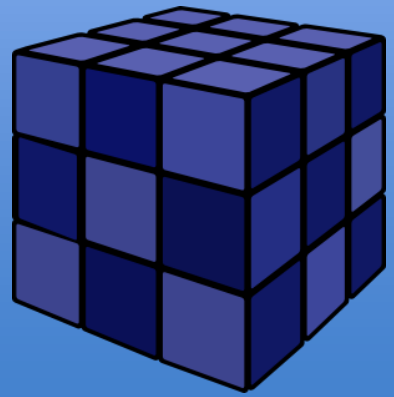
mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com

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

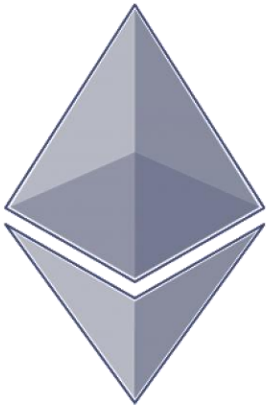
raj@acloudfan.com

@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

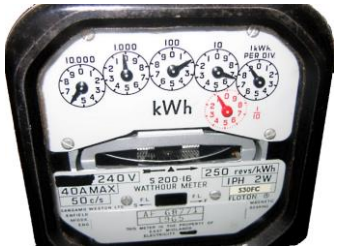
EVM

- 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

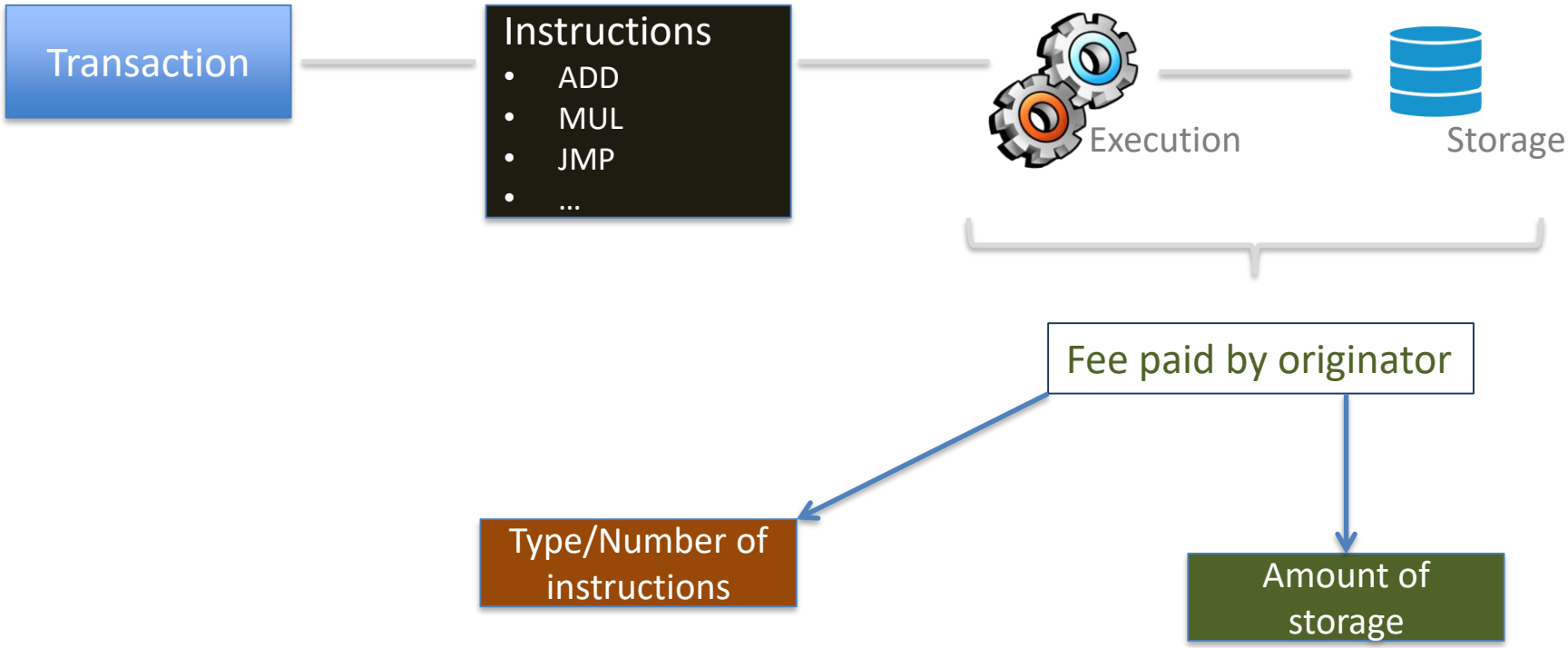


Measures: kWH used

Measures: Gallons of water used

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

Gas Calculations



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

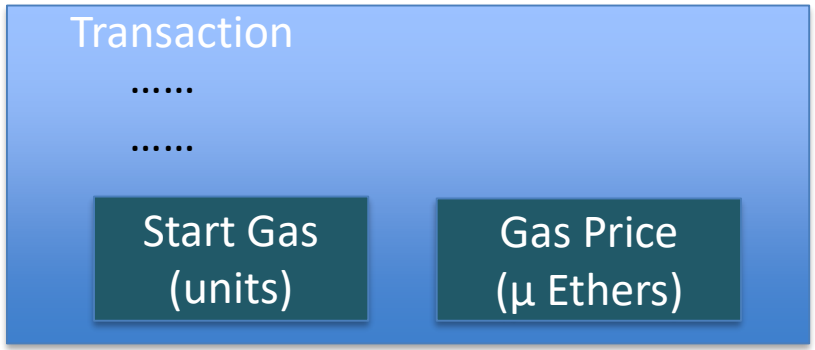
gasUsed = Instructions executed (summed up gas)

gasPrice = User specified in the transaction

Miners decides the minimal acceptable price

Transaction Fee = gasUsed * gasPrice

Transaction Fee : Parameters



- 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

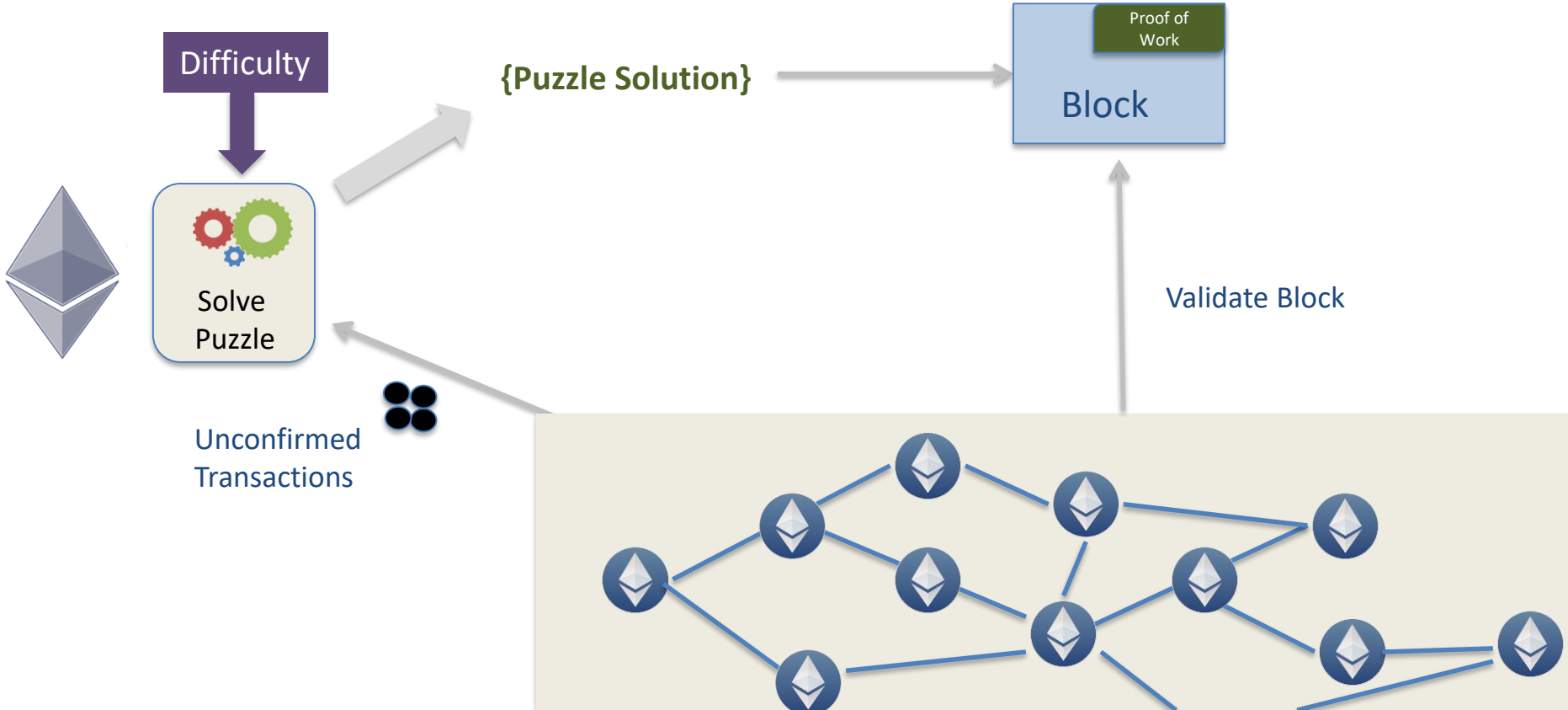
- Process by which blocks get created
  - Validate transactions
  - Secures the network

Proof of Work Proof of Stake

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

Proof of Work

- Computationally (CPU | Memory | Bandwidth) intensive



Ethereum: Proof of Work

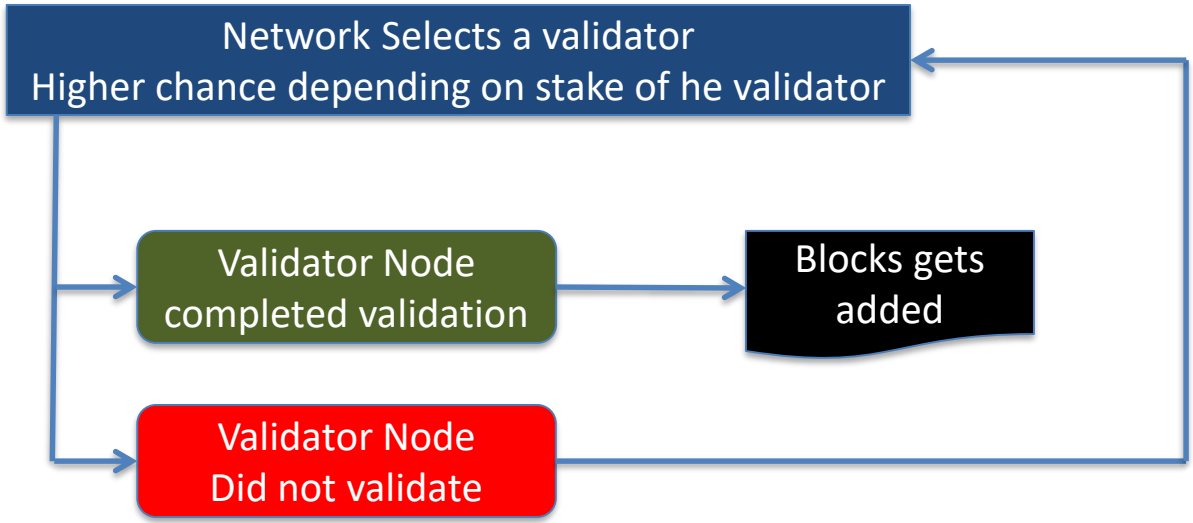
- Protocol: GHOST
- Algorithm: ETHash
- Difficulty: Network adjusted; block created ~14 seconds
- Incentive: 3 Ether

  Gas fee for transactions

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*

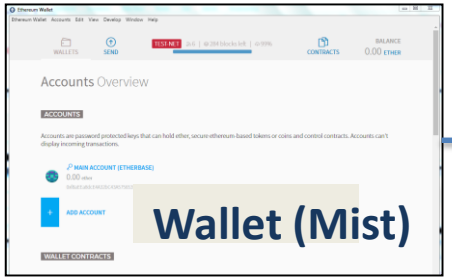
Private Network

- Network ID = Assigned

Private Network

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

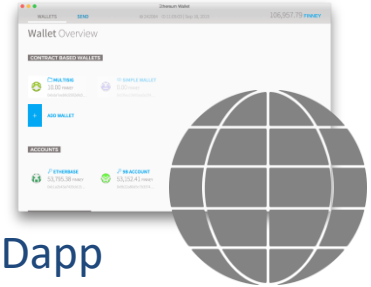
Interaction



Live Network

Test-Net

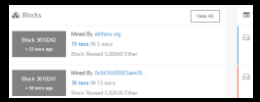
Private Network



Dapp

Developer

Block Explorer



Ethereum concepts:

- Proof of Authority consensus
- Clique

Discount Coupon Links to UDEMY courses:

https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

https://www.udemy.com/rest-api/?couponCode=DKRST1099

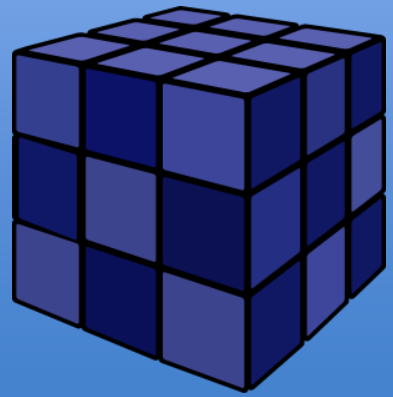
mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com

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

raj@acloudfan.com

@acloudfan

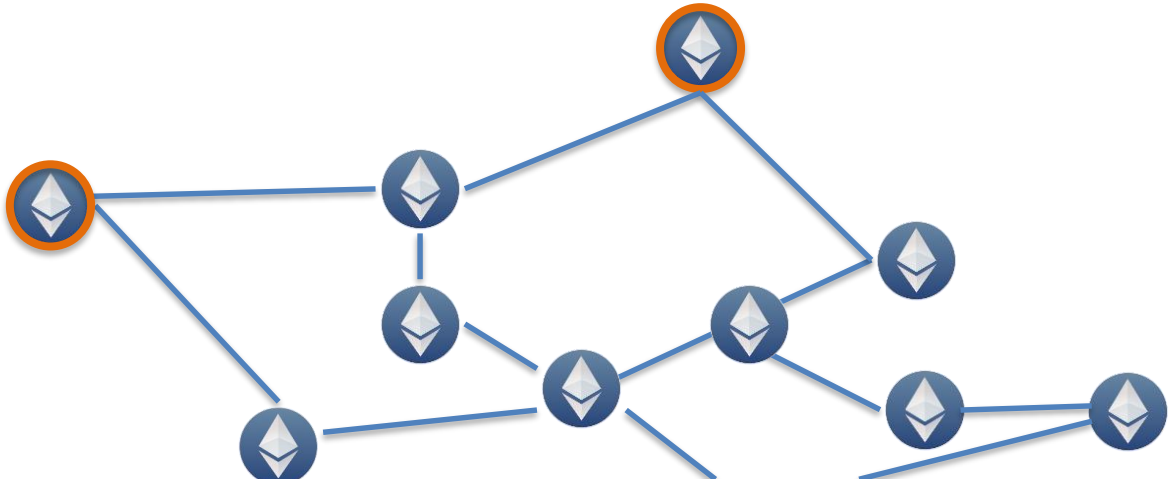
http://ACloudFan.com



Proof of Authority

Consensus Model

- No concept of mining or miners
- *Pre-approved Authority nodes* validate the transaction
  - Blocks are said to be “Sealed by the nodes”



Ethereum: Proof of Authority

- Ethereum network can be configured to use PoA

- Protocol: CLIQUE

Refer to lectures on Private Network to see
- *How to setup a Clique private network*
- *How Puppeth and Bootnode tools are used*

Proof of Authority

Where is it used?

Network ID = 4 Rinkeby

Private Network

- More Secure: Nodes with validation authority are trusted
- Configurability of Block times
- Computationally less intensive

Ethereum concepts:

- Wallet
- Explorer
- Account types

Discount Coupon Links to UDEMY courses:

https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

https://www.udemy.com/rest-api/?couponCode=DKRST1099

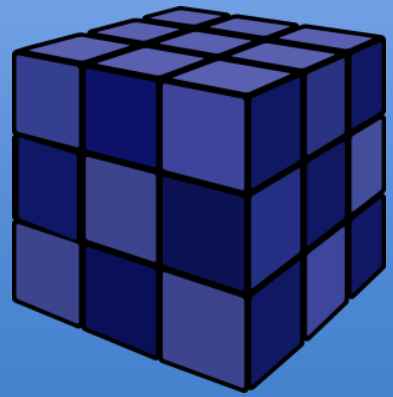
mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com

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

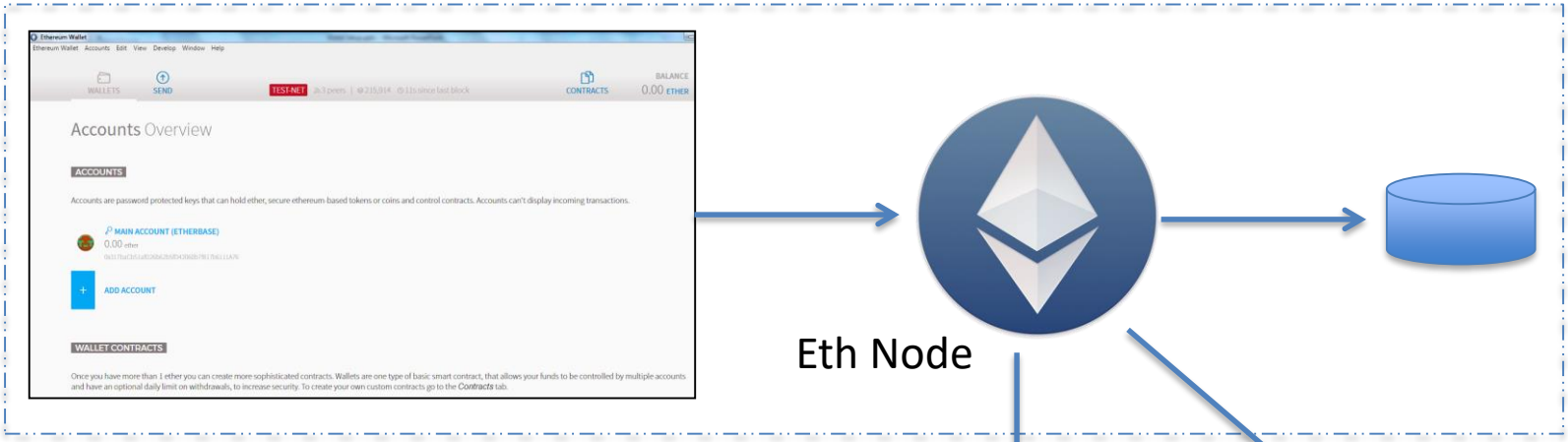
raj@acloudfan.com

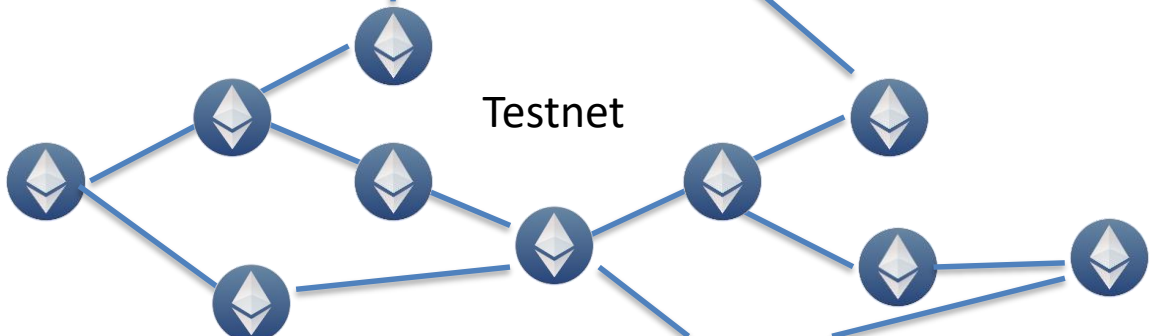
@acloudfan

http://ACloudFan.com



Wallet Architecture





Blockchain explorer

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

Etherscan
The Ethereum Block Explorer

https://etherscan.io/

https://testnet.etherscan.io/

ether.camp

https://live.ether.camp/

Etherchain.org

https://etherchain.org/

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

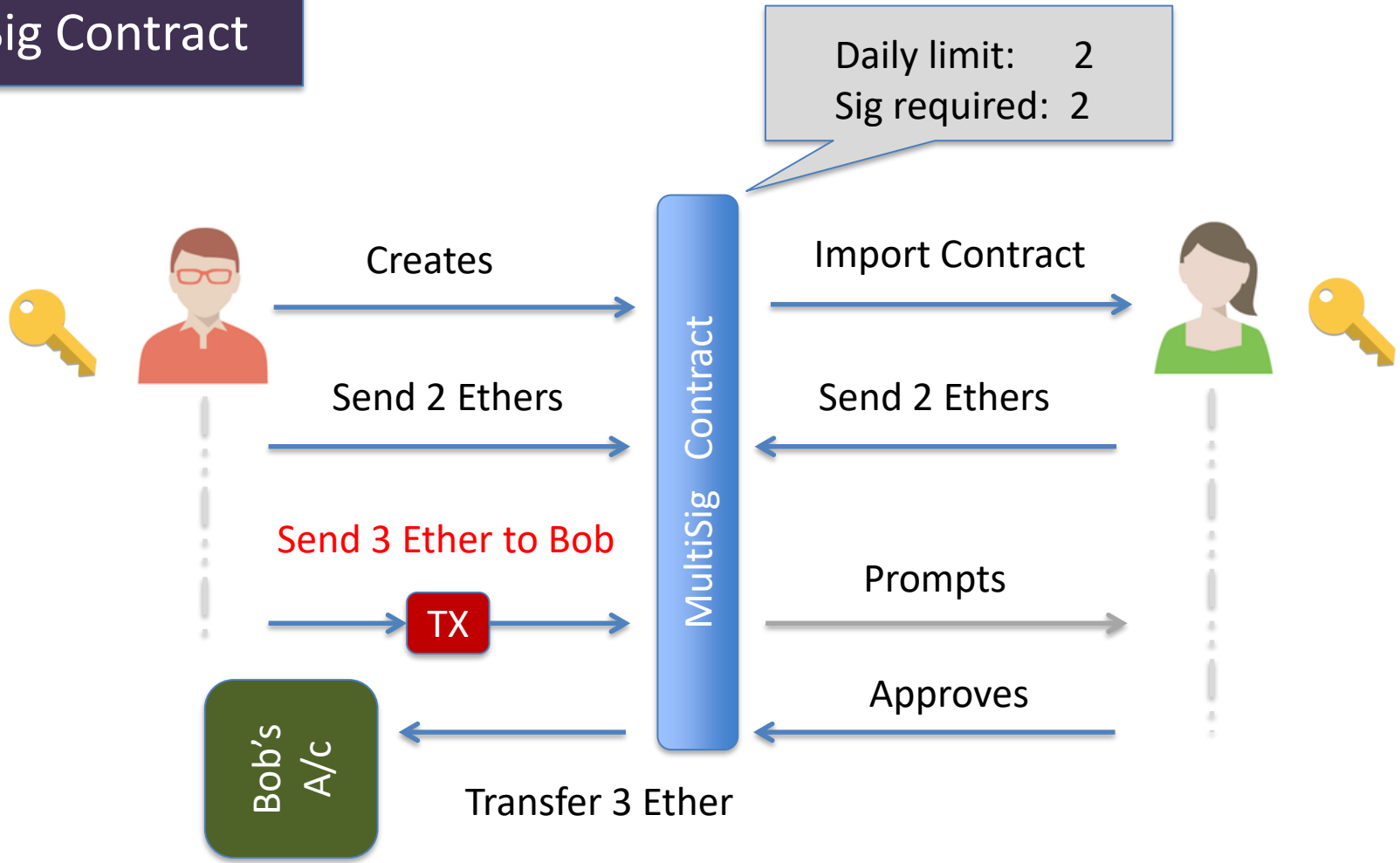
    N = Number of owners

    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 Links to UDEMY courses:

https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

https://www.udemy.com/rest-api/?couponCode=DKRST1099

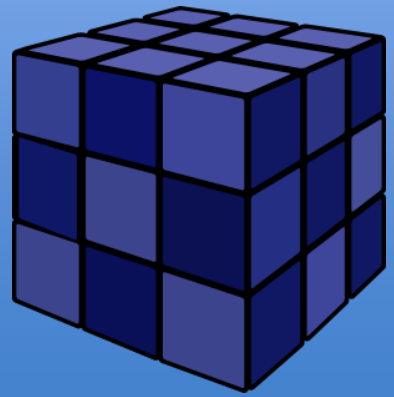
mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com

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

raj@acloudfan.com

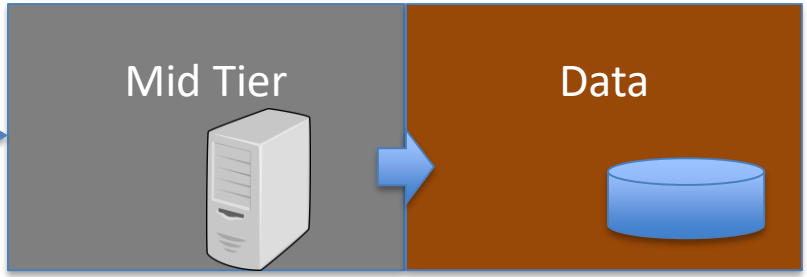
@acloudfan

http://ACloudFan.com

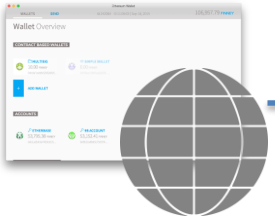


Web App ➡ DAPP

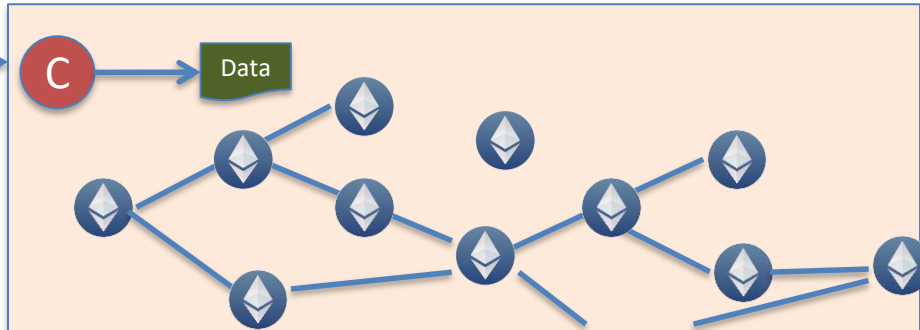
Centralized Resources
Owned by the organization



Front end apps

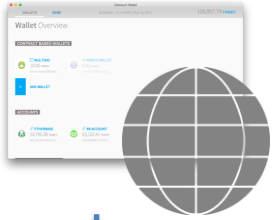


Decentralized Resources
Public domain



Working of Dapp

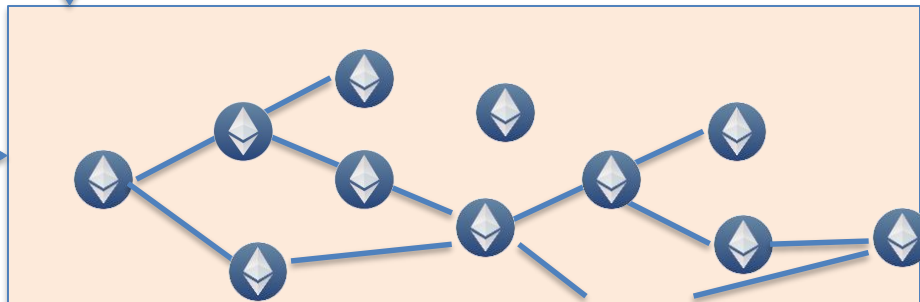
Invoke Contract



- App user pays *gas/fee*

- Manage funds
- Invoke Contracts

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



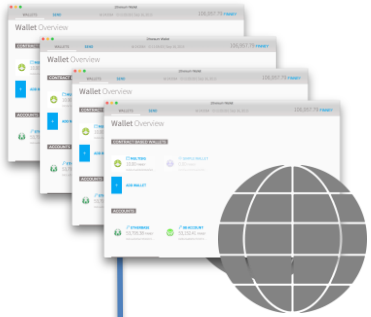
Example DAPP Bidding

Ship Goods

Seller Application

Event: BidReceived

Buyer Application



withdrawFunds()

Bid()

Contract

DAPP Technology Stack

web3

Java

python

Microsoft .NET

C++

OLIDITY

Serpent

Lisp Like Language

Decentralized Apps

- MetaMask

Discount Coupon Links to UDEMY courses:

https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

https://www.udemy.com/rest-api/?couponCode=DKRST1099

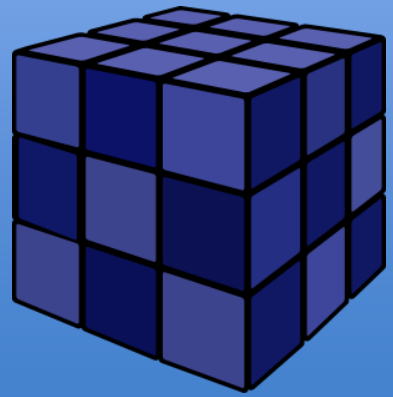
mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com

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

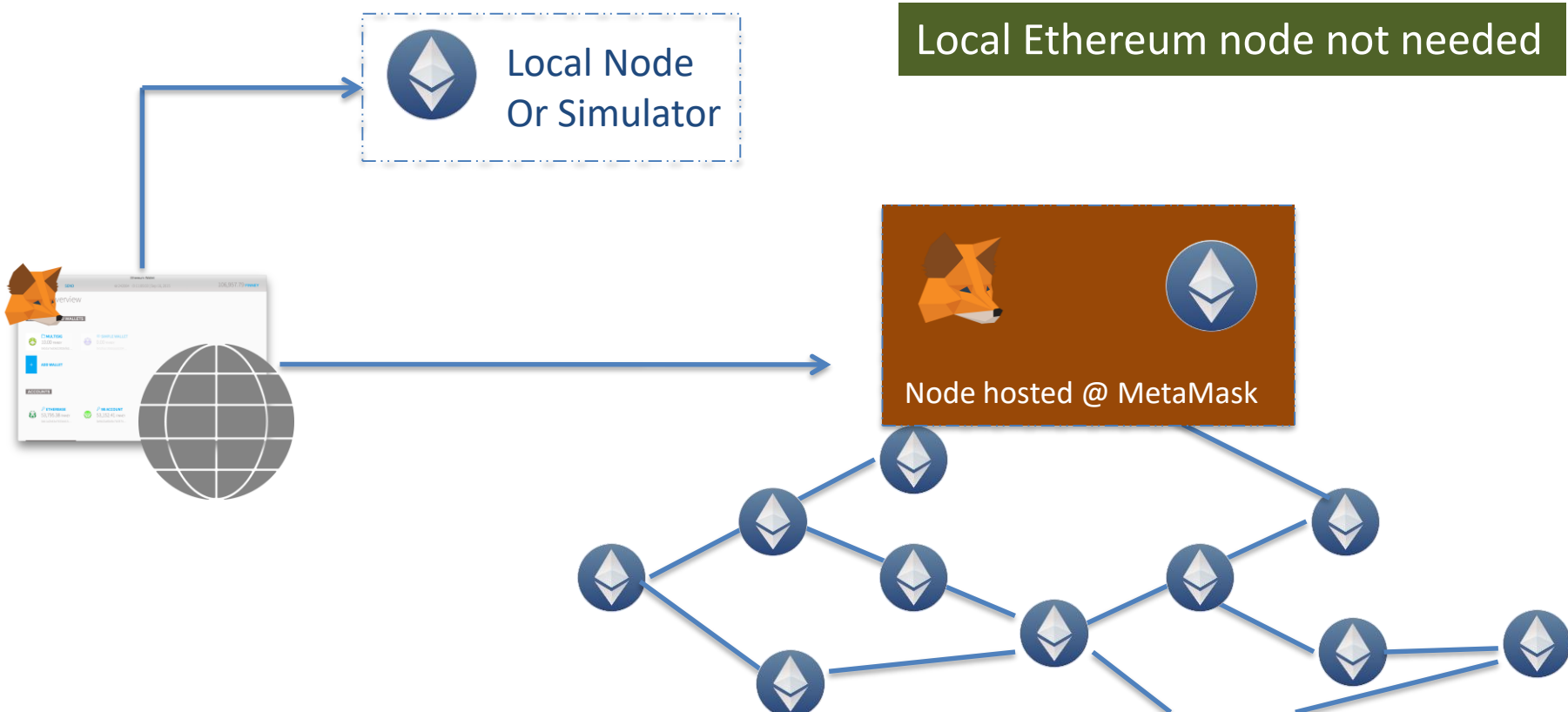
METAMASK

Brings Ethereum to your browser

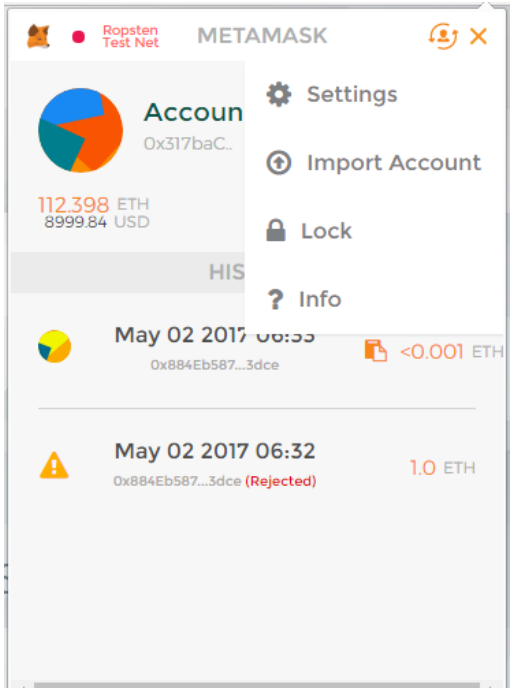
GET CHROME PLUGIN

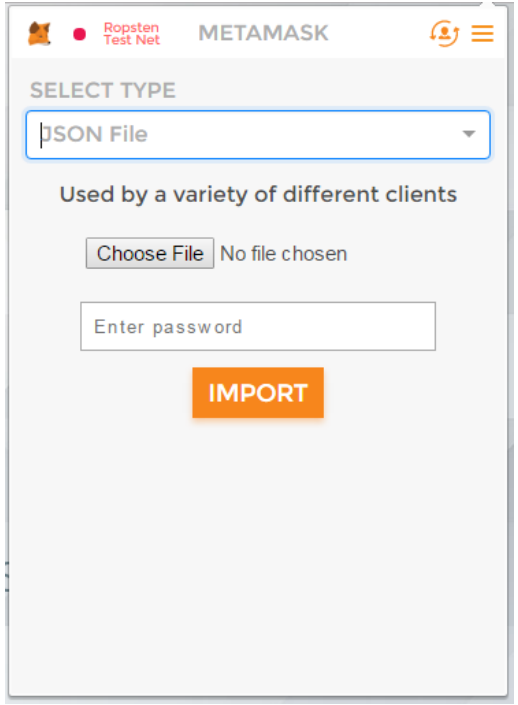
Meta Mask

Chrome plugin turns browser into DAPP container



METAMASK


Ropsten Test Net
METAMASK
Settings
Import Account
Lock
Info
112.398 ETH
8999.84 USD
May 02 2017 06:32
0x884Eb587...3dce
<0.001 ETH
May 02 2017 06:32
0x884Eb587...3dce (Rejected)
1.0 ETH


Ropsten Test Net
METAMASK
SELECT TYPE
JSON File
Used by a variety of different clients
Choose File
No file chosen
Enter password
IMPORT

- 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 Links to UDEMY courses:

https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

https://www.udemy.com/rest-api/?couponCode=DKRST1099

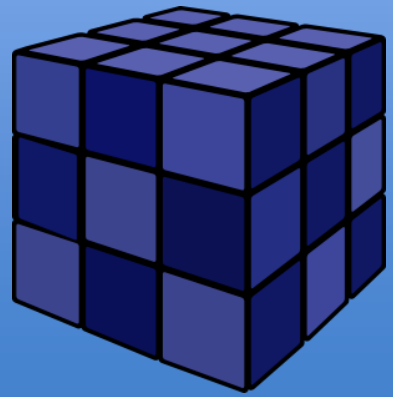
mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com

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

raj@acloudfan.com

@acloudfan

http://ACloudFan.com



Remix

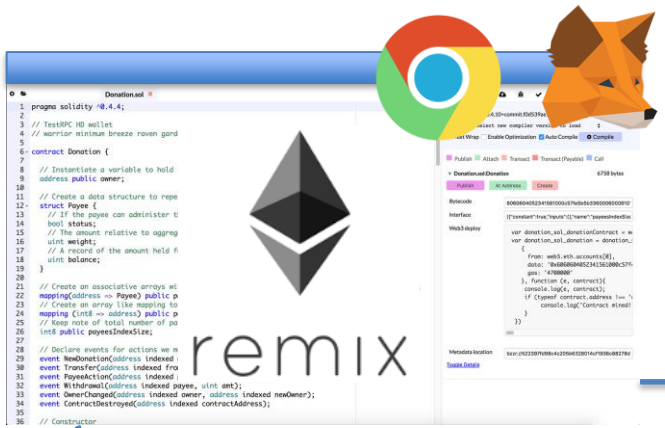
https://ethereum.github.io/browser-solidity

- 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



Node hosted @ MetaMask

Local Geth

Javascript VM

Memory

Decentralized Apps

- Online Wallet

Discount Coupon Links to UDEMY courses:

https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

https://www.udemy.com/rest-api/?couponCode=DKRST1099

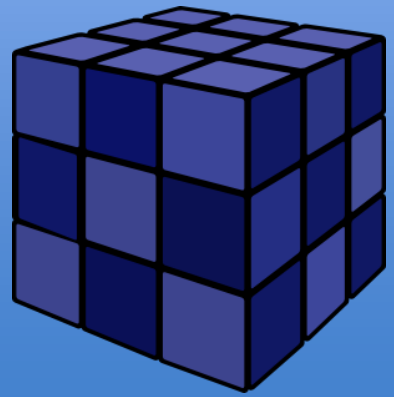
mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com

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

raj@acloudfan.com

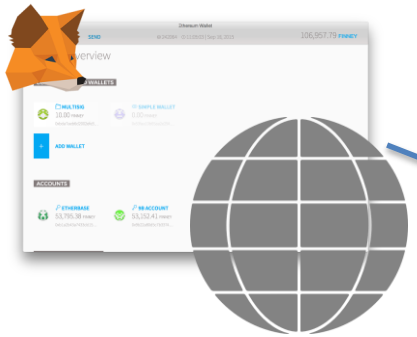
@acloudfan

http://ACloudFan.com

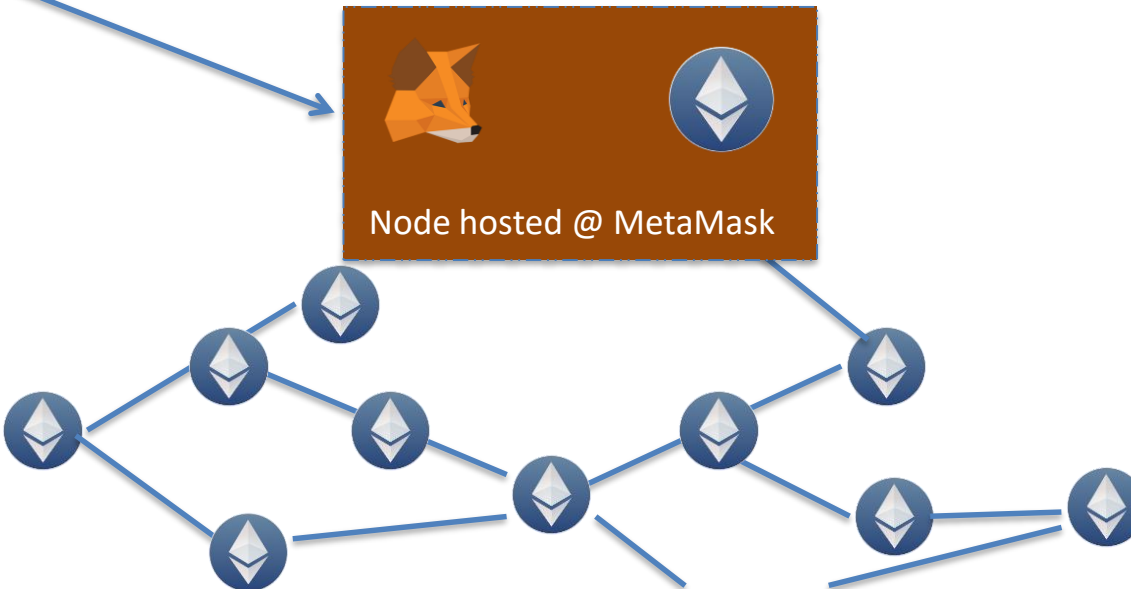


Online Wallet

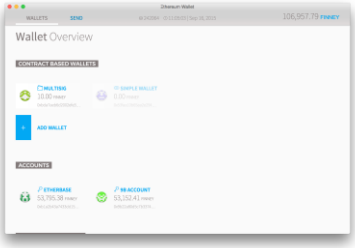
- Available at http://wallet.ethereum.org
  - Accounts managed in *MetaMask*

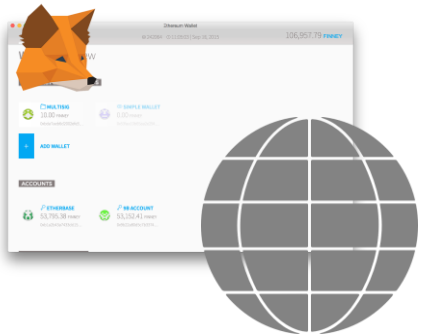


Wallet.Ethereum.org



Local versus Online Wallet





No mining option

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

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