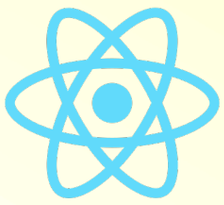
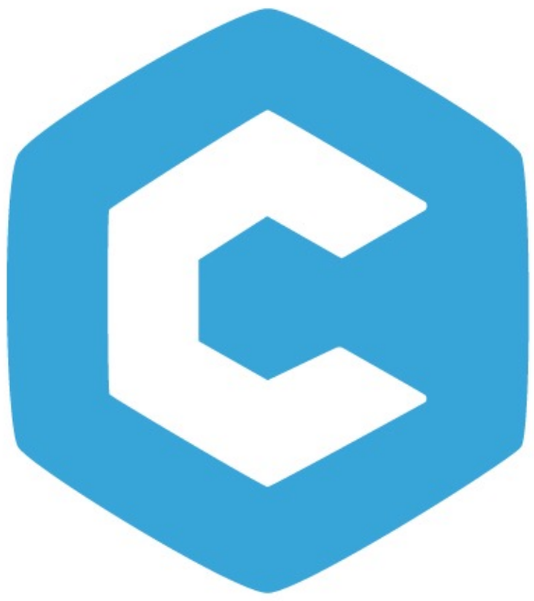


ETHEREUM & REACT

An introduction to building your first web dApp

RYAN HAGERTY

Front-End Developer



CHROMATIC

chromatichq.com

@HOTPIZZAS

GOAL

MHK

(minimal hacking knowledge)

1

IDEA

1

IDEA

2

TOOLS

1

IDEA

2

TOOLS

3

PROJECT

WHAT WE'LL LEARN

Blockchain

Ethereum & Smart Contracts

Tools & Frameworks You Need

Basics of Solidity

Sample Hello World Project

React Components with Ethereum/web3

Testing

BLOCKCHAIN

(crash course)

(HOLD ON TO YOUR BUTTS)

WHAT WE WON'T COVER

WHAT WE WON'T COVER

~~Cryptography~~

WHAT WE WON'T COVER

~~Cryptography~~

~~Proof of Work vs. Proof of Stake~~

WHAT WE WON'T COVER

~~Cryptography~~

~~Proof of Work vs. Proof of Stake~~

~~Byzantine Generals' Problem~~

WHAT WE WON'T COVER

~~Cryptography~~

~~Proof of Work vs. Proof of Stake~~

~~Byzantine Generals' Problem~~

~~Etc.~~

1

THE IDEA

THE INTERNET

(as it is)

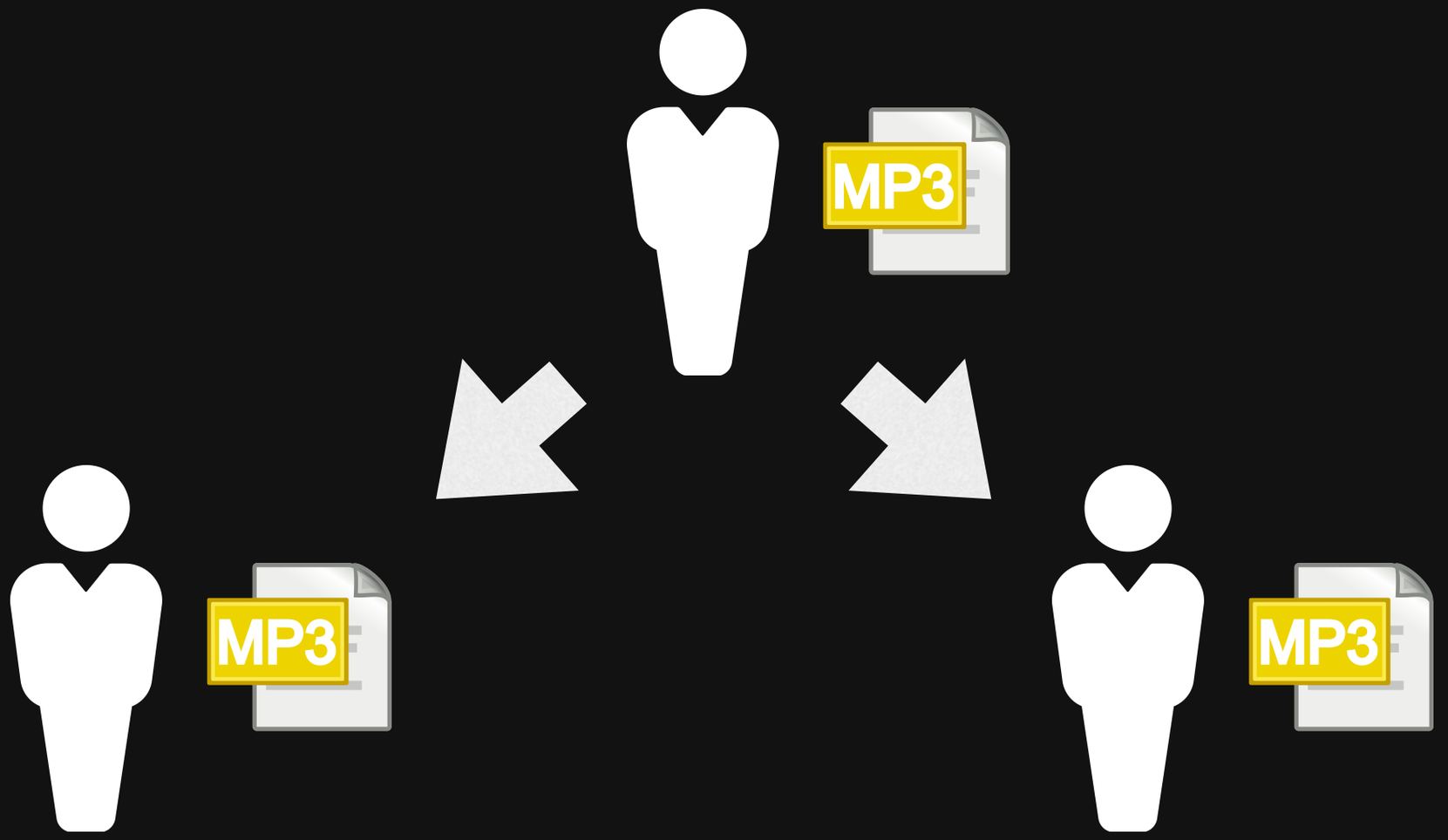
or

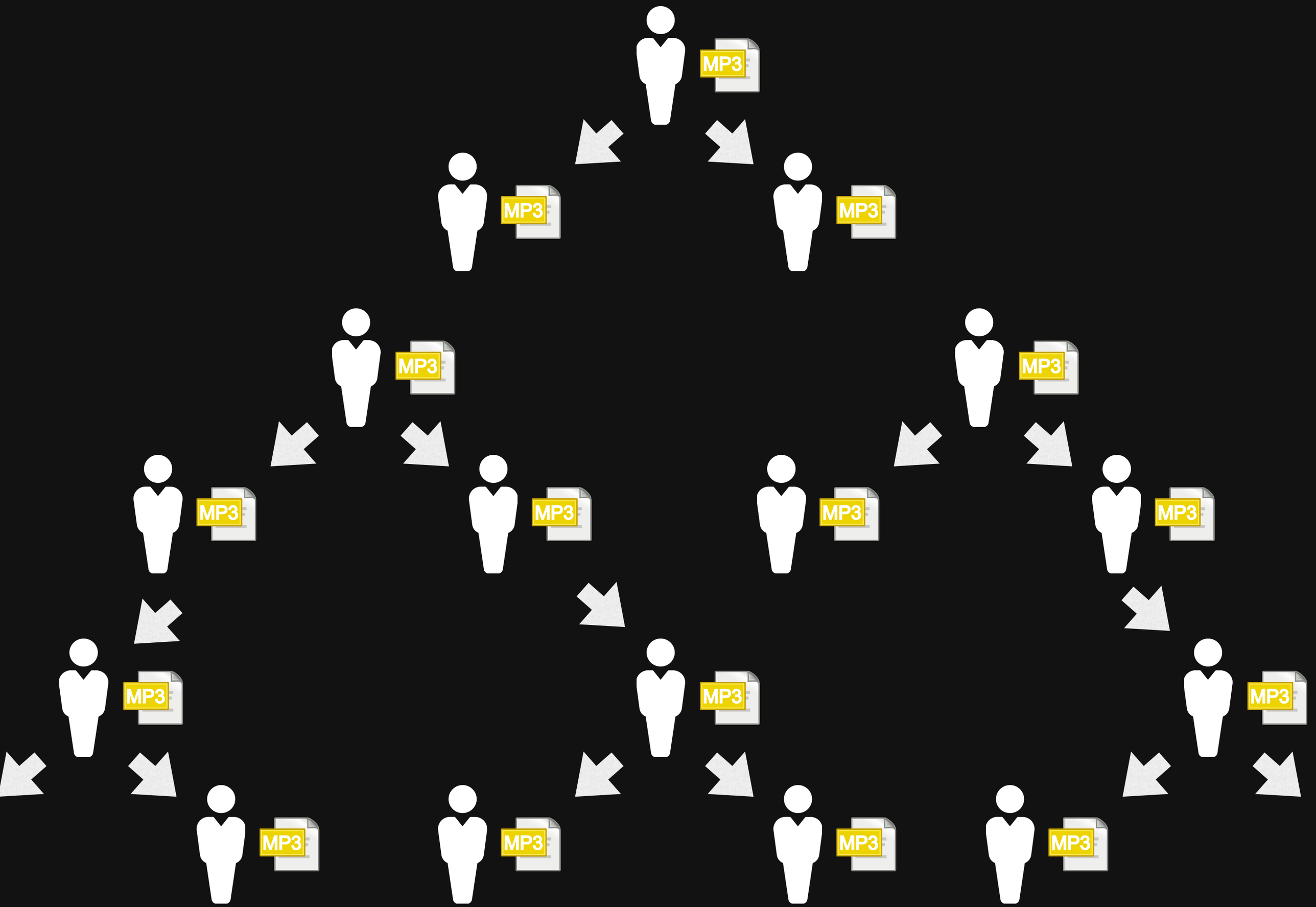
THE INTERNET OF INFORMATION

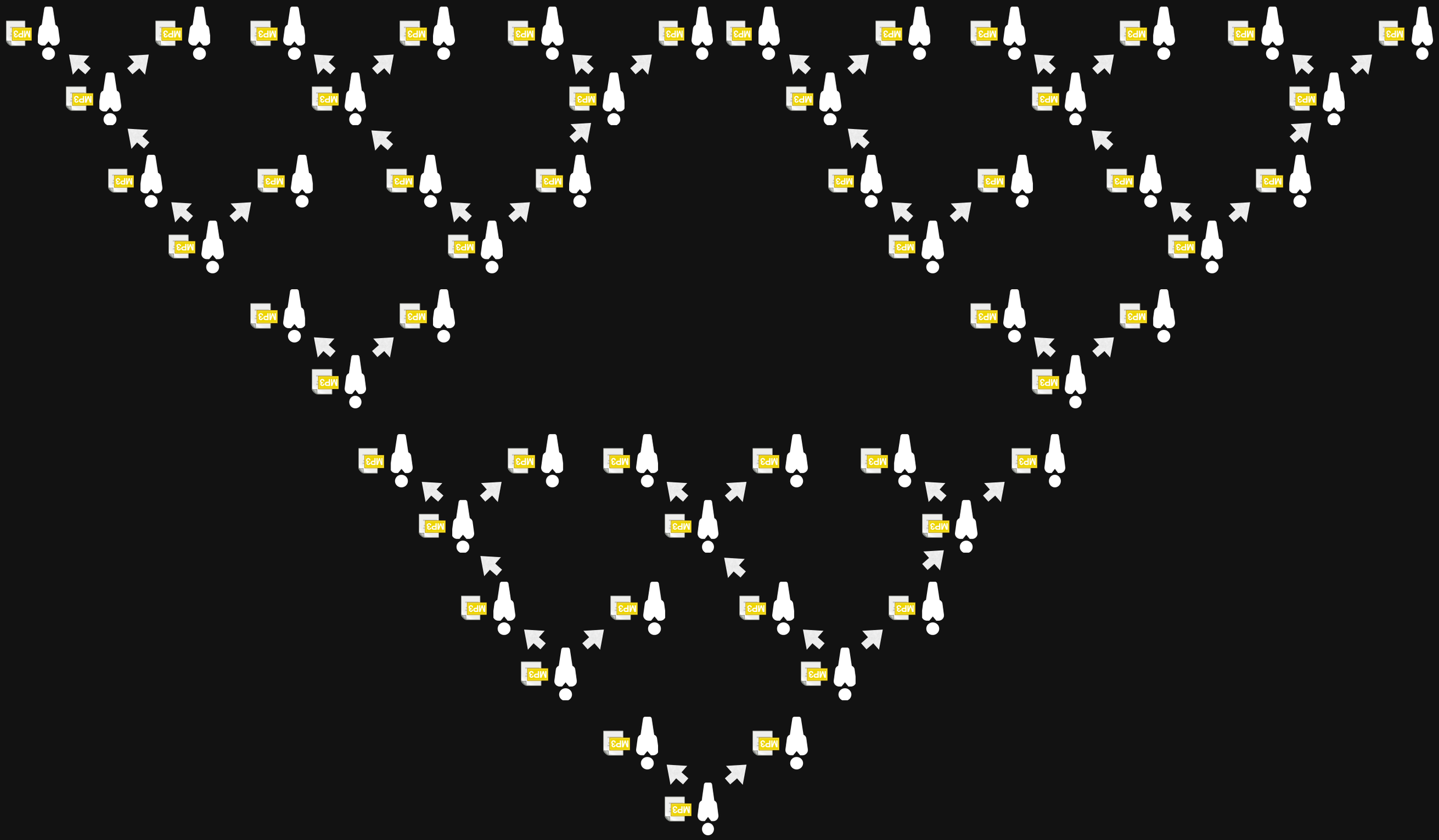
TRANSMIT INFORMATION

TRANSMIT INFORMATION

TRANSMIT INFORMATION




MP3


MP3

THE INTERNET

(as it could be)

or

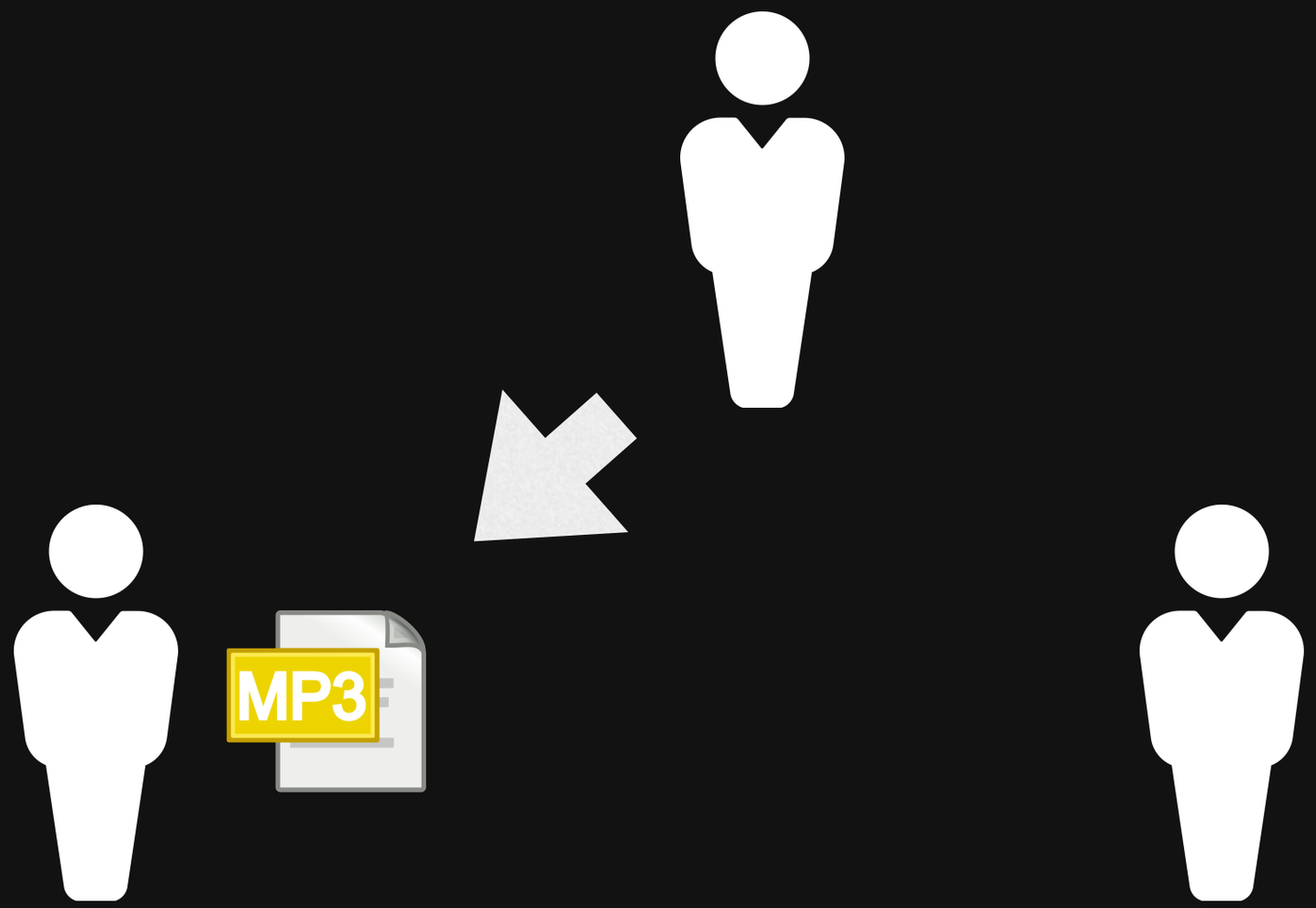
THE INTERNET OF VALUE

BLOCKCHAIN

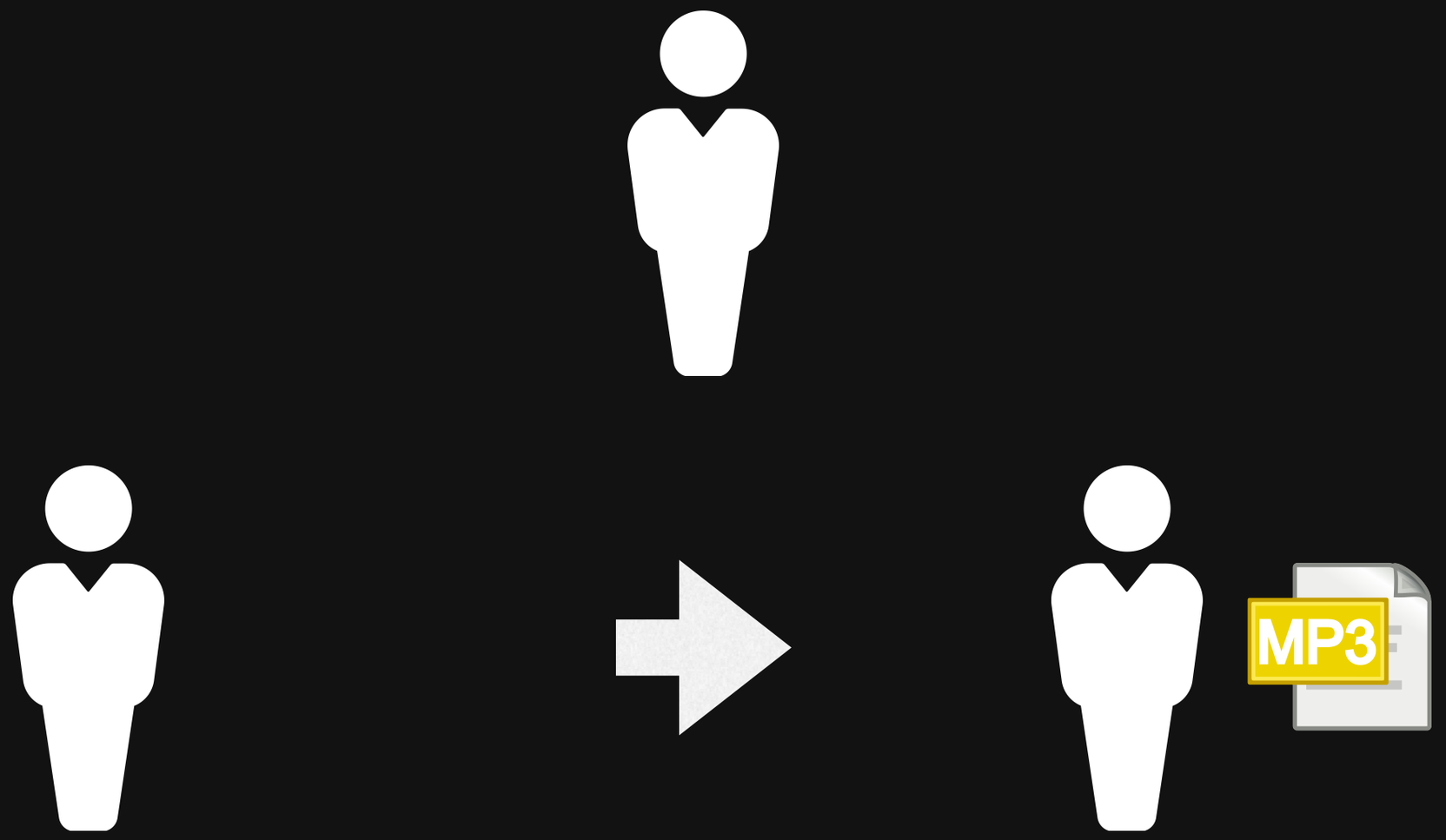
(how to transmit value)

TRANSMIT VALUE

TRANSMIT VALUE



TRANSMIT VALUE

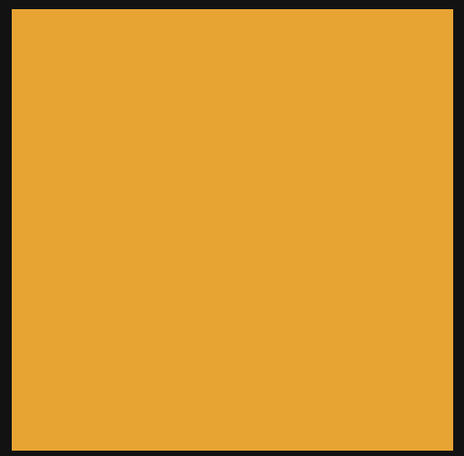


MONEY

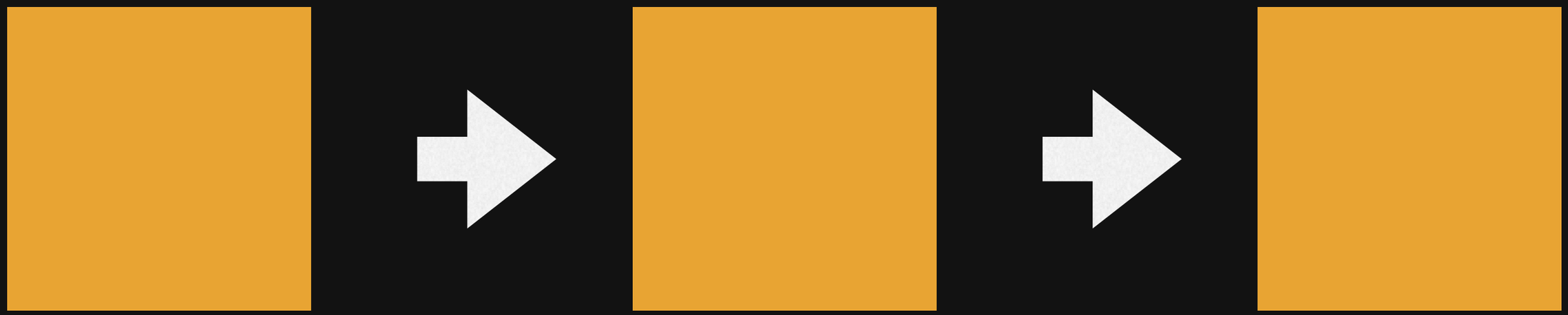

BUT HOW?

THE LEDGER

BLOCKCHAIN



BLOCKCHAIN



each block represents a piece of history

AWESOME BENEFITS


DECENTRALIZED


IMMUTABLE


PERMISSIONLESS

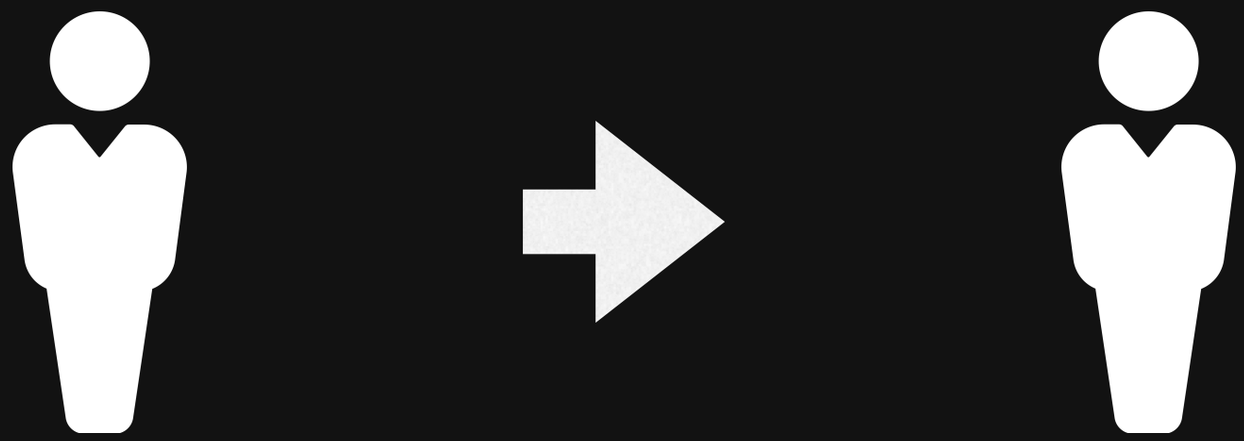
BASIC OPERATION

1 BTC

0

BASIC OPERATION

BASIC OPERATION

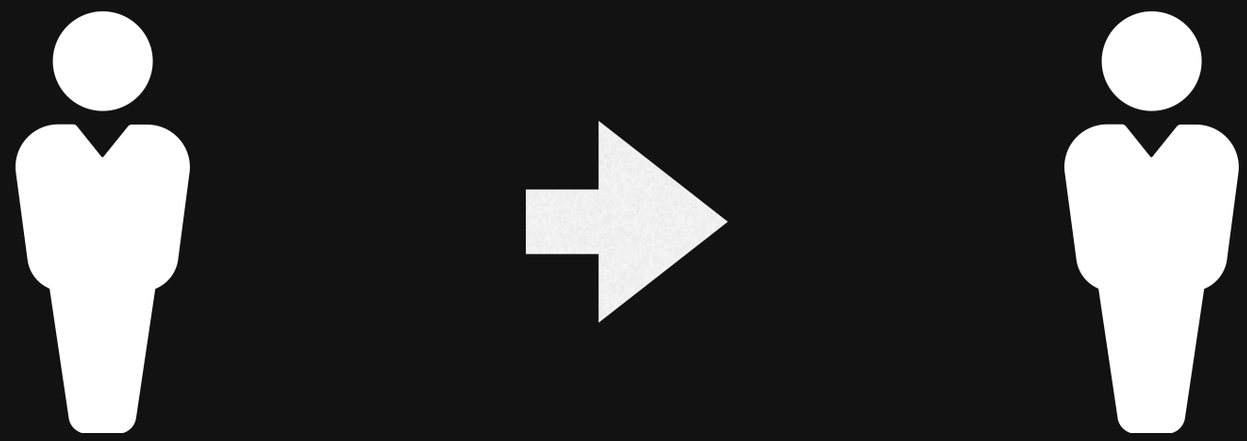


1 - 0.25

0.75 BTC

0

BASIC OPERATION



1 - 0.25

0.75 BTC

0 + 0.25

0.25 BTC

STILL BASIC LEDGER

BEYOND MONEY

&

RECORD *ALL* VALUE

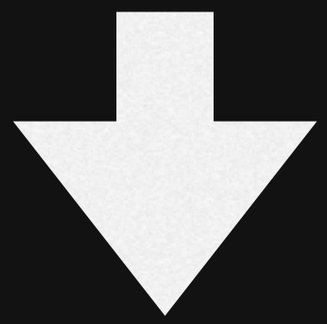
ETHEREUM

LEDGER

PROGRAMMING LANGUAGE

LEDGER

DISTRIBUTED LEDGER



DISTRIBUTED COMPUTER

ETHEREUM VIRTUAL MACHINE

TRANSMIT VALUE OF

TRANSMIT VALUE OF

TRANSMIT VALUE OF

Real Estate

TRANSMIT VALUE OF

Real Estate

Insurance

TRANSMIT VALUE OF

Copyrighted Material

Real Estate

Insurance

Legal Contracts

TRANSMIT VALUE OF

Copyrighted Material

Real Estate

Insurance

Legal Contracts

Supply Chains

TRANSMIT VALUE OF

Copyrighted Material

Real Estate

Insurance

Legal Contracts

Supply Chains

Identity

TRANSMIT VALUE OF

Copyrighted Material

Real Estate

Insurance

Legal Contracts

Supply Chains

Identity

AND MORE! 👍

ETHEREUM SMART CONTRACTS AND YOU

ETHEREUM

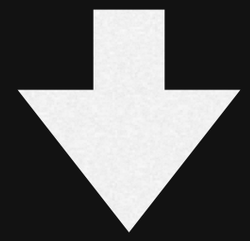
VS.

ETHER

ETHEREUM

ETHER

ETHEREUM



ETHEREUM VIRTUAL MACHINE

ETHER

ETHEREUM

↓

ETHEREUM VIRTUAL MACHINE

ETHER

↓

CURRENCY*


EVM
(ETHEREUM VIRTUAL MACHINE)

“The EVM, or Ethereum Virtual Machine, is a sandboxed virtual stack machine embedded within each full Ethereum node, responsible for executing contract bytecode.”

— Moe Aboulkheir
September 12, 2017


ETHER

UTILITY CURRENCY

GAS

First Prev Page 1 of 10000 Next Last

k	Age	From		To	Value	[TxFee]
130	15 secs ago	0xc2f9f063ced69d1…		0x5809b2aff185335…	0.0013 Ether	0.000021
130	15 secs ago	0x345fde54632516…		0x11fb6aef2b0e35e…	0.0004 Ether	0.000021
130	15 secs ago	0xcfe6af4dd3f2d68f…		0xd9a72fec8683db…	0 Ether	0.00008431
130	15 secs ago	0xad79b730a5d0e4…		CryptoKittiesSalesA…	0.5 Ether	0.00006285
130	15 secs ago	0xb014d8b572dc7f…		TerraminerToken	0 Ether	0.00007298
130	15 secs a	0x…7c495f…c…		0x3e0…e9ea9d…	0 Ether	0.00007448
130	15 secs ago	0x…		…Fir…	0 Ether	0.00009117
130	15 secs ago	0x0027a9e6afdc419…		0x47a8a30a59eea5…	0 Ether	0.00009035
130	15 secs ago	0xd3aa7ee8691700…		0…b5074e…52dbd…	0.00011 Ether	0.000042
130	15 secs ago	0xf7b449b69fdcb2e…		0…7050a9…21…48	0.000379947442413 Ether	0.000042
130	15 secs ago	0xccbd83e519bd20…		0x4202f381b817e4…	0.0001 Ether	0.000042
130	15 secs ago	0x874aad201cae89…		0x955616617695be…	0.3522 Ether	0.000042
130	15 secs ago	0x4886404ecfb86b…		CryptoKittiesCore	0.008 Ether	0.00015997
130	15 secs ago	0xf07a621a4022b14…		BeautyChainToken	0 Ether	0.00004468
130	15 secs ago	0xc0ce0357615ebe…		0xd6c3dc9e3a2215…	0 Ether	0.00012458
130	15 secs ago	0x554bd839f375de…		0x45555629aabfea1…	0 Ether	0.00007436
130	15 secs ago	0xd64c6d86b93ecc…		IDEX_1	0 Ether	0.00019853

TRANSACTION FEES

FUNCTION

RESULT

Estimates over last 1,500 blocks - Last update: Block 5231168

Change Currency

Std Cost for Transfer	Gas Price Std (Gwei)	SafeLow Cost for Transfer	Gas Price SafeLow (Gwei)	Median Wait (s)	Median Wait (blocks)
$0.046	3	$0.031	2	30	2

Gas-Time-Price Estimator: For transactions sent at block: 5231215

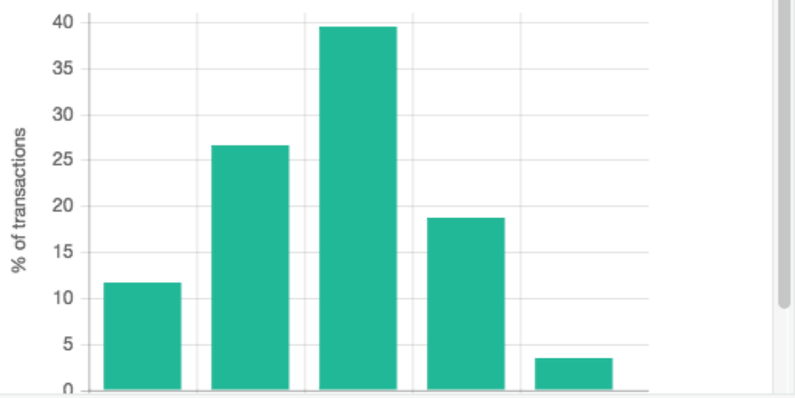
Adjust confirmation time

Avg Time (min)	3.82	Gas Used*	21000
95% Time (min)	9.55	Avg Time (blocks)	15.36
Gas Price (Gwei)*	3	95% Time (blocks)	38.4
Tx Fee (Fiat)	$0.046	Tx Fee (ETH)	0.00006

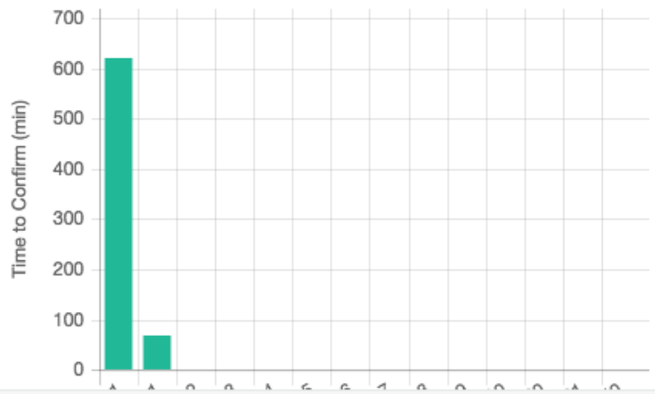
Real Time Gas Use: % Block Limit (last 10)

Last Block: 5231215

Transaction Count by Gas Price



Confirmation Time by Gas Price



Recommended Gas Prices

(based on current network conditions)

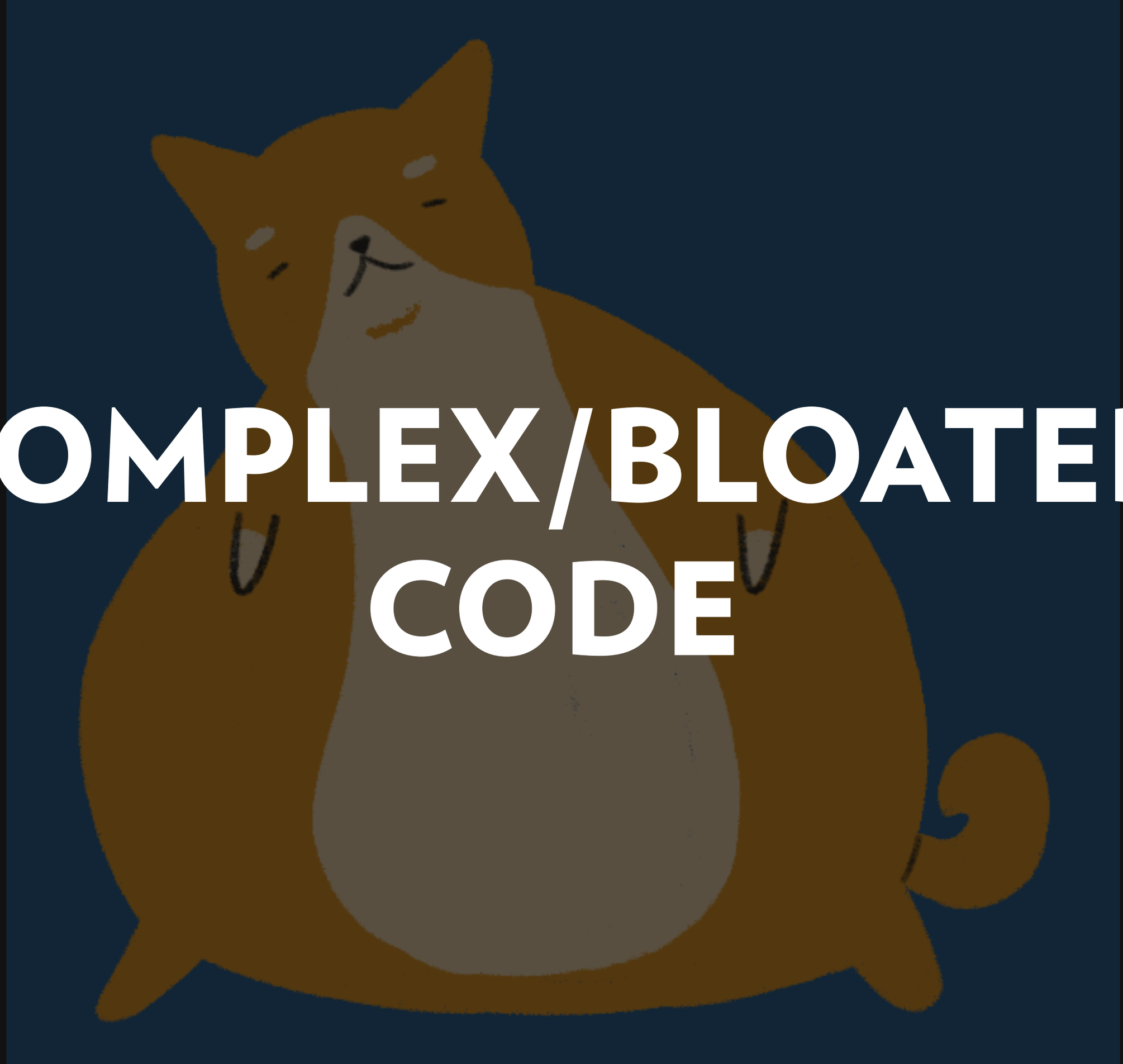
Speed	Gas Price (gwei)
SafeLow (<30m)	2
Standard (<5m)	3
Fast (<2m)	20

Note: Estimates not valid when multiple transactions are batched from the same address or for transactions sent to addresses with many (e.g. > 100) pending

Top 10 Miners by Blocks Mined: Support for user transactions

Misc Stats (Last 1,500 blocks)

https://ethgasstation.info/


COMPLEX/BLOATED
CODE

1MB

OVER 100 STEPS

— https://hackernoon.com/ether-purchase-power-df40a38c5a2f

```
6060604052600436106100 4c576000357c0100000000000000000000000000000000000000000000000000000000900463ffffffff16806343 5ffe9414610051578063 8da9b772146100ae575b600080fd5b341561005c57600080fd5b6100ac600480803590602001908201803590602001908080601f016020809104026020016040519081016040528093929190818152602001838380828437820191505050505050919050506101 3c565b005b34156100b957600080fd5b6100c161015656 5b6040518080602001828103825283818151815260200191508051906020019080838360005b838110156101015780820151818401526020810190506100e6565b505050509050908101906 01f16801561012e57808203805160018360200361010 00a031916815260200191505b509250505060405180910390f35b806000908051906020019061015292919061 06101fe565b5050565b61015e61027e565b600080546001816001161561010002031660029004806 01f016020809104026020016040519081016040528092919081815260200182805460018160011615610100020316600290048015610 1f45780601f106101c9576101008083540402835291602001916101f4565b820191906000526020600020905b8154815290600101906020018083116101d7578290036 01f168201915b505050505090509056 5b828054600181600116156101000203166002900490600052602060002090601f016020900481019282601f1061023f57805160ff1916838001178555610 26d565b828001600101855582156 1026d579182015b828111156 1026c57825182559160200191906001019061025 1565b5b509050610 27a919061029256 5b5090565b602060405190810160405280600081525090565b6102b491905b808211156102b057600081600090555060010161029856 5b5090565b905600a165627a
```


BYTECODE


```
6060604052600436106100 4c576000357c0100000000000000000000000000000000000000000000000000000000900463ffffffff16806343 5ffe9414610051578063 8da9b772146100ae575b600080fd5b341561005c57600080fd5b6100ac600480803590602001908201803590602001908080601f016020809104026020016040519081016040528093929190818152602001838380828437820191505050505050919050506101 3c565b005b34156100b957600080fd5b6100c161015656 5b6040518080602001828103825283818151815260200191508051906020019080838360005b838110156101015780820151818401526020810190506100e6565b505050509050908101906 01f16801561012e57808203805160018360200361010 00a031916815260200191505b509250505060405180910390f35b806000908051906020019061015292919061 06101fe565b5050565b61015e61027e565b600080546001816001161561010002031660029004806 01f016020809104026020016040519081016040528092919081815260200182805460018160011615610100020316600290048015610 1f45780601f106101c9576101008083540402835291602001916101f4565b820191906000526020600020905b8154815290600101906020018083116101d7578290036 01f168201915b505050505090509056 5b828054600181600116156101000203166002900490600052602060002090601f016020900481019282601f1061023f57805160ff1916838001178555610 26d565b828001600101855582156 1026d579182015b828111156 1026c57825182559160200191906001019061025 1565b5b509050610 27a919061029256 5b5090565b602060405190810160405280600081525090565b6102b491905b808211156102b057600081600090555060010161029856 5b5090565b905600a165627a
```

TOKENS

ERC20

ERC20

Standard for how to interact with a smart contract

ERC20

Standard for how to interact with a smart contract

Its own entity stored on top of Ethereum blockchain

ERC20

Standard for how to interact with a smart contract

Its own entity stored on top of Ethereum blockchain

ERC stands for Ethereum Request for Comments

0x Project

Aragon

district0x

FunFair

ERC721

ERC721

Non-fungible token

ERC721

Non-fungible token

Each token is unique / non divisible
with its own characteristics

ERC721

Non-fungible token

Each token is unique / non divisible
with its own characteristics

Cryptokitties!


IT'S DEVELOP
TIME!

WARNING

Documentation sucks

WARNING

Documentation sucks

Few best practices as of now

WARNING

Documentation sucks

Few best practices as of now

Little information on what tools to use

WARNING

Documentation sucks

Few best practices as of now

Little information on what tools to use

Breaking changes can and probably will happen

DON'T PANIC

2

TOOLS

GANACHE

trufflframework.com/ganache/

```
(0) 0x4632d1b5f88d3aed78d76523063f142e46cb1122
(1) 0x4430ce7e737e96319b6849ed0fbb89cc616466b3
(2) 0xd4fd8a7adc9030400143f8fc3ca731d6af2e8347
(3) 0x73aaf73679815917be7f229e65984000cc071aa0
(4) 0x0b18d768660524a17f90b8a24a296cbc27fe1e86
(5) 0x8bafee2c61b3a01ec3484dddcf65b88ab04a3aa7
(6) 0x5120bb8059e4c6f62e87f0c430ad932308e9d7e0
(7) 0x811dc4647ef2d7c6363649e98aebe7faec5017e3
(8) 0x3430f25ee29117ffb5ee58983470d1e83c75877d
(9) 0x251fe3fc162ca85e24cc73e76a3a6a8f8951eb19

Private Keys
==================
(0) b45994fd93c4925144df1ebc00d23ca6ee3f19bfccfed4d69068833dbdc287f2
(1) 5a00e08a9e545710ff7ef4c07a90eebdf0ffb9db9dd5021883ef11e8bc5b69f5
(2) bef015b0fdf19882a25e53c2bc45be1cc3ee623b167e1ed40c4417656d8fa5d9
(3) 809112213e5e87772bb8f0acf45a9fcade2bb0c79afa02c3444c82a652dda8cb
(4) 388da552b42bdcd6ee45a8d471a233ba00b3f5ab86a7df005d4527a55bb42d3a
(5) 571af57f3120a44af22e0132a0646530c5f4e1c9d82a55542b9993709829bb5d
(6) 01c71f538bfcb1b8454b053121d24ff0d4fa0fda2c430e4d2b44b7844c7a7a0f
(7) 7c05431da0161029ed9b3322e2cb1898d808a23526ba74946b5c28ec10d92c5b
(8) e144efcd7e25be4fc41b7a3d6cef1a53e106fa02eb34632da6b589127acaf27e
(9) 39d8b55ab56eb7e5a762cfb6563d0abe280ddf88a71c8c12df5e8a8e2a228a66

HD Wallet
==================
Mnemonic:      base raise lab sport again hospital require thumb ladder laugh nominee s
alad
Base HD Path:  m/44'/60'/0'/0/{account_index}

Listening on localhost:8545
```

TESTRPC

Ganache

ACCOUNTS | BLOCKS | TRANSACTIONS | LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
3	20000000000	6721975	5777	HTTP://127.0.0.1:7545	5 SEC BLOCK TIME

MNEMONIC
candy maple cake sugar pudding cream honey rich smooth crumble sweet treat

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×627306090abaB3A6e1400e9345bC60c78a8BEf57	100.00 ETH	0	0
0×f17f52151EbEF6C7334FAD080c5704D77216b732	100.00 ETH	0	1
0×C5fdf4076b8F3A5357c5E395ab970B5B54098Fef	100.00 ETH	0	2
0×821aEa9a577a9b44299B9c15c88cf3087F3b5544	100.00 ETH	0	3
0×0d1d4e623D10F9FBA5Db95830F7d3839406C6AF2	100.00 ETH	0	4
0×2932b7A2355D6fecc4b5c0B6BD44cC31df247a2e	100.00 ETH	0	5
0×2191eF87E392377ec08E7c08Eb105Ef5448eCED5	100.00 ETH	0	6
0×0F4F2Ac550A1b4e2280d04c21cEa7EBD822934b5	100.00 ETH	0	7
0×6330A553Fc93768F612722BB8c2eC78aC90B3bbc	100.00 ETH	0	8

Ganache

ACCOUNTS | BLOCKS | TRANSACTIONS | LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
82	20000000000	6721975	5777	HTTP://127.0.0.1:7545	5 SEC BLOCK TIME

BLOCK 51	MINED ON 2018-03-10 14:15:13	GAS USED 26981	1 TRANSACTION
BLOCK 50	MINED ON 2018-03-10 14:15:08	GAS USED 284156	1 TRANSACTION
BLOCK 49	MINED ON 2018-03-10 14:15:03	GAS USED 41981	1 TRANSACTION
BLOCK 48	MINED ON 2018-03-10 14:14:58	GAS USED 269543	1 TRANSACTION
BLOCK 47	MINED ON 2018-03-10 14:14:53	GAS USED 0	NO TRANSACTIONS
BLOCK 46	MINED ON 2018-03-10 14:14:48	GAS USED 0	NO TRANSACTIONS
BLOCK 45	MINED ON 2018-03-10 14:14:43	GAS USED 0	NO TRANSACTIONS
BLOCK 44	MINED ON 2018-03-10 14:14:38	GAS USED 0	NO TRANSACTIONS
BLOCK 43	MINED ON 2018-03-10 14:14:33	GAS USED 0	NO TRANSACTIONS
BLOCK 42	MINED ON 2018-03-10 14:14:28	GAS USED 0	NO TRANSACTIONS
BLOCK 41	MINED ON 2018-03-10 14:14:23	GAS USED 0	NO TRANSACTIONS
BLOCK 40	MINED ON 2018-03-10 14:14:18	GAS USED 0	NO TRANSACTIONS

Ganache

ACCOUNTS | BLOCKS | TRANSACTIONS | LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
62	20000000000	6721975	5777	HTTP://127.0.0.1:7545	5 SEC BLOCK TIME

TX HASH
0×f36163615f41ef7ed8f4a8f192149a0bf633fe1a2398ce001bf44c43dc7bdda0

CONTRACT CALL

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×627306090abab3a6e1400e9345bc60c78a8bef57	0×8cdaf0cd259887258bc13a92c0a6da92698644c0	26981	0

TX HASH
0×937c08c92749efb7348d3b21bd9ba442af69c7c0c827069d4a45c4d78b7b1dcf

CONTRACT CREATION

FROM ADDRESS	CREATED CONTRACT ADDRESS	GAS USED	VALUE
0×627306090abab3a6e1400e9345bc60c78a8bef57	0×345ca3e014aaf5dca488057592ee47305d9b3e10	284156	0

TX HASH
0×d7bc86d31bee32fa3988f1c1eabce403a1b5d570340a3a9cdba53a472ee8c956

CONTRACT CALL

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×627306090abab3a6e1400e9345bc60c78a8bef57	0×8cdaf0cd259887258bc13a92c0a6da92698644c0	41981	0

TX HASH
0×6de7718d241405256d3b8a3a3f9dd9c5be5d75f4ec23af78e5b19c5f52464103

CONTRACT CREATION

FROM ADDRESS	CREATED CONTRACT ADDRESS	GAS USED	VALUE
0×627306090abab3a6e1400e9345bc60c78a8bef57	0×8cdaf0cd259887258bc13a92c0a6da92698644c0	269543	0

Ganache

SERVER ACCOUNTS & KEYS CHAIN ADVANCED

SERVER

HOSTNAME

127.0.0.1

The server will accept R
port.

PORT NUMBER

7545

NETWORK ID

5777

Internal blockchain iden

AUTOMINE

Process transactions ins

MINING BLOCK TIME (SECONDS)

5

The number of seconds to
transactions.

RPC SERVER

HTTP://127.0.0.1:7545

HD PATH

m/44'/60'/0'/0/account_index

TX COUNT	INDEX
4	0

METAMASK

METAMASK

GET CHROME EXTENSION

Chrome Firefox Opera

OR

GET BRAVE BROWSER

metamask.io

METAMASK

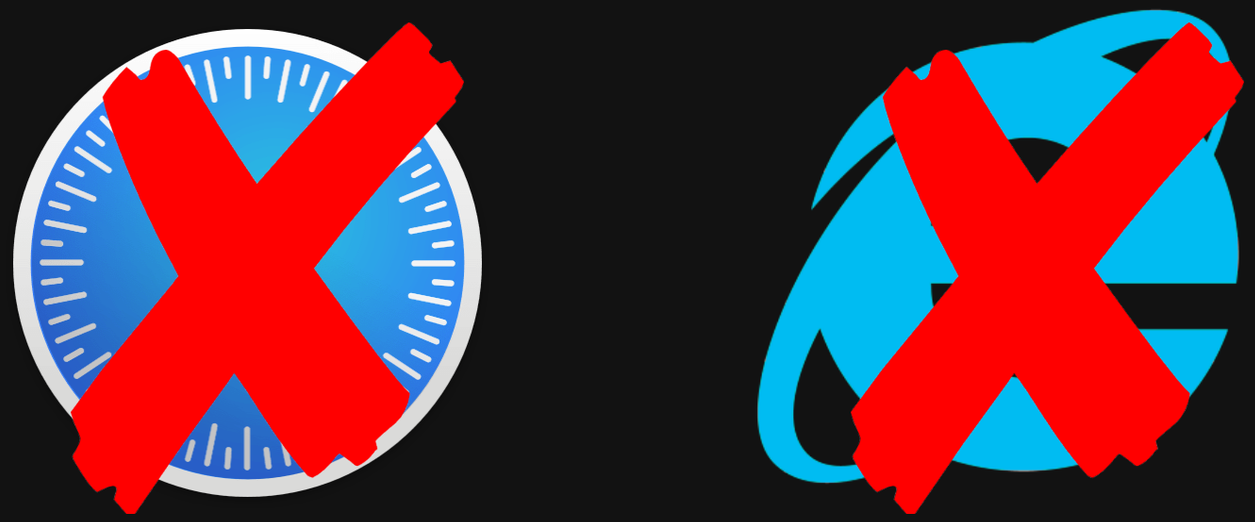
METAMASK

METAMASK



METAMASK

METAMASK



web store

ryan@chromatich

Featured

Add "MetaMask"?

It can:

- Read and change all your data on the websites you visit
- Communicate with cooperating websites
- Modify data you copy and paste

Cancel | Add extension

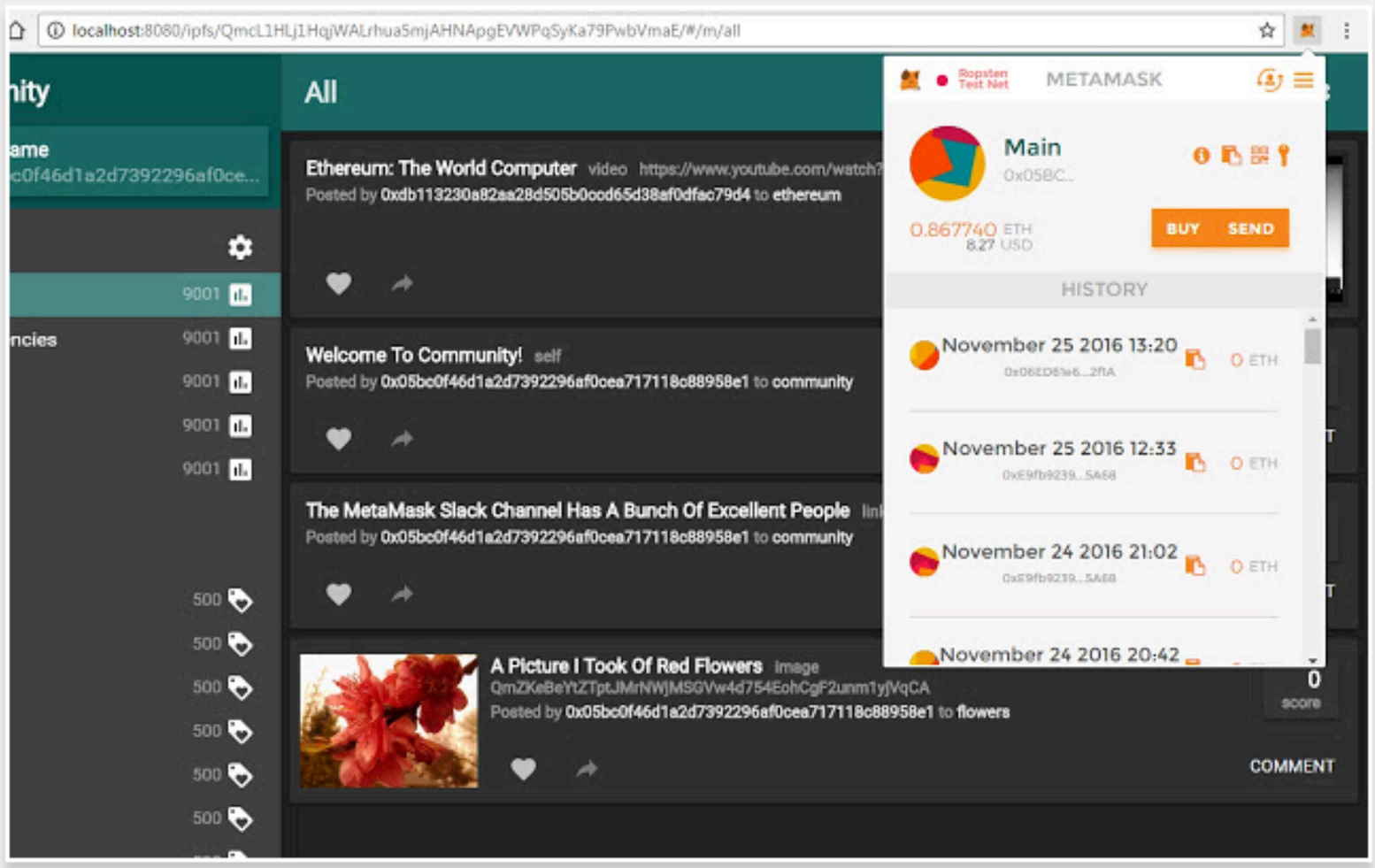
MetaMask

offered by https://metama

★★★★☆ (769) | Productivity | *1,066,130 users*

CHECKING...

OVERVIEW | REVIEWS | SUPPORT | RELATED



Compatible with your device

Ethereum Browser Extension

MetaMask is an extension for accessing Ethereum enabled distributed applications, or "Dapps" in your normal Chrome browser!

The extension injects the Ethereum web3 API into every website's javascript context, so that dapps can read from the blockchain.

MetaMask also lets the user create and manage their own identities, so when a Dapp wants to perform a transaction and write to the blockchain, the user gets a secure interface to review the transaction, before approving or rejecting it.

Website

Report Abuse

Additional Information

Version: 4.2.0

Updated: March 6, 2018

Size: 5.38MiB

Languages: See all 6

RELATED

MyEtherWallet ★★★★½ (210)

Some Rich Asshole ★★★★★ (64)

EtherAddressLookup ★★★★★ (57)

Cryptonite by MetaCert ★★★★½ (113)

METAMASK BETA

Main Network

Please be aware that this version is still under development

Create Password

New Password (min 8 characters)

Confirm Password

CREATE

Import with seed phrase

MetaMask is a secure identity vault for Ethereum.

It allows you to hold ether & tokens, and interact with decentralized applications.

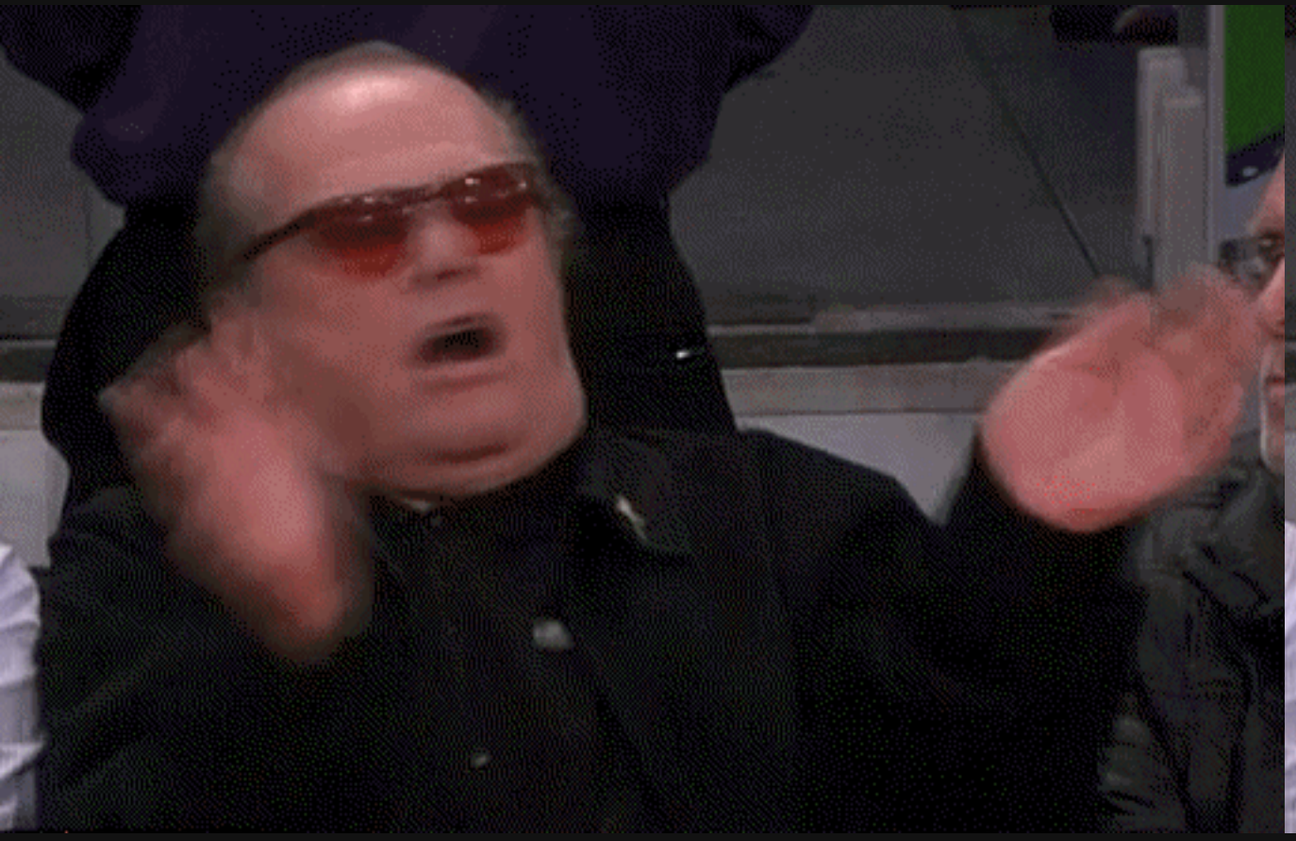
Ganache

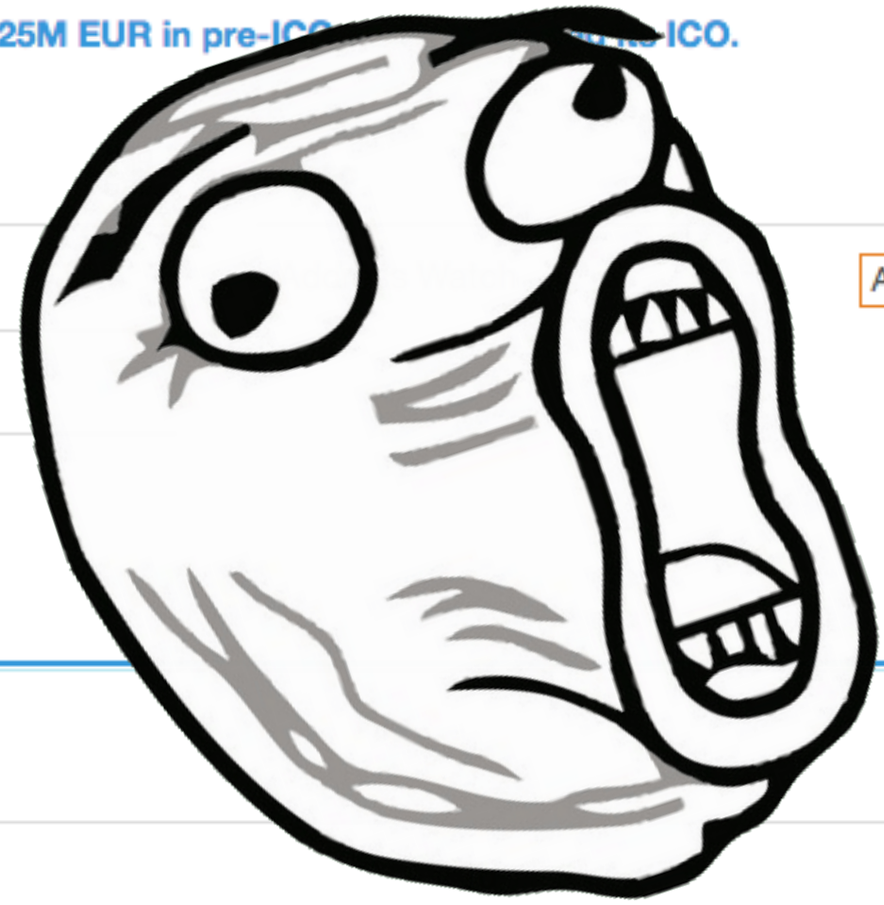
ACCOUNTS BLOCKS TRANSACTIONS LOGS

CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
615	20000000000	6721975	5777	HTTP://127.0.0.1:7545	5 SEC BLOCK TIME

MNEMONIC

candy maple cake sugar pudding cream honey rich smooth crumble sweet treat





Overview

ETH Balance:	0.580940828823033356 Ether
ETH USD Value:	$484.35 (@ $833.73/ETH)
No Of Transactions:	38 txns

Add To Watch List

Transactions | Comments

Latest 25 txns from a total Of 38 transactions

TxHash	Block	Age	From		To	Value
0x54b2828f130d65...	5072173	3 hrs 48 mins ago	0x627306090abab3...	IN	0x2d7311279a3ba8...	0.0000545454
0x3890afa938fb7d8...	5053565	3 days 6 hrs ago	0xf17f52151ebef6c...	IN	0x2d7311279a3ba8...	0.0000909090
0x76739de44466f1...	5052969	3 days 8 hrs ago	0x627306090abab3...	IN	0x2d7311279a3ba8...	0.0019051249
0xa81ae159719cb0...	5049911	3 days 21 hrs ago	0x627306090abab3...	IN	0x2d7311279a3ba8...	0.0081818181
0x8705aac42769a4...	5049079	4 days 39 mins ago	0x627306090abab3...	IN	0x2d7311279a3ba8...	0.0001160000
0xa0f39daa1448d2...	5047550	4 days 6 hrs ago	0x627306090abab3...	IN	0x2d7311279a3ba8...	0.0008462499
0xddc8584badf032...	5047310	4 days 7 hrs ago	0x627306090abab3...	IN	0x2d7311279a3ba8...	0.0000000000
0x540f32df03512b5...	5043167	5 days 26 mins ago	0x627306090abab3...	IN	0x2d7311279a3ba8...	0.0001818181
0xcc4b57a275777af...	5041756	5 days 6 hrs ago	0x627306090abab3...	IN	0x2d7311279a3ba8...	0.0004766835

Terms of Use

Terms of Use

THIS AGREEMENT IS SUBJECT TO BINDING ARBITRATION AND A WAIVER OF CLASS ACTION RIGHTS AS DETAILED IN SECTION 13. PLEASE READ THE AGREEMENT CAREFULLY.

Our Terms of Use have been updated as of September 5, 2016

1. Acceptance of Terms

MetaMask provides a platform for managing Ethereum (or "ETH") accounts, and allowing ordinary websites to interact with the Ethereum blockchain, while keeping the user in control over what transactions they approve, through our website located at https://metamask.io/ and browser plugin (the "Site") — which includes text, images, audio, code and other materials (collectively, the "Content") and all of the features, and services provided. The Site, and any other features, tools, materials, or other services offered from time to time by MetaMask are referred to here as the "Service." Please read these Terms of Use (the "Terms" or "Terms of Use") carefully before using the Service. By using or otherwise accessing the Services, or clicking to accept or agree to these Terms where that option is made available, you (1) accept and agree to these Terms (2) consent to the collection, use, disclosure and other handling of information as described in our Privacy Policy and (3) any additional terms, rules and conditions of participation issued by MetaMask from time to time. If you do not agree to the Terms, then you may not access or use the Content or Services.

2. Modification of Terms of Use

ACCEPT

METAMASK BETA

Main Network

Account 1

DETAILS

0x6a...6520

0 ETH

Add Token

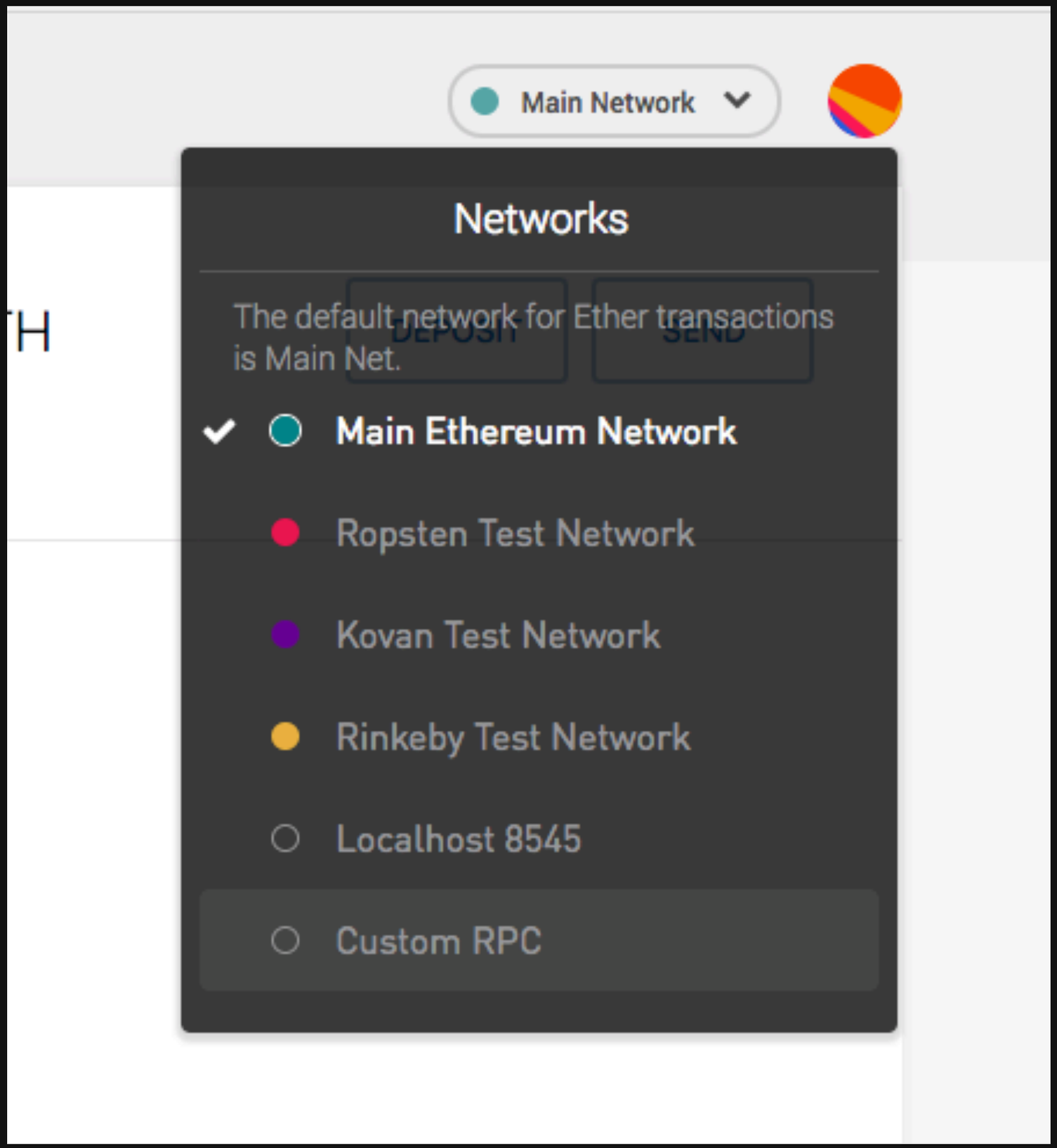
0 ETH

DEPOSIT

SEND

Transactions

No Transactions


Main Network
Networks
The default network for Ether transactions is Main Net.
Main Ethereum Network
Ropsten Test Network
Kovan Test Network
Rinkeby Test Network
Localhost 8545
Custom RPC

METAMASK BETA

Main Network

Settings Info

Current Conversion

Updated Sat Mar 10 2018 14:58:36 GMT-0500 (EST)

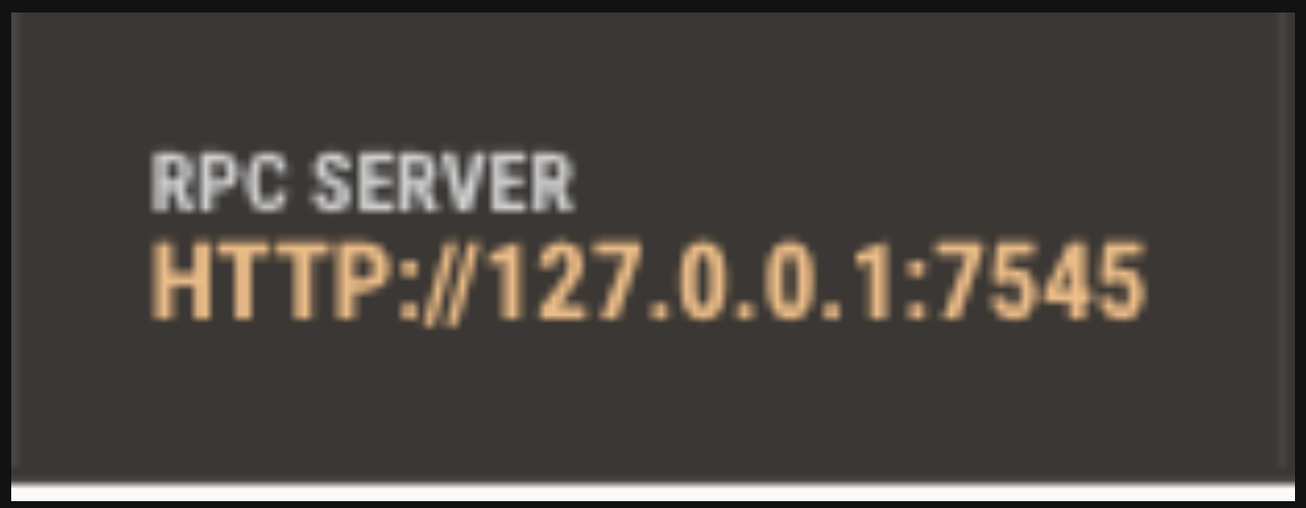
USD - United States Dollar

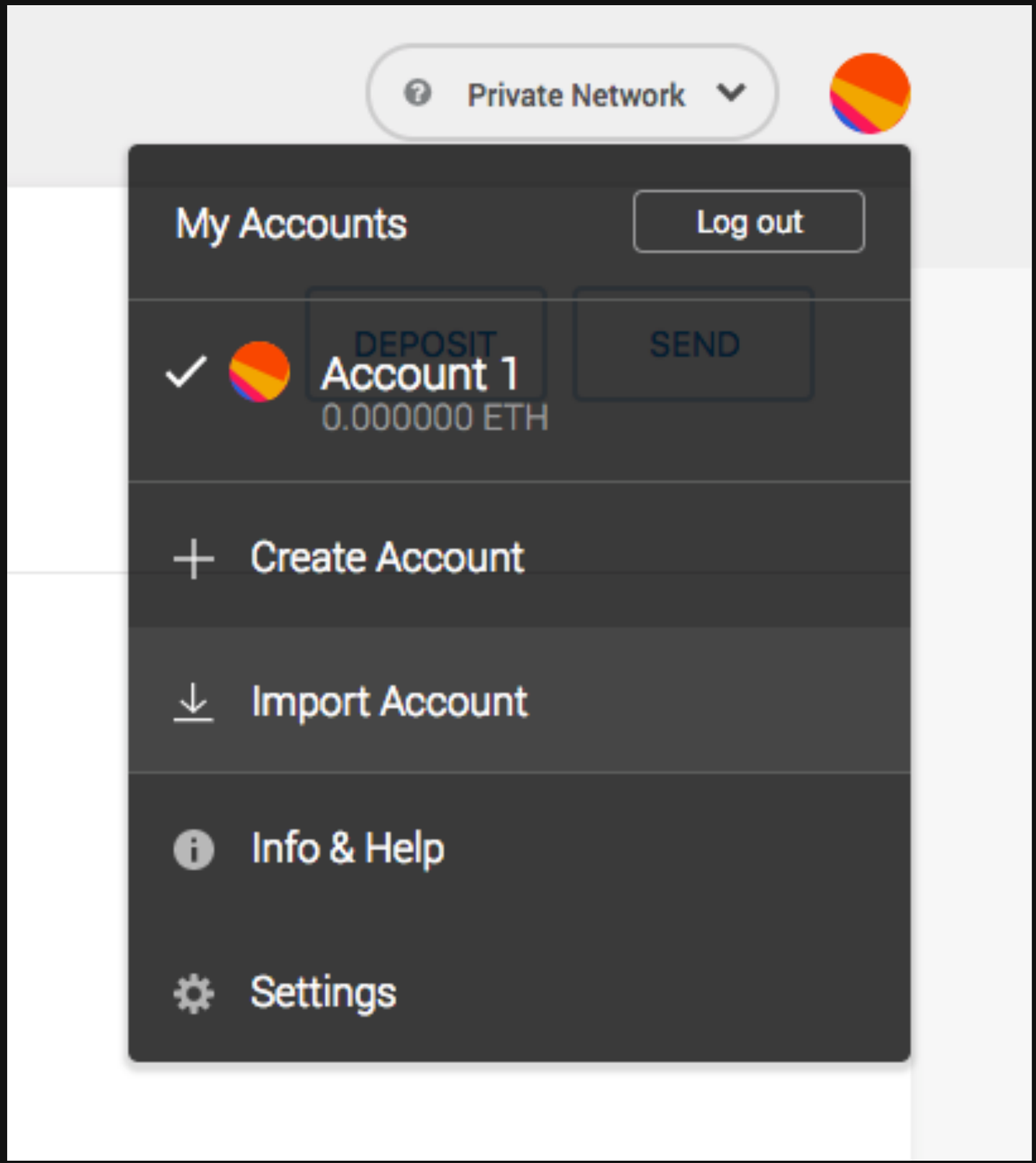
New RPC URL

http://127.0.0.1:7545

SAVE

Ganache
RPC Server




Private Network
My Accounts
Log out
DEPOSIT
SEND
Account 1
0.000000 ETH
Create Account
Import Account
Info & Help
Settings

HD PATH
m/44'/60'/0'/0/account_index

TX COUNT	INDEX
4	0

BALANCE
6C7334FAD080c5704D77216b732 100.00 ETH TX COU 0

TX COU 0

TX COU 0

TX COU 0

BALANCE
fecc4b5c0B6BD44cC31df247a2e 100.00 ETH TX COU 0

0x627306090abaB3A6e1400e9345bC60c78a8BEf57

PRIVATE KEY

c87509a1c067bbde78beb793e6fa76530b6382a4c0241e5e4a9ec0a0f44dc0d3

DONE

METAMASK BETA

Private Network

New Account

Create | Import

Imported accounts will not be associated with your originally created MetaMask account seedphrase. Learn more about imported accounts here

Select Type: Private Key

Paste your private key string here:

••

CANCEL | IMPORT

METAMASK BETA

Private Network

IMPORTED

Account 2

DETAILS

0x62...ef57

99.937 ETH
71254.60 USD

Add Token

99.937 ETH
71254.60 USD

DEPOSIT

SEND

Transactions

No Transactions

TRUFFLE

truffleframework.com

INSTALL TRUFFLE

```
MP/htdocs/awesome-eth-app  npm install -g truffle
```

DOWNLOAD REACT BOX

```
/htdocs/awesome-eth-app  truffle unbox react
```

LOTS OF BOXES

Status
A Mobile Ethereum OS

status-im/ truffle-box-status

★ Star 39

This box comes with everything you need to start using smart contracts from a react app on your mobile. Of course, testing of this box requires you to have iOS/Android device with Status installed on it.

status react webpack webapp

Quintor/ angular-truffle-box

★ Star 26

This Truffle Box provides a base for working with the Truffle Framework and Angular. It provides a basic working example of the MetaCoin contracts with Angular components. This project is generated with Angular CLI.

angular

ENS · BID
The Best ENS Trading Market

ens-bid/ ens-bid-truffle-box

★ Star 4

This box comes with everything you need to start using smart contracts on Ethereum blockchain and interact with MetaMask to send transactions.

material-ui react redux sass

limelabs

DON'T PANIC

```
npm ERR! npm  v3.10.9
npm ERR! code ELIFECYCLE

npm ERR! scrypt@6.0.3 install: `node-gyp rebuild`
npm ERR! Exit status 1
npm ERR!
npm ERR! Failed at the scrypt@6.0.3 install script 'node-gyp rebuild'.
npm ERR! Make sure you have the latest version of node.js and npm installed.
npm ERR! If you do, this is most likely a problem with the scrypt package,
npm ERR! not with npm itself.
npm ERR! Tell the author that this fails on your system:
npm ERR!     node-gyp rebuild
npm ERR! You can get information on how to open an issue for this project with:
npm ERR!     npm bugs scrypt
npm ERR! Or if that isn't available, you can get their info via:
npm ERR!     npm owner ls scrypt
npm ERR! There is likely additional logging output above.

npm ERR! Please include the following file with any support request:
npm ERR!     /Applications/MAMP/htdocs/awesome-eth-app/npm-debug.log

    at ChildProcess.exithandler (child_process.js:211:12)
    at emitTwo (events.js:106:13)
    at ChildProcess.emit (events.js:191:7)
    at maybeClose (internal/child_process.js:885:16)
    at Process.ChildProcess._handle.onexit (internal/child_process.js:226:5)
```

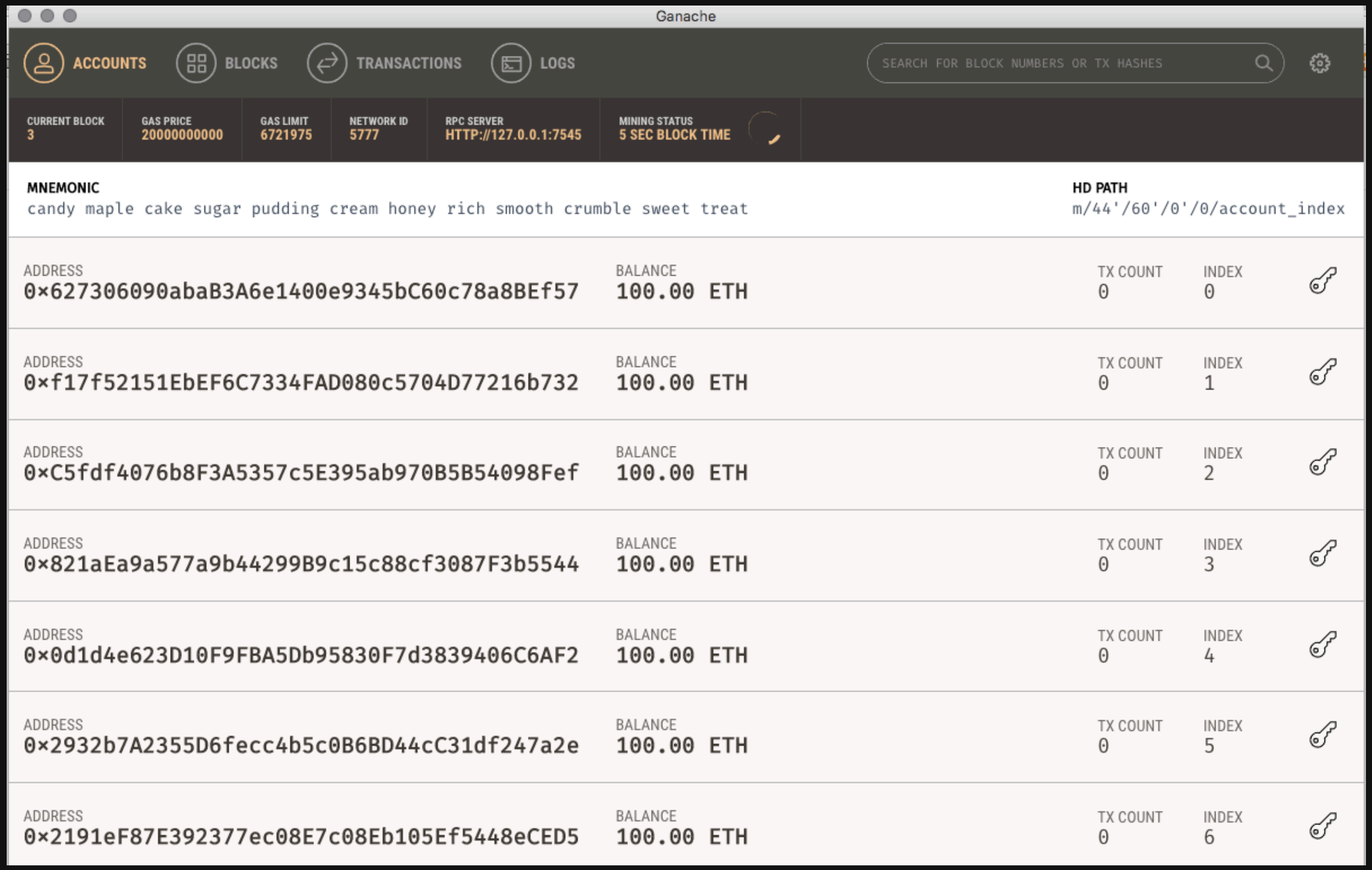
TRUFFLE COMPILE

```
✘ ryanhagerty@Ryans-MBP /Applications/MAMP/htdocs/awesome-eth-app truffle compile
Compiling ./contracts/Migrations.sol...
Compiling ./contracts/SimpleStorage.sol...
Writing artifacts to ./build/contracts
```

TRUFFLE MIGRATE

```
ryanhagerty@Ryans-MBP /Applications/MAMP/htdocs/awesome-eth-app truffle migrate
Error: No network specified. Cannot determine current network.
    at Object.detect (/usr/local/lib/node_modules/truffle/build/webpack:/~/truffle-core/lib/environment.js:31:1)
    at /usr/local/lib/node_modules/truffle/build/webpack:/~/truffle-core/lib/commands/migrate.js:91:1
    at finished (/usr/local/lib/node_modules/truffle/build/webpack:/~/truffle-workflow-compile/index.js:53:1)
    at /usr/local/lib/node_modules/truffle/build/webpack:/~/truffle-compile/index.js:301:1
    at /usr/local/lib/node_modules/truffle/build/webpack:/~/truffle-compile/profiler.js:157:1
    at /usr/local/lib/node_modules/truffle/build/webpack:/~/async/dist/async.js:3874:1
    at /usr/local/lib/node_modules/truffle/build/webpack:/~/async/dist/async.js:473:1
    at replenish (/usr/local/lib/node_modules/truffle/build/webpack:/~/async/dist/async.js:993:1)
    at iterateeCallback (/usr/local/lib/node_modules/truffle/build/webpack:/~/async/dist/async.js:983:1)
    at /usr/local/lib/node_modules/truffle/build/webpack:/~/async/dist/async.js:958:1
```

DON'T FORGET GANACHE

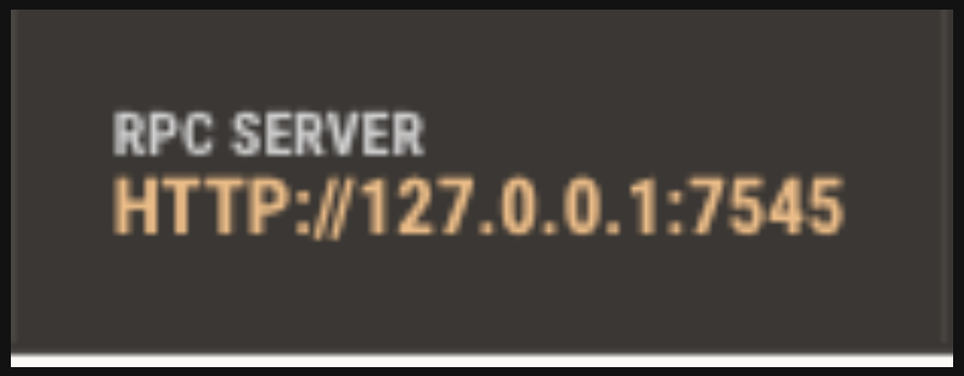


SET OUR NETWORK

JS truffle.js ×

```
1   module.exports = {
2     // See <http://truffleframework.com/docs/advanced/configuration>
3     // to customize your Truffle configuration!
4   };
5
```

SET OUR NETWORK



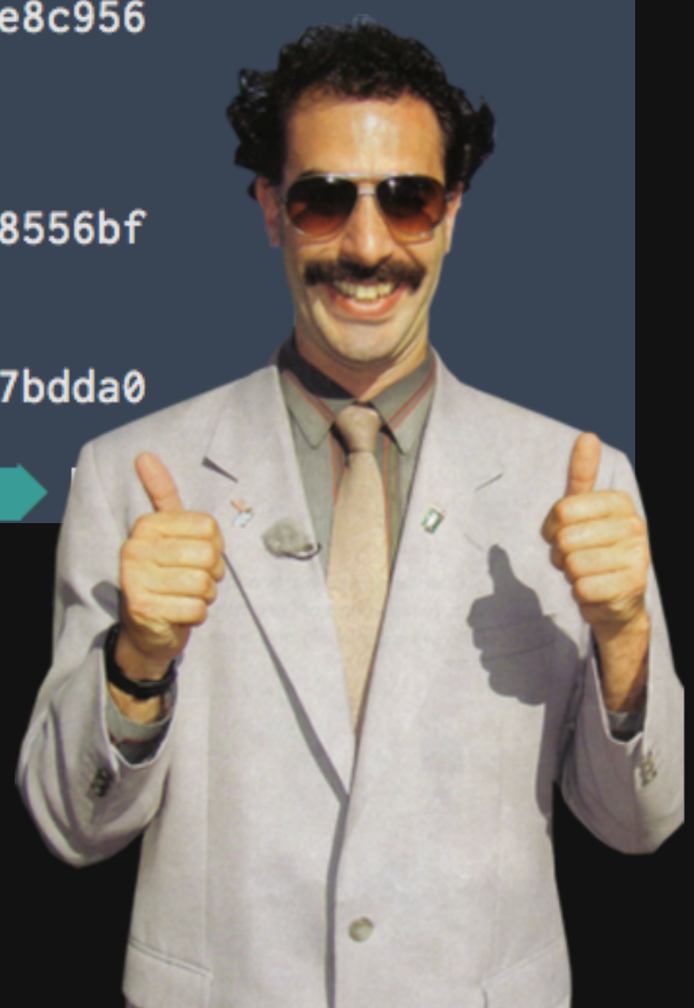
JS truffle.js

```
module.exports = {
  networks: {
    development: {
      host: "127.0.0.1",
      port: 7545,
      network_id: "*" // Match any network id
    }
  }
};
```

GREAT SUCCESS!

```
✘ ryanhagerty@Ryans-MBP /Applications/MAMP/htdocs/awesome-eth-app truffle migrate
Using network 'development'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
  ... 0x61ca4447d9c15f40d6182447f96bde374591c722770f3be61f46c619476fc679
  Migrations: 0x8cdaf0cd259887258bc13a92c0a6da92698644c0
Saving successful migration to network...
  ... 0xd7bc86d31bee32fa3988f1c1eabce403a1b5d570340a3a9cdba53a472ee8c956
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying SimpleStorage...
  ... 0x19d8b43872c3d1e6c432d9d2e1df8838f81e350eaec199fcfa566debc38556bf
  SimpleStorage: 0x345ca3e014aaf5dca488057592ee47305d9b3e10
Saving successful migration to network...
  ... 0xf36163615f41ef7ed8f4a8f192149a0bf633fe1a2398ce001bf44c43dc7bdda0
Saving artifacts...
ryanhagerty@Ryans-MBP /Applications/MAMP/htdocs/awesome-eth-app
```



GREAT SUCCESS!

Ganache

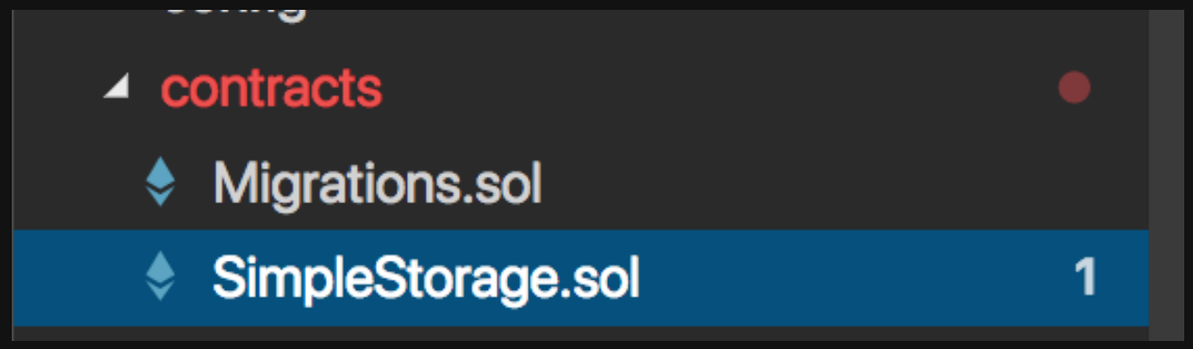
ACCOUNTS BLOCKS TRANSACTIONS LOGS SEARCH FOR BLOCK NUMBERS

CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
192	20000000000	6721975	5777	HTTP://127.0.0.1:7545	5 SEC BLOCK TIME

MNEMONIC
candy maple cake sugar pudding cream honey rich smooth crumble sweet treat

ADDRESS	BALANCE
0×627306090abaB3A6e1400e9345bC60c78a8BEf57	99.96 ETH

INCLUDED SMART CONTRACT



SimpleStorage.sol

```
1   pragma solidity ^0.4.18;
2
3   contract SimpleStorage {
4     uint storedData;
5
6     function set(uint x) public {
7       storedData = x;
8     }
9
10    function get() public view returns (uint) {
11      return storedData;
12    }
13  }
14
```

GET IT RUNNING

```
/Applications/MAMP/htdocs/awesome-eth-app  npm run start
```

Truffle Box

Good to Go!

Your Truffle Box is installed and ready.

Smart Contract Example

If your contracts compiled and migrated successfully, below wi

Try changing the value stored on line 59 of App.js.

The stored value is: 0

SOLIDITY

SOLIDITY BASICS

Statically typed

```
contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

SOLIDITY BASICS

"Contracts in Solidity are similar to classes in object-oriented languages."

```
contract SimpleStorage {
  uint storedData;

  function set(uint x) public {
    storedData = x;
  }

  function get() public view returns (uint) {
    return storedData;
  }
}
```

SOLIDITY BASICS

Similar to JavaScript!

```
contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

SOLIDITY BASICS

structs similar to objects

```
struct Person {
    uint age;
    string name;
    string profession;
}
```

SOLIDITY

SOLIDITY

STATE

SOLIDITY

STATE FUNCTIONS

?

SOLIDITY

BYTECODE

BYTECODE

"60606040523415610000f57600080
fd5b6040805190810160405280600
c81526020017f48656c6c6f20576f
726c6421000000000000000000000
0000000000000000000815250600
9080519060200190610005a9291906
10060565b50610105565b82805460
018160011615610100020316600290
0049060005260206000209060 1f01
6020900481019282601f106100a15
7805160ff1916838001178555610 0

OPCODES

```
0x30    ADDRESS         Get address of currently executing account
0x31    BALANCE         Get balance of the given account
0x32    ORIGIN          Get execution origination address
0x33    CALLER          Get caller address. This is the address of the account that i
0x34    CALLVALUE       Get deposited value by the instruction/transaction responsibl
0x35    CALLDATALOAD    Get input data of current environment
0x36    CALLDATASIZE    Get size of input data in current environment
0x37    CALLDATACOPY    Copy input data in current environment to memory This pertair
0x38    CODESIZE        Get size of code running in current environment
0x39    CODECOPY        Copy code running in current environment to memory
0x3a    GASPRICE        Get price of gas in current environment
0x3b    EXTCODESIZE     Get size of an account's code
0x3c    EXTCODECOPY     Copy an account's code to memory
```

list of opcodes

OUR PROJECT

"6060604052341561000f57600080
fd5b60408051908101604052806000
c81526020017f48656c6c6f20576f
726c6421000000000000000000000
0000000000000000000815250600
90805190602001906100a9291906
10060565b50610105565b82805460
018160011615610100020316600290
0049060005260206000209060 1f01
6020900481019282601f106100a15
7805160ff1916838001178555610

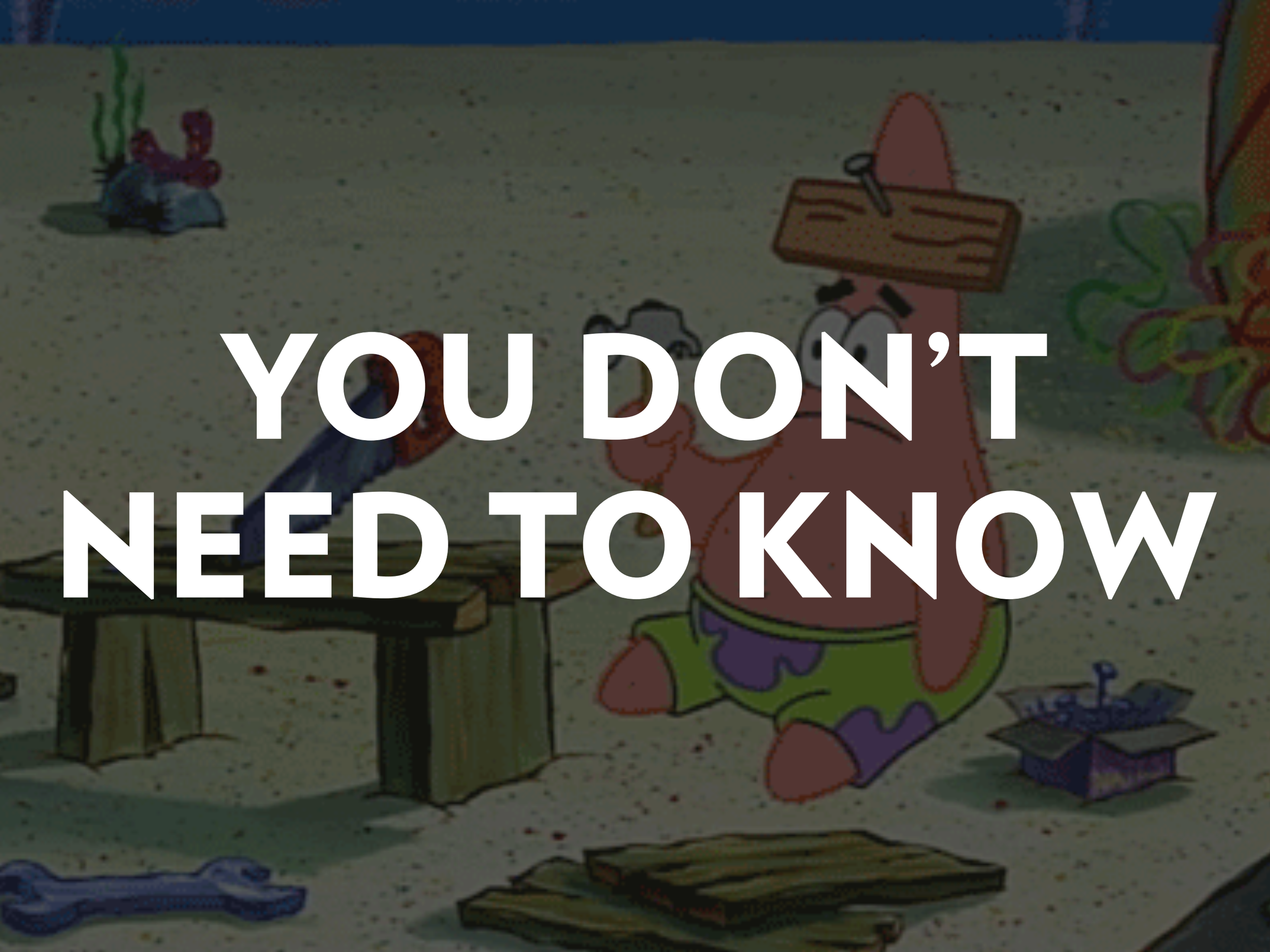
60606040 52

60606040 PUSH1 X3
BLOCKHASH

Store 0x60 at memory location 0x40.

52 MSTORE

Save word to memory


YOU DON'T
NEED TO KNOW

SECURITY

SECURITY

“every execution of a smart contract is publicly visible”

Security Considerations

Current Best Practices

```
class ContractInput extends React.Component {
  submit(e) {
    e.preventDefault();
    const message = this.message.value;
    const state = this.props.state;
    const web3 = state.web3;
    const instance = state.instance;

    const setHelloRequest = async () =>
      const result = instance.setHello(     age, { from: state.web3.eth.accoun
        this.props.initModal(0);
        return instance.getHello()
      });
      return result
    }

    const getHelloRequest = async () => {
      this.props.initModal(1);
      const result = await setHelloRequest();
      this.props.updateHello(result);
    }

    getHelloRequest();
  }
```

3 PROJECT

WHAT WE'RE GOING TO DO

WHAT WE'RE GOING TO DO

1. Deploy our contract on our testnet

WHAT WE'RE GOING TO DO

1. Deploy our contract on our testnet
2. See our predefined hello world message stored on the blockchain

WHAT WE'RE GOING TO DO

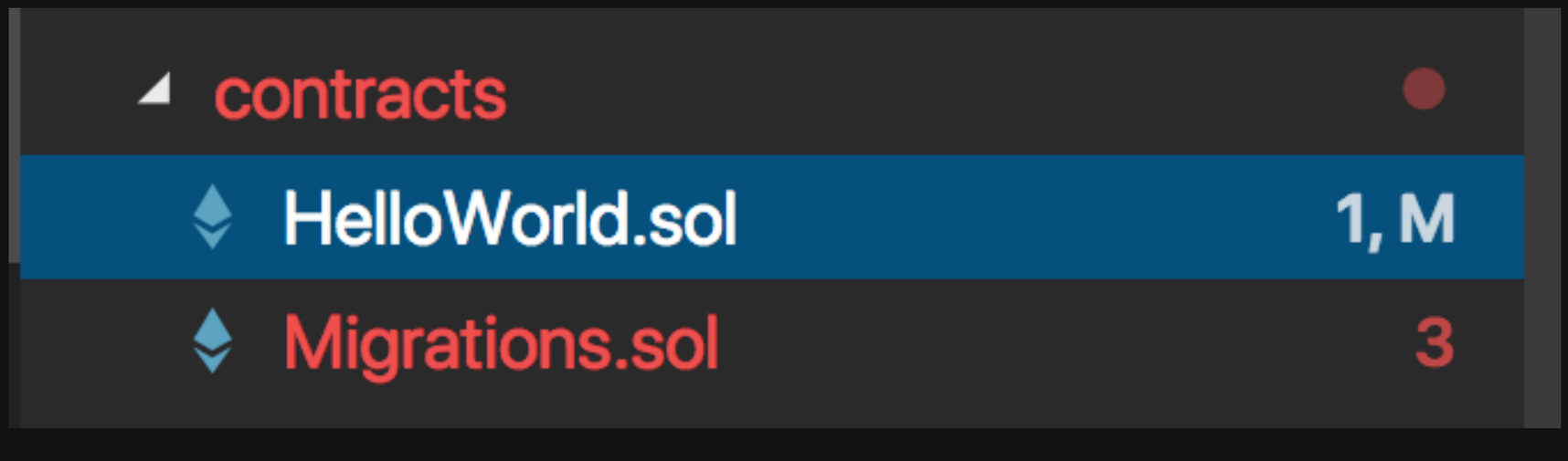
1. Deploy our contract on our testnet
2. See our predefined hello world message stored on the blockchain
3. Take user input from React component to change our message and store it!


DON'T
FORGET!

SIX STEPS

1. Start Ganache
2. Unlock MetaMask with Local Network
3. Switch Accounts
4. truffle compile
5. truffle migrate
6. npm run start

OUR CONTRACT



App.js

```
import HelloWorldContract from '../build/contracts/HelloWorld.json'
```

OUR CONTRACT

```
pragma solidity ^0.4.18;

contract HelloWorld {
  string hello;

  function HelloWorld() public {
    hello = "Hello World!";
  }

  function setHello(string _hello) public {
    hello = _hello;
  }

  function getHello() public view returns (string) {
    return hello;
  }
}
```

PRAGMA & CONTRACT

```
pragma solidity ^0.4.18;

contract HelloWorld {
    string hello;
}
```

CONSTRUCTOR

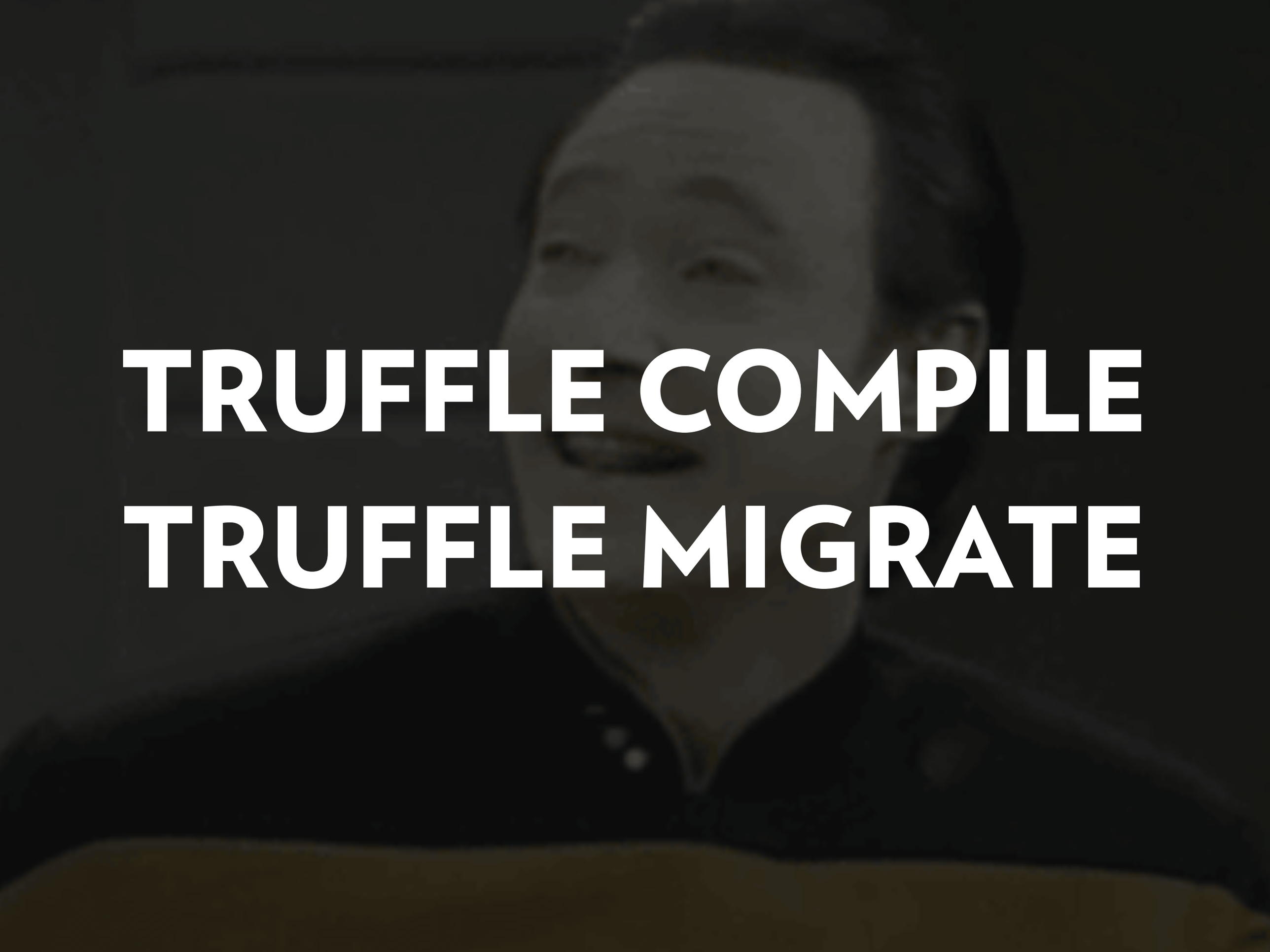
```
function HelloWorld() public {
    hello = "Hello World!";
}
```

SETHELLO()

```
function setHello(string _hello) public {
    hello = _hello;
}
```

GETHELLO()

```
function getHello() public view returns (string) {
    return hello;
}
```


TRUFFLE COMPILE
TRUFFLE MIGRATE

APP.JS

```
import React, { Component } from 'react'  22.2K (gzipped: 7.4K)
import HelloWorldContract from '../build/contracts/HelloWorld.json'
import getWeb3 from './utils/getWeb3'
import ContractInput from './components/ContractInput'
import Modal from './components/Modal'

import './css/roboto.css'
import './css/rubik.css'
import './css/milligram.min.css'
import './App.css'

class App extends Component {
  constructor(props) {
    super(props)
    this.updateHello = this.updateHello.bind(this);
    this.initModal = this.initModal.bind(this);

    // ^^ Change initial states and add new ones here.
    this.state = {
      hello: "I'm waiting to say hello...",
      contractAddress: "Waiting on contract address...",
      modal: 0,
```

WHAT WE NEED

1. Import everything we need.

2. Set our initial state.

3. Get web3

4. Instantiates our contract

5. Renders our HTML/components

Ethereum and React

Looks like Truffle React Box is up and running 👍👍

Hello World

Our First Smart Contract

If your contracts compiled and migrated successfully, we'll show your contract address and the hello message below.

Your contract address is:

0x8c7ef141e529c5263e2a45581d1c8a39f64dc5df

The hello message from your contract is:

Hello World!

Hello World text to change

SUBMIT

The hello message from your contract is:

Hello World!

HELLLOOOO NASHVILLE

SUBMIT

MetaMask Notification

Account 2 → New Recipient

0
USD

From	Account 2 ...ef57
To	New Recipient ...c5df
Gas Fee	0.03 USD 0.000051 ETH
Total Amount + Gas	**0.03 USD** 0.000051 ETH

CANCEL CONFIRM

Ou ct

contracts compiled

the hello message

0x8 5df

Waiting on latest block to mine...

Hello World!

HELLLOOOO NASHVILLE

SUBMIT

The hello message from your contract is:

HELLLOOOO NASHVILLE

HELLLOOOO NASHVILLE

SUBMIT

IMPORT

```
import React, { Component } from 'react'  22.2K (gzipped: 7.4K)
import HelloWorldContract from '../build/contracts/HelloWorld.json'
import getWeb3 from './utils/getWeb3'
import ContractInput from './components/ContractInput'
import Modal from './components/Modal'

import './css/roboto.css'
import './css/rubik.css'
import './css/milligram.min.css'
import './App.css'
```

SET STATE

```
this.state = {
  hello: "I'm waiting to say hello...",
  contractAddress: "Waiting on contract address...",
  modal: 0,
  instance: null,
  web3: null
}
```

GET WEB3

```
componentWillMount() {
  // Get network provider and web3 instance.
  // See utils/getWeb3 for more info.
  getWeb3
    .then(results => {
      this.setState({
        web3: results.web3
      })

      // Instantiate contract once web3 provided.
      this.instantiateContract()
    })
    .catch(() => {
      console.log('Error finding web3.')
    })
  }
```

GET WEB3

```
Injected web3 detected.                                    getWeb3.js:18
                                                           App.js:69
▼ Web3 {_requestManager: RequestManager, currentProvider: MetamaskInpageProvider, eth:
  Eth, db: DB, shh: Shh, …} i
  ▶ currentProvider: MetamaskInpageProvider {mux: e.exports, publicConfigStore: e, rpcEngin
  ▶ db: DB {_requestManager: RequestManager, putString: ƒ, getString: ƒ, putHex: ƒ, getHex:
  ▼ eth: Eth
      accounts: (...)
      blockNumber: (...)
    ▶ call: ƒ ()
      coinbase: (...)
    ▶ compile: {solidity: ƒ, lll: ƒ, serpent: ƒ}
    ▶ estimateGas: ƒ ()
      gasPrice: (...)
    ▶ getAccounts: ƒ (callback)
    ▶ getBalance: ƒ ()
    ▶ getBlock: ƒ ()
    ▶ getBlockNumber: ƒ (callback)
    ▶ getBlockTransactionCount: ƒ ()
    ▶ getBlockUncleCount: ƒ ()
    ▶ getCode: ƒ ()
    ▶ getCoinbase: ƒ (callback)
```

INSTANTIATE CONTRACT

```
instantiateContract() {
  const contract = require('truffle-contract')  217.2K (gzipped: 67.4K)
  const helloWorld = contract(HelloWorldContract)
  let helloWorldInstance
  helloWorld.setProvider(this.state.web3.currentProvider)

  helloWorld.deployed().then((instance) => {
    helloWorldInstance = instance
    this.setState({ instance: helloWorldInstance })
    this.setState({ contractAddress: helloWorldInstance.address })

    return helloWorldInstance.getHello()

  }).then((result) => {
    return this.setState({ hello: result })
  })
}
```

INSTANTIATE CONTRACT

```
Injected web3 detected.                                   getWeb3.js:18

                                                          App.js:72
▼ TruffleContract {constructor: ƒ, abi: Array(3), contract: Contract, setHel
lo: ƒ, getHello: ƒ, …}
  ▶ abi: (3) [{…}, {…}, {…}]
    address: "0x8065f4c7b8c2bf53561af92d9da2ea022a0b28ca"
  ▶ allEvents: ƒ ()
  ▶ constructor: ƒ TruffleContract()
  ▶ contract: Contract {_eth: Eth, transactionHash: null, address: "0x8065f4c7b8
  ▶ getHello: ƒ ()
  ▶ send: ƒ (value)
  ▶ sendTransaction: ƒ ()
  ▶ setHello: ƒ ()
    transactionHash: null
  ▶ __proto__: Contract

>
```

RENDER

```
render() {
  return (
    <div className="App">
      <div className="top-bar">
        <a href="#" className="title-link">🍕 Ethereum and React</a>
        <div className="notice-box">Looks like Truffle React Box is up and running 👍👍</div>
      </div>

      <main className="container">
        <h1>Hello World</h1>
        <h2>Our First Smart Contract</h2>
        <div className="contract-status">
          <p>If your contracts compiled and migrated successfully, we'll show your contract ad
          <div>Your contract address is: <span className="contract-address">{this.state.contrac
        </div>
        <p className="message">The hello message from your contract is: <strong className="hel
        <ContractInput state={this.state} updateHello={this.updateHello} initModal={this.initMo
      </main>
      <Modal modal={this.state.modal} />
    </div>
  );
}
```

CONTRACTINPUT.JS

```
render() {
  return (
    <form className="hello-form" onSubmit={(e) => this.submit(e)}>
      <input ref={(input) => this.message = input} type="text" className="he
      <button type="submit" value="Submit" className="button-submit js-butto
    </form>
  )
}
```

CONTRACTINPUT.JS

```
submit(e) {
  e.preventDefault();
  const message = this.message.value;
  const state = this.props.state;
  const instance = state.instance;

  const setHelloRequest = async () => {
    const result = instance.setHello(message,
      this.props.initModal(0);
      return instance.getHello()
    });
    return result
  }

  const getHelloRequest = async () => {
    this.props.initModal(1);
    const result = await setHelloRequest();
    this.props.updateHello(result);
  }

  getHelloRequest();
}
```

CONTRACTINPUT.JS

```
const getHelloRequest = async () => {
  this.props.initModal(1);
  const result = await setHelloRequest();
  this.props.updateHello(result);
}

getHelloRequest();
```

CONTRACTINPUT.JS

```
const setHelloRequest = async () => {
  const result = instance.setHello(message, { from: state.web3.eth.accounts[0]}).then((result) => {
    this.props.initModal(0);
    return instance.getHello()
  });
  return result
}
```

DEMO TIME


TESTING

TESTS/HELLOWORLD.JS

```
var HelloWorld = artifacts.require("./HelloWorld.sol");

contract('HelloWorld', function(accounts) {

  it("...should set and get the Hello World value", function() {
    return HelloWorld.deployed().then(function(instance) {
      helloWorldInstance = instance;

      return helloWorldInstance.setHello('This is a hello test', {from: accounts[0]});
    }).then(function() {
      return helloWorldInstance.getHello.call();
    }).then(function(storedData) {
      assert.equal(storedData, 'This is a hello test', 'Uh-oh, it did not set the Hello
    });
  });

});
```

TESTS/HELLOWORLD.JS

```
var HelloWorld = artifacts.require("./HelloWorld.sol");

contract('HelloWorld', function(accounts) {

```

TESTS/HELLOWORLD.JS

```
it("...should set and get the Hello World value", function() {
  return HelloWorld.deployed().then(function(instance) {
    helloWorldInstance = instance;
```

TESTS/HELLOWORLD.JS

```
  return helloWorldInstance.setHello('This is a hello test', {from: accounts[0]});
}).then(function() {
  return helloWorldInstance.getHello.call();
}).then(function(storedData) {
  assert.equal(storedData, 'This is a hello test', 'Uh-oh, it did not set the Hell
});
```

TRUFFLE TEST

```
Using network 'development'.

Compiling ./contracts/HelloWorld.sol...


  Contract: HelloWorld
    ✓ ...should set and get the Hello World value (5128ms)


  1 passing (5s)
```

DEPLOYMENT

DEPLOYMENT

Local → Development → Prod

DEPLOYMENT

Local → Development → Prod

Local → Testnet → Mainnet

DEPLOYMENT

Local → Development → Prod

Local → Testnet → Mainnet

Ropsten

Kovan

Rinkeby

ETHEREUM & REACT

WHAT DID WE LEARN?

Blockchain

Ethereum & Smart Contracts

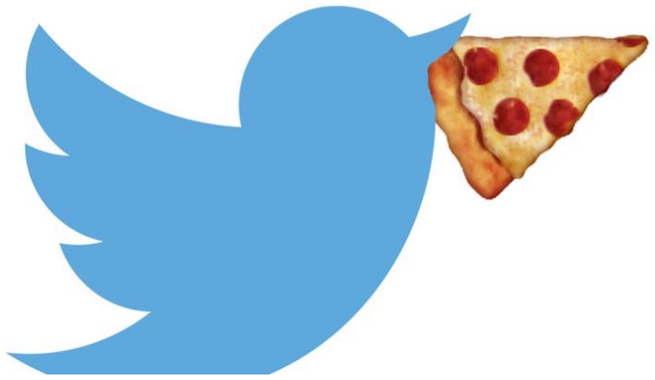
Tools & Frameworks You Need

Basics of Solidity

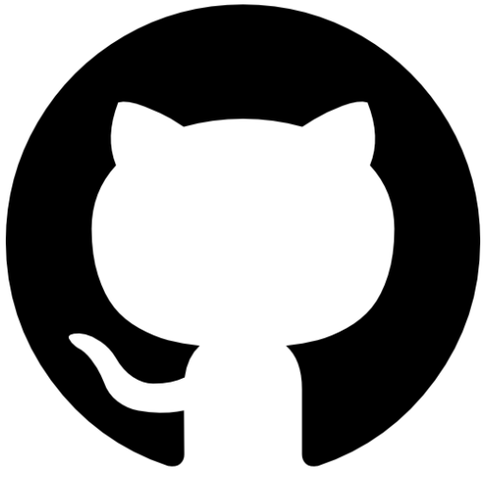
Sample Hello World Project

React Components with Ethereum/web3

Testing



twitter.com/hotpizzas



github.com/ryanhagerty/eth-react

THANK YOU!