

Intro to Blockchain

By: Made Adi

Bali Blockchain Meetup

27 Jan 2018

meetup.com/bali-blockchain/

facebook.com/groups/baliblockchain

Agenda

Blockchain

- Distributed Ledger
- Hashing
- Mining

Ethereum

- Intro to Ethereum
- Distributed App
- Intro of Development on Ethereum

About Me

Director at Spinroam Technology

Computer Engineer by Training

Blockchain Enthusiast

Chat with me

- Handle: @madeadi
- [Bali Blockchain Facebook](#)
- [Tanyadev Slack Channel](#)

Blockchain

Ledger

Ledger

Dave	12.5	
Alice	323	
Bob	6.2	+5.2
Carol	10	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	

Bob has 6.2
Carol owns 10.

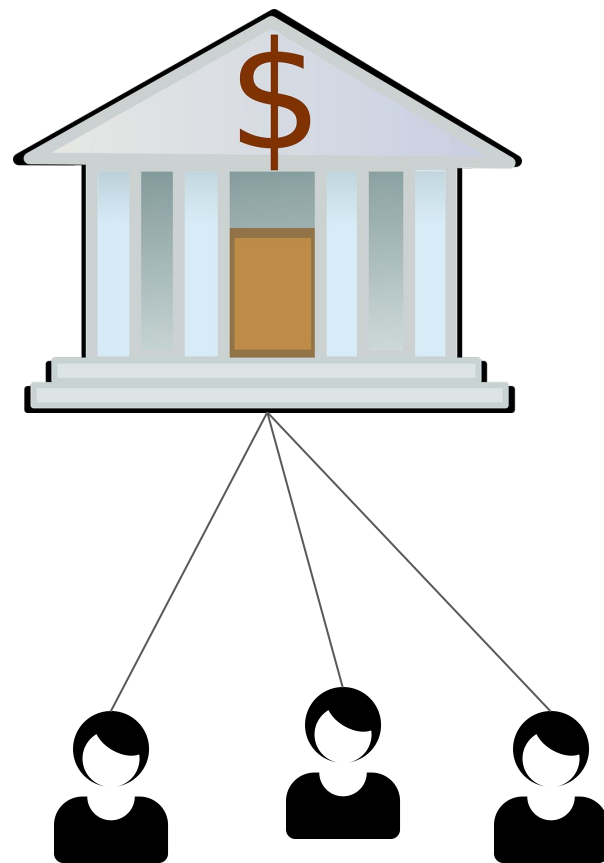
Carol pay Bob 5.2

Final status:

- Bob = $6.2 + 5.2 = 11.4$
- Carol = $10 - 5.2 = 4.8$

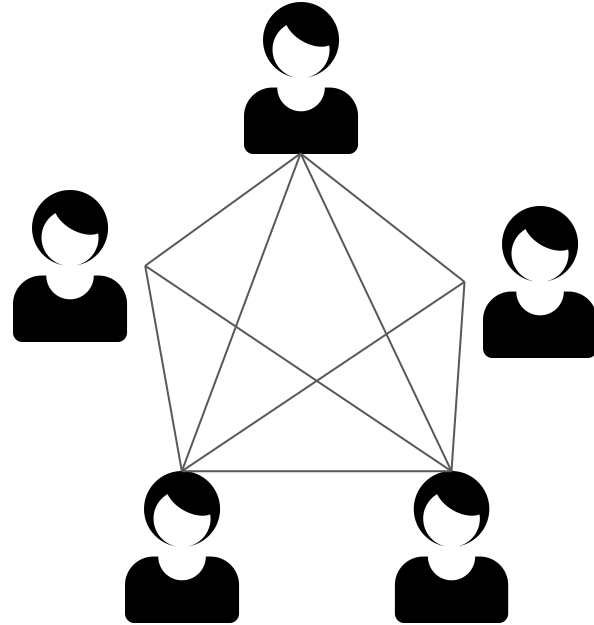
Ledger

Dave	12.5	
Alice	323	
Bob	6.2	+5.2
Carol	10	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	

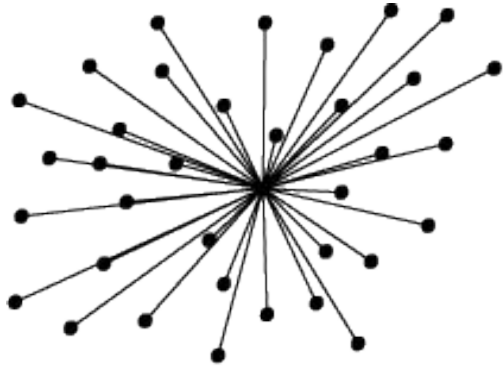


Ledger

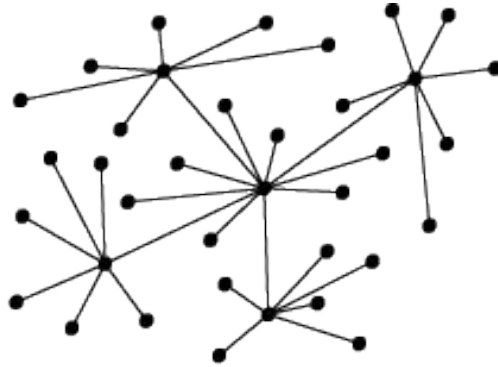
Dave	12.5	
Alice	323	
Bob	6.2	+5.2
Carol	10	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	



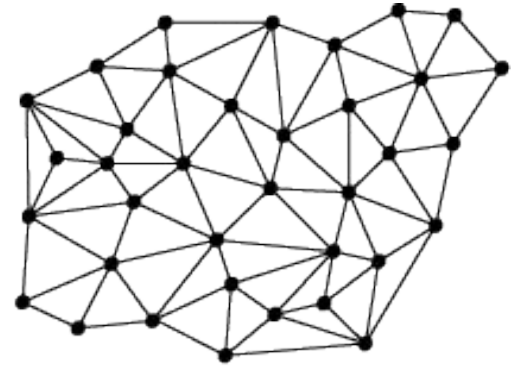
Centralised vs Distributed



centralised



decentralised



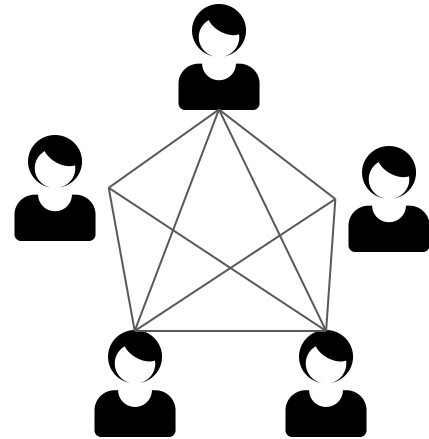
distributed

Ledger

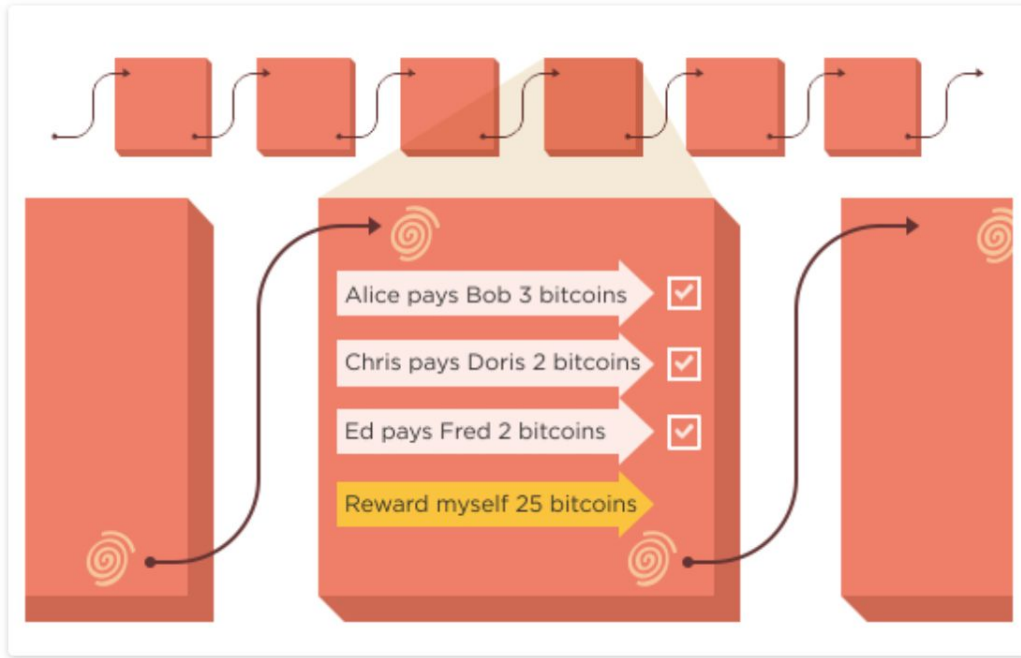
Dave	12.5	
Alice	323	
Bob	6.2	+5.2
Carol	10	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	



New Node



Each node stores the whole history.
In linked list.



- **Blocks** are linked cryptographically
- Network must agree to new blocks
- Each blocks contains **transactions**
- **Mining** is a race to create block (proof of work)
- A miner is **rewarded** when it found a block

Hashing

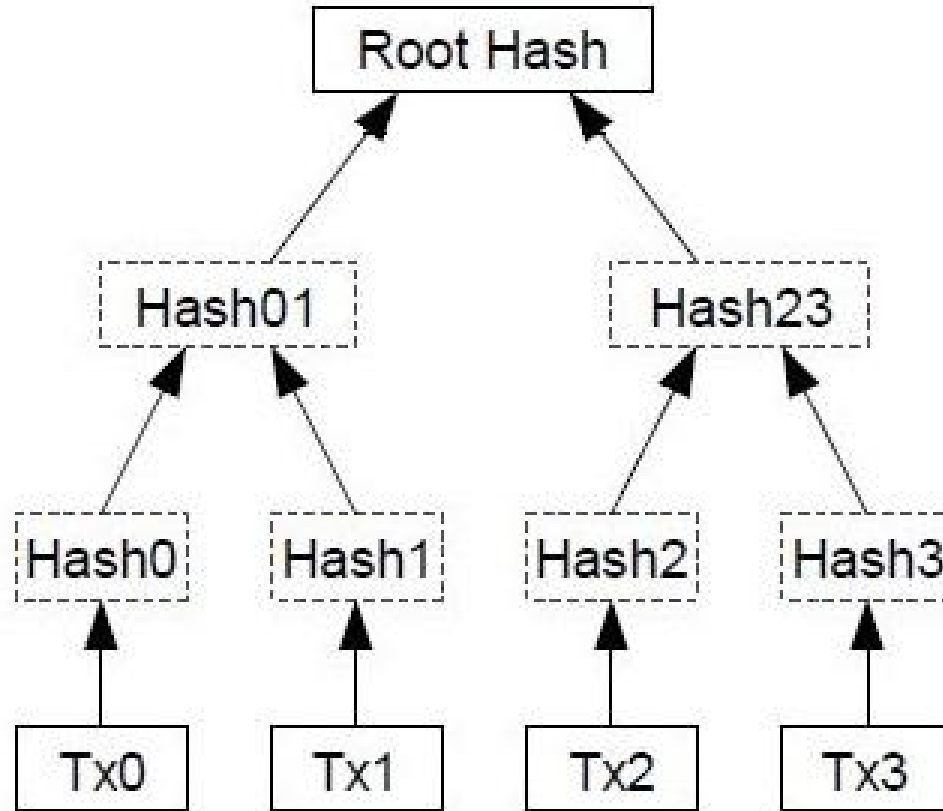
jane@example.com



hash function

8c87b489ce35cf2e2f39f80e282cb2e804932a56a213983eeeb428407d43b52d

Merkle Tree



Mining == Finding a Block

Ledger

Dave	12.5	
Alice	323	
Bob	6.2	+5.2
Carol	10	-5.2

Carols
creates
Transaction

Mempool

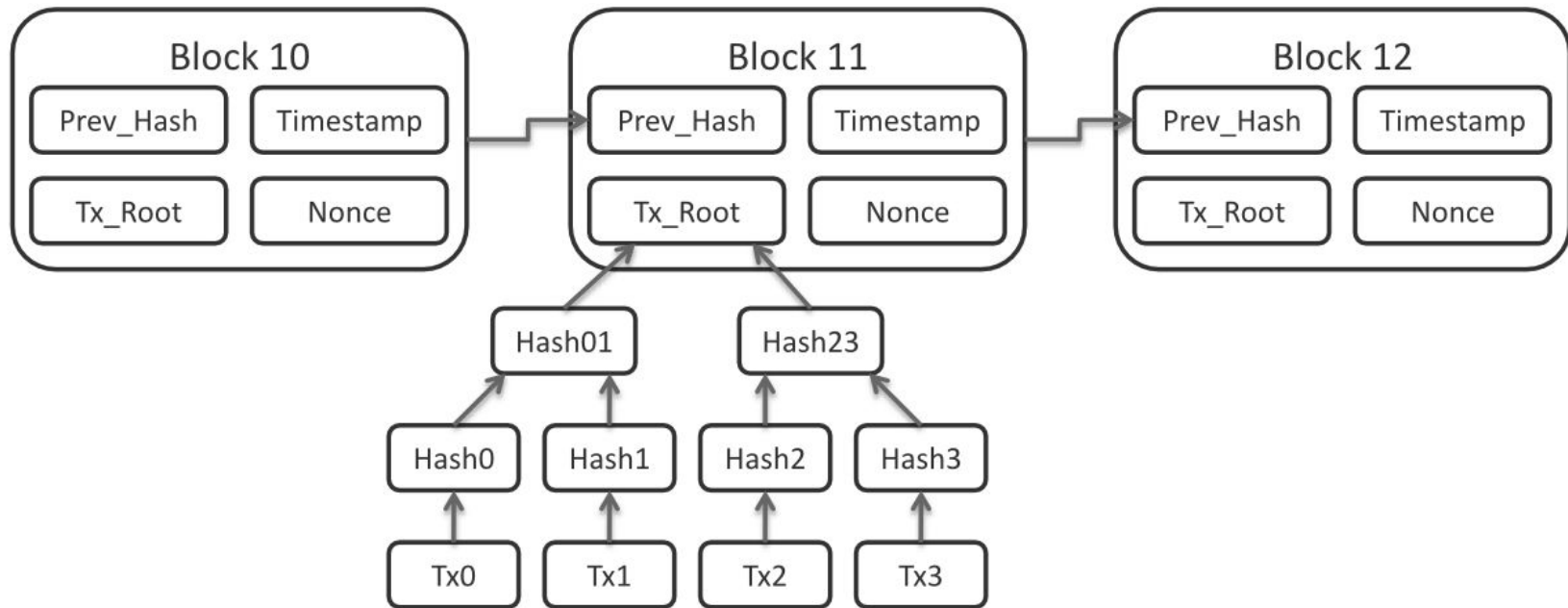
Miner A

Miner B

Miner C

When block is found,
the miner who creates it
will be rewarded.

Found Block



That's Blockchain

1. Distributed ledgers
2. Each node stores the whole history
3. Data structure → linked list + cryptography
4. Blocks contains transactions
5. Miners are racing to find valid blocks and earn rewards

How to cheat?

Statistics <https://blockchain.info/charts>

Some of the Famous Ones

Bitcoin

Ripple

Hyperledger

Litecoin

EOS

IOTA

Ethereum

Steemit

Monero

OmiseGO

Dogecoin

Ethereum

What's Ethereum

- Founded by Vitalik Buterin
- Ethereum Virtual Machine (EVM)
- Ether = token, the fuel
- Gas = pricing mechanism
- Possible to write smart contract

Cryptokitties, <https://www.cryptokitties.co/>



Miaooo

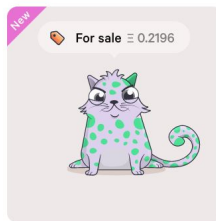
[Copy address](#) · [Settings](#)

All Kitties

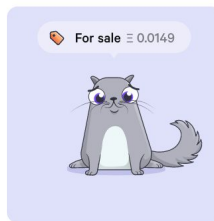
Sort by Youngest first

You don't have any Kitties.

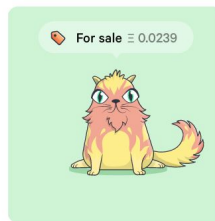
Here are some Kitties that are looking for a new home.



Kitty 483968 · Gen 0 · Fast

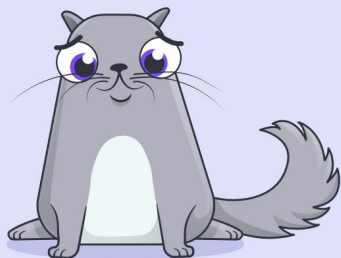


Kitty 483956 · Gen 2 · Swift



Kitty 483954 · Gen 8 ·
Snappy

Cryptokitties, <https://www.cryptokitties.co/>



Wild7/8 Trioculus +Gan...

Kitty 483956 · Gen 2 · Swift Cooldown ⓘ

♥ Like 1

Buy now price

0.0149

Time left

6 days

SoManyKitties!

Owner



Buy now

Bio

Hiya. I'm Wild7/8 Trioculus +GanadoR2. I want to live in a world where people believe that pigs really can fly, they just hide it very well. Some people say I'm the Ross Geller of the group. Let's make magic together.

Cattributes

lemonade

munchkin

shadowgrey

sizzurp

thicccbrowz

totesbasic

whixtensions

icy

Parents





Vitalik Buterin
@VitalikButerin

Follow



I actually like the digital cat games. They illustrate very well that the value of a blockchain extends far beyond applications that would literally get shut down by banks or governments if they did not use one.

alex van de sande @avsa

The hottest thing in ethereum right now is a dumb kittie game. Dumbs isn't meant to be derogatory: we all really needed a break from hundred million dollar ICOs with grandiose claims

2:25 AM - 4 Dec 2017



Udi Wertheimer **[#reckless]** @udiWertheimer · 4 Dec 2017



Did you read the cryptokitty contract? Ownership can change, owners can shut down the system at any time, and replace the contract arbitrarily

5

1

32



Vitalik Buterin @VitalikButerin · 4 Dec 2017



All wise things to do in the first month of a new application's existence. And if there's a serious conflict between owners and community any time soon, I suspect the community will just hard fork the kitties.

10

10

85



Udi Wertheimer **[#reckless]** @udiWertheimer · 4 Dec 2017



Past attempts show that hard forking the kitties can only enjoy partial success (bcash, eth classic). At the very least it's a painful mess. But if you're OK with a forkable, transparent kitty ledger with a centralized point of failure, you don't need a blockchain.

3

2

29



Vitalik Buterin @VitalikButerin · 4 Dec 2017



You don't *need* a blockchain, but it sure is damn convenient.

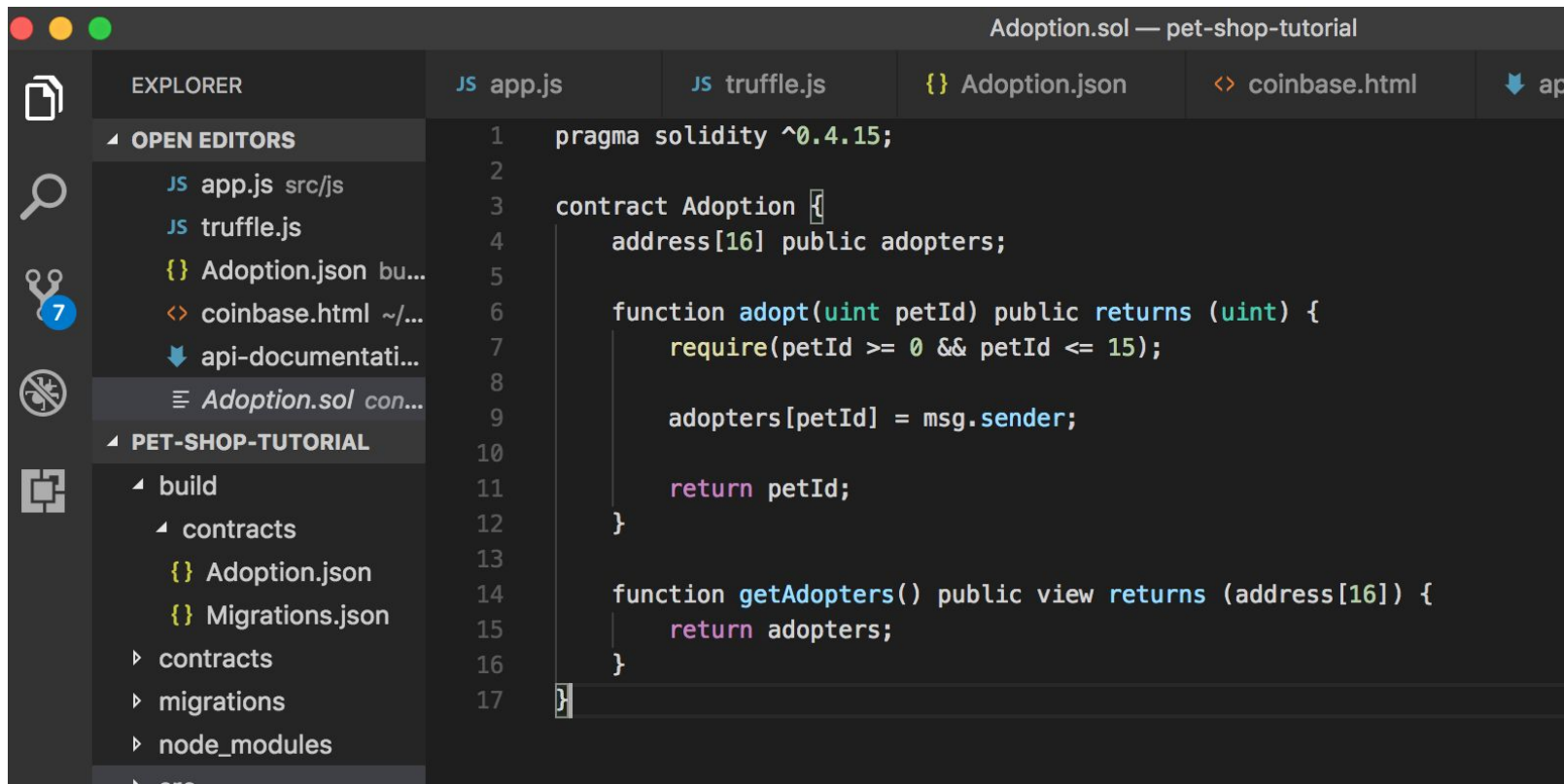
2

5

40

Kickstart Development on Ethereum

Solidity




```
Adoption.sol — pet-shop-tutorial


EXPLORER
└─ OPEN EDITORS
   ├── JS app.js src/js
   ├── JS truffle.js
   ├── {} Adoption.json bu...
   ├── <> coinbase.html ~/...
   ├── ⬇ api-documentati...
   └── ≡ Adoption.sol con...
└─ PET-SHOP-TUTORIAL
   ├── build
   │   └── contracts
   │       ├── {} Adoption.json
   │       └── {} Migrations.json
   ├── contracts
   ├── migrations
   └── node_modules

1  pragma solidity ^0.4.15;
2
3  contract Adoption {
4      address[16] public adopters;
5
6      function adopt(uint petId) public returns (uint) {
7          require(petId >= 0 && petId <= 15);
8
9          adopters[petId] = msg.sender;
10
11         return petId;
12     }
13
14     function getAdopters() public view returns (address[16]) {
15         return adopters;
16     }
17 }
```

Truffle: Ethereum Framework





TRUFFLE

DOCS TUTORIALS BOXES BLOG SUPPORT  GANACHE

YOUR ETHEREUM SWISS ARMY KNIFE

Truffle is the most popular development framework for Ethereum with a mission to make your life a whole lot easier.

★ Star 4,196  Fork 528  gitter [join chat](#)

INSTALL VIA NPM

```
$ npm install -g truffle
```

Requires NodeJS 5.0+. Works on Linux, macOS, or Windows.

[DOCUMENTATION](#) [TUTORIALS](#)

Don't know where to start? Get yourself a [Truffle Box!](#)

Blockchain: Ganache

ACCOUNTS

BLOCKS

TRANSACTIONS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK
0

GAS PRICE
20000000000

GAS LIMIT
6721975

NETWORK ID
5777

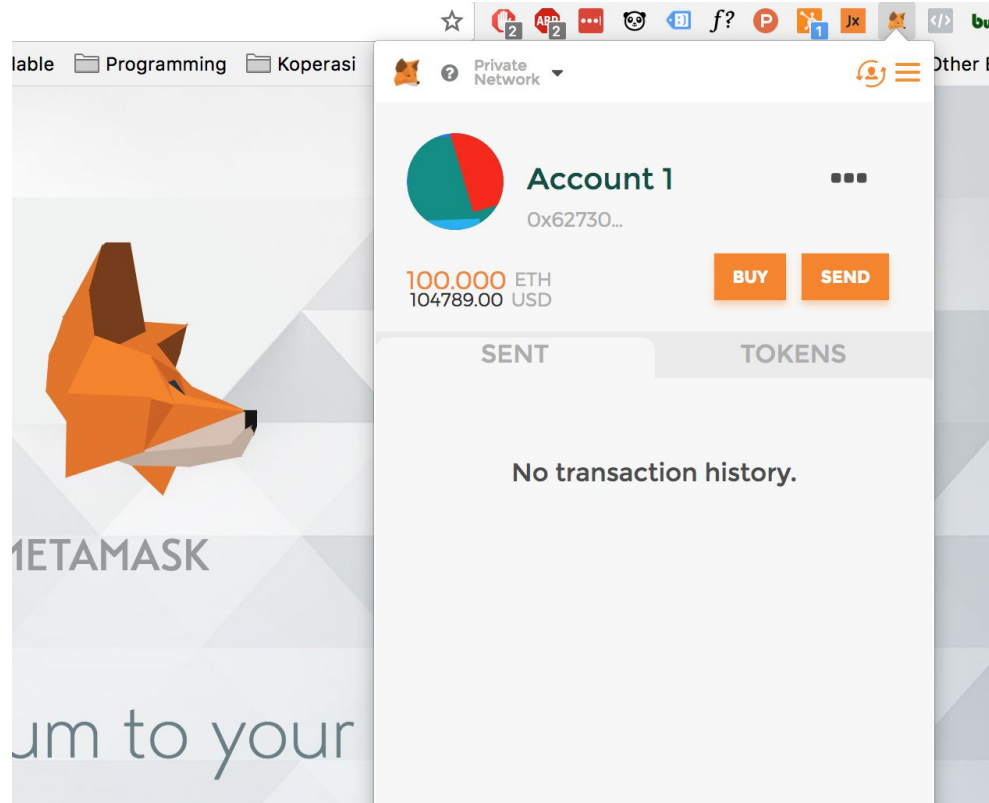
RPC SERVER
HTTP://127.0.0.1:7545

MINING STATUS
AUTOMINING

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

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

Interaction: Metamask



Frontend

Nodejs

Laravel

etc

Conclusion

Blockchain

- Distributed Ledger
- Hashing
- Mining

Ethereum

- Intro to Ethereum
- Example of Dapp
- Start development on Ethereum

Links

Go to Google!

Tutorial to develop on Ethereum

<http://truffleframework.com/tutorials/pet-shop>