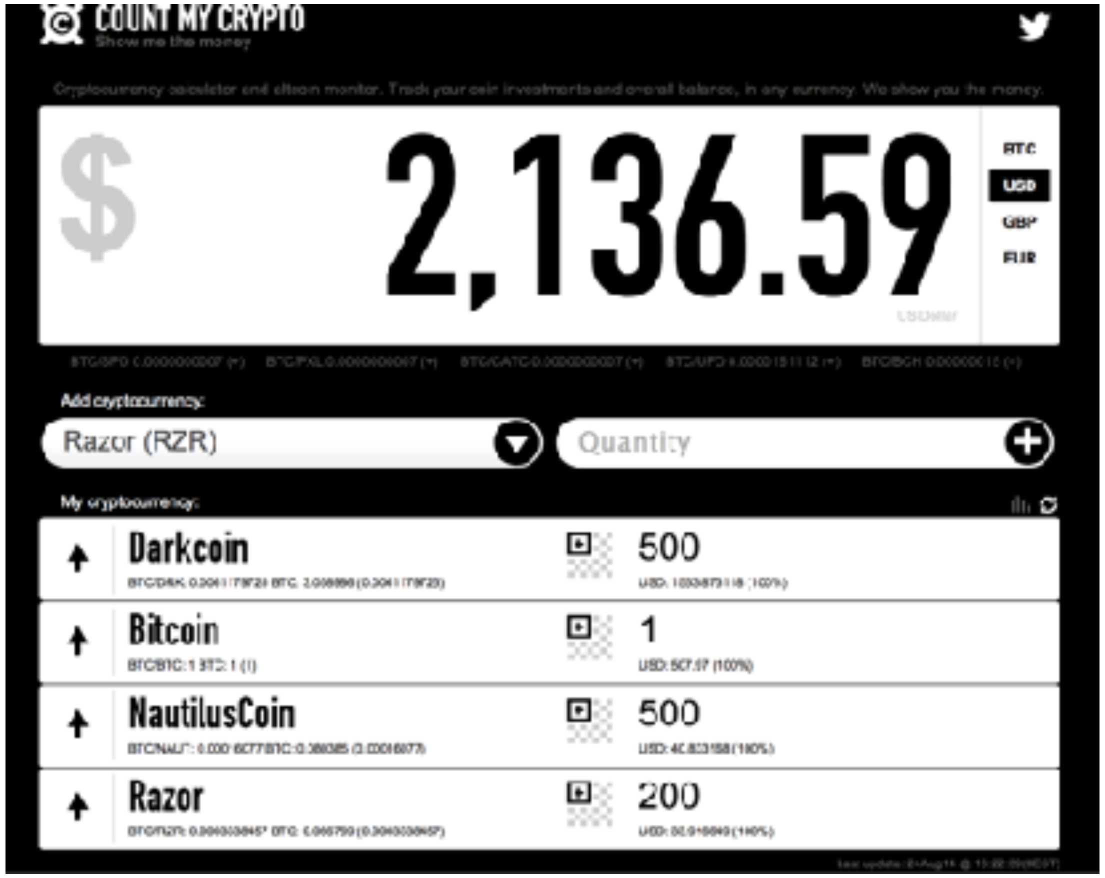
Public blockchains

What could possibly go wrong?

Rhian Lewis @rhian_is

About me

- Test automation engineer
- Co-developer of Count My Crypto
- Founder of London Women in Bitcoin
- Teacher on the B9Lab.com Ethereum QA Engineer course
- Writer about blockchain at medium.com/@rhian_is



COUNT MY CRYPTO
Show me the money

Cryptocurrency calculator and altcoin monitor. Track your coin investments and overall balance, in any currency. We show you the money.

$ 2,136.59

USDollar

[illegible]

Add cryptocurrency:

Razor (RZR) ▼ | Quantity ⊕

My cryptocurrency:

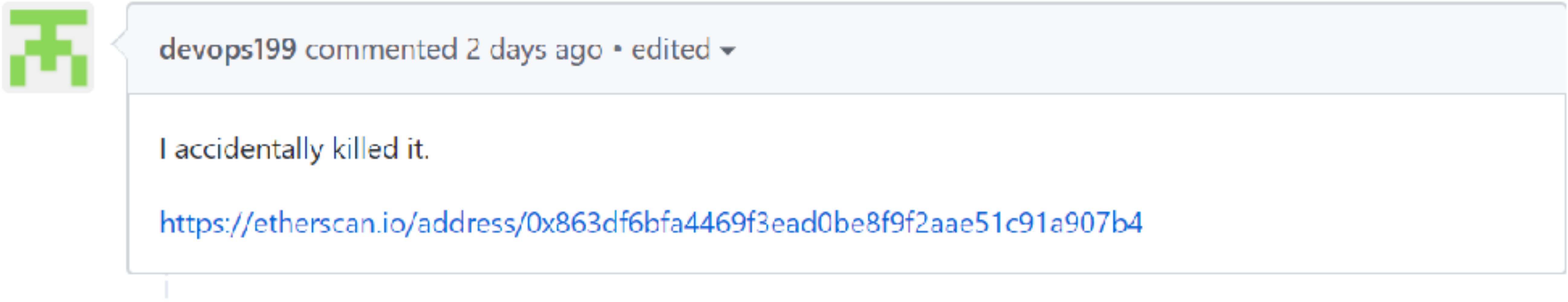
↑	**Darkcoin** [illegible]	500 [illegible]
↑	**Bitcoin** BTC/BTC: 1 BTC: 1 (1)	1 USD: 567.57 (100%)
↑	**NautilusCoin** [illegible]	500 [illegible]
↑	**Razor** [illegible]	200 [illegible]

[illegible]

Themes in this talk

- Why should you be concerned about this technology
- How blockchains work
- Differences between private and public blockchains
- Examples of protocols
- How to test and testing challenges
- Examples of vulnerabilities and how to mitigate
- Tools and tips

November 6, 2017



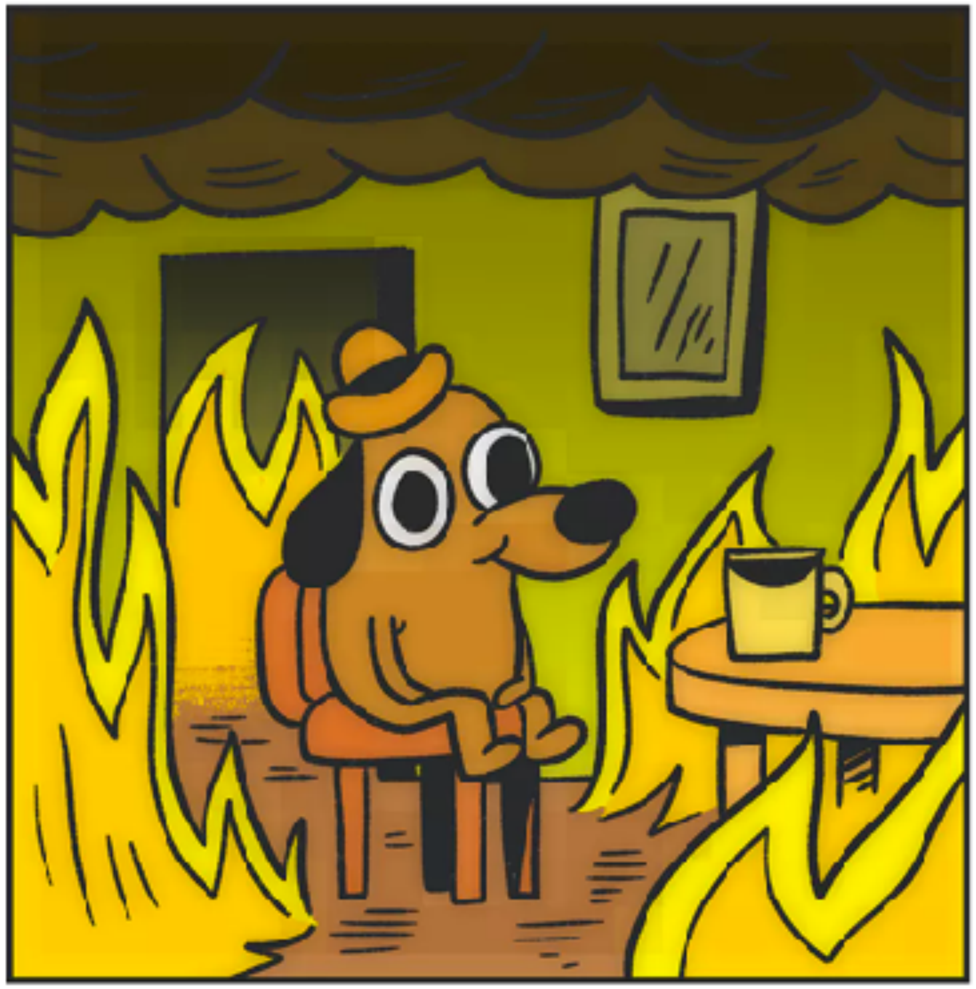
devops199 commented 2 days ago • edited

I accidentally killed it.

https://etherscan.io/address/0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4

Imagine this

- Your code is on thousands of computers over the world
- Hundreds of millions of other people’s money is locked up in their accounts
- YOU CANNOT REDEPLOY!
- THERE IS NO FIX FOR THIS!
- Everyone can see the issue that caused it



To be continued….

Why care about blockchains?

Nestlé
SAMSUNG
f
MITSUBISHI
MOTORS
Walmart
Microsoft
Goldman
Sachs
IBM
aws
AMERICAN
EXPRESS
TOYOTA
阿里巴巴
Alibaba.com
Ford
MAERSK
WELLS
FARGO
Allianz
HSBC
BANK OF ENGLAND

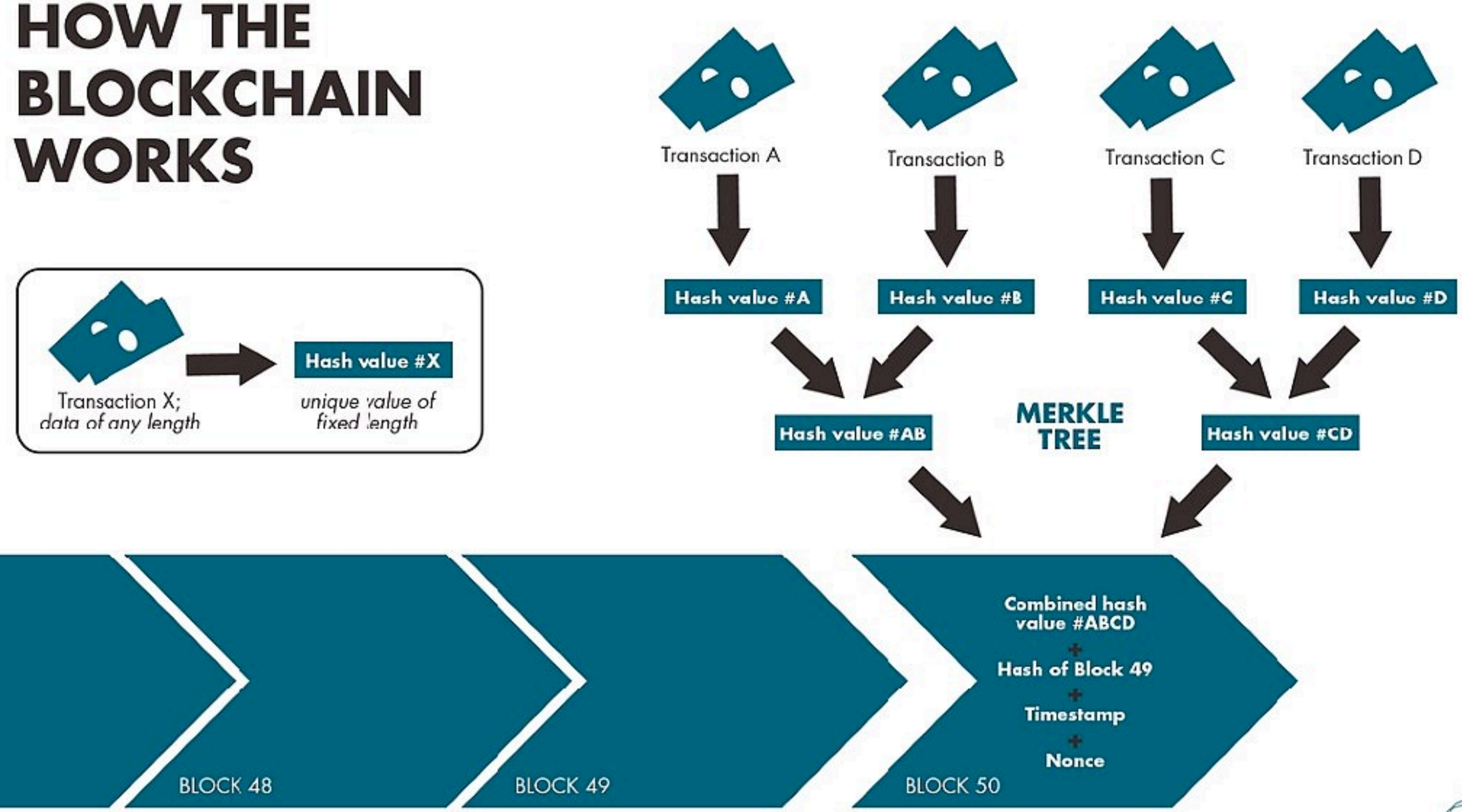
Blockchain definition: 1

- Data structure spread across many nodes
- If public, anyone can download and run the software and participate in maintaining the record
- If private, runs on a limited number of nodes to which are controlled and agreed

Blockchain definition: 2

- Immutable data structure because all transactions are bundled into blocks which are cryptographically linked together from the beginning of time
- Single source of truth
- Transparent and decentralised, with no down time

HOW THE BLOCKCHAIN WORKS



Transaction X; *data of any length*

Hash value #X

unique value of fixed length

Transaction A

Transaction B

Transaction C

Transaction D

Hash value #A

Hash value #B

Hash value #C

Hash value #D

Hash value #AB

MERKLE TREE

Hash value #CD

BLOCK 48

BLOCK 49

BLOCK 50

Combined hash value #ABCD
+
Hash of Block 49
+
Timestamp
+
Nonce

Reproduction of an original figure in "The Great Chain of Being Sure About Things" by the Economist

BITCOIN • DIGITAL • DECENTRALIZED • PEER TO PEER
999 FINE COPPER

BLOCKCHAINS: NOT JUST FOR CRYPTOCURRENCIES

Examples of protocols

- Bitcoin - Proof of Work / C++ codebase / clients in many languages. No specific smart contract functionality

- Ethereum - Proof of Work, moving to Proof of Stake / EVM has four main client implementations / smart contracts written in Solidity (some similarities to JavaScript)

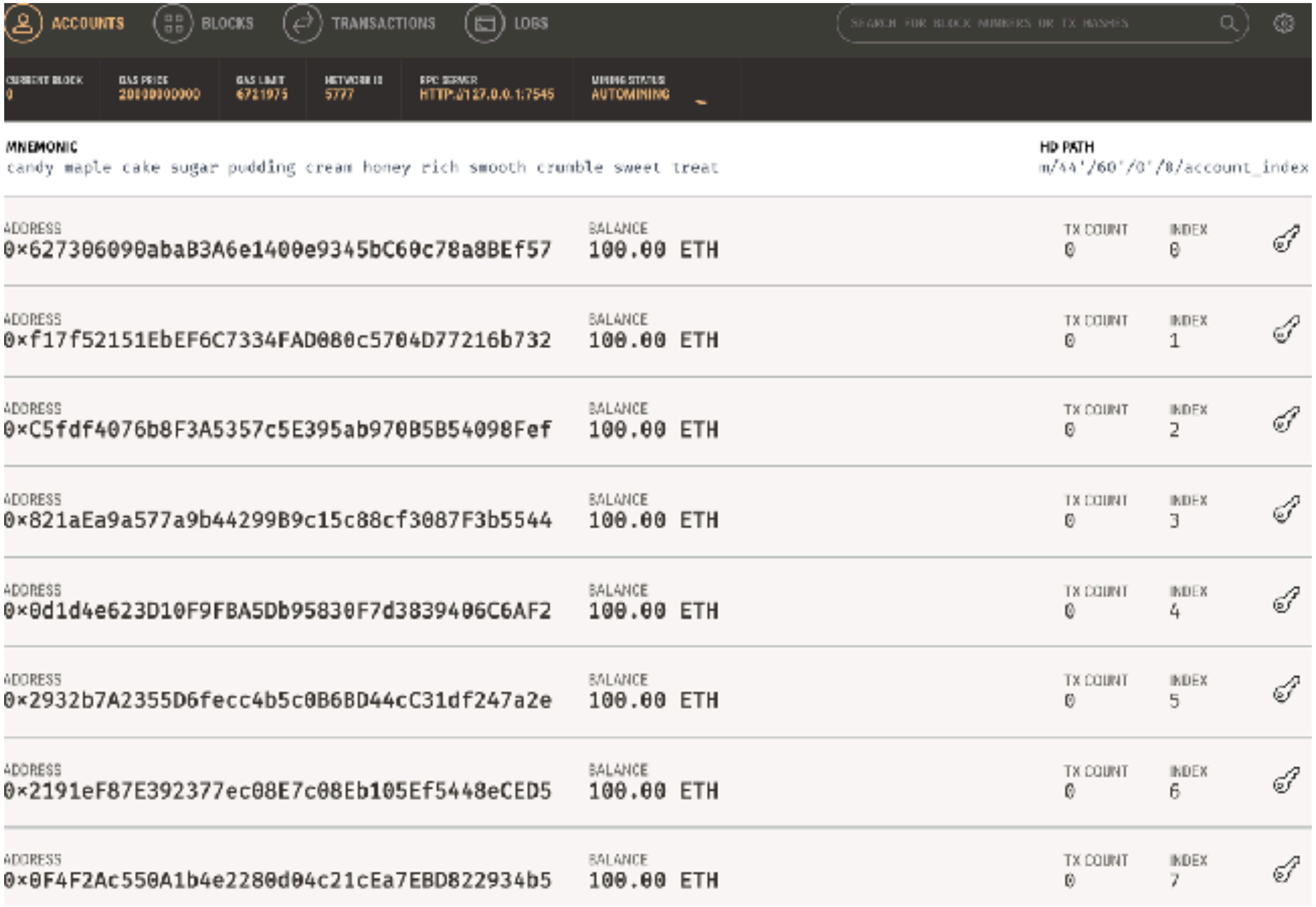
- Hyperledger - open source blockchains and tools / Hyperledger Fabric chaincode can be written in Go or JavaScript

- EOS - delegated proof of stake / smart contracts written in C++, compiled to Web Assembly

Difference between public and private chains

- Need permission to join a private chain
- Transactions are validated on public chains by members of the public who are rewarded for their efforts
- Public chains are more transparent
- Private chains have a purpose but cannot solve the trust issue
- Hybrids where private Proof of Authority chains link to a larger public chain

Public	Consortium	Private
Anyone can join	Permissioned	Permissioned
Open source	Open source or proprietary	Open source or proprietary
Thousands or even millions of participants	Limited number of participants	Limited number of participants
Likely to have a token (currency)	Unlikely to have a token (currency)	Unlikely to have a token (currency)
Governance by consensus	Equal weight to participants	Owner can set the rules



CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
0	20000000000	6721975	5777	HTTP://127.0.0.1:7545	AUTOMINING

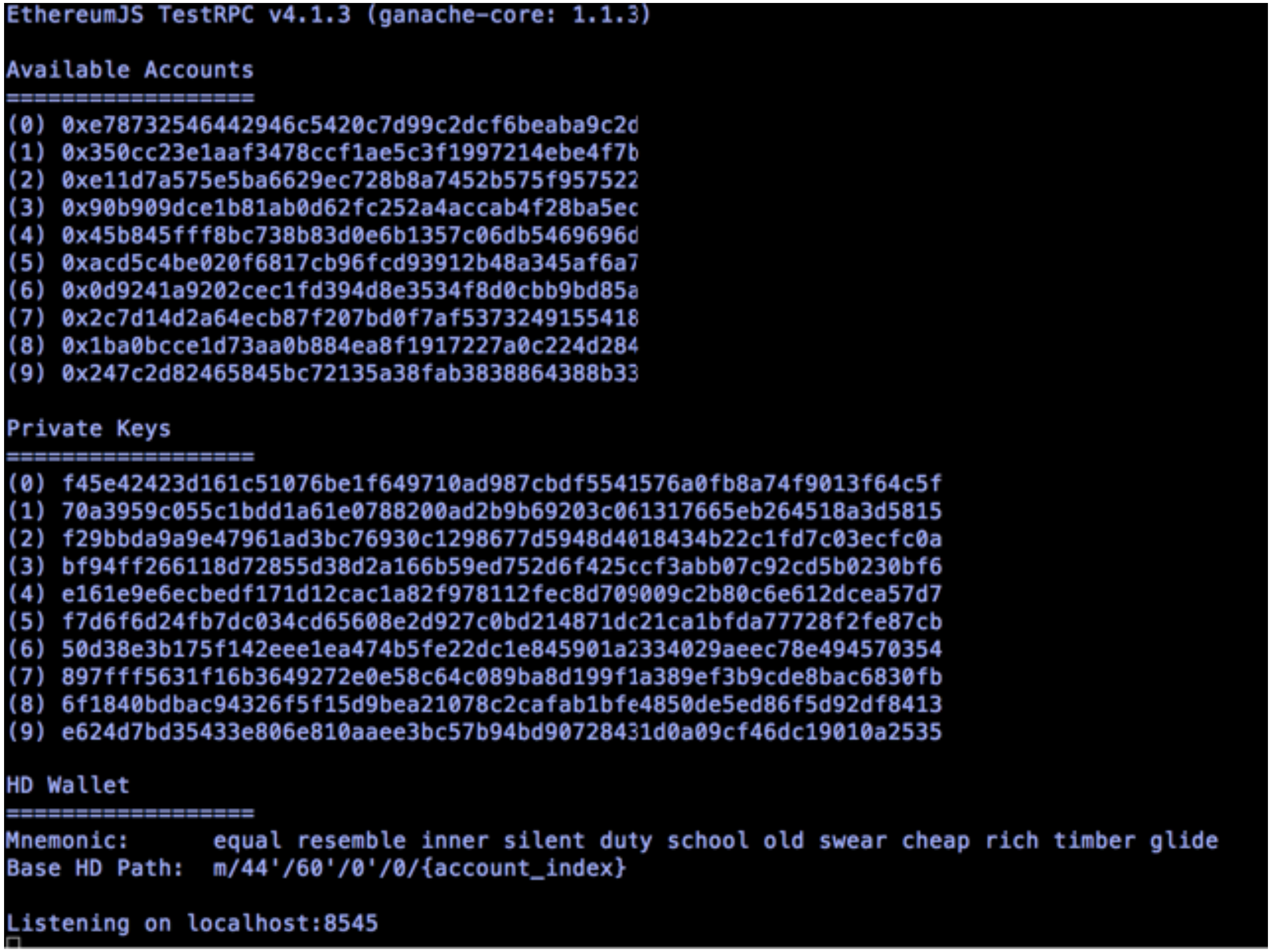
MNEMONIC
candy maple cake sugar pudding cream honey rich smooth crumble sweet treat

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

ADDRESS	BALANCE	TX COUNT	INDEX
0x627306090abaB3A6e1400e9345bC60c78a8BEf57	100.00 ETH	0	0
0xf17f52151EbEF6C7334FAD080c5704D77216b732	100.00 ETH	0	1
0xC5fdf4076b8F3A5357c5E395ab970B5B54098Fef	100.00 ETH	0	2
0x821aEa9a577a9b44299B9c15c88cf3087F3b5544	100.00 ETH	0	3
0x0d1d4e623D10F9FBA5Db95830F7d3839406C6AF2	100.00 ETH	0	4
0x2932b7A2355D6fecc4b5c0B6BD44cC31df247a2e	100.00 ETH	0	5
0x2191eF87E392377ec08E7c08Eb105Ef5448eCED5	100.00 ETH	0	6
0x0F4F2Ac550A1b4e2280d04c21cEa7EBD822934b5	100.00 ETH	0	7

Mock blockchains: 1

This is an example of a virtual Ethereum node, using a tool called Ganache



```
EthereumJS TestRPC v4.1.3 (ganache-core: 1.1.3)

Available Accounts
==================
(0) 0xe78732546442946c5420c7d99c2dcf6beaba9c2d
(1) 0x350cc23e1aaf3478ccf1ae5c3f1997214ebe4f7b
(2) 0xe11d7a575e5ba6629ec728b8a7452b575f957522
(3) 0x90b909dce1b81ab0d62fc252a4accab4f28ba5ec
(4) 0x45b845fff8bc738b83d0e6b1357c06db5469696d
(5) 0xacd5c4be020f6817cb96fcd93912b48a345af6a7
(6) 0x0d9241a9202cec1fd394d8e3534f8d0cbb9bd85a
(7) 0x2c7d14d2a64ecb87f207bd0f7af5373249155418
(8) 0x1ba0bcce1d73aa0b884ea8f1917227a0c224d284
(9) 0x247c2d82465845bc72135a38fab3838864388b33

Private Keys
==================
(0) f45e42423d161c51076be1f649710ad987cbdf5541576a0fb8a74f9013f64c5f
(1) 70a3959c055c1bdd1a61e0788200ad2b9b69203c061317665eb264518a3d5815
(2) f29bbda9a9e47961ad3bc76930c1298677d5948d4018434b22c1fd7c03ecfc0a
(3) bf94ff266118d72855d38d2a166b59ed752d6f425ccf3abb07c92cd5b0230bf6
(4) e161e9e6ecbedf171d12cac1a82f978112fec8d709009c2b80c6e612dcea57d7
(5) f7d6f6d24fb7dc034cd65608e2d927c0bd214871dc21ca1bfda77728f2fe87cb
(6) 50d38e3b175f142eee1ea474b5fe22dc1e845901a2334029aeec78e494570354
(7) 897fff5631f16b3649272e0e58c64c089ba8d199f1a389ef3b9cde8bac6830fb
(8) 6f1840bdbac94326f5f15d9bea21078c2cafab1bfe4850de5ed86f5d92df8413
(9) e624d7bd35433e806e810aaee3bc57b94bd90728431d0a09cf46dc19010a2535

HD Wallet
==================
Mnemonic:      equal resemble inner silent duty school old swear cheap rich timber glide
Base HD Path:  m/44'/60'/0'/0/{account_index}

Listening on localhost:8545
```

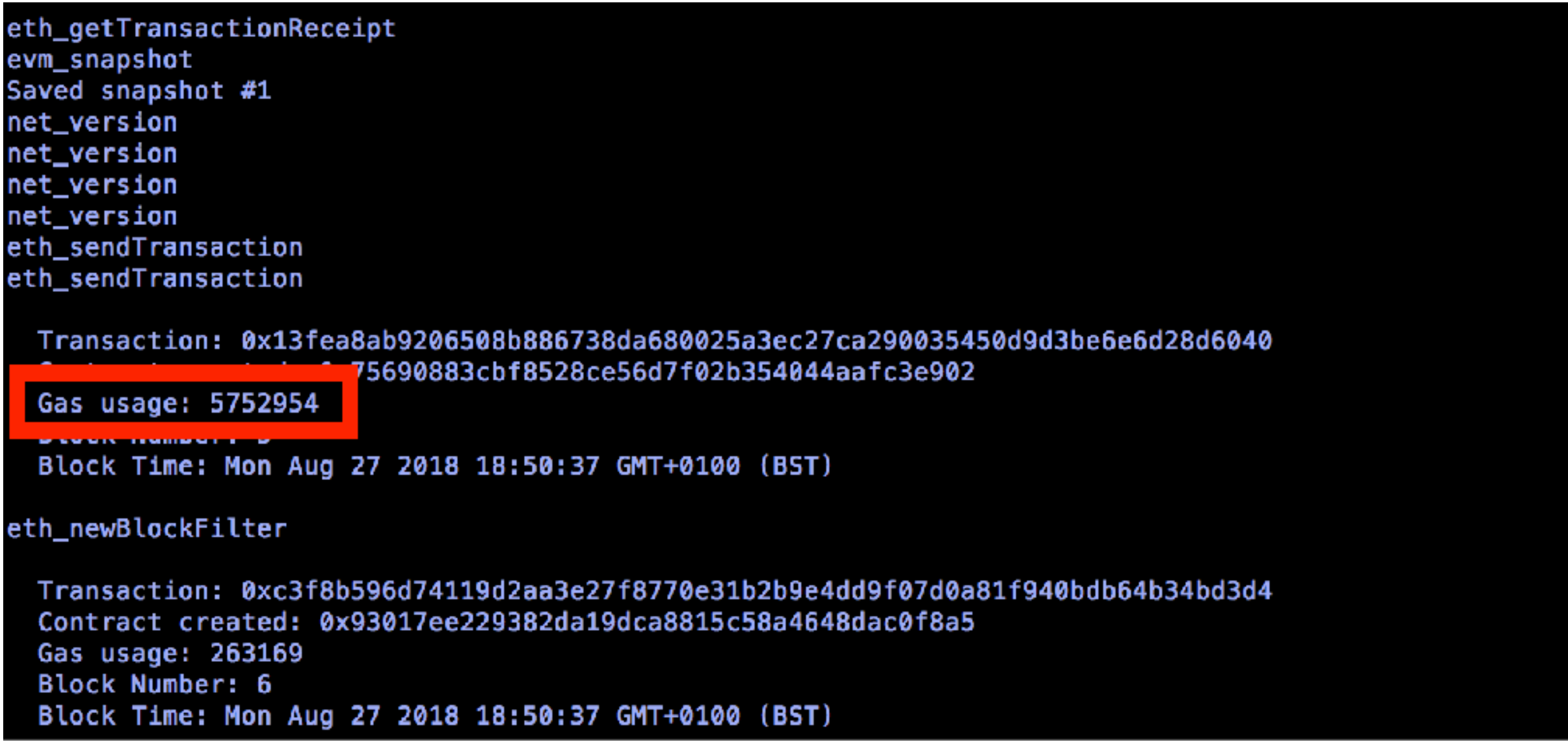
Mock blockchains: 2

You can interact with Ganache via the user interface (previous slide) or via the command line

Transaction Fees

- Not an issue for private chains
- Public chains like Bitcoin and Ethereum charge a transaction fee, which fluctuates
- Testing that the business model functions with fees at different levels is crucial
- For example, micropayments do not make sense if you pay $1 for every transaction

Testing transaction fees



```
eth_getTransactionReceipt
evm_snapshot
Saved snapshot #1
net_version
net_version
net_version
net_version
eth_sendTransaction
eth_sendTransaction

  Transaction: 0x13fea8ab9206508b886738da680025a3ec27ca290035450d9d3be6e6d28d6040
  Contract created: 0x75690883cbf8528ce56d7f02b354044aafc3e902
  Gas usage: 5752954
  Block Number: 5
  Block Time: Mon Aug 27 2018 18:50:37 GMT+0100 (BST)

eth_newBlockFilter

  Transaction: 0xc3f8b596d74119d2aa3e27f8770e31b2b9e4dd9f07d0a81f940bdb64b34bd3d4
  Contract created: 0x93017ee229382da19dca8815c58a4648dac0f8a5
  Gas usage: 263169
  Block Number: 6
  Block Time: Mon Aug 27 2018 18:50:37 GMT+0100 (BST)
```

Vulnerability: Re-entrance

```
pragma solidity ^0.4.8;
contract HoneyPot {
  mapping (address => uint) public balances;
  function HoneyPot() payable {
    put();
  }
  function put() payable {
    balances[msg.sender] = msg.value;
  }
  function get() {
    if (!msg.sender.call.value(balances[msg.sender])()) {
      throw;
    }
      balances[msg.sender] = 0;
  }
  function() {
    throw;
  }
}
```

Vulnerability: Ownership

```
// constructor is given number of sigs required to do protected
"onlymanyowners" transactions
// as well as the selection of addresses capable of confirming
them.
function multiowned(address[] _owners, uint _required) {
  m_numOwners = _owners.length + 1;
  m_owners[1] = uint(msg.sender);
  m_ownerIndex[uint(msg.sender)] = 1;
  for (uint i = 0; i < _owners.length; ++i) {
    m_owners[2 + i] = uint(_owners[i]);
    m_ownerIndex[uint(_owners[i])] = 2 + i;
  }
  m_required = _required;
}
```

Vulnerability: Initialisation

- A smart contract that generates addresses for many users needs to let the blockchain know about these addresses
- If you display the address before the blockchain transaction has been mined, there is a risk that a user might send money to it
- **DISASTER!**
- If a user tries to send money to a non-existent address, the cash will be lost for ever

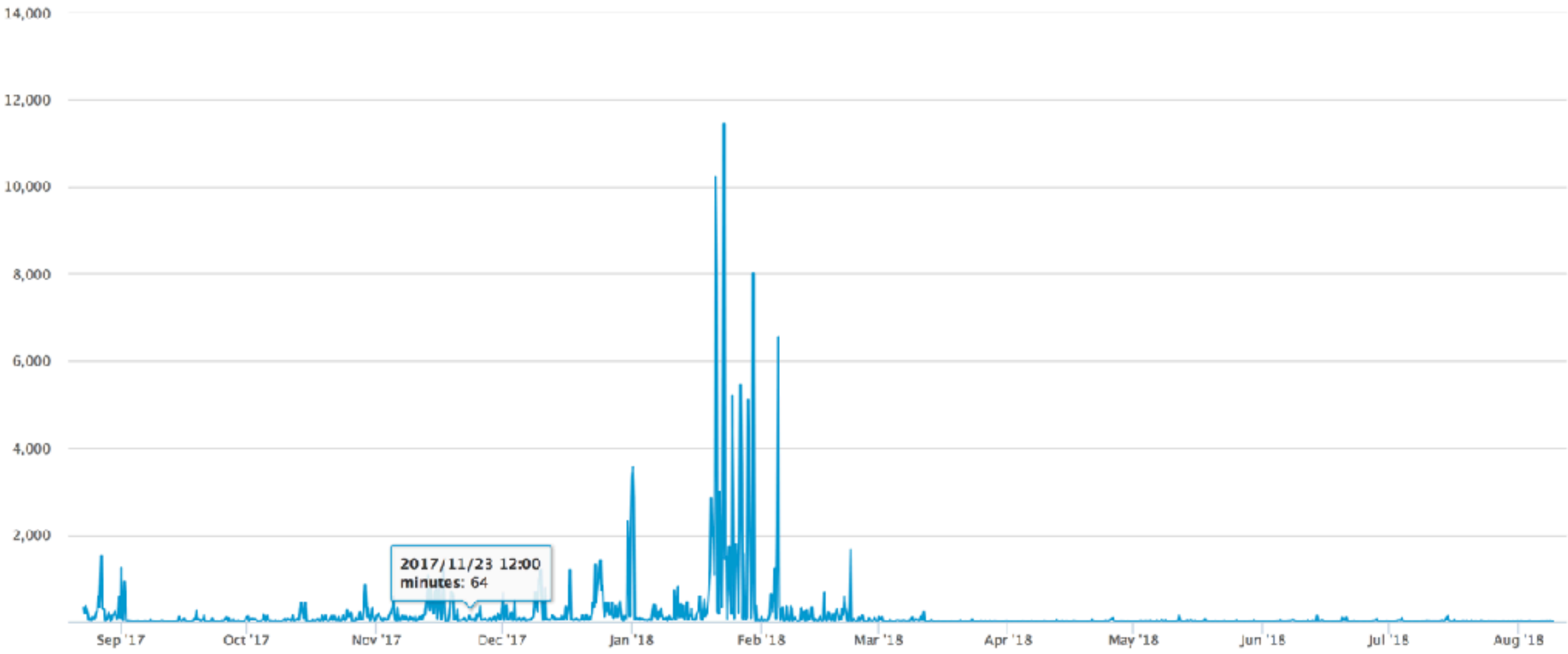
Not just contracts

- Decentralised applications are more than just a blockchain
- Focus on smart contracts can mean other vulnerabilities are neglected
- Augur framejacking vulnerability
- Nano hack where checks performed on client side only - users could run JavaScript locally

BITCOIN CRIME FEBRUARY 15, 2018 18:09

Questions Mount Over $170 Million BitGrail ‘Hack’

Performance and predictability



The y axis shows transaction confirmation times on the Ethereum blockchain, in minutes

Automation and Tools

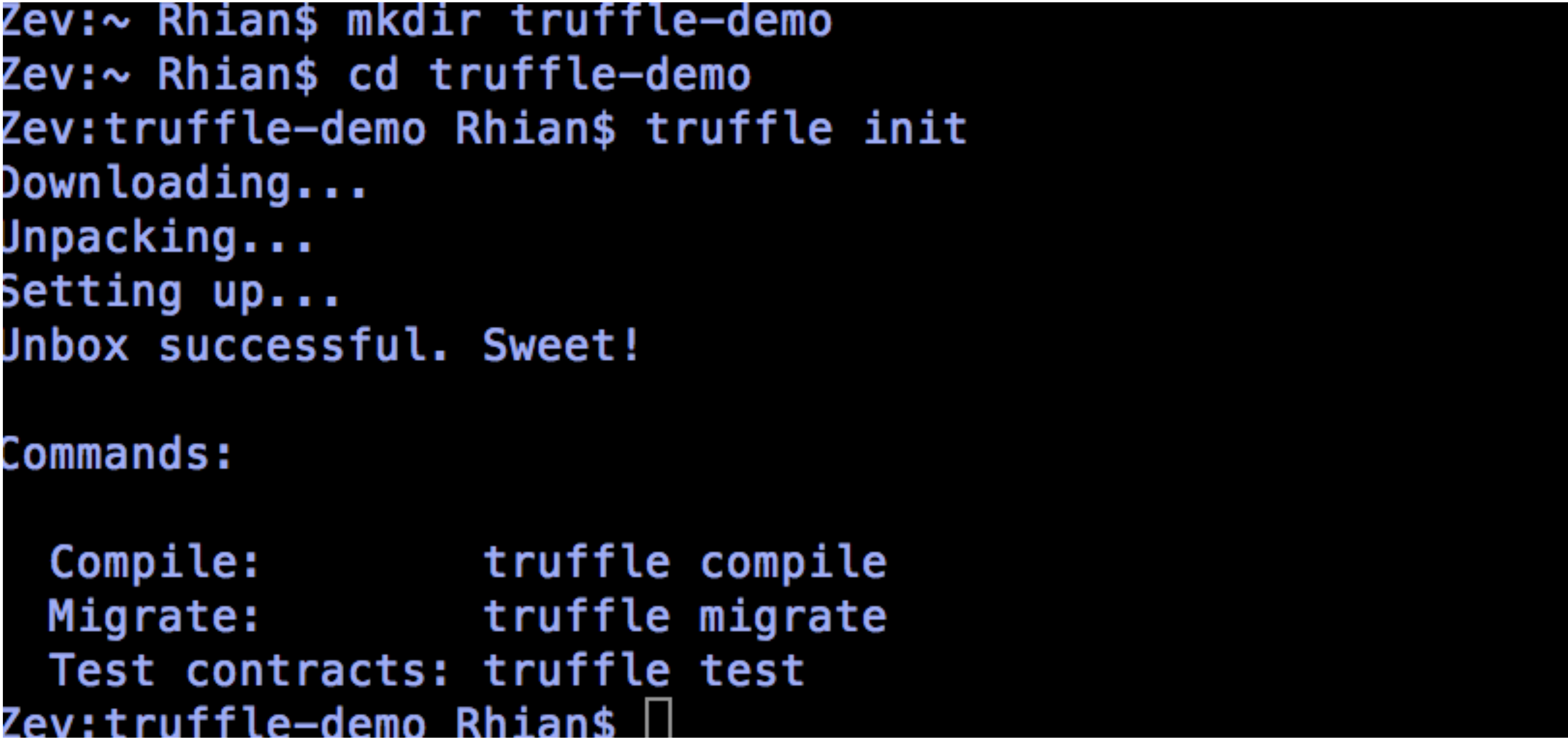
- Two useful tools for Ethereum: Truffle framework and Open Zeppelin libraries

- Truffle gives inbuilt test framework and a mock local blockchain

- Can be difficult to automate tests on public testnets because of latency and need to acquire test currencies

- Most people run tests against local nodes only

Truffle is easy to use!



```
Zev:~ Rhian$ mkdir truffle-demo
Zev:~ Rhian$ cd truffle-demo
Zev:truffle-demo Rhian$ truffle init
Downloading...
Unpacking...
Setting up...
Unbox successful. Sweet!

Commands:

  Compile:        truffle compile
  Migrate:        truffle migrate
  Test contracts: truffle test
Zev:truffle-demo Rhian$ 
```

Bug Bounties

- The opportunity to hone your testing skills
- The kudos of being able to add your discoveries to your resumé
- The chance to earn Ether or other tokens

- https://bounty.ethereum.org/
- https://hackenproof.com/

Thank you!

- In this talk we have learned:
- Why blockchains are powerful
- Why you should consider using a public blockchain
- Why public blockchains are dangerous
- What you can do to mitigate this by testing
- How you can get involved