# Ethereum in Enterprise Context

***Blockchain Innovation Week***

Djuri Baars – May 25th, 2018

Rabobank

# Introduction



we.trade
more trust. more trade.

ENTERPRISE
ETHEREUM
ALLIANCE

**Djuri Baars**

**Lead Blockchain Team**

*Djuri.Baars@rabobank.nl*

# Blockchain Acceleration Lab

Rabobank

Support organization with everything related to blockchain


# Our journey

Rabobank

2014 — 2015 — 2016 — 2017

ripple

Tradle

we.trade
more trust. more trade.

ENTERPRISE ETHEREUM ALLIANCE

TECH RUPTION

BC3 Dutch Blockchain Coalition
connect and create

Rabobank

**100+**

use cases

**10+**

proof-of-concepts
per year

**1**

In production
(summer 2018)

Rabobank


www.we-trade.com / blockchain@rabobank.nl

# Blockchain Innovation Conference

Rabobank

BLOCKCHAIN INNOVATION CONFERENCE

**"Beyond Proof of Concepts to real world productions"**
June 7th, 2018
Rabobank Utrecht (NL)

Students who are willing to help half a day can attend for free!

With talks by:
Arthur Camara (Cryptokitties)
Wiebe Draijer (Chairman of the Board)
Dutch Central Bank
World Bank
And **50+** others

**blockchaininnovationconference.com**
**+ bit.ly/BIC18**

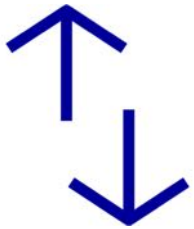
Get a 25% discount with code **"Rabobank"**
Less than 100 tickets left!

# Challenges (recap from Mark's talk)

Rabobank

Scalability


Privacy



Interoperability

Finality

Governance

# Work on challenges together

*because blockchain is all about collaboration*

Rabobank

BC3 Dutch Blockchain Coalition
connect and create

TECH RUPTION

ENTERPRISE ETHEREUM ALLIANCE

Dutch Payments Association

KYC platform

we.trade
more trust. more trade.

BLOCKCHAIN PROJECTS
DUTCH GOVERNMENT

Sustainable Pay Per Use

Identities

Value Transfers

Signing (e.g. documents)

# Enterprise Ethereum Alliance


joined in May ’17 - currently **500+** members

Multiple working groups including:
- Supply Chain WG
- Insurance WG
- Standards WG
- Quorum WG

Including:




ENTERPRISE ETHEREUM ALLIANCE

# The Enterprise Ethereum Architecture Stack

Providing the building blocks for the first, open-source, standards-based specification to accelerate the adoption of Enterprise Ethereum

Global Developer Community

Interoperability

Multiple Vendors of Choice

Testing & Certification

Learn more and view the stack at entethalliance.org/resources

# Enterprise Ethereum Alliance (2)

Rabobank

Their most recent work (May 16th):


*By using the EEA Specification, Ethereum developers can write code that enables interoperability, motivating enterprise customers to select EEA specification-based solutions over proprietary offerings.*

# Quorum?


- Fork of Ethereum by JP Morgan Chase (september 2016)
- Surprisingly well documented and testable !
- Permissioned version of Ethereum which supports:
  - Governance
  - Confidentiality
  - Alternative Consensus Mechanisms

# Hybrid: public and private


***Public tx***

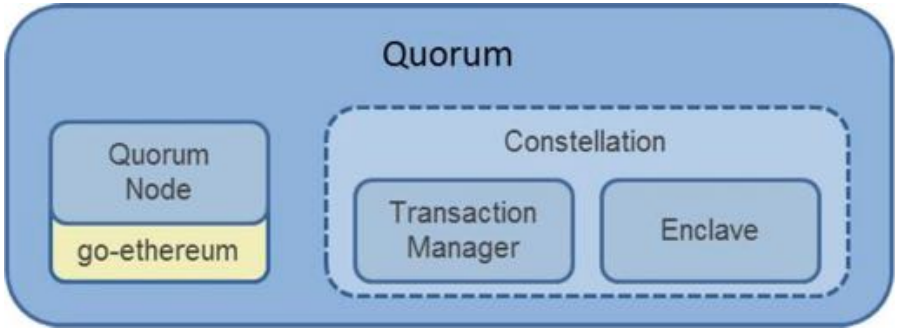
- Broadcast to everyone on (permissioned) network (for now)
- Like "normal" Ethereum but free
  - Does not use ETH
  - Uses gas, but gas is free

***Private tx***

- Sent between specified recipients
- Hash of private tx still included on shared public state

# Components

Rabobank



# Quorum Node

Rabobank

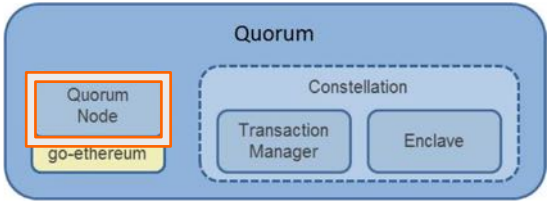
Lightweight fork of go ethereum

Updated in-line with new geth releases

Block generation+validation modified to handle public/private state

PoW replaced with pluggable consensus (voting, RAFT, Istanbul BFT)

State Patricia trie split in public/private state trie



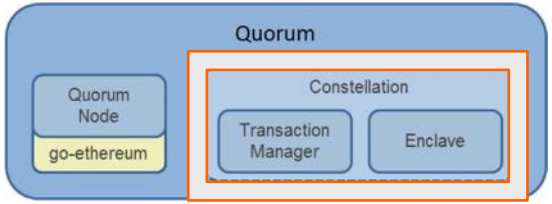
# Constellation

Rabobank

Two components

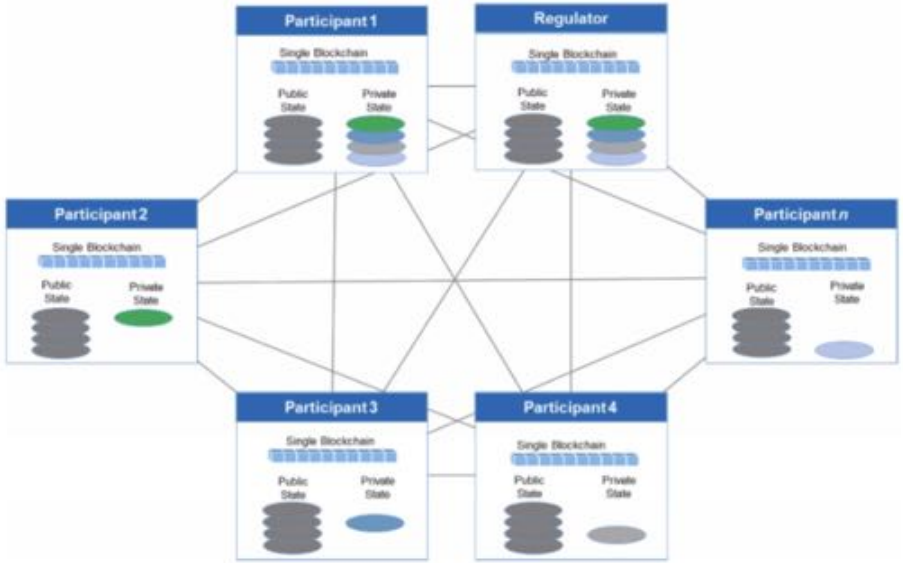
1. Transaction Manager: Responsible for tx-privacy
   Stores/allows access to encrypted tx data
   Exchanges encrypted payloads

2. Enclave: “virtual HSM”



# Drawbacks?

Default transaction privacy does not support prevention of double-spending

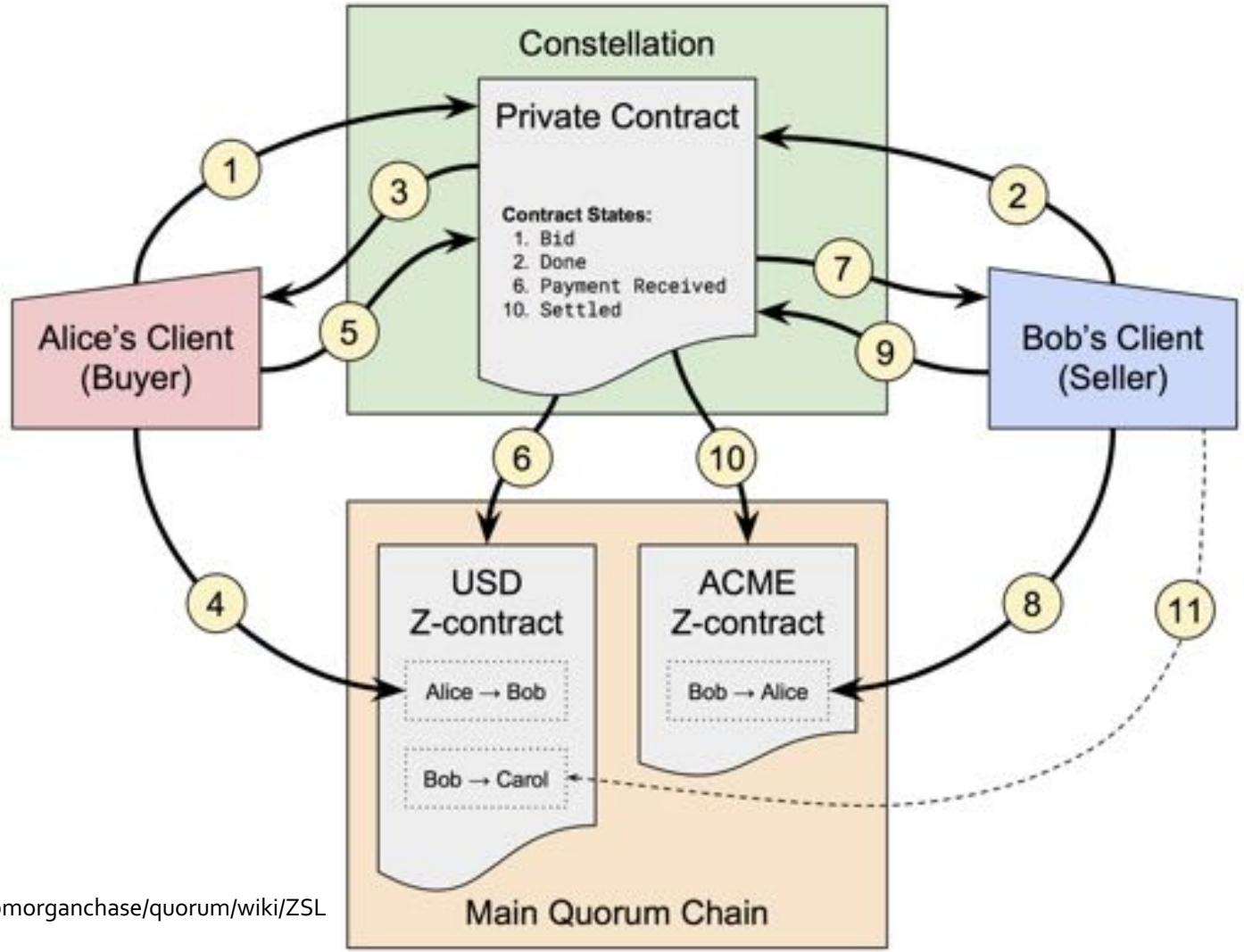


# Zero-knowledge security layer


ZSL: protocol by Zcash team – utilize zk-SNARK functionality

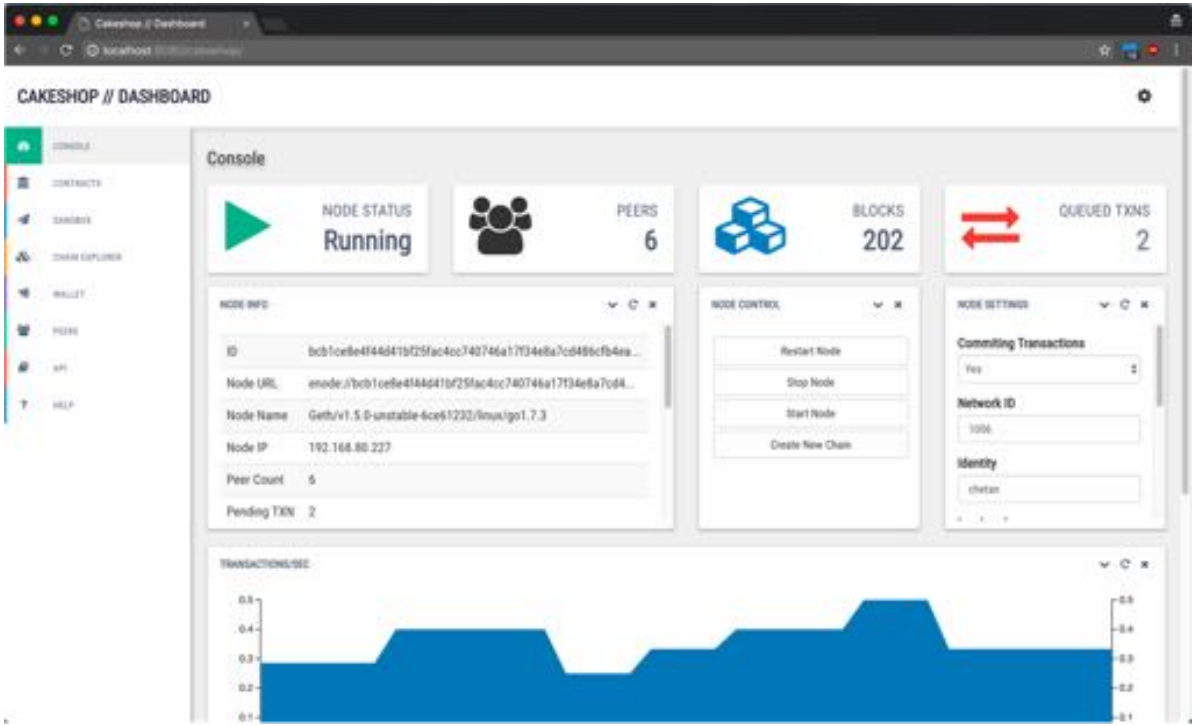
JPM Chase + Zcash partnered to create a PoC to issue digital assets using ZSL-enabled (public) smart contracts (z-tokens)

Obligations from private contract can be settled using z-tokens (shielded)




Source:
https://github.com/jpmorganchase/quorum/wiki/ZSL

# CakeShop




Also works with ”normal” Ethereum (just like ethstats works with quorum nodes)

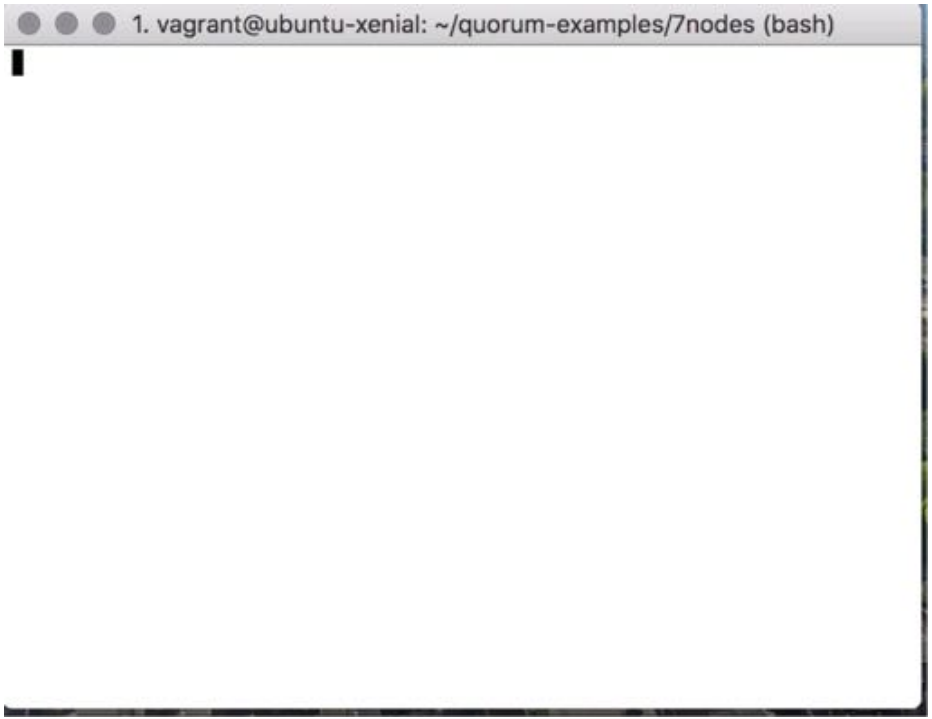
Rabobank

## *Demo time*

HashiCorp Vagrant


git

# Demo! (set up dev-env)




Rabobank

Prerequisites:

1. Install VirtualBox, vagrant (and git)
2. Clone examples repository:

```
git clone https://github.com/jpmorganchase/quorum-examples
cd quorum-examples
```

3. Go to examples directory
4. Initalize quorum chain with 7 nodes and RAFT consensus

VirtualBox: https://www.virtualbox.org/
Vagrant: https://www.vagrantup.com/

Like the colored bash git prompt?
**bit.ly/gimmecolorbash**

# Explanation of script1.js

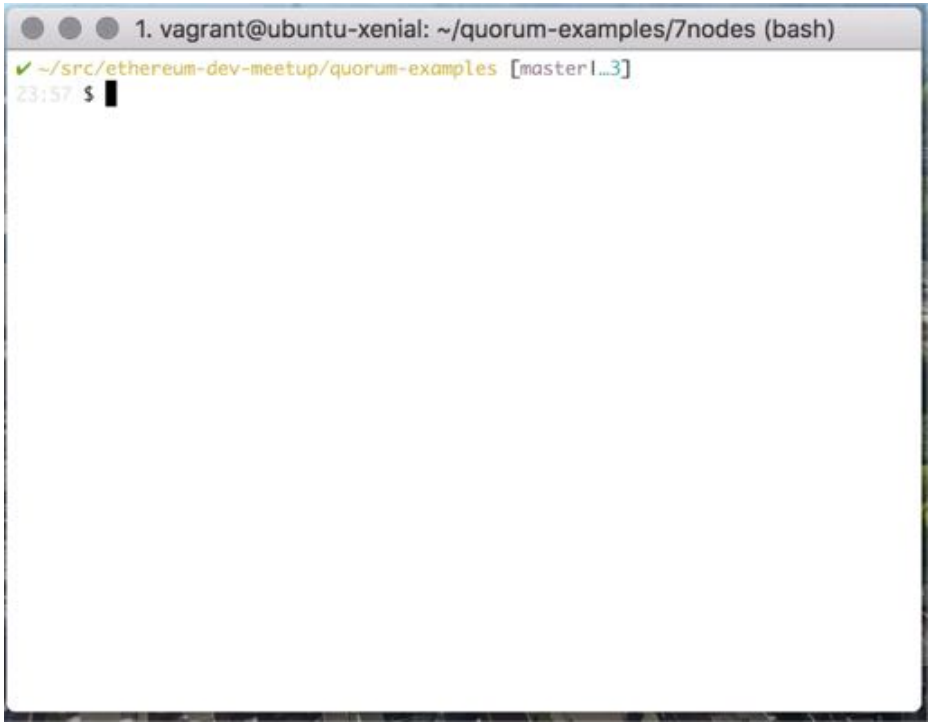

the final step […] is the sending of a private transaction to generate a (private) smart contract […] sent from node 1 "for" node 7 (denoted by the public key passed via privateFor: ["ROAZBWtSacxXQrOe3FGAqJDyJjFePR5ce4TSIzmJ0Bc="] in the sendTransaction call).

```
a = eth.accounts[0]
web3.eth.defaultAccount = a;

// abi and bytecode generated from simplestorage.sol:
// > solcjs --bin --abi simplestorage.sol
var abi = ["<removed to save space>"];

var bytecode = "<removed to save space>";

var simpleContract = web3.eth.contract(abi);
var simple = simpleContract.new(42, {from:web3.eth.accounts[0], data: bytecode, gas: 0x47b760, privateFor:
["ROAZBWtSacxXQrOe3FGAqJDyJjFePR5ce4TSIzmJ0Bc="]}, function(e, contract) {
        if (e) {
                console.log("err creating contract", e);
        } else {
                if (!contract.address) {
                        console.log("Contract transaction send: TransactionHash: " + contract.transactionHash + " waiting to be
mined...");
                } else {
                        console.log("Contract mined! Address: " + contract.address);
                        console.log(contract);
                }
        }
});
```

# Deploy contract with script.js

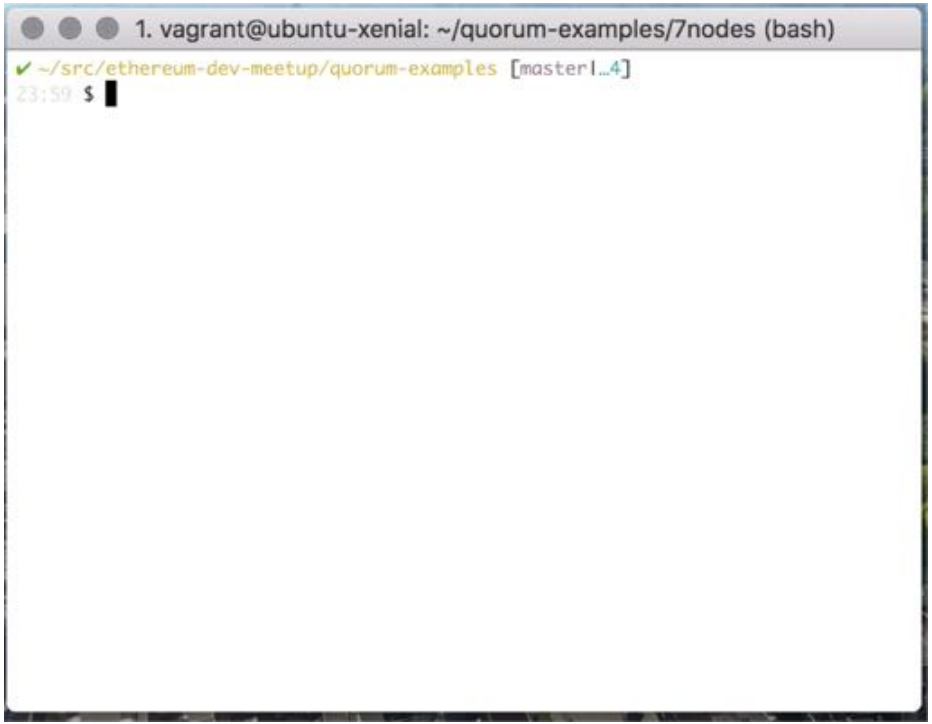

```
pragma solidity ^0.4.15;

contract simplestorage {
  uint public storedData;

  function simplestorage(uint initVal) {
    storedData = initVal;
  }

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

  function get() constant returns (uint retVal) {
    return storedData;
  }
}
```

# Demo! (node 1)



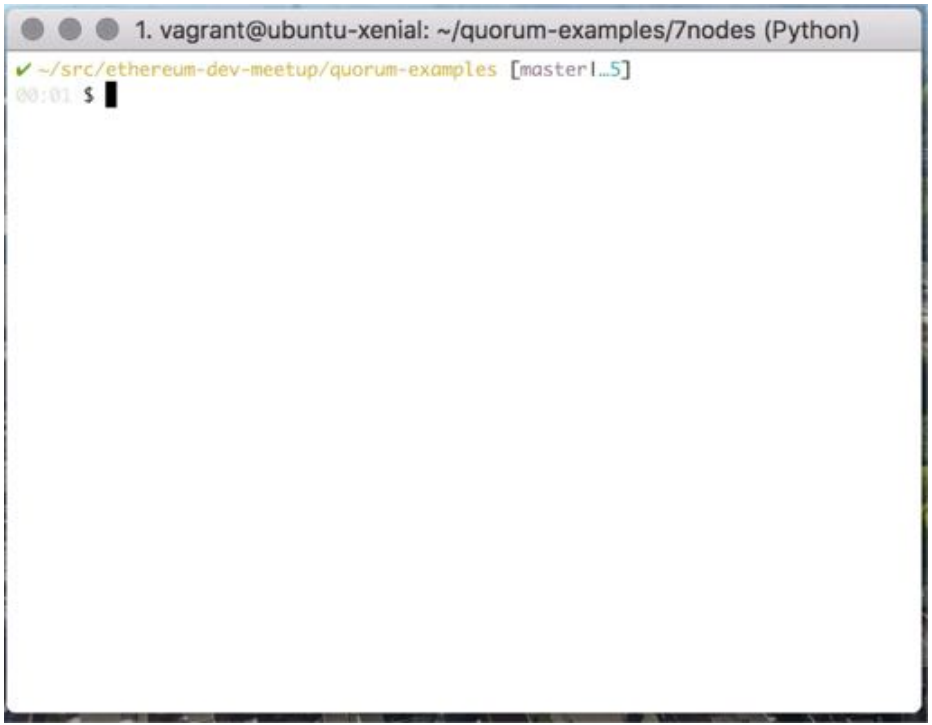

```
pragma solidity ^0.4.15;

contract simplestorage {
  uint public storedData;

  function simplestorage(uint initVal) {
    storedData = initVal;
  }

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

  function get() constant returns (uint retVal) {
    return storedData;
  }
}
```

# Demo! (node 4)




```
pragma solidity ^0.4.15;

contract simplestorage {
  uint public storedData;

  function simplestorage(uint initVal) {
    storedData = initVal;
  }

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

  function get() constant returns (uint retVal) {
    return storedData;
  }
}
```

# Demo! (node 7)




```
pragma solidity ^0.4.15;

contract simplestorage {
  uint public storedData;

  function simplestorage(uint initVal) {
    storedData = initVal;
  }

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

  function get() constant returns (uint retVal) {
    return storedData;
  }
}
```

# Questions?

For more information about Quorum, visit https://jpmorganchase.github.io/

Interested in the blockchain developer or internship vacancy?
Catch me during the break or mail us at **blockchain@rabobank.nl**

Rabobank