A QUICK INTRO TO QUORUM

쿼럼에 대한 간략한 소개

Quorum

Quorum in GitHub

389번의 포크	Forked 389 Times
컨트리뷰터 381명	381 Contributors
>10,700 활동빈도	>10,700 Commits
LGPL 3.0 라이센스	LGPL 3.0 License
3000개 이상의 별 보유	>3000 Stars

github.com/jpmorganchase/quorum

“이더리움 기반”의 Quorum

Quorum is "Ethereum Based"

ethereum

고이더리움(GETH) 및 패리티 노드(Parity Node) 등 여러 대안책들 활용

Utilizes Go-Ethereum (GETH) with other alternatives such as the Parity Node

작업증명방식 채택 Proof of Work (현재는)

POW Consensus (For now)

퍼블릭체인에 초점을 맞추고 있음

Public Chain Focused

EVM(이더리움 가상 머신)을 통해 스마트컨트렉트를 운용

Smart Contracts run on the EVM

Quorum

고이더리움 활용

Utilizes Go-Ethereum (GETH)

RAFT와 이스탄불 BFT 합의 알고리즘

RAFT & IBFT Consensus

기업형/프라이빗 블록체인에 초점을 맞추고 있음

Enterprise/Privacy Focused

EVM(이더리움 가상 머신)을 통해 스마트컨트렉트를 운용

Smart Contracts run on the EVM

이더리움과의 차이점 Differences with Ethereum

Not much!

Network ID

~ Mainnet Ethereum ID: 1

~ Rinkeby Ethereum ID: 4

~ Quorum Network ID = 10

(in our case)

Node Setup

~ 7 nodes를 위해서는 8GB RAM 필요

~ Requires 8GB RAM for 7 nodes.

~ 최소 100GB 필요

~ Requires at least 100GB

포트 구성

Ports configuration

Quorum network =

Nodes + Transaction Managers

트랜잭션 매니저(Transaction Managers)을 위해 포트를 여는 것을 잊지 마세요.

Don’t forget to open ports for transactions managers.

COMMODITY DERIVATIVES

INSURANCE ANNUITIES

SUPPLY CHAIN

REAL ESTATE

DASHBOARDS

BONDS

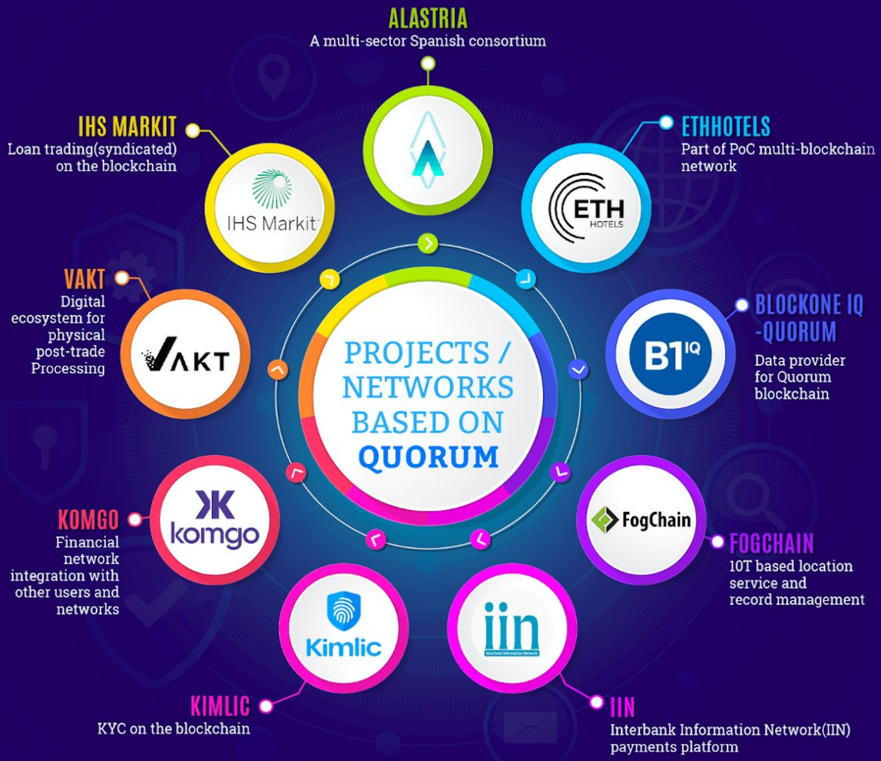
EQUITIES

DATA PROVISIONING

INDEX DERIVATIVES

PRIVATE NETWORK

PAYMENT SYSTEMS



PROJECTS / NETWORKS BASED ON QUORUM

ALASTRIA
A multi-sector Spanish consortium

ETHHOTELS
Part of PoC multi-blockchain network

BLOCKONE IQ -QUORUM
Data provider for Quorum blockchain

FOGCHAIN
10T based location service and record management

IIN
Interbank Information Network(IIN) payments platform

KIMLIC
KYC on the blockchain

KOMGO
Financial network integration with other users and networks

VAKT
Digital ecosystem for physical post-trade Processing

IHS MARKIT
Loan trading(syndicated) on the blockchain

WHAT IS QUORUM?

Quorum

Quorum is an enterprise-focused Ethereum blockchain aimed towards the finance sector. It is the brainchild of JP Morgan.

WHAT'S THE NEED FOR SUCH A SYSTEM?

Yes! Quorum provides financial sector the ability to use effective blockchain technology. Quorum offers permissioned network enabling organizations to customize to their own needs.

FEATURES OF QUORUM

Enhanced contract privacy and transaction

Better performance

Proper peer and network management

Voting-based consensus mechanisms

Open-source

Community-driven

Mature

Trustworthy and enterprise ready

QUORUM IS OPEN SOURCE!

318 ACTIVE CONTRIBUTORS

10,000+ COMMITS

LGPL 3.0 LICENSE

QUORUM ARCHITECTURE

Three key components

QUORUM NODE
A command line tool based on Geth

CONSTELLATION TRANSACTION MANAGER
It takes care of the transaction data until it gets completed

ENCLAVE
Enclave handles the sensitive information where the Transaction Manager delegates key functions such as encryption/decryption

CONSENSUS ALGORITHMS

RAFT-BASED CONSENSUS
Enables faster transaction, improves block storage

Istanbul BFT
provides fault tolerance, protects blockchain against bad nodes

CREATED BY 101BLOCKCHAINS.COM

PROOF

DEPLOYING DAPPS ON QUORUM

쿼럼에 디앱
(분산어플리케이션)
배포하기

Quorum

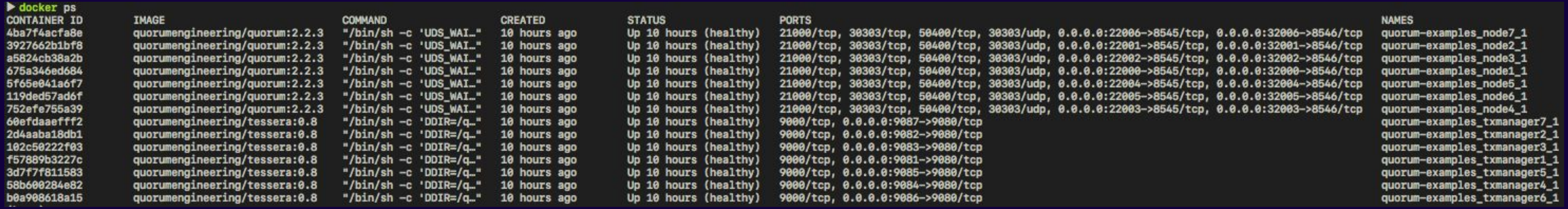
1. SETUP

- 7-노드 쿼럼 네트워크 7-node quorum network
- 쿼럼블록체인 활용시 도커(Docker) 또는 베이그런트(Vagrant) 셋팅 권장

  Recommended for starting with quorum: Docker or Vagrant setup
- https://github.com/jpmorganchase/quorum-examples

셋업이 완료되면 아래와 같은 화면이 보이게 될 것입니다.

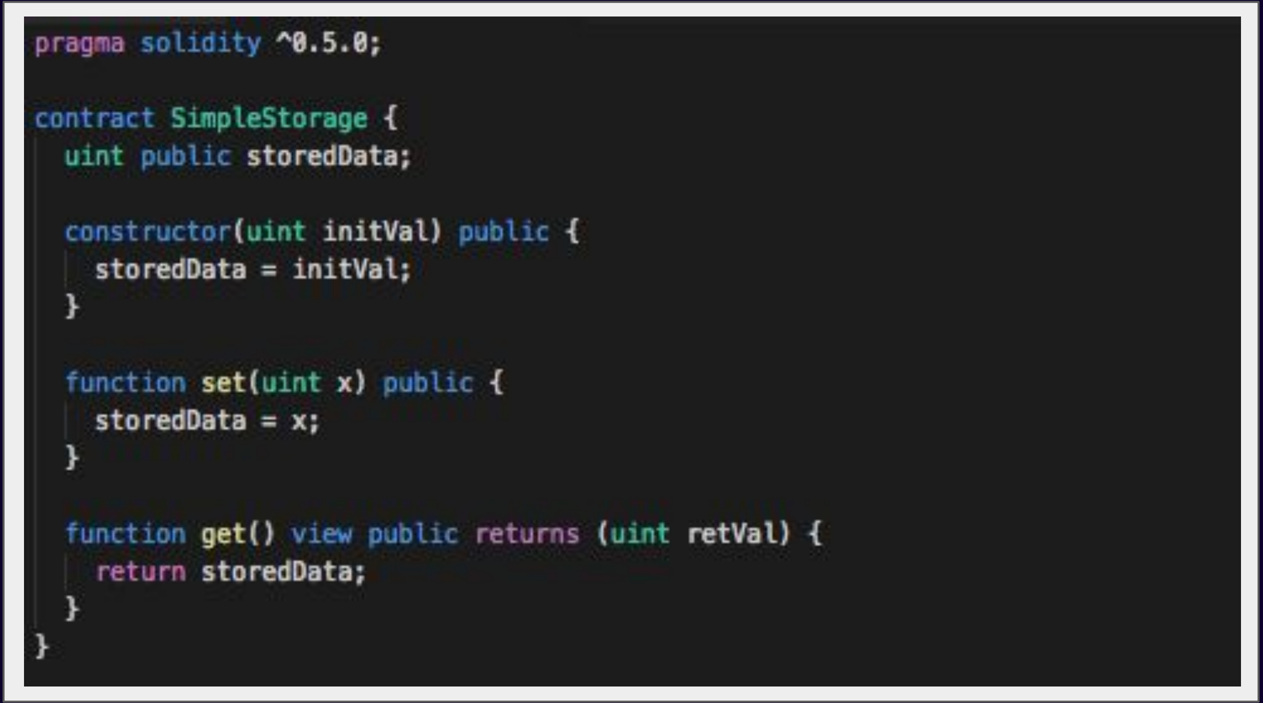
After setup, you should see something similar to the screen below:



```
▶ docker ps
CONTAINER ID        IMAGE                            COMMAND                  CREATED             STATUS                  PORTS                                                                                              NAMES
4ba7f4acfa8e        quorumengineering/quorum:2.2.3   "/bin/sh -c 'UDS_WAI…"   10 hours ago        Up 10 hours (healthy)   21000/tcp, 30303/tcp, 50400/tcp, 30303/udp, 0.0.0.0:22006->8545/tcp, 0.0.0.0:32006->8546/tcp   quorum-examples_node7_1
3927662b1bf8        quorumengineering/quorum:2.2.3   "/bin/sh -c 'UDS_WAI…"   10 hours ago        Up 10 hours (healthy)   21000/tcp, 30303/tcp, 50400/tcp, 30303/udp, 0.0.0.0:22001->8545/tcp, 0.0.0.0:32001->8546/tcp   quorum-examples_node2_1
a5824cb38a2b        quorumengineering/quorum:2.2.3   "/bin/sh -c 'UDS_WAI…"   10 hours ago        Up 10 hours (healthy)   21000/tcp, 30303/tcp, 50400/tcp, 30303/udp, 0.0.0.0:22002->8545/tcp, 0.0.0.0:32002->8546/tcp   quorum-examples_node3_1
675a346ed684        quorumengineering/quorum:2.2.3   "/bin/sh -c 'UDS_WAI…"   10 hours ago        Up 10 hours (healthy)   21000/tcp, 30303/tcp, 50400/tcp, 30303/udp, 0.0.0.0:22000->8545/tcp, 0.0.0.0:32000->8546/tcp   quorum-examples_node1_1
5f65e041a6f7        quorumengineering/quorum:2.2.3   "/bin/sh -c 'UDS_WAI…"   10 hours ago        Up 10 hours (healthy)   21000/tcp, 30303/tcp, 50400/tcp, 30303/udp, 0.0.0.0:22004->8545/tcp, 0.0.0.0:32004->8546/tcp   quorum-examples_node5_1
119ded57ad6f        quorumengineering/quorum:2.2.3   "/bin/sh -c 'UDS_WAI…"   10 hours ago        Up 10 hours (healthy)   21000/tcp, 30303/tcp, 50400/tcp, 30303/udp, 0.0.0.0:22005->8545/tcp, 0.0.0.0:32005->8546/tcp   quorum-examples_node6_1
752efe755a39        quorumengineering/quorum:2.2.3   "/bin/sh -c 'UDS_WAI…"   10 hours ago        Up 10 hours (healthy)   21000/tcp, 30303/tcp, 50400/tcp, 30303/udp, 0.0.0.0:22003->8545/tcp, 0.0.0.0:32003->8546/tcp   quorum-examples_node4_1
60efdaaefff2        quorumengineering/tessera:0.8    "/bin/sh -c 'DDIR=/q…"   10 hours ago        Up 10 hours (healthy)   9000/tcp, 0.0.0.0:9087->9080/tcp                                                                   quorum-examples_txmanager7_1
2d4aaba18db1        quorumengineering/tessera:0.8    "/bin/sh -c 'DDIR=/q…"   10 hours ago        Up 10 hours (healthy)   9000/tcp, 0.0.0.0:9082->9080/tcp                                                                   quorum-examples_txmanager2_1
102c50222f03        quorumengineering/tessera:0.8    "/bin/sh -c 'DDIR=/q…"   10 hours ago        Up 10 hours (healthy)   9000/tcp, 0.0.0.0:9083->9080/tcp                                                                   quorum-examples_txmanager3_1
f57889b3227c        quorumengineering/tessera:0.8    "/bin/sh -c 'DDIR=/q…"   10 hours ago        Up 10 hours (healthy)   9000/tcp, 0.0.0.0:9081->9080/tcp                                                                   quorum-examples_txmanager1_1
3d7f7f811583        quorumengineering/tessera:0.8    "/bin/sh -c 'DDIR=/q…"   10 hours ago        Up 10 hours (healthy)   9000/tcp, 0.0.0.0:9085->9080/tcp                                                                   quorum-examples_txmanager5_1
58b600284e82        quorumengineering/tessera:0.8    "/bin/sh -c 'DDIR=/q…"   10 hours ago        Up 10 hours (healthy)   9000/tcp, 0.0.0.0:9084->9080/tcp                                                                   quorum-examples_txmanager4_1
b0a908618a15        quorumengineering/tessera:0.8    "/bin/sh -c 'DDIR=/q…"   10 hours ago        Up 10 hours (healthy)   9000/tcp, 0.0.0.0:9086->9080/tcp                                                                   quorum-examples_txmanager6_1
```

2. 간단한 컨트렉트 배포 시연

DEPLOYING A VERY SIMPLE CONTRACT



```
pragma solidity ^0.5.0;

contract SimpleStorage {
  uint public storedData;

  constructor(uint initVal) public {
    storedData = initVal;
  }

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

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

쿼럼 블록체인에 디앱(분산 어플리케이션) 배포하는 다양한 방법

METHODS TO DEPLOY DAPPS ON QUORUM

Quorum.js

https://github.com/jpmorganchase/quorum.js/

Quorum.js는 쿼럼블록체인을 위한 web3의 수정된 버전입니다.

프라이빗 거래를 제외하고 같은 API 사용

Quorum.js is a modified version of web3 for the quorum blockchain

Identical API except for private transactions

Truffle

https://github.com/trufflesuite/truffle (Deployment Framework)

Truffle은 스마트콘트렉트 배포 및 테스팅 프레임워크입니다

Quorum과 사용 시 다양한 방향으로 적용 가능합니다.

Truffle is a smart contract deployment and testing framework

Works out of the box with quorum

Geth/Quorum Javascript Console

내장된 쿼럼 커맨드 라인으로도 간단한 콘트렉트를 배포할 수 있습니다.

It’s also possible to deploy simple contracts via the built-in quorum command line

2.1 커맨드라인으로 컨트렉트 배포하기

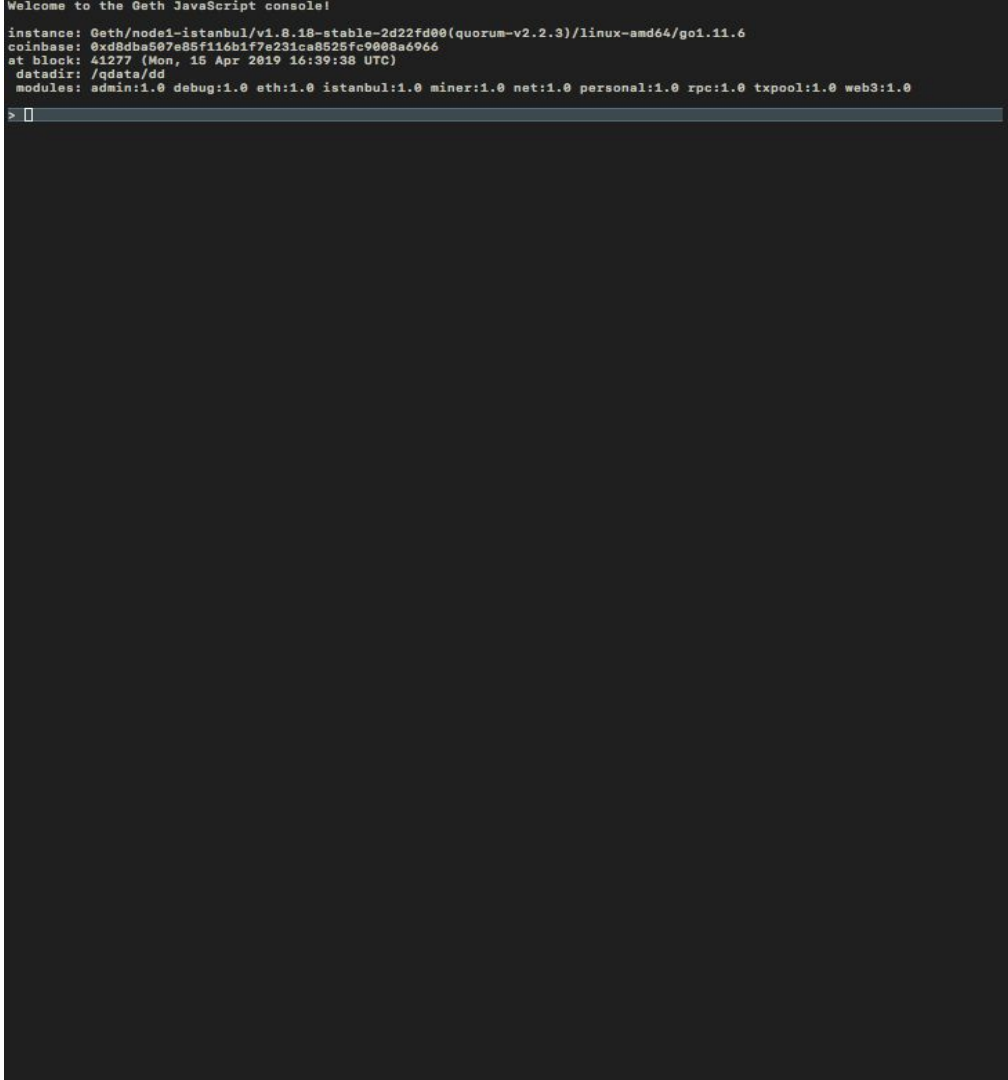
Deploying with the command line

게스(GETH) 및 쿼럼은 자바스크립트 콘솔을 통해 개발자가 선택하는 네트워크와 상호작용할 수 있도록 합니다.

Geth/Quorum features a javascript console that enables developers to interact with the network of their choice.

자바스크립트 콘솔은 “geth attach” 명령어를 통해 접속할 수 있습니다.

The javascript console can be accessed by the ***geth attach*** command

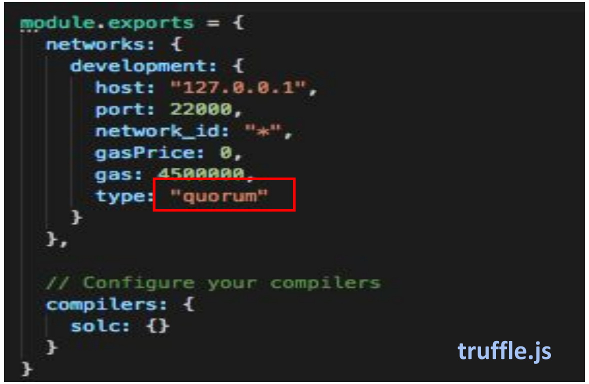


```
Welcome to the Geth JavaScript console!

instance: Geth/node1-istanbul/v1.8.18-stable-2d22fd00(quorum-v2.2.3)/linux-amd64/go1.11.6
coinbase: 0xd8dba507e85f116b1f7e231ca8525fc9008a6966
at block: 41277 (Mon, 15 Apr 2019 16:39:38 UTC)
 datadir: /qdata/dd
 modules: admin:1.0 debug:1.0 eth:1.0 istanbul:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

> 
```

2.2 Truffle로 컨트렉트 배포하기

Deploying with Truffle

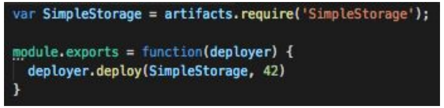
Truffle 커스텀 구성(Custom Truffle Configuration)**:**



```
module.exports = {
  networks: {
    development: {
      host: "127.0.0.1",
      port: 22000,
      network_id: "*",
      gasPrice: 0,
      gas: 4500000,
      type: "quorum"
    }
  },

  // Configure your compilers
  compilers: {
    solc: {}
  }
}
```

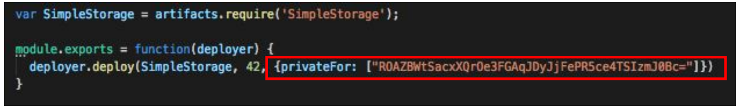
truffle.js

컨트렉트 배포(Contract Deployment)**:**



```
var SimpleStorage = artifacts.require('SimpleStorage');

module.exports = function(deployer) {
  deployer.deploy(SimpleStorage, 42)
}
```

프라이빗 컨트렉트 배포(Private Contract Deployment)**:**



```
var SimpleStorage = artifacts.require('SimpleStorage');

module.exports = function(deployer) {
  deployer.deploy(SimpleStorage, 42, {privateFor: ["ROAZBWtSacxXQrOe3FGAqJDyJjFePR5ce4TSIzmJ0Bc="]})
}
```

```
quorum/quorum-examples/example-dapp  master ×                                         10d
▶ 
```

이더리움과의 차이점 Differences with Ethereum

이벤트에 주의 기울이기 (Infura를 사용하지 않음) Listening to events (no more Infura)

승인 시간이 매우 짧기 때문에 직접 거래처리 여부를 확인해야 합니다.

Better rely on direct contract calls since the confirmation times are really short

GasPrice

거래 전 반드시 가스 가격을 0으로 설정해야 합니다.

Setting GasPrice to any value other than 0 will cause errors

이더스캔과 같은 리소스 사용이 불가함 Impossible to use resources like Etherscan

- 이더스캔과의 연결을 끊어야 합니다. Remove links to Etherscan
- 여러분만의 블록 탐색기로 이를 대체합니다. Replace by your own block explorer

On {..., privateFor: [...], ...} Transaction Key

privateFor는 거래키입니다. privateFor is a key in a transaction.

이 열은 참여자들의 퍼블릭 키들을 포함하고 있습니다.
The array contains the parties' public keys established at node deployment in config.

이 열에 있는 노드 아이디는 반드시 base64 방식으로 엔코딩해야 합니다.
You must base64 encode the node-id's inside of an Array to utilize.

콘트랙트를 배포할 때 `{privateFor: [...]}` 명령은 거래의 개별적인 상태에 대한 정보를 포함하고 있습니다. 짠! 이렇게 하면 쿼럼 블록체인에 프라이빗한 Dapp을 갖게 됩니다.
When deploying contracts the `{privateFor: [...]}` call carries the private state for all contracts. Voila! We have privacy scoped dapps on quorum!

참고: 퍼블릭과 프라이빗 콘트랙트 관련 콘셉트는 관념적일 뿐
NOTE: the concept of public and private contracts is notional only.

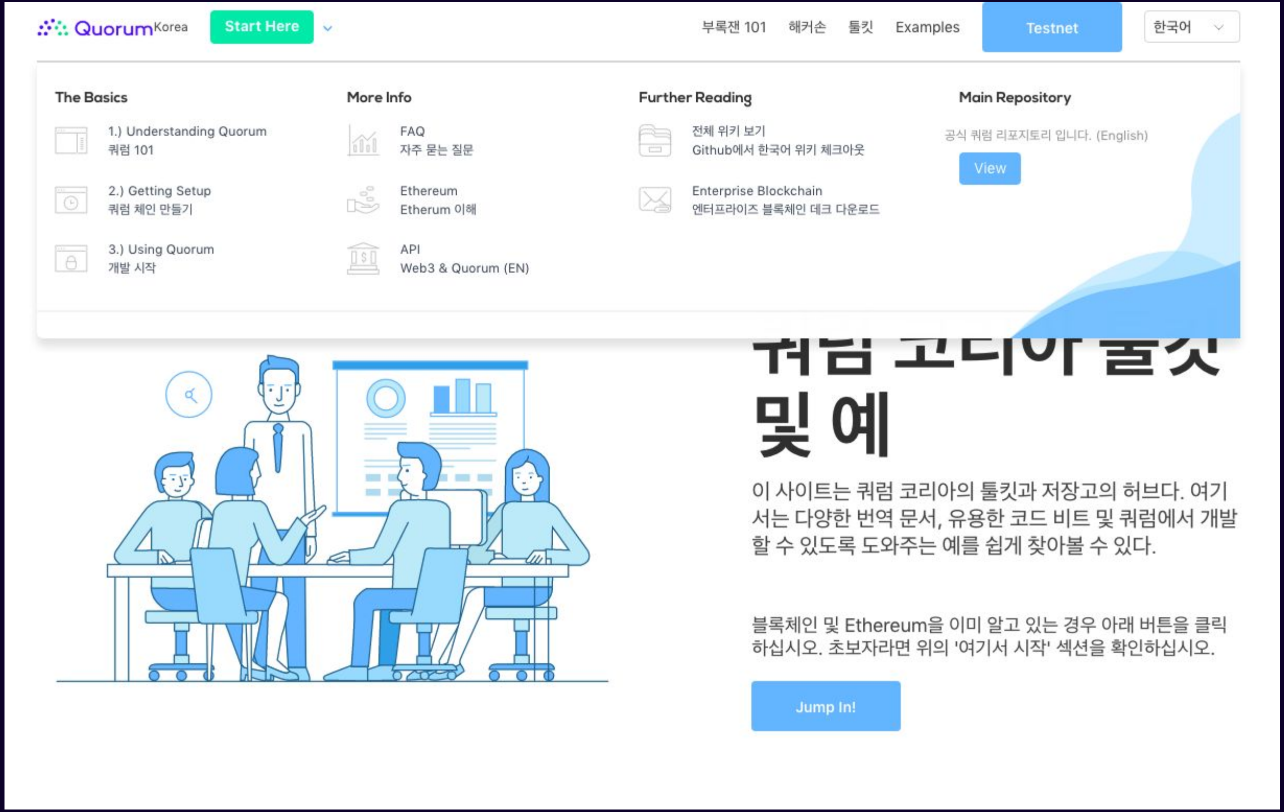
Base64 퍼블릭키들은 스핀업 타임 때 노드에 생성됩니다.
The Base64 "PublicKeys" are established in the node at spin up time.

```
// Example

const qEthTransaction =

{

…,

privateFor:

[

"BULeR8JyUWhiuuCMU/HLA0Q5pzkYT+cHII3ZKBey3Bo=",

 "QfeDAys9MPDs2XHExtc84jKGHxZgaj52DTh0vtA3Xc=",

 "oNspPPgszVUFw0qmGFfWwh1uxVUXgvBxleXORHj07g8="

],

…

}
```

Suggested Starting Hackathon Stack

Web3	https://github.com/ethereum/web3.js/
Truffle.js	https://github.com/trufflesuite/truffle
Geth	(Included in Quorum)
Base Code	https://github.com/jpmorganchase/quorum

QUORUMKOREA.PRFTECH.COM



쿼럼 코리아 툴킷 및 예

이 사이트는 쿼럼 코리아의 툴킷과 저장고의 허브다. 여기서는 다양한 번역 문서, 유용한 코드 비트 및 쿼럼에서 개발할 수 있도록 도와주는 예를 쉽게 찾아볼 수 있다.

블록체인 및 Ethereum을 이미 알고 있는 경우 아래 버튼을 클릭하십시오. 초보자라면 위의 '여기서 시작' 섹션을 확인하십시오.

Seoul-Quorum
Hackathon
On August 9-10th

How to Get Involved:

https://github.com/jpmorganchase/quorum

https://github.com/proofsuite

https://quorumhackathonkorea.com/

PROOF

THANK YOU

Quorum