Final Project

Quorum Blockchain Implementation

Staehle, Nicole

Deep Azure@McKesson

Dr. Zoran B. Djordjević

Problem Statement

With the advent of blockchain's private, permissioned networks, developers in various industries are tasked with implementing a daunting set of options to ensure transactional and institutional security.

Developed by J.P. Morgan Chase to address this task, Quorum supports transactional volumes per institution, with privacy at the transaction level. Quorum is a blockchain consortium (private network), with support for smart contract business logic applications, and a proprietary dashboard interface called Cakeshop for managing the network and contracts.

In this demo, we will:

- Discuss the security options of the Quorum Single Member Blockchain Network
- Deploy one, exploring PowerShell options for displaying and creating resources

Technology Background

Blockchain is a distributed, open-source ledger. The transactions are verified by multiple nodes, with each transaction constituting part of the chain and acting as an immutable record. This is a huge benefit for industries with a high level of transactions and required security, such as finance, healthcare, and shipping. However, the concern has been that blockchain is not secure, as transactions are public.

Ethereum is an enhanced blockchain that is:

- Turing-complete
- Built with a protocol layer
- Focused on smart contracts using the Solidity language

Quorum is a consortium (private) network built on the Ethereum protocol. It's scaled down with a single, shared blockchain. With security built-in for the enterprise, it includes contract-level privacy settings. All nodes execute a contract, even in private state, but unlike blockchain, nodes *and* contract parties verify the state of the contract.

Technology Background

Blockchain key concepts:

- Transactions- Executions against the ledger
- Consensus- Nodes' (and contract parties') agreement on the status (state) of a transaction
- Mining- Checking for valid blocks
- Blocks- Groups of transactions
- Smart Contracts- Apply business logic to programming to execute transactions between parties (written in Solidity language)

Technology Used

High-Level Overview of steps:

Install from Azure Portal:

- Quorum Single Member Blockchain Network

Configure:

- JSON template variables and parameters (if desired)
- PowerShell script for Automation Account

File Information:

- Format of code files: JSON (47 kb), .PS1 (4 kb)
- Hardware: Quorum Consortium blockchain VMs (2), Standard, LRS storage; Standard D1 v2 size
- Software: Ubuntu Server 16.04 (guest); Windows 7 (host)

Sources:

- Ethereum white paper
- Quorum white paper
- Quorum documentation link from Azure portal

Demo: Creation & Deployment

QUORUM SINGLE MEMBER BLOCKCHAIN NETWORK

Creating & Deploying the Quorum Single Member Blockchain Network

Steps	Per-Step Requirements
Step 1: Basics	▪ Set up VM passwords and usernames
Step 2: Network size and Performance	▪ Number of VMs, storage options, VM size
Step 3: Quorum-Specific Settings. Configure the Quorum	▪ Ethereum account password and passphrase to generate private key
Step 4: Summary	▪ Review all values and review template
Step 5: Buy	▪ Read TOS, pricing and template info

Creating & Deploying the Quorum Single Member Blockchain Network

Step 1: Basics

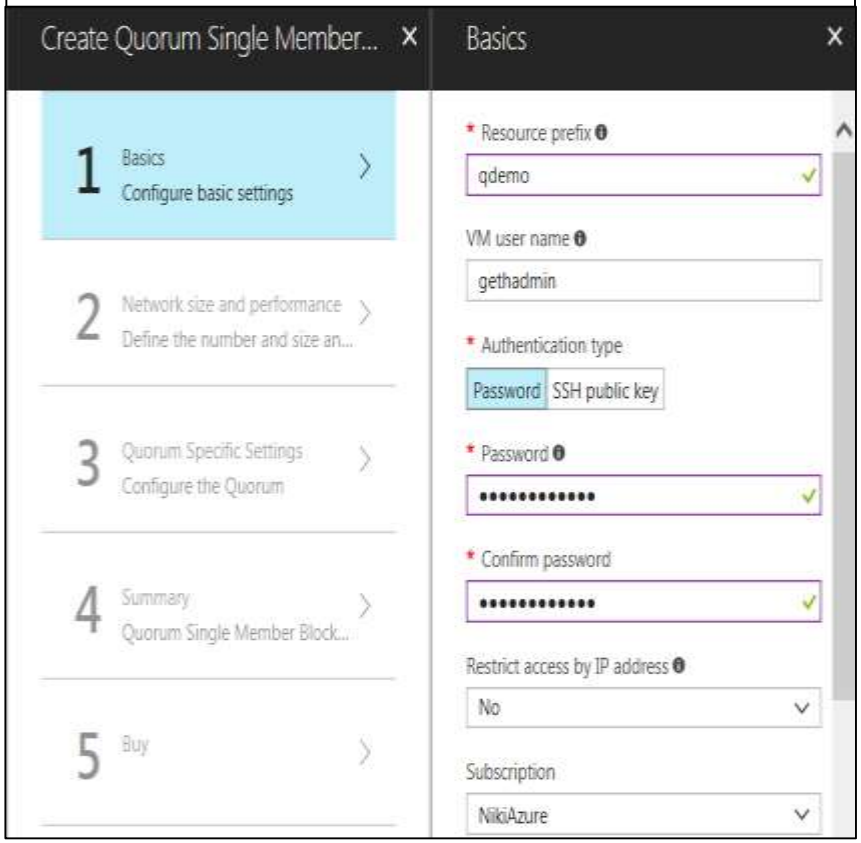
Resource prefix:

- Used to categorize resources
- Must begin with a lowercase letter, be between 2-6 characters, and can contain only numbers and lowercase letters

Password:

- Must be between 12-72 characters long and contain 3 of the following:
- ❑ 1 lowercase letter
- ❑ 1 uppercase letter
- ❑ 1 number
- ❑ 1 special character

Key Consideration: Resource Prefix & Password Requirements



Creating & Deploying the Quorum Single Member Blockchain Network

Step 2: Network Size and Performance

Consortium member id

- In a multi-member setup, each member should have a unique value to ensure that they can connect.

Number of block makers (1)

- Block makers create and propose blocks to the network (currently limited to 1 for this offer type).

Number of Voters (1)

- Voters vote on blocks.

Number of observers (0)

- Observers passively listen to traffic on the network like transactions and blocks.

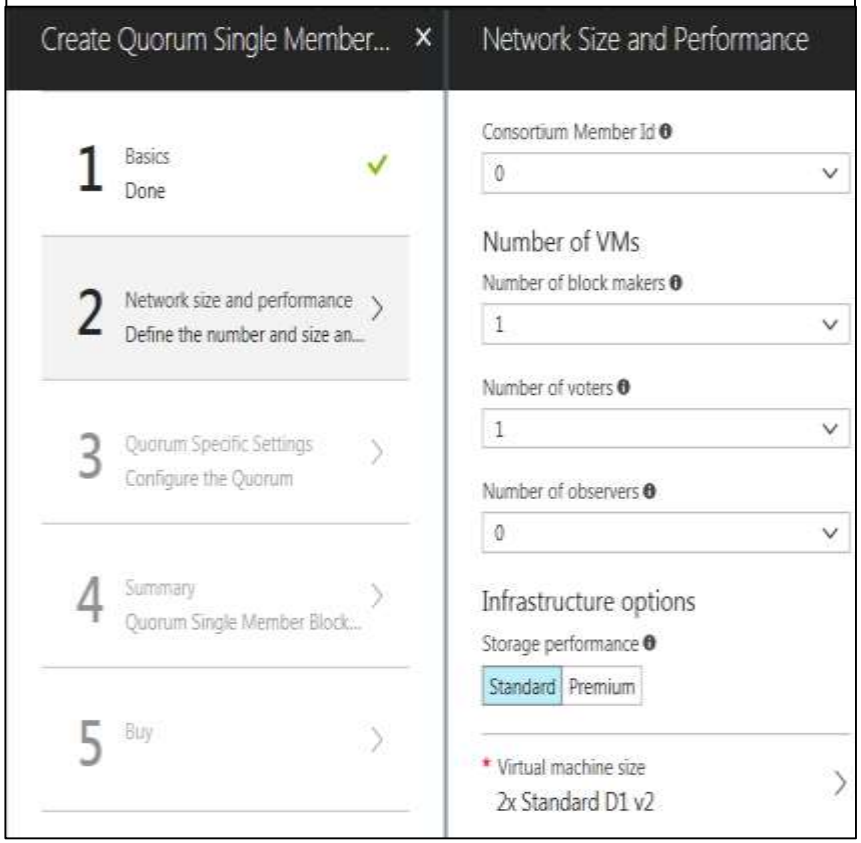
Infrastructure options

- Standard

Virtual Machine Size

- 2x standard D1 v2

Key Consideration: VM size & Storage Performance



Creating & Deploying the Quorum Single Member Blockchain Network

Step 3: Quorum Settings

Network ID

- Only nodes that share the same ID can peer with each other.

Ethereum account password

- Secures default account that is created.

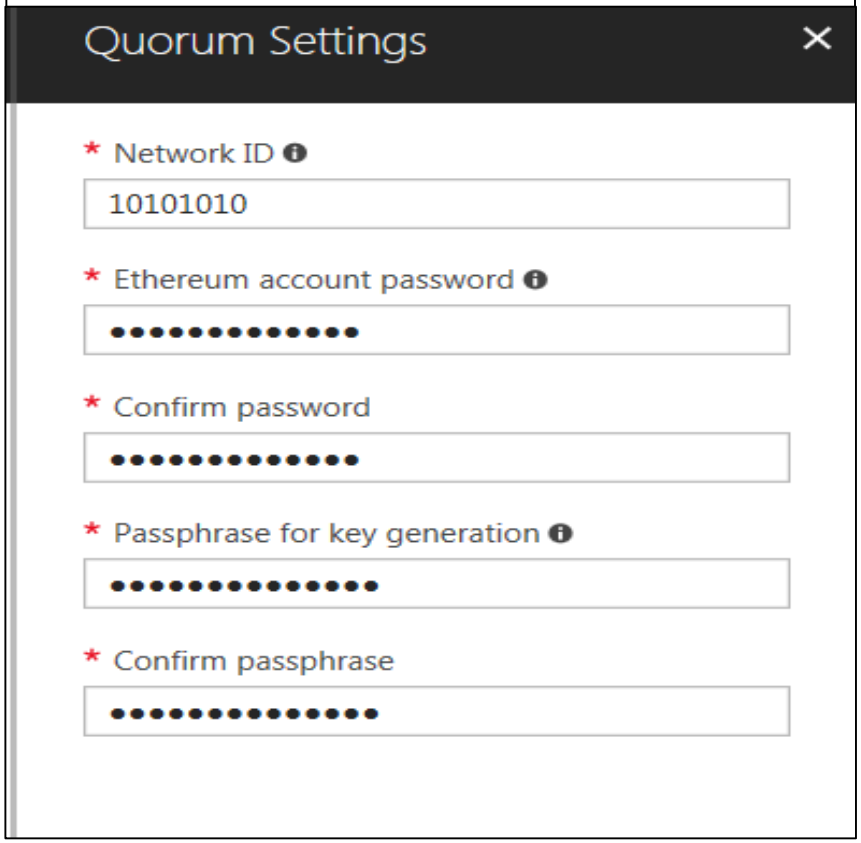
Requirements:

- ❑ 12+ characters
- ❑ 1 lower case
- ❑ 1 upper case
- ❑ 1 number
- ❑ No double quotes or forward slashes

Passphrase for key generation:

- Same requirements as Ethereum account password
- Needs to be random enough to generate a strong private key

Key Consideration: Password & Passphrase



Creating & Deploying the Quorum Single Member Blockchain Network

Step 4: Summary

You MUST review your template to see what Azure will create.

```
1 {
2     "$schema":
"https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3     "contentVersion": "1.0.0.0",
4     "parameters": {
5         "namePrefix": {
6             "type": "string",
7             "metadata": {
8                 "description": "String used as a base for naming resources (6
alphanumeric characters or less).  A unique hash is prepended to the string for some
resources, while resource-specific information is appended."
9             },
10            "maxLength": 6
11        },
12        "authType": {
13            "type": "string",
```

Key Consideration: Review Template!

Summary ×

Validation passed

Basics	
Subscription	NikiAzure
Resource group	Quorum
Location	East US
Resource prefix	qdemo
VM user name	gethadmin
Password	**********
Restrict access by IP address	No
Network Size and Performance	
Consortium Member Id	0
Number of block makers	1
Number of voters	1
Number of observers	0
Storage performance	Standard
Virtual machine size	Standard D1 v2
Quorum Settings	
Network ID	10101010
Ethereum account password	**********
Passphrase for key generation	**********

Creating & Deploying the Quorum Single Member Blockchain Network

Step 5: Buy

Click ‘Create’ or Deploy Using a Template or Runbook

Create

EEA Single Member Blockchain
by Enterprise Ethereum Alliance
Terms of use | privacy policy

Deploying this template will result in various actions being performed, which may include the deployment of one of more Azure resources or Marketplace offerings and/or transmission of the information you provided as part of the deployment process to one or more parties, as specified in the template. You are responsible for reviewing the text of the template to determine which actions will be performed and which resources or offerings will be deployed, and for locating and reviewing the pricing and legal terms associated with those resources or offerings.

Current retail prices for Azure resources are set forth here and may not reflect discounts applicable to your Azure subscription.

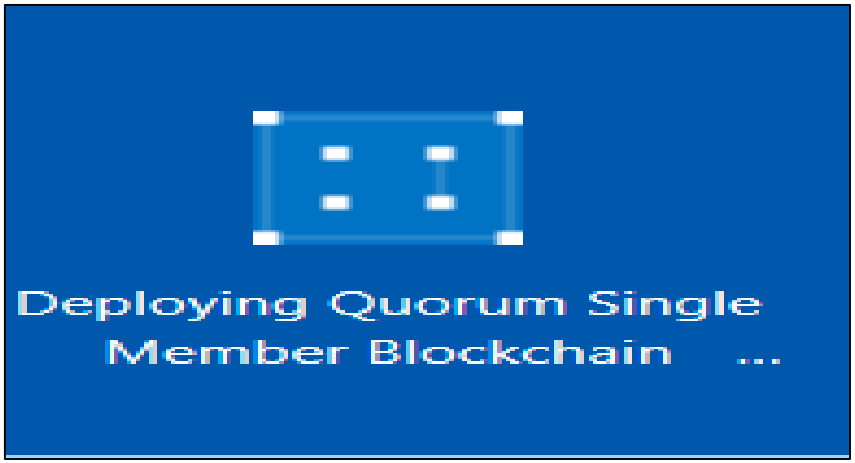
Prices for Marketplace offerings are set forth here, and the legal terms associated with any Marketplace offering may be found in the Azure portal; both are subject to change at any time prior to deployment.

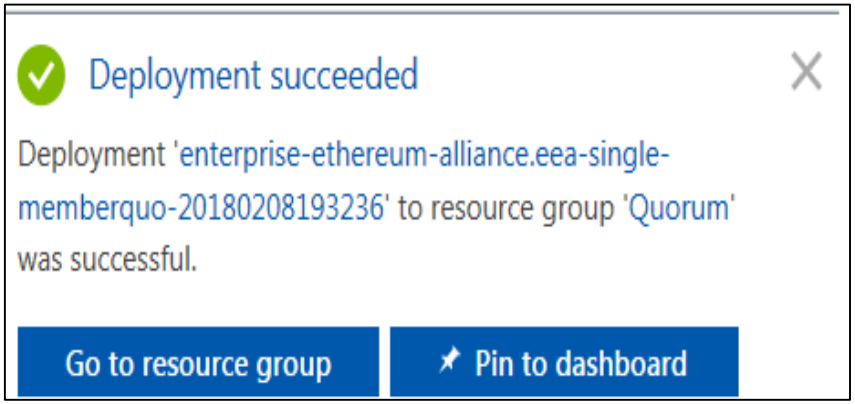
Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Template deployment is intended for advanced users only. If you are uncertain which actions will be performed by this template, which resources or offerings will be deployed, or what prices or legal terms pertain to those resources or offerings, do not deploy this template.

Creating & Deploying the Quorum Single Member Blockchain Network

Statuses





View Resource Group Items

NAME	TYPE	LOCATION
nic-bm0	Network interface	East US
nic-voter0	Network interface	East US
qdemo4b3g-bm0	Virtual machine	East US
qdemo4b3g-bm0_OsDisk_1_fb4b2fee3ff04e3c90ddd6d85...	Disk	East US
qdemo4b3g-LB	Load balancer	East US
qdemo4b3gnsg	Network security group	East US
qdemo4b3g-publicip	Public IP address	East US

Creating & Deploying the Quorum Single Member Blockchain Network

Get DNS address to go to admin portal

Resource group (change)
Quorum

Status
Running

Location
East US

Subscription (change)
NikiAzure

Subscription ID
[redacted]

Computer name
qdemo4b3g-bm0

Operating system
Linux

Size
Standard D1 v2 (1 vcpu, 3.5 GB memory)

Public IP address
[redacted]

Virtual network/subnet
qdemo4b3gvnet/befficslsz55i

DNS name
qdemo4b3g.eastus.cloudapp.azure.com

Creating & Deploying the Quorum Single Member Blockchain Network

Admin Portal: Home

Ethereum Node Status

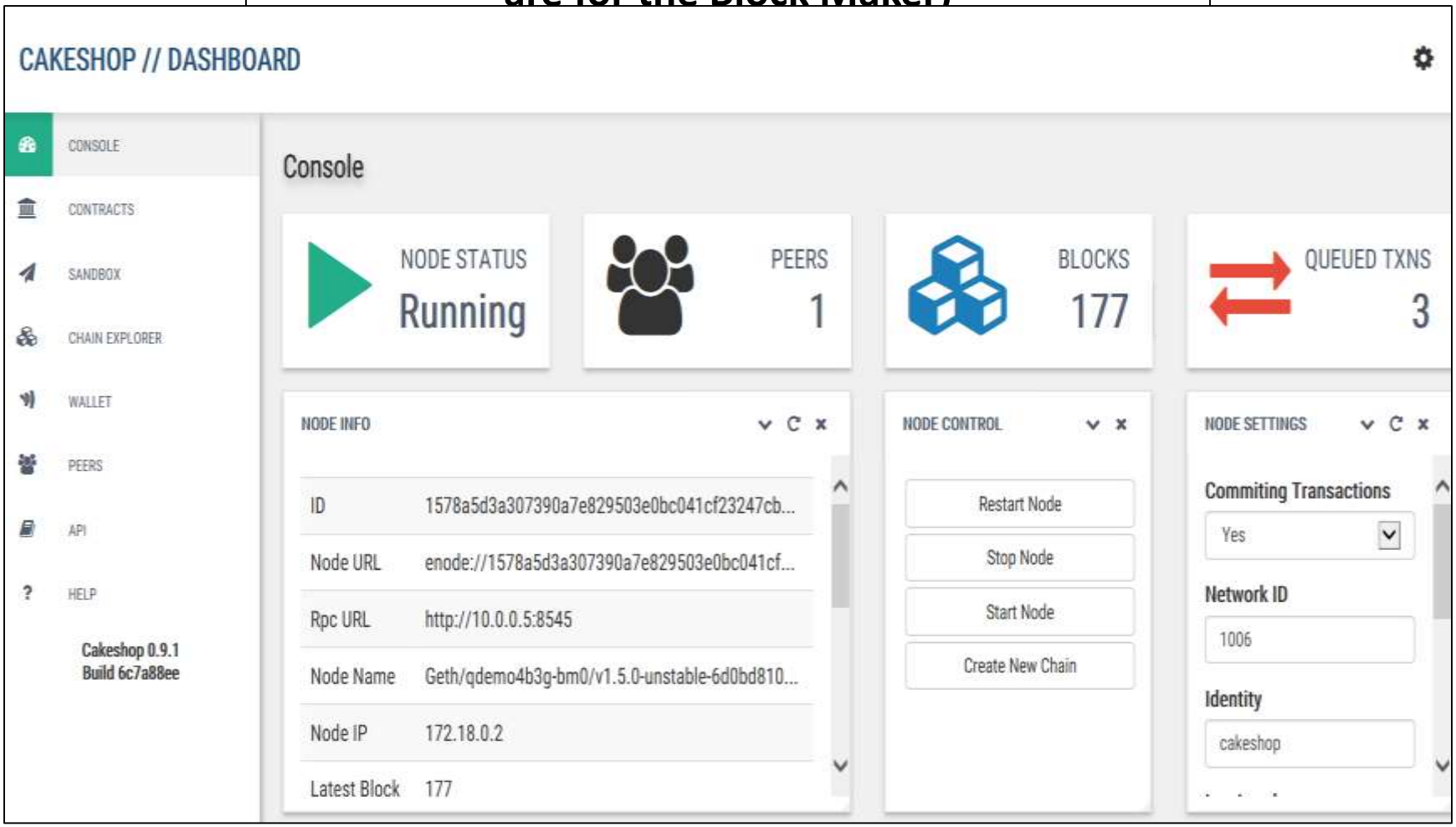
Node Hostname	Cakeshop	Peer Count	Latest Block Number
qdemo4b3g-bm0	qdemo4b3g-bm0	1	125
qdemo4b3g-vtr0	qdemo4b3g-vtr0	1	125

Block Maker

Voter

Creating & Deploying the Quorum Single Member Blockchain Network

Cakeshop Dashboard (the following screenshots are for the Block Maker)



Creating & Deploying the Quorum Single Member Blockchain Network

Cakeshop Chain Explorer

Chain Explorer

NODE STATUS
Running

PEERS
1

BLOCKS
431

QUEUED TXNS
1

BLOCK #429

ID	0x6c8cc3361a1aa8d9507d75211a6c37eb5862f61...
Number	429
Timestamp	08:23:49 PM 02/08/2018 (a few seconds ago)
Transactions	0x68291d57b5cd0e553d0e51c0b0cb775fc5d6ca5...
Difficulty	161293
Extra Data	0x1898b78e8ba00848d94b4399664e3bd4bd225ff...

BLOCK LIST

Block	Age	TXNs
#431	a few seconds ago	2
#429	a few seconds ago	1

FIND BLOCK / TRANSACTION

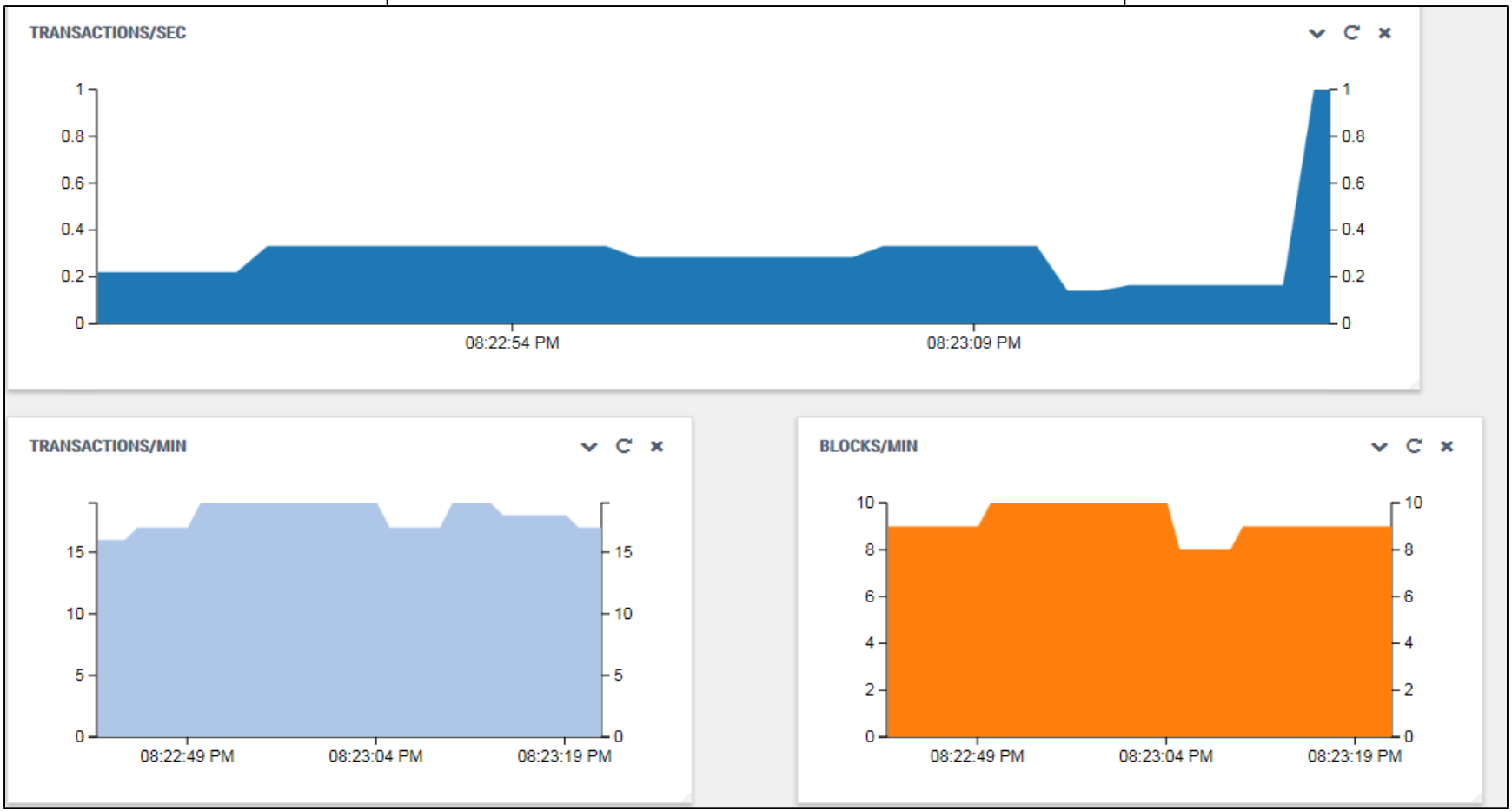
Identifier [number, hash, tag]

Block
Transaction

Find

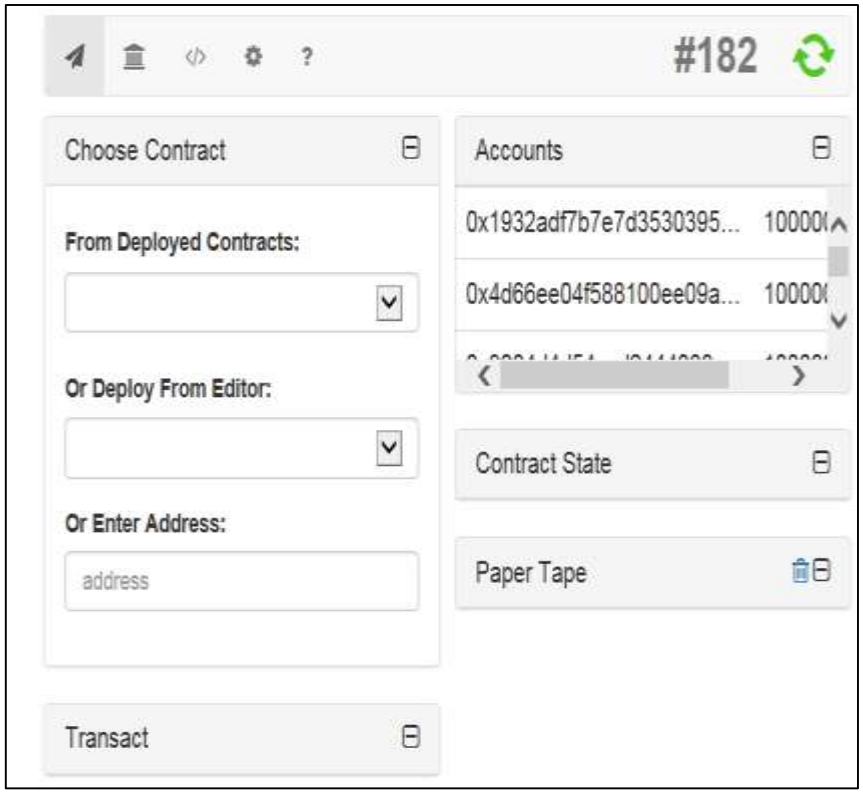
Creating & Deploying the Quorum Single Member Blockchain Network

Cakeshop Transactions



Creating & Deploying the Quorum Single Member Blockchain Network

Cakeshop Sandbox	Sandbox Contracts Editor- Example Contract




```
contract Owned {
  address owner;

  function Owned() { owner = msg.sender; }

  // This contract only defines a modifier but does not use it - it will
  // be used in derived contracts.
  // The function body is inserted where the special symbol "_" in the
  // definition of a modifier appears.
  modifier only_contract_owner { if (msg.sender == owner) _ }
}

contract Bank is Owned {

  bool enabled;

  struct Record {
    address owner;
    bytes32 id;
    uint value;
  }

  bytes32[] vault_ids;
  uint num_vault_ids;
  mapping (bytes32 => Record) vault;

  // only account owner or Bank owner is allowed
  modifier only_account_owner(bytes32 _id) { if (vault[_id].owner != 0 &&
  (vault[_id].owner == msg.sender || msg.sender == owner)) _ }
```

Creating & Deploying the Quorum Single Member Blockchain Network

Options for Viewing and Deploying Resources

PowerShell- View Resource Group Info

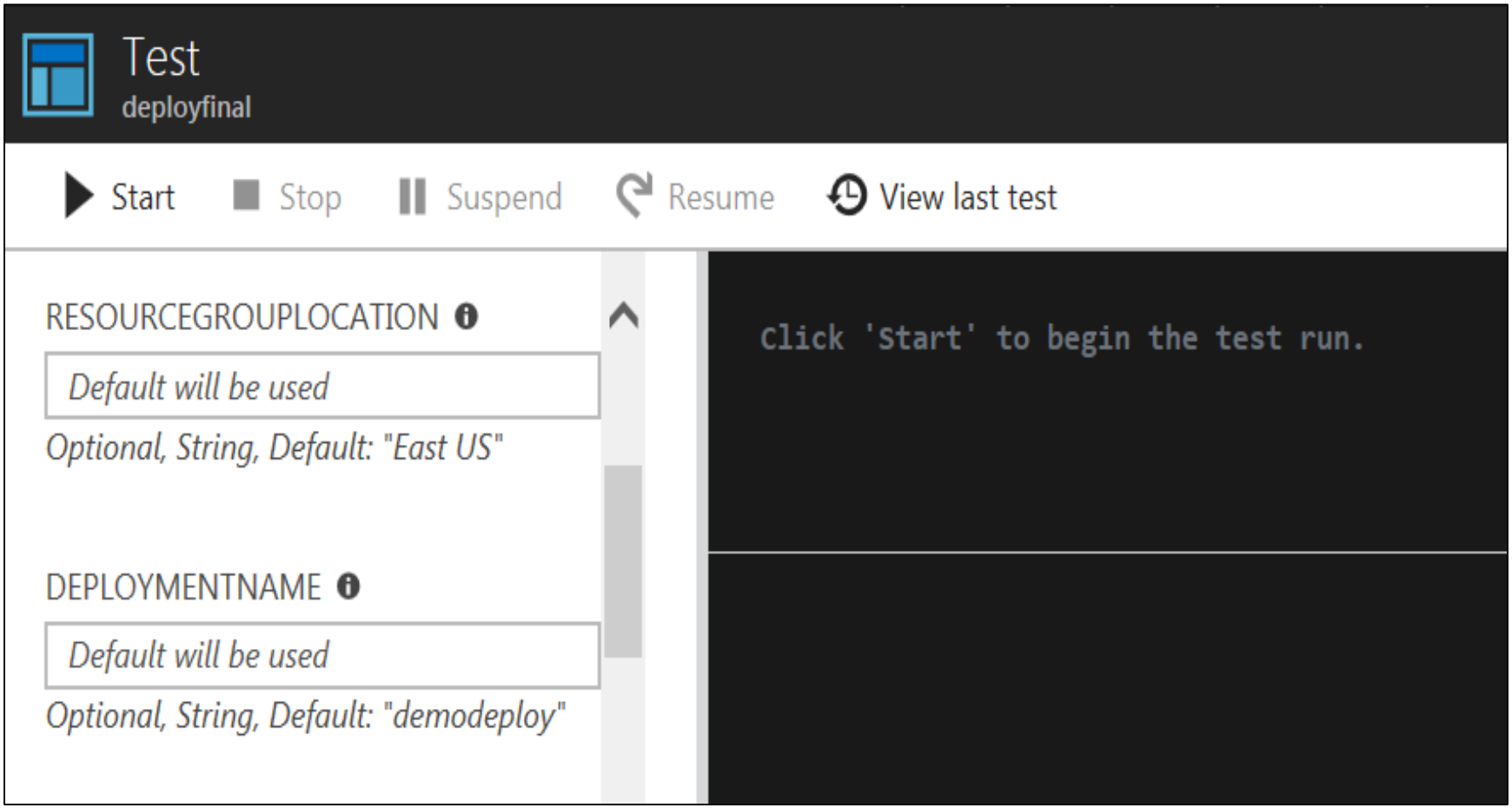
```
PS Azure:\> Get-AzureRMResourceGroup -name quorum


ResourceGroupName : Quorum
Location          : eastus
ProvisioningState : Succeeded
Tags              :
ResourceId        : /subscriptions/9d34afe4-302e-4
                    591-8c18-a08408735c57/resource
                    Groups/Quorum
```

Automation Account- Runbook (deploy template)

```
#*****************************************************************
# Script body
# Execution begins here
#*****************************************************************
#$ErrorActionPreference = "Stop"

# sign in
Write-Host "Logging in...";
Login-AzureRmAccount;

# select subscription
Write-Host "Selecting subscription '$subscriptionId'";
Select-AzureRmSubscription -SubscriptionID $subscriptionId;

# Register RPs
$resourceProviders = @("microsoft.compute","microsoft.network");
if($resourceProviders.length) {
    Write-Host "Registering resource providers"
```

Creating & Deploying the Quorum Single Member Blockchain Network

Test Environment for Runbooks (Automation Account)



Lessons Learned & Pros/Cons

Lessons Learned

- Blockchain is still a new, open-source technology, and SDKs are still being updated.

Pros

- Fast deployment
- High security is available, including at the transaction level and around permissions
- Ease of use with admin portal
- One language for smart contract writing
- Immutable ledger
- Smart contracts catch suspicious behavior

Cons

- Solidity not supported everywhere, limited IDEs; VS extension and Ethereum Studio deprecated

YouTube & GitHub URLs

- Short Video: https://www.youtube.com/watch?v=k5czvZfoHYY
- Long Video: https://www.youtube.com/watch?v=5g-Xy82pfKw
- GitHub Repository with all artifacts: https://www.github.com/healthdatachick/FinalProject